CRYPTOGRAPHY AND COMPUTER COMMUNICATIONS SECURITY

M.I. ADEKA

PHD

UNIVERSITY OF BRADFORD

2015

CRYPTOGRAPHY AND COMPUTER COMMUNICATIONS SECURITY

Extending the Human Security Perimeter through a Web of Trust

Muhammad Ibn-Umar ADEKA

BSc., MSc.

Submitted for the Degree of

Doctor of Philosophy

Faculty of Engineering and Informatics

University of Bradford

2015

Abstract

Muhammad Ibn-Umar Adeka

CRYPTOGRAPHY AND COMPUTER COMMUNICATIONS SECURITY

Extending the Human Security Perimeter through a Web of Trust

Keywords

Human Factor; Cryptology; Cybersecurity; Communication; Risk; Authentication; Security Perimeter; Web of Trust; Secret Sharing; Cloud Data Repository

This work modifies Shamir's algorithm by sharing a random key that is used to lock up the secret data; as against sharing the data itself. This is significant in cloud computing, especially with homomorphic encryption. Using web design, the resultant scheme practically globalises secret sharing with authentications and inherent secondary applications. The work aims at improving cybersecurity via a joint exploitation of human factors and technology; a human-centred cybersecurity design as opposed to technology-centred. The completed functional scheme is tagged CDRSAS.

The literature on secret sharing schemes is reviewed together with the concepts of human factors, trust, cyberspace/cryptology and an analysis on a 3-factor security assessment process. This is followed by the relevance of passwords within the context of human factors. The main research design/implementation and system performance are analysed, together with a proposal for a new antidote against 419 fraudsters. Two twin equations were invented in the investigation process; a pair each for secret sharing and a risk-centred security assessment technique.

The building blocks/software used for the CDRSAS include Shamir's algorithm, MD5, HTML5, PHP, Java, Servlets, JSP, Javascript, MySQL, JQuery, CSS, MATLAB, MS Excel, MS Visio, and Photoshop. The codes are developed in Eclipse IDE, and the Java-based system runs on Tomcat and Apache, using XAMPP Server. Its code units have passed JUnit tests. The system compares favourably with SSSS.

Defeating socio-cryptanalysis in cyberspace requires strategies that are centred on human trust, trust-related human attributes, and technology. The PhD research is completed but there is scope for future work.

Acknowledgements

In the words of Isaac Newton (5 February 1657), if one does not stand on the shoulders of giants, one would not achieve greater heights. Since I could not have been exempted from this golden rule, let me expend some lines to recognise a few of those who made it possible for me to be talking of a PhD Thesis at this stage of my earthly struggle.

From the home base, Nigeria, I am greatly indebted to the former Chief of Army Staff (COAS), Nigerian Army (NA), Lieutenant General AB Dambazau (PhD, retired), as well as his Director of Military Intelligence (DMI), Major General AT Umaru (retired) for their moral, psychological and other supports till date. I would also like to acknowledge the roles of the Petroleum Technology Development Fund (PTDF), Abuja, Nigeria, for its scholarship, and the NA for releasing me. Specifically, mention must be made of the Executive Secretaries, PTDF, Dr Muttaqha Rabe Darma, Dr Oluwole Oluleye, Mr Femi Ajayi, Mr Aminu Ahmed Galadima and their staffs at all levels from the various departments; especially training, finance, protocol and security departments. I must also mention the former Chief of Defence Staff, Air Chief Marshal O Petinrin, former COAS, Lieutenant General OA Ihejirika and his Principal Staff Officers; especially Major General LP Ngubane (Training and Operations) and Major General SY Audu (former DMI). I am also greatly indebted to the current COAS, Lieutenant General TY Buratai, for his interventions at critical moments.

Here in the UK, I am greatly indebted to Dr M.J. Ngala of Heaton Education, Bradford, for his various facilitating efforts at linking me up with the University of Bradford, and his continuous effort to make me feel at home in Bradford; ditto to our friend, Engr. Bako Wakili, of NCC, Abuja, Nigeria.

Rightly or wrongly, the success or failure of a research effort could be a reflection of the quality of supervision and other facilities; in addition to the personal disposition of the research student. It is in this context that I would like to express my profound gratitude to my supervisors, Prof. Simon J. Shepherd and Prof. Raed A. Abd-Alhameed, both of the School of Electrical Engineering and Computer Science (SoEECS), University of Bradford; for their diligence and understanding. Similarly, I am greatly indebted to the Library, ICT, Hub Research and other services of the University of Bradford, just as I am to various colleagues and staff of the SoEECS. To Dr Kelvin O. Anoh and other fellow research students, especially those in B3.26 Labs, Chesham Building, I say thank you for your positive colleagueship.

Finally, my wife, Saudat, and all the children/wards – Ayatullah, Saadiq, Mawaddah, Mardiyyah, Raheemah, Muhammad, Ishaq and ‘Uncle’ Dogo; may Allah reward you all for your various supports.

Ultimate gratitude is due to Allah, the Creator of His Creation; the only One that makes whatever happens to happen – out of His Wisdom.

Dedication

My wife, children, parents, brothers/sisters, teachers, friends and those who perceive themselves as enemies; those who made positive contributions to the making of Nigeria and the Nigeria Project; those who stand for humanity against the workers of iniquity from the Big Bang till Eternity; and ultimately, the Heir of all inheritors.

Table of Contents

List of Figures

List of Tables

List of Acronyms

(**NB**: For glossary of terms, Appendix 1 might be of help)

AAA	Authentication, Authorisation and Accounting
AES	Advanced Encryption Standard
AFN	Armed Forces of Nigeria
A-GPS	Assisted-GPS
API	Application Programming Interface
APT	Advanced Persistent Threat
ARPANET	Advanced Research Projects Agency net
AS	Autonomous System
ATM	Asynchronous Transfer Mode
ATPESS	Adeka's Twin Probability Equations on Secret Sharing
ATREs	Adeka's Twin Risk Equations
BAF	British Armed Forces
BCE	Before the Common Era (Equivalent to BC)
BDC	Bureau de Change
BDS	BeiDou Satellite Navigation System (the COMPASS) … China
BS	Base station
CA	Certification Authority
CBR	Constant Bit Rate
CDRSA	Cloud Data Repository Secure Access
CDRSAS	Cloud Data Repository Secure Access Scheme
CDRSAS-DT	Cloud Data Repository Secure Access Scheme – Deployment Type
CDRSAS-PT	Cloud Data Repository Secure Access Scheme – Prototype
CDS	Chief of Defence Staff (Nigeria)
COAS	Chief of Army Staff's (Nigeria)
COO	Cell of Origin
CRM	Composite Risk Management
CRU	Climate Research Unit
CSEPS	Certified Social Engineering Prevention Specialist
CSS	**C**ascading **S**tyle **S**heets
CYBERCOM	Cyber Command

DDoS	Distributed Denial-of-Service
DES	Data Encryption Standard
DH	Named after Diffie-Hellman (Whitfield **Diffie** and Martin **Hellman**)
DIA	Defence Intelligence Agency (Nigeria)
DLL	Down Line Loading
DAI	Director (-ate) of Air Intelligence (Nigeria)
DMI	Director (-rate) of Military Intelligence (Nigeria)
DNI	Director (-ate) of Naval Intelligence (Nigeria)
DoS	Denial-of-Service
DSA	Digital Signatures Algorithm
DSS	Department of State Security (Nigeria; same as SSS)
E-CID	Enhanced-Cell ID
EFCC	Economic and Financial Crimes Commission
E-OTD	Enhanced Observed Time Difference
eNB	evolved-Node B
ESN	Electronic Serial Number
EW	Electronic Warfare
FIPS	Federal Information Processing Standard (US)
FM	Field Manual
FMECA	Failure Modes Effects and Criticality Analysis
FMEA	Failure Mode and Effects Analysis
GCA	Global Cybersecurity Agenda
GCC	Global Culture of Cybersecurity
GCHQ	Government Communications Headquarters (UK)
GET	An HTTP request method between a Client and Server; ‘GET’ Requests data from a specified resource
GLONASS	Globalnaya Navigationnaya Sputnikovaya Sistema …Russia
GNSS	Global National Satellite System (Galileo) …EU
GPS	Global Positioning System …USA
GSon	Google GSon (a Java Library)
HASH	a Hash Algorithm
HeNB	Home e-Node B
HF&E	Human Factors and Ergonomics

HFES	Human Factors and Ergonomics Society
HTML	**H**yper**T**ext **M**arkup **L**anguage
HTTP	HyperText Transfer Protocol
ICC	International Criminal Court
ICT	Information and Communication Technology
IDE	Integrated Development Environment (Eclipse)
IDEA	International Data Encryption Standard
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
IPng	next generation IP
IPS	Internet Protocol Suite
IQRF	Information Query Radio Frequency
ISO	International Organisation for Standardisation (based in Europe)
ISP	Internet Service Provide
IPSec	IP Security
IPTv	IP Television
IPv4	IP Version 4
IPv6	IP Version 6
IT	Information Technology
ITU	International Telecommunication Union
ISP	Internet Services Provider
JANET	Joint Academic NETwork
JDK	Java Development Kit
JQuery	Java Query (Library)
JRE	Java Runtime Environment
JSON	JavaScript Object Notation
JSP	Java Server Pages
JSTL	JSP Standard Tag Library
KEK	Key Encryption Key
KTK	Key Transfer Key
LAN	Local Area Network

LBA	Location-Based Authentication
LBS	Location Based Service
LSSS	Linear Secret Sharing Scheme
LTE	Long Term Evolution
LTE-A	LTE-Advanced
MAC	Message Authentication Code
MATLAB	MATrix LABoratory
MDC	Manipulation Detection Code
MDMP	Military Decision-Making Process
MD5	Message Digest 5 (An algorithm for a one-way hash function)
MIC	Message Integrity Check
MIL-STD-1629	Military Standard
MIN	Mobile Identification Number
MitM	Man-in-the-Middle
MSC	Mobile Switching Centres
MSP	Mobile Service Provider
MU	Mobile User
MySQL	My **S**tructured **Q**uery **L**anguage
NA	Nigerian Army
NAF	Nigerian Air Force
NAIC	Nigerian Army Intelligence Corps
NAWANI	Nigerian Army Wide Area Network Infrastructure
NCC	Nigerian Communications Commission
NCP	Network Control Protocol
NCSP	National Cybersecurity Programme (UK)
NFIU	Nigeria Financial Intelligence Unit
NIA	National Intelligence Agency (Nigeria)
NIST	National Institute of Standards and Technology (US)
NN	Nigerian Navy
NNPC	Nigerian National Petroleum Corporation
NP	Nigeria Police
NSA	National Security Agency (US)
NTC	National Training Centre
OCSIA	Office for Cybersecurity and Information Assurance (UK)

OCSP	Online Certificate Status Protocol
OSI	Open Systems Interconnection
OTAR	Over The Air Re-keying
OTP	One-Time Pad
PAN	Personal Area Network
PBE	Password-Based Encryption
PC	Personal Computer
PGP	Pretty Good Privacy
PHP	**H**y**p**ertext **P**re-processor (Originally: Personal Home Page)
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POST	An HTTP request method between a Client and Server; 'POST' Submits the data to be processed to a specified resource
PRNG	Pseudo-Random Number Generator
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RA	Registration Authority
RDBMS	Relational Database Management System
RFID	Radio Frequency Identification Device
Rijndael	Named after Vincent **Rij**men and Joan **Dae**men
ROT-13	Rotate by 13 places
RPN	Risk Priority Number
RSA	Named after Ron **R**ivest, Adi **S**hamir and Leonard **A**dleman
SCR	Service Capacity Ratio
SDH	Synchronous Digital Hierarchy
SE	Social Engineering
SFU	Special Fraud Unit
SHA	Secure Hash Algorithm
SHA – (0-3)	Secure Hash Algorithm; Versions 0 - 3.
SONET	Synchronous Optical NETworking
SPKI	Simple Public-Key Infrastructure
SSS	Secret Sharing Scheme
SSS	State Security Service (Nigeria)
SSSS	Shamir's Secret Sharing Scheme

STAT	Space-Time Authentication Technique
TCP	Transmission Control Protocol
TDOA	Time Difference of Arrival
TOA	Time of Arrival
TTP	Trusted Third Party
URL	Universal Resource Locator
US-CERT	United States Computer Emergency Readiness Team
UUID	Universally Unique Identifier
VA	Validation Authority
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSS	Verifiable Secret Sharing
WAN	Wide Area Network
WCS	Worldwide Cybersecurity Summit
WHO	World Health Organisation
WISD	World Information Society Day
WSIS	World Summit on Information Society
WWW	World Wide Web
WW1	First World War (Ditto for WW2, WW3)
XAMPP	An open-source cross-platform web server solution stack [5].
XOR	Exclusive OR (a logic operation)
3GPP	3rd Generation Partnership Project
419	Advance Fee Fraud (The term ‘419’ was coined from Section 419 of the Nigerian Criminal Code (part of Chapter 38: Obtaining Property by False Pretences; Cheating)
419-ners	Advance-fee fraud stars

Chapter 1

Introduction

Computer communication or computer-mediated communication is defined as "any communicative transaction that occurs through the use of two or more networked computers" [6]. The latest global estimate of Internet users as at 30th June 2016 is 3,631,124,813 users [7]. Given the estimated human population of 7,340,094,096, Internet users account for 49.47% of the total population; approximately half of the global population. The number of computers connected to the Internet at any given time varies; a rough estimate shows an average of 605.6 million computers on the Internet worldwide [8].

While IPv4 (Internet Protocol Version 4) uses 32 bits for an IP address on the net, and can therefore support 2^{32} (4,294,967,296) addresses, IPv6 uses 128-bit addresses, so the new address space would have a capacity for 2^{128} (approximately 340 undecillion [9] or 3.4×10^{38}) addresses. Both versions of IP addresses are currently in use; with IPv4 transiting to IPv6. Based on these statistics, it is clear that the Internet is virtually everywhere, and has proved indispensable in virtually all fields of human activities; including research/academic activities, military, medical, finance, economy and administration. This yields the practical definition of Computer Communications.

With the above realities in mind within the context of a glaring possibility that, for a foreseeable future, human technological advancement will be computer-based, cybersecurity in forms of its computers, the network as well as its stored and transmitted data is already a matter of great concern to every human.

Using a technology-centred cybersecurity mechanism, it has been discovered that the state of insecurity in a cyber network is directly proportional to its complexity; i.e., the more complex a cyber network is, the more insecure it becomes [10]. This 6-chapter Thesis explores the possibility of a people-centred cybersecurity design, focusing on trust-centred human attributes that could be used to gauge trustworthiness in trustees. The exploration was conducted

within the framework of trusted secret sharing, cryptography and a secure cyber network.

This chapter will briefly cover the study background, motivation and statement of the research problem, the research aims and objectives, the scope of the research, research philosophy, importance and contributions of the research, and closes with the layout of the entire Thesis.

1.1 Study Background

Ross [11] noted that “Out of the crooked timber of humanity, no straight thing was ever made.” Thus, in a situation that is akin to the disruptions/destructions by highway robbers and sea pirates, both the wired and wireless information super-highways are also permeated by sundry criminals. These exploit both human factors and technological tools to perpetrate various forms of crimes. A computer crime, or cybercrime, refers to any crime that involves a computer and a network [12]. The computer may have been used in the commission of a crime, or it may be the target [13]. Net crime, on the other hand, refers to a criminal exploitation of the Internet [14]. Distributed Denial of Services (DDoS) attacks are considered as the most potent/disruptive of cyberattacks [15]. Further details on the state of cyber threat landscape are in Section 2.6 [16].

In an attempt to draw requisite attention to the growing threats to global cybersecurity, the ITU’s Global Cybersecurity Agenda (GCA) noted that Information and Communication Technologies (ICTs) have become an integral part of the information society since ICT networks are regarded as part of basic national infrastructure [17]. As global reliance on ICTs grows, so does vulnerability to attacks on critical infrastructure through cyberspace. Kevin Mitnick [18] believes that hacking is best accomplished by using a combination of technical and nontechnical means (social engineering; exploitation of human factors) [19-21]. Since the analysis of the threats reveals a combination of technical and nontechnical means of cyberattacks, defensive strategies ought to reflect this mixture as well. While procedural measures and social engineering will counter nontechnical attack approaches, cryptography becomes handy as a tool for technical cyber defence.

Evidence abound to show that the global community is reasonably aware of the threats posed by cyberattacks. This is demonstrated by the various cyber defence measures in the offing at local, regional and global levels. In January 2002, the UN General Assembly endorsed a proposal for a global summit on ICT related issues, with the International Telecommunications Union (ITU) as the lead agency. Consequently, the ITU organised the event, which included the participation of more than 50 heads of states and many international, regional and national organisations. This resulted in the World Summit on Information Society (WSIS) [22], which was held in 2 phases; in Geneva (December 2003) and Tunis (November 2005). One of the chief aims of the WSIS was to bridge the global digital divide separating rich countries from poor countries, by spreading access to the Internet in the developing world. The conferences established 17th May as World Information Society Day (WISD).

As a follow up to the Tunis phase of the World Summit on Information Society (WSIS) (2005) [22], the ITU launched the Global Cybersecurity Agenda (GCA) in 2007, as a framework for international cooperation aimed at enhancing confidence and security in the information society [17]. Its main objective is to promote a Global Culture of Cybersecurity (GCC), taking into account all the different actors from divergent sectors in the information society, as illustrated in Table 1.1. This leads to the motivation for this research and the statement of the research problem; the research question.

Table 1.1. ITU framework for a global culture of cybersecurity [22]

	Area of Cybersecurity Requirement	Professional Responsibility
1.	Political Culture of Cybersecurity	Legislatures, Executives, Stakeholders, …
2.	Legal Culture of Cybersecurity	The court, Judge, Prosecutor, Attorney, Regulator, Law Enforcement, …
3.	Economic & Managerial Culture of Cybersecurity	Auditors, Executive Manager, Production Manager, Human Resources Manager, CIO, CISO, ...
4.	Technical Culture of Cybersecurity	System, Network Engineer, System Administrator, Software Developer, …
5.	Social Culture of Cybersecurity	Not assigned to any professional group due to lack of requisite appreciation of its significance by the ITU

1.2 Motivation and Statement of the Research Problem

While highlighting the trend in the incidence of network insecurity within a spate of about three years, Schneier concluded that computer security is not a problem that technology can solve [10]. Security solutions have a technological component, but security is fundamentally a people problem. On the other hand, Ferguson [23] agrees that a security system cannot be stronger than its weakest link, while Hadnagy [24] is of the view that the biggest security weakness is the human infrastructure. Similarly, Mitnick [18] concludes that "the human factor is truly security's weakest link." Thus, in line with Kessler's position that, "if you know the enemy and know yourself your victory will not stand in doubt;…" [25] and, "if you know the enemy and know yourself you need not fear the results of a hundred battles," as expounded by Sun Tzu [26], it implies that an effective security arrangement, of any kind, is infeasible without the security engineer taking into cognisance relevant human factors, which are the main vulnerabilities usually exploited by the attackers.

Most existing security arrangements seem to underplay the significance of human factors (social engineering) in cyber defence. Examples include the ITU's GCC design in Table 1.1 which fails to assign the responsibility for the social culture of cyber-security to any group of professionals. This underestimation of the significance of social engineering input in cyber defence

is also indicative of the current UK NCSP which allocated only one percent of the £650 million earmarked for cybersecurity, from 2011-2015 to education [27].

The apparent lack of requisite attention on the social/nontechnical aspect of cyber defence, in both past and present efforts, inspired the conduct of this research in the chosen topic of 'Cryptography and Computer Communications Security: Extending the Human Security Perimeter through a Web of Trust.' This research was carried out within the framework of trusted secret sharing, cryptography and a secure cyber network; it adapted a technological scheme combined with the human factor of trust, using a secure web environment, in an effort to enhance cybersecurity. This aimed at increasing or expanding the security perimeter relative to human trust in an effort to answer the main research question: 'Solving for insecurity in computer networks; is it a technology-centred or human-centred problem?' Consequently, the research addressed the above question as broken down into the following components:

- What is security engineering?
- What are the nature and scope of contemporary cyber threats?
- What are the security challenges in countering the prevalent and foreseeable cyber threats?
- What is the context of cryptography in cybersecurity?
- Technology versus social engineering; what are their relative weights in cybersecurity?
- In a human-centred cybersecurity design, what are the most critical human factors that could be used to gauge trustworthiness in an interpersonal human relationship?
- How can technology be combined with trust-centred human factors in an effort to improve cybersecurity?
- Aside from theoretical analysis, would it be feasible to pragmatically demonstrate the synergy of technology and human trust factor in aid of cybersecurity?

Next are the aim and objectives of the research effort in order to answer the above research questions.

1.3 Aim and Objectives

The primary aim of this study was to find a way of devising a new or adapted technological scheme that would combine the capabilities of technology with the human factor of trustworthiness in an effort to enhance cybersecurity. This was designed to increase or expand the human trust security perimeter. In order to achieve this aim, it was broken down into the following specific objectives:

- Situate a pragmatic context of security engineering.
- Clearly, determine the nature and scope of the threats to cyber-security in the contemporary world.
- Highlight the major challenges in cyber-security and identify the weakest link of the cybersecurity system.
- Bring out the relative contributions of technological and human factor considerations, in relation to the effectiveness of cybersecurity.
- Design or adapt a technological scheme that could combine the capabilities of technology with trust-centred human attributes to enhance cybersecurity.
- Using the research findings, demonstrate, pragmatically, a new scheme that combines a scientific technology with the human factor of trust and show how the synergy enhances cybersecurity.
- Suggest or work out ways and means through which the Third World environment, especially Nigeria, could benefit optimally from the research work.

In order to fulfil the above aim and its resultant objectives, the scope of this research is defined as presented in the next section.

1.4 Scope of the Research

The research proposes a globalisation of a web-based practical implementation of secret sharing, with a focus on modifying the algorithm for Shamir's Secret Sharing Scheme (SSSS), in forms of addition, subtraction and/or replacement of some elements. The research proposes to modify the SSSS algorithm by sharing a much shorter (than most secret data) randomly generated key that is

used to lock up the secret data; as opposed to encrypting/sharing the secret data itself. This would be extremely significant in cloud computing. The performances of the SSSS would also be compared with those of the resultant scheme to identify their relative strong and weak points, using appropriate metric parameters. This is done in an effort to resolve some of the identified weaknesses and unresolved questions in the (k, n) - threshold schemes. As a by-product, the resultant system implementation should also serve as a secure cloud data repository.

The overall system implementation is geared towards conceptualising, planning, designing, developing and launching a computer-based web server that practically implements the combination of interaction between the human factor of trust and technology in an effort to improve security within the cyberspace. This is achieved via a form of secret sharing scheme; the (k, n)-Threshold algorithm, using the modified SSSS as one of the cryptographic primitives. The system is built up using HTML5, PHP, Java, Servlets, JSP, Javascript, MySQL, JQuery, and CSS. The codes are written in Eclipse IDE. These are running on Tomcat and Apache databases using XAMPP Server. The functioning prototype passes JUnit tests and has also been tested for performances and compared with the SSSS. There are other libraries used, which include the Database Connector, Joda Time, Google's JSON parser and Shamir's Algorithm. The source code is object oriented and adheres to software engineering tools and principles. The success of this research effort, epitomised by a functional web-based prototype, should pave way for further work aimed at upgrading the system into a multi-functional mass operating system for public or organisational deployment.

With the research topic in mind, shaped by the research question, motivation, aim/objectives and the resultant scope of the research, the appropriate research philosophy, methods and methodology will now be decided upon and outlined next.

1.5 Research Philosophy

In the context of the philosophy of research, there are four main features of research design, which are distinct, but closely related [28]. These include:

❖ **Ontology** - the researcher's view about the real world and his/her assumptions about its nature;

❖ **Epistemology** – the assumptions that the researcher makes about the best way to investigate the world and about reality;

❖ **Methodology** – the way the researcher puts together his/her research techniques in order to arrive at a coherent picture; and

❖ **Methods and Techniques** – these relate to what the researcher actually does in order to collect his data and carry out his investigations.

It is required that all of the above four research principles must be coherent and consistent in order to be able to create a viable research design. These principles remain the same, regardless of whether one engages in a scientific research in a laboratory or one sends out a customer questionnaire [28]. According to Easterby-Smith et al. [28], there are four main schools of ontology (how reality is constructed), as summarised in Table 1.3.

Table 1.3. The four schools of ontology and the summaries of their conclusions [28]

School / Conclusions	Realism	Internal Realism	Relativism	Nominalism
Summary	The world is 'real,' and science proceeds by examining and observing it	The world is real, but it is almost impossible to examine it directly	Scientific laws are basically created by people to fit their view of reality	Reality is entirely created by people, and there is no external 'truth'
Truth	There is a single truth	Truth exists, but is obscure	There are many truths	There is no truth
Facts	Facts exist, and can be revealed through experiments	Facts are concrete, but cannot always be revealed	Facts depend on the viewpoint of the observer	Facts are all human creations

In addition to the guidance from the research philosophy, there are also different epistemological approaches within the social sciences; i.e., the way in which the researcher chooses to investigate the world. The two main approaches are Positivism and Social Constructionism [28]:

- A Positivist posits that the best way to investigate the world is via objective methods, such as observations in a laboratory. Thus, positivism is in tune with realist ontology.

- A Social Constructionist believes that reality does not exist by itself. Rather, it is constructed and given meaning by people. Thus, the focus is on feelings, beliefs and thoughts, as well as how people communicate these attributes. Hence, Social Constructionism fits better with relativist ontology.

These philosophical approaches, both ontological and epistemological, are valid. There are many renowned researchers working in all of these traditions and schools. There are others who draw on multiple approaches depending on what they are investigating [29, 30]. The important thing is that the research should be internally systematic and consistent. If a researcher adopts the Social Constructionist approach within relativist ontology, the research would need to involve conversations; since mere observation of people 'doing what they do' would not produce the results that would be required to answer the research questions.

From the conclusion in the previous paragraph, it would necessitate that the chosen ontology and epistemology have implications on methodology. Thus, Realists tend to use a positivist epistemology. They start with hypotheses, and then gather facts through experiments, with a view to proving or disproving their hypotheses, and thereby confirming, or otherwise, their theory. Clinical trials for new drugs or treatments are good examples of Realist/Positivist research. On the other hand, Relativists tend to take a Social Constructionist view. They start with questions, and then use case studies and surveys to gather both words (views) and numbers, which they compare in order to generate theories. Thus, Social Constructionist approaches tend to draw on qualitative sources of data, while Positivist approaches are inclined to quantitative data.

A researcher may choose to use primary or secondary data for studies, and also combine both quantitative (quantities and numbers) and qualitative (nature, using descriptive words) techniques. Both have their advantages and disadvantages, hence, the wisdom of most researchers in combining the two approaches, leading to what is called Mixed Methods Research [29, 30]**.**

1.5.1 Pragmatism and Mixed Methods Research Approaches

Mixed Methods Research is a methodology for conducting research which involves the integration of quantitative and qualitative research methods, techniques, approaches, concepts or language in a single study [29, 30]. From the philosophical point of view, mixed research uses the pragmatic method and system of philosophy. The logic of inquiry for mixed methods includes the use of induction (discovery of patterns), deduction (testing of theories and hypotheses) and abduction (uncovering and relying on the best of a set of explanations for understanding the results). Mixed Methods Research permits the use of multiple approaches to answer the research questions, as opposed to restricting or constraining researchers' choices; i.e., it rejects dogmatism [29, 30]. This naturally leads to the perception that Pragmatic Research is the philosophical partner for Mixed Methods Research [31, 32]. The term pragmatic, as the opposite of idealistic, describes a philosophy of "doing what works best" [33]. From its etymology in Greek (pragma; deed), the word has historically described philosophers and politicians who were more interested in the real-world application of ideas as opposed to abstract notions. Pragmatism takes an explicitly value-oriented approach to research.

1.5.2 Research Methodology

From the primary research question or statement of the research problem (Solving for insecurity in computer networks: is it a technology-centred or human-centred problem?) and the aim of this research effort, it is obvious that the concepts of human factors and trust among humans must interplay within a technological setting in order to arrive at a value-oriented research outcome. This is essentially a social science oriented investigation in a technological

science environment; i.e., using technological tools. Thus, it seems that a Relativist/Social Constructionist approach would be at home with this research; without being able to do away with the Realist/Positivist research completely. Hence, the study adopted the Pragmatic Research approach; using Mixed Methods research with the integration of both Qualitative and Quantitative research techniques.

In most cases, secondary data were sourced from published and unpublished materials such as books, journals, newspapers, seminars, Internet, live telecasts, conference papers and other earlier research works. A technological system that could combine the capabilities of technology with human trust to enhance cybersecurity was adapted from the SSSS {the (k, n)-Threshold secret sharing algorithm} and applied using other cryptographic primitives/mathematical concepts via a web design implementation. The landmark results are as recorded by the web-based system tagged Cloud Data Repository Secure Access Scheme (CDRSAS) in Chapter 4. Further details on the web design and implementation concepts are in Section 4.1, while the comparative performances of the CDRSAS and the Shamir's algorithm are presented in Section 4.10.

Two surveys were conducted; both employed questionnaires and structured interviews, with an examination of official documents from government agencies. The first survey was designed to assess the level of awareness on password security by Internet users in Africa, using Nigeria as a case study; the questionnaire for this is attached as Appendix 2. The results showed that employees among the junior staff were generally more security-conscious than their senior counterparts. Since the senior staff is administratively in charge of organisations, this finding would significantly affect the measure of assurance in computer networks negatively; i.e., the degree of trust to be placed on the network system is reduced. The second survey aimed at appreciating the state of cyber insecurity and establishing some statistics on the use of GSM mobile phones in Nigeria, as it concerns roaming of services. This survey established that the overall effect of GSM roaming on location-based authentication is negligible. This would engender greater trust and confidence in cyber networks; i.e., by improving cybersecurity as a result of minimising the negative impacts of

419-ners (advance-fee fraud stars). It was part of the data obtained from this survey that facilitated the proposal in Chapter 5; the questionnaire for this is attached as Appendix 3.

Having decided on the research setting as outlined above, there are needs to both preview and review the significance and possible contributions of this research outcomes to human civilisation. This is presented in the next section.

1.6 Importance and Contributions of the Research

In general terms, it is optimistic that the outcome of this study would be of great benefit to governments, corporate organisations and individuals who have one thing or the other to do with the ICT industry. The work is also aimed at stimulating interest in this subject area among the upcoming generation of engineers in the developing countries, especially Nigeria. In specific terms, the results attained in this work have uncovered many areas of new knowledge. As projected in the research outline plan, the main novelties that have been accomplished relate to modifications, in form of additions and replacement of some elements, in the SSSS algorithm, in an effort to resolve some of the identified weaknesses in the (k, n)- threshold schemes. The contributions are in two categories: namely, key contributions and contributions relating to the general research work. All these are highlighted hereunder.

1.6.1 Key Contributions

❖ The CDRSAS-PT has modified the SSSS algorithm by sharing a much shorter (than most secret data) randomly generated key that is used to lock up the secret data; as opposed to encrypting/sharing the secret data itself. This would be extremely significant in cloud computing, especially if homomorphic encryption becomes a reality. In a nutshell, it costs more in terms of bandwidth and delay in a typical communication link to encrypt the data and share the resulting information among servers (as done in SSSS) compared to sharing the keys only (as proposed in the CDRSAS). Theoretically, the strong points of this modification are demonstrated in Section 4.10, using four QoS metric

parameters; namely, server bandwidth, system scale, service capacity ratio and real-time performance (time delay).

❖ Other novelties associated with the CDRSAS-PT include the following:

- The geographical spread of participants (trustees) which is now global in nature as against a one-location based recombination process envisaged in previous secret sharing schemes. This revolution in the science of secret sharing is illustrated in Figure 6.2.
- As a consequence of globalisation, location-based user authentication techniques are introduced. These are the employment of the GPS coordinates and SMS text mobile authentication codes; thus greatly enhancing the security of the system.
- Inherent capability for location-based automatic mutual authentication; a novelty in the public civil domain.
- In an effort to minimise the chances of hacking, a dynamic time window is introduced within which secret sharing and recombination processes must be accomplished. Consequently, a digital clock and timer (down counter) are incorporated into the system, since time restriction is among the logic tests in the greatly enhanced Shamir's secret sharing algorithm.
- Other long-standing unresolved issues in relation to secret sharing, which have now been resolved in the Cloud Data Repository Secure Access Scheme (CDRSAS), include the following:

    - Who is the Combiner;
    - Where should the recombination take place; and
    - Who is entitled to have access to the reconstructed secret?

    These questions have now been resolved with the designation of an Authorised User (non-permanent) in the scheme, to be programmed by the Admin for every secret sharing session, as would be dictated by particular circumstances.

❖ It is also instructive to note that the practical implementation of a web-based authentication secret sharing scheme, with all the complements of the CDRSAS, has no precedence.

❖ **The risk assessment discoveries are:**

- Of particular significance is the ability of this study in discovering the need for a 3-factor (Risk, Threat and Vulnerability) based security assessments, contrary to the haphazard and non-systematic practice in most armed forces throughout the world. This discovery made it possible for the author to be the only person with military background whose paper made a chapter in a recent defence publication in Nigeria [34].
- Adeka's Twin Risk Equations (ATREs), a by-product of the above discovery, facilitate an easy and pragmatic understanding of the systematic quantitative risk-based security assessment process (Section 2.5.1; Equations (2.28) and (2.29); Figure 2.9).
- Adeka's Twin Probability Equations on Secret Sharing (ATPESS) serve as mathematical instruments to prove that secret sharing (using a network of human trustees) enhances the security of the secret data under protection (Section 2.3.3; Equations (2.25) and (2.27); Figure 2.7).

1.6.2 Contributions Relative to the General Research Work

❖ Information warfare is a potent weapon for industrial espionage, thus constituting a great threat to all corporate organisations. Hence, any organisation that has competitors and whose operations are computerised, such as the Nigerian National Petroleum Corporation (NNPC), will benefit from the knowledge and experience acquired via this study.

❖ This study has contributed to the existing body of knowledge, hence, it would serve as a useful reference material for future researchers; by filling literature gaps on the subject matter.

❖ The research is of great significance because its informed proposal to use a combination of location-based authentication and further digitisation of GSM country code into smaller area codes would be an antidote to the fraudulent 419 (advance fee fraud) crimes in Nigeria and many countries in the world.

❖ The outcome of this study will be of great benefit to the Nigerian Armed Forces, in particular, and the nation at large. Specifically, the experience from

this study could be handy in streamlining the security arrangements for projects like the Nigerian Army Wide Area Network Infrastructure (NAWANI) at minimal costs.

- The subject of Cryptography and Computer Communications Security will always remain indispensable, as long as technological developments remain computer-driven.
- Finally, it is hoped that this work will stimulate further research on the need to fully exploit the various techniques associated with the Art of Human Hacking in countering cyber threats/attacks.

Now that it has been decided that this research effort is both viable and feasible, the readers of its Thesis are now provided with a preview of its contents as laid out in the next section.

1.7 Layout of the Thesis

The Thesis contains 6 chapters, beginning with the introduction in Chapter 1 and ending with Conclusion in Chapter 6. Apart from Chapters 1 and 6, every chapter ends with a deductive section which records important deductions in the chapter. Similarly, apart from Chapter 6, every chapter begins with an unlabelled/unnumbered section which serves as an introduction to the chapter. Chapters 2 – 5 are now briefly introduced in this segment, with each of the chapters organised as follows:

- Chapter 2 deals with literature review. It covers secret sharing schemes, the concepts of trust and the extension of human security perimeter through a web of trust (an exposition on the subtitle of this Thesis). It also discusses the concept of security and the military security assessment process, a 3-factor security assessment process (risk-centred security assessment technique) and analysis/synthesis. This is followed by the concepts of cyber/cyberspace with its threat landscape and national cyber threats/vulnerabilities. The chapter ends with highlights on cryptography/cryptanalysis and social engineering before deductions.
- Chapter 3 focuses on passwords and password security purgatory, with an analytical presentation on a password survey, designed to estimate the level

of awareness on passwords by Internet users in Africa, using Nigeria as a case study.

- Chapter 4 discusses the Cloud Data Repository Secure Access Scheme (CDRSAS), which is a web-based authentication scheme. It is primarily designed to implement the sharing, distribution and reconstruction of a sensitive secret data. This is carried out in a secure web environment, globally. Though primarily designed as a secret-sharing system, it could be adapted to serve as a cloud data repository and secure data communication system. This chapter highlights the web design concept, the design/development and presents its performance characteristics with practical results; with identified areas of novelties. The performances are compared with the Shamir's algorithm to identify possible areas of improvements and deficiencies, with a projection for future work.
- Encouraged by the results in Chapter 4, Chapter 5 exploits the inherent security enhancement characteristics of various location-based authentication techniques, with a focus on the role that Global Positioning System (GPS) could play in optimising this authentication approach. This would go a long way in facilitating successful socio-technological countermeasures against feigned-location based fraud related crimes; such as the 419 advance fee fraud practised in Nigeria and many countries in the world. This also contains a survey analysis, designed to appreciate the state of cyber insecurity and estimate the possible negative impact of GSM roaming on LBA, with encouraging results.
- Conclusions and recommendations are covered in Chapter 6. These comprise of the summary of conclusions, challenges and recommendations for future work. This is followed by appendices. The Thesis terminates with the author's contributions.

The Thesis proceeding now continues with the literature review in the next chapter – Chapter 2.

Chapter 2

Trusted Secret Sharing within the Framework of Cybersecurity and Cryptology

This literature review begins with discussions on the theories of secret sharing algorithms. This covers the theoretical basis for (k, n)-Threshold schemes, a historical overview of Secret Sharing Schemes (SSS) globally and their comparative analysis. These are followed by highlights on cryptographic key management, focusing on key recovery schemes. The concepts of trust and the extension of human security perimeter through a web of trust (an exposition on the subtitle of this Thesis) is then treated. It also discusses the concept of security and the military security assessment process, an examination of a 3-factor security assessment process (risk-centred security assessment technique) and analysis/synthesis. These are followed by the concepts of cyber and cyberspace with its threat landscape, as well as national cyber threats and vulnerabilities. The chapter ends with highlights on cryptography/cryptanalysis and social engineering before deductions.

2.1 Requisite Theoretical Background on Secret Sharing Schemes

This section deals with the theoretical basis for SSSS, an overview of Secret Sharing Schemes (SSS) globally and cryptographic key management with highlights on key recovery schemes.

2.1.1 The Theoretical Basis for the (k, n)-Threshold Schemes

In cryptography, secret sharing is a method by which a given secret is distributed among a set of participants (trustees), each of whom is given only a share of the secret. Reconstruction of the secret would only be possible when all the participants or a stringently defined minimum subset of participants (access structure or authorised set) pool their shares together. In other words, both individual shares and any number of shares less than the authorised set are of no use on their own. Thus, generally, the access structure of a (k, n)-

threshold scheme normally partitions the set of all subsets of participants into authorised sets who can recover the secret and unauthorised sets who cannot; some schemes feature an intermediate third class of subsets, who are neither authorised nor unauthorised [35-37]. The aim of the scheme is to provide tight control over the sensitive data and remove the single-point vulnerability.

The objective of a secret sharing scheme is to make a given secret D (say some data, e.g., key combination) inaccessible to unauthorised persons while making it accessible to authorised persons when the need arises. It is assumed that non-mechanical solutions which could manipulate this data in the process are allowed [38]. The goal is to divide D into n pieces $D_i,\ldots,D_n$ such that:

- Knowledge of any k or more D_i pieces makes D easily reconstructable.
- Knowledge of any k-1 or fewer D_i pieces leaves D completely indeterminable (in the sense that all its possible values are equally likely; assumed absolute randomness).

This assumption is supported by the concept of entropy in information theory. The entropy H, of a discrete random variable X, measures the level of uncertainty associated with the value of X [39, 40]. It is a key property of entropy that it is at a maximum when all the messages in the given message space have the same probability of occurrence or most unpredictable. That is, $p(x) = 1/n$, for $p(x_1),\ldots,p(x_n)$. Thus yielding $H(X) = \log n$. This attribute is illustrated by the entropy of a Bernoulli trial (Equation 2.1), a function of success probability, usually termed the Binary Entropy Function:

$$H_b(p) = -p\log_2 p - (1-p)\log_2(1-p) \qquad (2.1)$$

The entropy is maximised at 1 bit per trial when the two possible outcomes are equiprobable; similar to the case of an unbiased tossing of a coin. This is illustrated in Figure 2.1 [38].

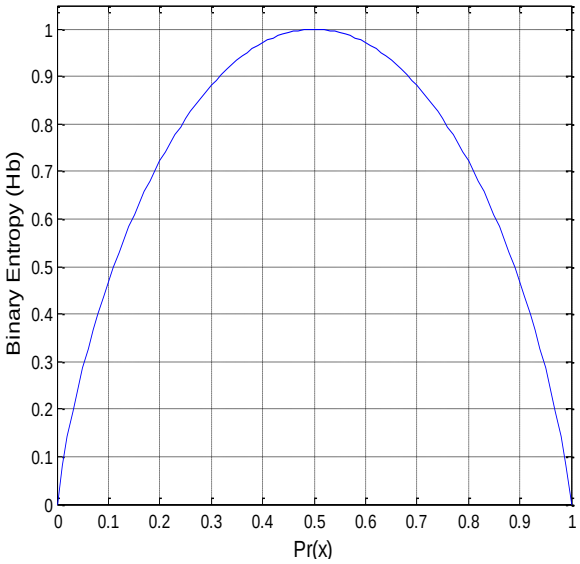


Figure 2.1. Binary entropy function $H_b(p)$ [39]

Threshold schemes are suitable for an environment where a group of mutually suspicious individuals, with conflicting interests, must work together. Since this cooperation might be against the individual consent of some participants, the veto power inherent in the system could paralyse the activities of the group. Hence, there is a need to be circumspect in defining the boundary of the access structure (selection of k) relative to the entire set of participants (n) [38, 41]; hence, the nomenclature (k, n)-threshold scheme. This is necessary so that a reasonable majority of the participants should be able to function effectively, and a reasonable minority should be able to block possible undesirable actions. This versatile cryptographic primitive has been employed in various applications. These include access control, electronic voting, key recovery mechanisms, online auctions, distributed certificate authorities, secure multiparty computation and protection of cryptographic keys [35, 42].

Usually, secret sharing schemes have two fundamental attributes [35, 43]; privacy and recoverability. That is, respectively, the unauthorised sets should not be allowed to know the secret and the authorised sets should be able to recover the secret by pooling requisite shares together. Similarly, secret sharing schemes have two functionalities which are usually carried out by an entity, who could be a neutral third party or one of the participants. The Dealer is usually responsible for organising the system parameters, generating the secret,

creating the initial shares and distributing them among the participants. Next is the Combiner who pools requisite shares together to recombine the secret. In most cases, the Dealer is also the Combiner; however, one of the unanswered questions is the entity that should have access to the recombined secret - whether this should be the Dealer, a participant or an entirely different entity.

Mathematical Definition

The main idea behind the SSSS is based on polynomial interpolation [38]. The polynomials could be replaced by any other functions which are easy to evaluate and to interpolate. This idea is rooted in the notion that two points are enough to define a line, three points are required to define a quadratic expression, four points are required to define a cubic function and so on. In other words, it requires 'k' points to define a polynomial of order 'k-1' [44].

Given k points in the Cartesian plane $(x_1, y_1),...,(x_k, y_k)$ with distinct x_i's, there is one and only one polynomial $g(x)$ of order k-1 such that $g(x_i) = y_i$ for all i. Without losing generality, it can be assumed that the data D is a number or it could be made a number. In order to divide it into pieces D_i, pick a random k - 1 degree polynomial

$$g(x) = a_0 + a_1 x + ... + a_{k-1} x^{k-1} \quad (2.2)$$

where $a_0 = D$. Then evaluate:

$$D_1 = g(1), ..., D_i = g(i), ..., D_n = g(n).$$

Using any subset of k of the D_i values, the coefficients of g(x) can be found by interpolation, and then evaluate D = g(0). Knowledge of just k-1 of these values, on the other hand, is not enough to calculate D. In order to make this claim more precise, Shamir uses modular arithmetic; i.e., finite field arithmetic or arithmetic in the Galois Field [GF(p)] instead of real arithmetic; the set of integers modulo a prime number p forms a field within which interpolation can be carried out.

Example 1

As an illustration for the (k, n)-threshold scheme [38, 44], using integer arithmetic rather than the GF, for simplicity, it is required to share a secret D where k < n. Then randomly, choose the coefficients a_1, a_2, $a_{3, \ldots,}$ a_{k-1}, and let $D = a_0$ and g(x) is as defined in Equation (2.2) above. Construct n points {i, f(i)}, for i = 1, 2, 3,…,n. Given any subset of k of these pairs, the coefficients of the polynomial g(x) can be determined through Lagrange interpolation, and then the value a_0 = D, which is the secret, can be evaluated.

Distribution of Shares

Let:

$$\begin{aligned} D &= 1234; \\ n &= 6; \\ k &= 3; \end{aligned}$$

and the random integers are:

$$\begin{aligned} a_1 &= 166; \\ a_2 &= 94. \end{aligned}$$

From Equation (2.2), it follows that:

$$g(x) = 1234 + 166x + 94x^2 \qquad (2.3)$$

Now, construct 6 points from the polynomial g(x), resulting in the following 6 pairs of secret share points:

$$(1, 1494), (2, 1942), (3, 2578), (4, 3402), (5, 4414), (6, 5614)$$

Give each participant a different single share point {x and g(x)}.

Recombination of Shares

In order to reconstruct the secret, any 3 points are sufficient. Consider the following 3 points:

$$(x_0, y_0) = (2, 1942); \quad (x_1, y_1) = (4, 3402); \quad (x_2, y_2) = (5, 4414)$$

Applying Lagrange polynomial interpolation:

$$l_0 = (x - x_1)/(x_0 - x_1) * (x - x_2)/(x_0 - x_2) = (x-4)/(2-4) * (x-5)/(2-5)$$

$$= \left(1/6x^2\right) - \left(11/2x\right) + \left(31/3\right)$$

$$l_1 = (x - x_0)/(x_1 - x_0) * (x - x_2)/(x_1 - x_2) = (x-2)/(4-2) * (x-5)/(4-5)$$

$$= \left(-1/2x^2\right) - \left(31/2x\right) - (5)$$

$$l_2 = (x - x_0)/(x_2 - x_0) * (x - x_1)/(x_2 - x_1) = (x-2)/(5-2) * (x-4)/(5-4)$$

$$= \left(1/3x^2\right) - (2x) + \left(22/3\right)$$

Recalling that:

$$g(x) = \sum_{j=0}^{2} y_j \, l_j(x) \qquad (2.4)$$

Therefore:

$$g(x) = \sum_{j=0}^{2} y_j \, l_j(x)$$

$$= 1942\left(1/6x^2 - 11/2x + 31/3\right) + 3402\left(-1/2x^2 - 31/2x - 5\right) + 4414\left(1/3x^2 - 2x + 22/3\right)$$

$$g(x) = 1234 + 166x + 94x^2$$

Recall that the secret D is the constant coefficient, thus:

$$D = 1234.$$

Example 2

In a threshold scheme, a secret data (a prime number) is shared among 5 trustees. The key can be recovered by using any 2 shares. Show that the secret can be recovered from any 2 of the following shares and hence determine the secret data. (Consider the use of graphical observation/interpolation; hence, start by plotting the points to solve the problem).

$$S_1 = (-3, 13); \quad S_2 = (-1, 9); \quad S_3 = (2, 3); \quad S_4 = (4, -1); \quad S_5 = (6, -5).$$

Plotting the points (S_i) as given will produce the graph in Figure 2.2. It is clear that any two points are sufficient to reproduce the line since all of the points above lie on it. Thus, the secret data, represented by the point at which the graph intersects the y-axis, is clearly 7.

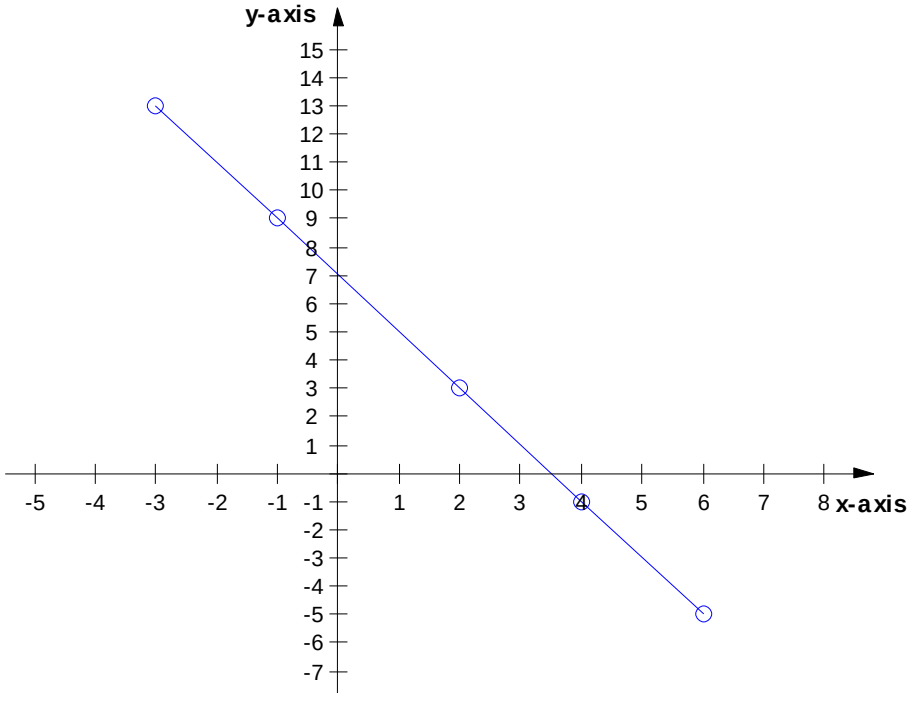


Figure 2.2. Determining the secret data for a straight line graph

Mathematically, the above result can be verified as follows. Using the general formula for a line:

y = mx + c, where m is the gradient = (change in y)/(change in x) between two points

Take two points on the line e.g. (4, -1) and (6, -5)

The gradient m is:

$$(-5-(-1))/(6-4) \quad = \quad -4/2 \quad = \quad -2$$

Using the point (4, -1) and substituting m = -2 into the above equation gives:

$$-1 \quad = \quad -2(4)+c$$
$$c \quad = \quad 7$$

Similarly, checking with point (6, -5) gives:

$$-5 = -2(6)+c$$
$$= -12+c$$

Again,

$$c \quad = \quad 7$$

The equation of the line is y = -2x + 7 and holds true for all the points above and can be recovered from any two of the above points, using the technique demonstrated for (4, -1) and (6, -5).

Hence, the secret data is 7.

Example 3

Given that the equation of a straight line is y = mx + c, where m represents the slope of the line and c represents the secret data (a prime number). Generate six shares that can be used by six trustees for a threshold scheme requiring a minimum of two shares for key recovery.

For this problem, a value should be chosen for the secret data. Let the secret data = 9. Then, the equation of the line can be determined as y = -8x + 9; assuming the line passes through the point (1, 1). In this case, '9' is fixed and '-8' is chosen randomly. Using the straight line obtained, any six share points can be worked out, e.g.:

Share points = $(1,1),(-3,33),(4,-23),(-1,17),(-2,25),(3,-15)$

Example 4

show that the following shares can recover the secret prime number when any three shares are used and hence determine the secret value and the degree of the generating polynomial.

$S_1 = (-3,40), \quad S_2 = (-1,18), \quad S_3 = (1,12), \quad S_4 = (3,22),$

$S_5 = (4,33), \quad S_6 = (5,48).$

From the question, it is obvious that the threshold k = 3. Therefore, the generating polynomial is of degree 2; a quadratic function. Hence, to solve this problem, it is required to plot the points and show that the resulting curve is quadratic. All quadratics require 3 points to be reconstructed uniquely. All of the points above lie on this curve. Thus, any three of them can be used to determine the secret value; i.e., the point at which the curve intersects the y-axis. The corresponding plot is shown in Figure 2.3.

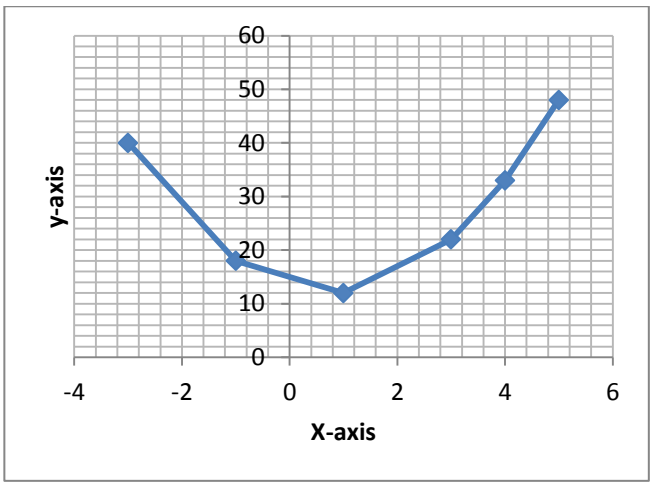


Figure 2.3. Determining the secret data for a quadratic function using threshold shares

From Figure 2.3, the Secret number (the point at which the graph crosses the y-axis) is 13.

2.1.2 An Overview of Secret Sharing Schemes

Imagine a situation where the president and his Chief of Defence Staff (CDS) have a different key, each, for unlocking the trigger for the nuclear missile launch; both of whom must be present simultaneously to launch a nuclear missile. The digital equivalent of this would be that both of them have a secret piece of information or data, and only the combination of both items of information would be acceptable as a working key by the launch computer. This scenario is referred to as secret sharing in cryptography. In addition to its use in warfare management as illustrated above, this cryptographic primitive has several other applications in real life situations. Modern cryptographic secret sharing, as originally attributed to Shamir [38] and Blakley [45], was initially designed for safeguarding keys. However, it has been applied in other areas far beyond this original intent. Nowadays, secret sharing is a valuable instrument in electronic voting [46], metering schemes [47], distributed key distribution [48] and secure multi-party computation [49, 50].

The simplest form of secret sharing is the scheme whereby all n participants are required to be present before the secret could be unlocked; while the secret

remains hidden for any smaller group less than n. More complex secret sharing involves designs where a threshold number of participants must cooperate in order to reconstruct the secret. There are also more flexible schemes in which pre-defined groups of people are allowed to unlock the secret using what is called an access structure. Basically, secret sharing may fall into one of three categories [51]. These are simple secret sharing, threshold secret sharing schemes and linear secret sharing.

Simple Secret Sharing

Additive Secret Sharing is an example of secret sharing schemes where all participants must come together or cooperate before a secret can be reconstructed, as illustrated in this segment.

Given a secret s $\in$ F, the dealer D selects n – 1 random integers $\Re = \{r_1, r_2, r_{n-1}\}$ uniformly from F. D then calculates

$$s_n = s - \sum_{i=i}^{n-1} r_i \text{ mod F} \qquad (2.5)$$

D then sends each player p_i, $1 \le i \le n-1$: the share $s_i = r_i$ and the share s_n is sent to p_n.

The reconstruction of the secret s $\in$ F is a trivial solution; a mere addition of all the shares:

$$s = \sum_{i=1}^{n} s_i \text{ mod F}$$

From the above, it is clear that in the additive secret sharing scheme, the secret can only be reconstructed, if and only if, all participants pool all their shares together. If one or more participants refuse to cooperate, no information about the original secret can be recovered. Such a scheme is referred to as a perfect secret sharing scheme.

Theorem: Perfect Secret Sharing

A perfect secret sharing scheme is perfect in an information theoretic sense when the required P participants can reconstruct the secret s $\in$ F, but any smaller set cannot discover anything about the secret [51, 52].

Proof

Given a secret s $\in$ F and a random uniform distribution of the shares of the secret among P participants, all participants are needed to reconstruct the secret. Imagine a situation where $|P|-1$ participants try to reconstruct the secret s:

$$s' = \sum_{i=1}^{|p|-1} s_i \qquad (2.6)$$

If they add their respective values of shares together, they can calculate the value for s' = s + s$|P|$. However, since the random value s$|P|$ is unknown, they have no information with which to determine the true value of the secret s [53].

Definition 1: Ideal Secret Sharing

Secret sharing schemes with information rate 1 are called idea [52, 54]. A scheme is said to be ideal if its share has the same length as the secret. The ideal property could be perceived as the efficiency of the scheme.

Definition 2: Information Rate

In secret sharing, information rate as studied by Stinson [55] is a measure of the amount of information that participants need to keep secret. The information rate for a particular shareholder is the bit-size ratio {i.e., (size of the shared secret)/(size of that user's share)}. As for a secret sharing scheme itself, the information rate is the minimum such rate for all participants [52, 56]. The efficiency of a secret sharing scheme is measured by its information rate.

Threshold Secret Sharing Schemes

Both Shamir and Blakley presented simple, but powerful, secret sharing schemes that allowed a k-threshold of n participants, where k $\leq$ n, to reconstruct the secret. Both solved an impractical real world problem often found in combinatorics texts [44]:

> "Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of keys to the locks each scientist must carry?"

In the real world, the number of locks on the cabinet would be $\binom{11}{5} = 462$, while the number of keys to be carried by each scientist would be $\binom{10}{5} = 252$. Luckily, mathematics offers a much cleaner and more practical solution. In geometry, for instance, it is known that given two arbitrary distinct points on the circumference of a circle, there is no enough information to reconstruct the entire circle. However, given three distinct points, the entire circle can be reconstructed. Considering this circle as the secret, it could be seen that a simple 3-threshold secret sharing scheme has just been constructed. While this circle obviously has severe limitations, there exist other structures which can have an arbitrary number of points and hence an arbitrarily sized threshold. One such scheme was constructed by Shamir in [38, 57]. His solution used curves and reconstructed the secret by interpolation when a threshold of *k* people supplied their parts, as illustrated in Section 2.1.2, under Shamir's Secret Sharing Scheme. Blakley [45], also invented a similar scheme which used the intersection of hyperplanes, as opposed to polynomial interpolation, to reconstruct the secret. Another secret sharing scheme, by Asmuth and Bloom [58], uses congruence classes to solve the secret sharing problem. The Shamir Secret Sharing Scheme (SSSS) is analysed in further details below.

Definition

A (k,n)-threshold secret sharing scheme is a scheme which can divide a secret s $\in$ F into shares $\{s_1, s_2, s_3, \ldots, s_n\} \in F$ such that k $\leq$ n, and:

- Given any set of k or more shares s_i, s can be reconstructed.
- Any set of fewer than k shares gives no information about s at all.

Shamir's Secret Sharing Scheme

Given n participants P = $\{p_1, p_2, p_3, \ldots, p_n\}$, polynomial interpolation could be used to construct a (k, n)-threshold secret sharing scheme that will require a subset A$\subseteq$P, $|A| \geq k$ in order to successfully reconstruct the secret.

❖ Creating the Shares

The dealer D first selects a secret s $\in$ F in order to create the shares. He then constructs a random polynomial f(x) with a degree of k-1.

$$f(x) = s + r_1 x + r_2 x^2 + \ldots + r_{k-1} x^{k-1} \text{ mod F} \qquad (2.7)$$

subject to the following conditions:

- The field F >n, where F is a GF(q) for some prime power q.
- The secret s $\in$ F.
- The threshold k $\leq n$.
- The coefficients $\{r_1, \ldots r_{k-1}\}$ are chosen independently and randomly from the interval [0, F).

Each share s_i of the secret can then be created by an evaluation of the function f(x). That is:

$$s_1 = f(1), \quad s_2 = f(2), \quad \ldots, \quad s_n = f(n). \qquad (2.8)$$

❖ Example (Polynomial construction)

Let F = 17, s = 4, k = 3, and r{1… k−1} ={3, 6}. The polynomial is then, as stated in Equation (2.7),

$$f(x) = 4 + 3x + 6x^2 \text{ mod } 17 \tag{2.9}$$

and some of the secret shares are:

$$\begin{aligned} s_1 = f(1) &= 4 + 3(1) + 6(1)^2 \text{ mod } 17 = 13 \\ s_2 = f(2) &= 4 + 3(2) + 6(2)^2 \text{ mod } 17 = 0 \\ s_3 = f(3) &= 4 + 3(3) + 6(3)^2 \text{ mod } 17 = 16 \quad \text{s3 = f(3) = 16} \\ s_7 = f(7) &= 4 + 3(7) + 6(7)^2 \text{ mod } 17 = 13 \end{aligned} \tag{2.10}$$

❖ Reconstructing the Secret

The secret can be reconstructed using polynomial interpolation. A minimum of k participants, one more than the degree of the polynomial, must contribute their shares to the reconstruction of the polynomial. The information needed from each participant is a tuple consisting of his value for x and the output of the polynomial function on x. In other words, each participant has a tuple (x, q(x) = s_x). Since no two participants share the same value for x, the tuples are in Lagrange form, and the interpolation polynomial in the Lagrange form is defined as [51]:

$$L(z) = \sum_{i=1}^{k} q(x_i) . \prod_{j=1}^{k, j \neq i} \frac{z - x_j}{x_i - x_j} \text{ mod F} \tag{2.11}$$

Since own interested is only in the first value, s, Equation (2.11) can be simplified by setting z = 0

$$L(0) = \sum_{i=1}^{k} q(x_i) . \prod_{j=1}^{k, j \neq i} \frac{0 - x_j}{x_i - x_j} \text{ mod F}$$

$$= \sum_{i=1}^{k} q(x_i). \prod_{j=1}^{k, j \neq i} \frac{x_j}{x_i - x_j} \text{ mod F}$$

$$= \sum_{i=1}^{k} q(x_i). \prod_{j=1}^{k, j \neq i} x_j . (x_j - x_i)^{-1} \text{ mod F} \quad (2.12)$$

Equation (2.12) can be generalised a bit more by writing it in the form

$$L(0) = \sum_{i=1}^{k} q(x_i).\ \lambda_i \text{ mod F}$$

$$\lambda_i = \prod_{j=1}^{k, j \neq i} x_j . (x_j - x_i)^{-1} \quad (2.13)$$

From Equation (2.13), it is seen that λ_i is independent of the shares and only depends on the number of shares used in the reconstruction of the polynomial. Thus, the values of λ_i could be pre-computed and then used later when recombining the secret.

❖ Definition 1

The vector $\lambda = \{\lambda_1, \ldots, \lambda_n\}$ such that $s = \sum_{i=1}^{k} s_i \lambda_i$ is called the recombination vector.

❖ Example (Reconstruction of the secret using polynomial interpolation)

Consider the previous example where a polynomial mod 17 was constructed and the shares $s_1 =$ 13, $s_2 =$ 0, $s_3 =$ 16, $s_7 =$ 13 were generated. To reconstruct the secret using Equation (2.12) and three of the shares created (e.g., $s_1, s_2 \text{ and } s_7$), the secret is:

$$L(0) = \sum_{i=1}^{k} q(x_i) . \prod_{j=1}^{k, j \neq i} x_j \, . \, (x_j - x_i)^{-1} \bmod 17$$

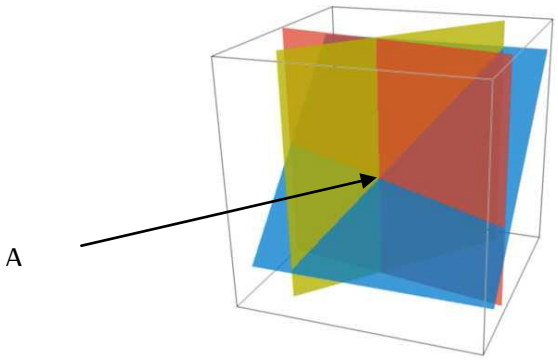
$$= 13. \prod_{j=1}^{k, j \neq i} x_j . (x_j - x_i)^{-1} + 0. \prod_{j=1}^{k, j \neq i} x_j . (x_j - x_i)^{-1} + 13. \prod_{j=1}^{k, j \neq i} x_j . (x_j - x_i)^{-1} \bmod 17$$

$$= 13. \left(2.(2-1)^{-1}.7.(7-1)^{-1}\right) + 0 + 13. \left(1.(1-7)^{-1}.2.(2-7)^{-1}\right) \bmod 17$$

$$= 13. (2.1.7.3) + 13. (1.14.2.10) \bmod 17 = 4.$$

Blakley's Scheme

The idea behind Blakley's threshold secret sharing scheme [45], is that, given n-dimensional non-parallel hyperplanes, they will intersect at a given point. Some coordinate of this point of intersection gives the secret. This is illustrated in three dimensions as in Figure 2.4. The secret corresponds to the position where all the three planes intersect; Point A.



.

Figure 2.4. Illustration of Blakley's secret sharing scheme in three dimensions [45].

Asmuth and Bloom Secret Sharing Scheme

This scheme was first proposed by Asmuth and Bloom [58], and the idea behind it is that the keys or shares, usually referred to as shadows, are congruence classes of a number associated with the original key or secret.

❖ Creating the Shares

In order to share the secret $s, s > 0,$ among n people with a k-threshold, choose a number $p > s$ and a set of numbers $m_1 < m_2 < m_3 < \cdots m_n$ such that the $\gcd(m_i, m_j)$ = 1 for $i \neq j$, $\gcd(m_i, p) = 1 \forall i, and \prod_{i=1}^{k} m_i > p\prod_{i=1}^{k-1} m_{n-i+1}.$ Then, calculate the value $M = \prod_{i=1}^{k} m_i$ and select an arbitrary integer A such that $0 \leq y < M,$ where $y = x + A.p$. The shares would then be $S_i = y \bmod m_i.$

❖ Example: Key Construction

Let the secret be $s = 2,$ then, select a set of numbers that meet the constraints mentioned above. For instance, let p = 3, k = 3, n = 4, and $m_1, m_2 m_{3,} m_4 = 5,7,9,11$ respectively. Hence, the number $M = 5.7.9 = 315.$ Let the random integer 'A' be 50. Therefore, $y = x + A.p = 2 + 50 * 3 = 152,$ which clearly satisfies the condition $0 \leq y < M.$

Thus, the keys (shares) created to be given to the n participants would be

$$\begin{aligned} s_1 &= 152 \bmod 5 = 2; \\ s_2 &= 152 \bmod 7 = 5; \\ s_3 &= 152 \bmod 9 = 8; \\ s_4 &= 152 \bmod 11 = 9. \end{aligned} \qquad (2.14)$$

❖ Reconstructing the Secret

In this scheme, the reconstruction of the shared and distributed secret is fairly simple. First, find the original y-value by applying the Chinese remainder theorem on the set of congruences. That is, solve the congruence system:

$$
\begin{aligned}
&y \equiv s_1 \bmod m_1;\\
&y \equiv s_2 \bmod m_2;\\
&y \equiv s_3 \bmod m_3;\\
&\cdots\\
&y = s_k \bmod m_k.
\end{aligned}
\tag{2.15}
$$

.

After reconstructing the values of y, the original secret is then obtained from

$$s = y \bmod p \tag{2.16}$$

where p is a public variable that was chosen during the construction of the keys (shares).

For example, given k keys or shadows from the shadows $s_1, \cdots s_n$ that were created during key construction above, the secret s could be rediscovered by first finding the y-values using the Chinese remainder theorem on k = 3 of the congruences used earlier:

$$
\begin{aligned}
&y \equiv 5 \bmod 7;\\
&y \equiv 8 \bmod 9;\\
&y \equiv 9 \bmod 11.
\end{aligned}
\tag{2.17}
$$

Since y = 152, by Equation (2.16) the secret is found to be s = 152 mod 3, i.e., s = 152 mod 3 = 2.

Mignotte's Threshold Secret Sharing Scheme

Mignotte's threshold secret sharing scheme [59] is another scheme that uses the Chinese remainder theorem to solve the problem of secret sharing. It is similar to the Asmuth and Bloom Secret Sharing Scheme but differs in the requirements and restrictions on the input data and choice of coprime moduli.

❖ Creating Shares

In order to share a secret among $n \geq 2$ people with a threshold $k \leq n$, create n coprime integers such that $m_1 < m_2 < \cdots < m_{n-1} < m_n$, $m_{n-k+2}.m_{n-k+3}.\cdots m_n. < m_1.m_2.\cdots m_k$ and choose a secret s which lies within the interval $\left[m_{n-k+2}.m_{n-k+3}.\cdots m_n, m_1.m_2.\cdots m_k\right]$. Each share is then $s_i = s \bmod m_i$.

❖ Reconstructing the Secret

Given a set of k shares, the secret can be reconstructed by using the Chinese remainder theorem on the given set of congruence classes:

$$s \equiv s_{i_1} \bmod m_{i_1};$$
$$\ldots$$
$$s \equiv s_{i_k} \bmod m_{i_k}.$$

Linear Secret Sharing

An interesting aspect of all the above secret sharing schemes is that they use ideas from linear algebra to solve the problem of secret sharing. Actually, if the Asmuth & Bloom scheme were to be used on polynomials instead of integers, it would have generalised the Asmuth & Bloom scheme to Shamir's scheme. In fact, with small modifications, all the above schemes can be generalised as was shown in [60]. As they are nearly equivalent, many features, such as key updating algorithms, are easily applied across the different schemes. Other traits, such as information security, are equally as good from one scheme to the next. From here on, this work will focus on different traits and security aspects of linear secret sharing schemes (LSSSs), primarily using Shamir's scheme, but the methods used apply equally as well to the LSSSs.

❖ Updating the Keys

In some cases, such as a company where employees may come and go and where board members are exchanged annually, it may be necessary to secretly update the keys held by the remaining active participants. This can be easily accomplished. First, generate k − 1 random α-values. Thereafter, create a new polynomial, with zero as the first coefficient:

$$P(x) = 0 + \sum_{i=1}^{k-1} \alpha_i . x^i \bmod F \tag{2.18}$$

and calculate the shares $s_1' \cdots s_n'$ with this polynomial. Once this is done, distribute each share s_i' to the participant with the corresponding s_i share and have him calculate his new share $s_i^{new} = s_i' + s_i$. As soon as the new share is created, both s_i and s_i' should be destroyed. In this way, anybody with the old share s_i can no longer participate in the secret sharing scheme, and hence, all former employees that have left an organisation would not pose any security threat to the scheme.

❖ Example

Supposing that the secret s = 5 and the Shamir secret sharing polynomial $f(x) = 5 + 3x + 2x^2 \bmod 7$. For the four participants, $P = \{p_1, p_2, p_3, p_4\}$, the dealer would create the following shares:

$$\begin{aligned} s_1 &= f(1) = 3; \\ s_2 &= f(2) = 5; \\ s_3 &= f(3) = 4; \\ s_4 &= f(4) = 0. \end{aligned} \tag{2.19}$$

Now suppose that the dealer does not want the participant p_3 to hold a valid share any longer. In order to exclude p_3, he creates a new polynomial $p(x) = 0 + 6 . x^1 + 1 . x^2 \bmod 7$ and generates the shares:

$$\begin{aligned} s_1' &= p(1) = 0 \\ s_2' &= p(2) = 2; \\ s_4' &= p(4) = 5 \end{aligned} \tag{2.20}$$

and distributes them to their corresponding participants. Each player that receives s_i' then computes his new share (s_i^{new}) in the scheme as shown earlier:

$$\begin{aligned} s_1^{new} &= s_1 + s_1' = 3 + 0 = 3; \\ s_2^{new} &= s_2 + s_2' = 5 + 2 = 0; \\ s_3^{new} &\text{ does not exist } (\text{but } s_3 = 4); \\ s_4^{new} &= s_4 + s_4' = 0 + 5 = 5. \end{aligned} \tag{2.21}$$

Using the new shares the participants can reconstruct the secret correctly. On the other hand, any combination of two new shares and the share s_3 cannot reconstruct the secret.

❖ Definition: Homomorphic Encryption

Homomorphic encryption is an encryption scheme that allows operations, such as multiplication and addition, to be performed on ciphertext values, resulting in a ciphertext that is equal to performing identical operations on the plaintext prior to encryption [58, 61].

❖ Verifying the Shares

In [62], Feldman introduced a verifiable secret sharing (VSS) scheme based on the Shamir's scheme. Using homomorphic encryption (as defined above) the Feldman scheme allows the participants to verify whether or not the shares they

have received are consistent. It should be noted, however, that while the Feldman scheme binds a player to a given share, the secret is now only computationally secure, i.e., retrieving the secret without the correct number of shares is computationally impossible. The use of discrete logarithms is an example of a homomorphic encryption method that facilitates the use of this scheme.

Another method of VSS is a method by Pedersen [63]. In this method, like the Feldman's, the secret remains secure in the information theoretic sense, but the consistency of the shares is only computationally secure, The Pedersen VSS scheme allows a player to non-interactively check whether the share he has received is consistent.

Security

As seen in the simple secret sharing schemes, the linear threshold secret sharing schemes are also perfectly secure. It was shown that any subset of participants consisting of at least k members can reconstruct the secret. Assuming that an adversary has obtained $k-1$ shares, then, for each possible value in the (half-open) interval $[0, F)$, he can construct one unique polynomial f' with degree k−1 such that $f'(0) = s'$. Even though one of these values will contain the correct secret, each of the values are equally likely, hence by knowing k − 1 of the shares the adversary still has learned nothing about the secret.

Limitations

As powerful as they are, threshold schemes have some impractical limitations [64]. For instance, in a threshold scheme, it is presumed that all participants are equal. However, to borrow from George Orwell [65], some participants "are more equal than others". In other words, in most circumstances, some participants are trusted more than others. For instance, in a network of computers, where each computer represents a participant, a higher threshold for computers that are more likely to be corrupted, like those connected to the Internet, and a lower threshold for the more trusted computers would be required. That is, it might be necessary or better to define differently sized

subsets of the participants needed to reconstruct the secret. The structure consisting of all these sets is called an access structure, as briefly discussed in the next segment.

The Concepts of Access Structures and Monotone Span Programmes

The threshold secret sharing schemes presented in the previous sections only allow any subset of a size k or greater to reconstruct the secret. This approach has obvious disadvantages where it is required that a more fine-grained configurable scheme be emplaced. Ideally, it would be preferred to have a method where a set of potentially differently sized authorised subsets could be defined; this flexibility is the main purpose and/or advantage of an access structure. As introduced in [66], an access structure, denoted by Γ, consists of a set of authorised subsets where each authorised subset has the ability to reconstruct the secret [67].

Definition

A perfect secret sharing scheme realising the access structure Γ is a method of sharing a secret S among a set of n participants (denoted by P), in such a way that the following two properties are satisfied [55]:

- If an authorised subset of participants $B \subseteq P$ pool their shares, then they can determine the value of S.
- If an unauthorised subset of participants $B \subseteq P$ pool their shares, then they can determine nothing about the value of S.

Definition 1

The unauthorised or adversary structure, denoted by Δ, consists of all the sets that are not in Γ. The tuple (Γ, Δ) is an access structure if $\Gamma \cap \Delta = \phi$. An access structure is said to be complete if $\Gamma \cup \Delta = P$.

Definition 2

An access structure Γ is said to be monotone increasing if it satisfies the following property:

- If $B \subseteq P$ is an authorised subset of Γ and $B \subseteq C$ then C is also an authorised subset of Γ.

Similarly, the unauthorised set Δ is monotone decreasing, in other words, if a set A is in Δ then any set $B \subset A$ is also in Δ.

❖ Definition 3

All subsets of Γ that cannot be split into smaller authorised subsets are known as minimal sets. The collection of these sets forms the access structure. This set of minimal subsets is denoted by Γ_0.

❖ Example

Supposing there are five participants $(p_1, p_2, \cdots, p_5)$ and an access structure Γ with the authorised sets $\{p_1, p_2\}, \{p_1, p_3, p_5\}, \{p_2, p_3, p_4\}, \{p_1, p_2, p_3\}$, then,

$$\Gamma_0 = \{p_1, p_2\}, \{p_1, p_3, p_5\}, \{p_2, p_3, p_4\} \qquad (2.22)$$

and hence,

$$\Gamma = \Gamma_0 \cup (p_1, p_2, p_3).$$

Since the set $(p_1, p_2, p_3) \supset (p_1, p_2)$, it is not part of the basis access structure Γ_0.

2.1.3 Cryptographic Key Management

In cryptography, key management is concerned with the secure generation, distribution, and restoration of keys [68]. It is extremely important to ensure that secure methods of key management are emplaced; such that once a key is randomly generated, it should remain secret to avoid its compromise[69]. This is significant because, in most cases, attacks on public-key are directed at the key management level, rather than the cryptographic algorithm itself. Thus, such secure arrangement must be maintained while users are able to obtain a suitable key pair requisite for both their efficiency and security needs; users are able to legitimately access other people's public keys, and also publicise their own public keys. If security is not ensured, unauthorised persons could either change public keys listed in a directory or impersonate other users. In order to ensure that certificates used for these transactions cannot be forged, the issuing of certificates must be conducted in a way that is impervious to attacks. This is ensured through positive authentication of both the identity and public key of an individual prior to issuance of certificates.

In the event that someone's private key is lost or compromised, others must be promptly informed so as to desist from either encrypting messages using the invalid corresponding public key or accepting messages signed using the invalid private key. Users should also be able to store their private keys securely to avert unauthorised access, without hindering legitimate access. It is a significant managerial security requirement, that a key should have a life span during which it is valid; its expiration date must be chosen carefully and publicised in an authenticated channel [68].

2.1.4 Key Recovery in Cryptography

Definitions

It is generally understood that one of the hindrances to the widespread use of encryption, in some instances, is the fact that when a key is lost, any data encrypted with that key becomes inaccessible, and could be rendered useless. Key recovery is a general term encompassing the various ways through which

emergency access to encrypted data could be guaranteed [68]. Key recovery first became popular as a result of US Government's policies on exporting strong cryptography. In a nutshell, the Government agreed to permit the export of systems employing strong cryptography as long as a key recovery method that allows the Government to read encrypted communications was incorporated; this was to be facilitated through the use of escrow agencies.

In the use of secret-key cryptosystems, users must, first of all, agree on a session key; i.e., a secret key to be used for the duration of one message or communication session. In accomplishing this requirement, a risk exists that the key will be intercepted during transmission. This is an important key management problem, for which Public-key cryptography offers an attractive solution within a framework termed digital envelope or key encapsulation. The digital envelope consists of a message that is encrypted using secret-key cryptography and an encrypted secret key [70]. While digital envelopes usually use public-key cryptography to encrypt the secret key, this is not mandatory; Alice and Bob could use an already established secret key to encrypt the secret key in the digital envelope. In a nutshell, the digital envelope is accomplished as follows: Alice chooses a secret key and encrypts the message with it, then encrypts the secret key using Bob's public key. She sends both the encrypted secret key and the encrypted message to Bob. When Bob wants to read the message, he first decrypts the secret key, using his private key, and then decrypts the message, using the secret key. In a multi-addressed communications environment such as e-mail, this can be extended directly and usefully [51].

The Need for Key Recovery

If one loses one’s car or house keys, one can call a locksmith or car dealer who can procure a new one. However, if one loses one’s cryptographic key, there is nobody to call; it’s gone. Many companies protect themselves against this problem by implementing a key recovery strategy. When Alice generates a symmetric key to encrypt her files or a private/public key pair to be used for key distribution, she stores the keys in such a way that only she can recover them. If Alice has a key recovery plan, she also creates copies of the keys and stores them in such a way that someone else can recover them. Similarly, it is possible

for Alice to store them so that it takes more than one person to recover the keys. This way, no one single individual can surreptitiously recover the keys and examine Alice's secret information.

Using the Digital Envelope for Key Recovery

The most common form of key recovery is the RSA digital envelope [58]. Alice has a software program that encrypts her files. It generates a symmetric session key and uses that key to encrypt each file. Alice stores the session key securely, possibly using Password-Based Encryption (PBE). When the session key is generated, Alice can also encrypt it using a key recovery RSA public key. This arrangement is essentially a digital envelope. If Alice loses her key, the owner of the key recovery RSA private key, a recovery agent, can open the digital envelope and retrieve Alice's encrypting session key.

Key Recovery via a Trusted Third party

There are three basic entities that can act as a key recovery agent:

- A Trusted Third Party (TTP).
- A group of trustees, each holding a portion of the key.
- A group of trustees using a threshold scheme.

A TTP is more of a company than a person (e.g., Verisign, Thawte). One of its jobs is to distribute session keys (and KEKs) to parties wishing to communicate securely. Consider a case where Alice decides to use the TTP as her key recovery agent; this requires a certain amount of trust. To act as the key recovery agent, the TTP generates an RSA key pair and distributes the public key to Alice. When Alice generates her keys (the session key or private/public key pair), she encrypts them using the public key that was generated by the TTP (the digital envelope). Alice doesn't send the digital envelope to the TTP because trust should have some limits. She stores the envelope somewhere safe like on a USB stick or smart card; probably, more than one copy. If Alice forgets her password, has a hard drive failure, etcetera, she can take the digital envelope to the TTP. The TTP can open it using the RSA private key and give the contents to Alice. When Alice uses the recovered key (or keys) she once again protects them using PBE.

Advantages/Disadvantages of Using TTPs

The advantage of this system is that key recovery is simple and straight forward. One disadvantage of this scheme is that the TTP has a potential access to all the keys. The main disadvantage (from her employer's point of view) is that the TTP may go out of business. In this case, the company will have to get a new TTP, generate a new key recovery key pair, distribute the new public key and have everyone create new digital envelopes of their keys.

Key Recovery via a Group of Trustees

Many companies and individuals do not like the idea of one company (or person) having access to all of the keys. In such situations, it seems better to break the key into parts and distribute them to several individuals or companies (called trustees). Suppose Alice has a 128-bit symmetric key that she uses to encrypt the files on her hard drive. Alice can split this key into three parts containing 5 bytes, 5 bytes, and 6 bytes. She can now create three digital envelopes using the public keys of three trustees. The advantage here is that no one person can reconstruct the key. All three of the trustees must gather to reconstruct the data. However, the problem here is that one of the trustees could recover part of the key (the one entrusted to him) and try to brute-force the remaining portion that he does not have. If a trustee has 6 bytes (48 bits) he would only need to brute force the unknown 80 bits. This attack may be unlikely, but cryptography is an art that does not allow unnecessary uncertainty. One way to overcome this problem is to use a 384-bit value as a seed in a Pseudo-Random Number Generator (PRNG). The PRNG uses the 384-bit value to generate a 128-bit session key. The 384-bit seed can be split into three parts, each 128 bits long. Each trustee receives a digital envelope containing 128 bits of the total value. More importantly, each trustee is missing 256 bits of the required seed. It is computationally infeasible to attempt to brute-force a 256-bit key within a reasonable timeframe; given the amount of resources and timeframe it requires to brute-force a 128 bit key, as illustrated in Table 2.6 (Section 2.92).

Advantages/Disadvantages of Using a Group of Trustees

The splitting of the secret into multiple digital envelopes has the advantage of preventing one individual from yielding too much power. However, this approach is more difficult to implement and suffers from the same type of problems encountered with the TTP. If one of the trustees goes on holiday, the key is lost. If one of the trustees leaves the company, the key recovery process must start all over again from scratch. In large companies, requiring all users to create totally new digital envelopes can be time-consuming and costly.

Key Recovery via Threshold Schemes

Threshold schemes are often referred to as secret sharing or secret splitting. A secret (such as a session key or private/public key pair) is split into several shares, a subset of which must be combined to recover the secret. For instance, a secret might be split into 6 shares and any 3 might be needed to recover it. The value 3 in the above scheme is called the threshold number. Any reasonable share size and recovery threshold are possible (provided the threshold number is less than or equal to the share count). In order that the secret data or key be recoverable, it must be an RSA private key [39]. The RSA cryptographic algorithm consists of three main steps; namely, key generation, encryption, and decryption. RSA algorithm involves a public key and a private key. While the public key can be known to everyone and is used for encrypting messages, all messages encrypted with the public key can only be decrypted with the use of the private key, which is kept secret and known only to its owner, the originator.

If Alice's company were to implement a threshold scheme, it might work like this: The Company decides how many shares there will be, how many are needed for the key recovery and who the trustees will be. To start the process, all trustees gather to generate and collect shares. First, a key recovery RSA key pair is generated. Then the threshold program splits the private key into the required number of shares. Each trustee gets one share. The program generates the shares by taking as input the private key, the number of shares required and the threshold value. Each trustee is responsible for protecting their share (PBE). Once the shares have been generated the key recovery public key is distributed and the private key is destroyed. The key recovery public key can be used by any employee to encrypt their keys into a digital envelope. If an

employee loses their key they take their digital envelope to an available trustee. That trustee finds any two of the other trustees (assuming three are needed). The three trustees give their shares to the program running the threshold algorithm. The program combines the shares to reconstruct the previously destroyed private key. The private key is used to open the digital envelope and is then destroyed again.

Creating Private Key Shares

Consider a situation where one is required to split up a secret data into a given number of shares; ensuring that any fixed subset of those shares can recover the secret. In order to do this successfully, one would need to create shares that are points on a polynomial (of appropriate degree) which intersects the y-axis at the secret value. This is because a polynomial of degree n needs exactly n+1 points to define it uniquely.

❖ Examples

As an example, take the simplest kind of polynomial – a straight line. The line y = 6x+11 is a straight line that intersects the y-axis at the value 11. Any number of points that lie on this line can be generated. More importantly, given any two points on the line, the above equation could be uniquely reconstructed, and so the secret value could be determined. This is illustrated in Figure 2.5.

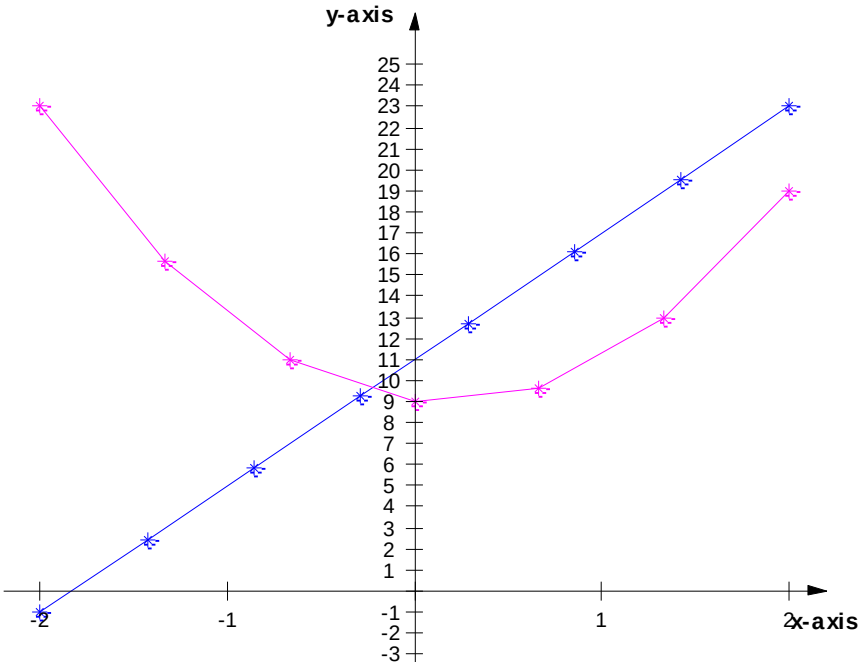


Figure 2.5. Linear and quadratic functions showing shares

- The quadratic polynomial $y = 3x^2 – x + 9$ intersects the y-axis at the value 9. Since it has degree 2 (the value of the highest power) it requires 3 points in order to reconstruct the equation and determine the secret. The constant value at the end of the equation is always the secret value. The other values can be chosen randomly. See Figure 2.5.

- The threshold scheme sequence is as follows:
  - Decide on a threshold value (say k); Choose a polynomial that has degree (k-1); Set the constant in the polynomial to the secret value and choose random numbers for the remaining terms; Decide how many trustees are required (say n, where n > k) and generate these n points (shares) from the polynomial; and Give one share to each trustee.

After the overview of the theoretical background for the secret sharing schemes as discussed above, a comparative analysis of the various secret sharing methods will now be undertaken in the next segment of this chapter.

2.2 A Comparative Analysis of the Various Secret Sharing Methods

Traditionally, secret sharing models make the following important assumptions concerning the potentially malicious disposition of entities involved in the sharing and reconstruction mechanisms. This potentially malicious behaviour is usually modelled as an adversary with the following presumptions [35, 38, 71]:

Trusted Dealer - An adversary cannot corrupt the dealer; he is fully trusted.

Passive - An adversary can capture shares, but otherwise the protocol is executed correctly; shares are never corrupted.

Polarised Participants - Participants are either completely honest or completely malicious (there are no intermediate positions).

While these assumptions could be reasonable in some situations, they would not necessarily be applicable in many environments. Obviously, they fall below the requirement of the high-security demands placed on computationally secure cryptographic primitives that are modelled using provable security [35, 72, 73]. Quite a few recent works on secret sharing schemes have focused on the problems of secret sharing in situations where some of these assumptions are challenged; i.e., most of the recent works involve active adversaries, as opposed to the passive ones in the traditional presumptions. In the new re-orientation, schemes are designed with the assumption that adversaries are able to take full control of participants and corrupt their shares.

Tompa and Woll [74] were the first to challenge the traditional secret sharing adversary model. Their paper demonstrated how an active adversary could exploit the Shamir threshold scheme; their attack model can be applied to any linear secret sharing system. The paper assessed the impact of an active adversary that takes the form of a participant who maliciously submits a fake share during the reconstruction of a secret. This led to various secret sharing models to cater for the undesirable consequences that would emerge as a result of the active adversary notion in secret sharing. Table 2.1 illustrates the characteristics of some secret sharing schemes with expected possible attacks based on the notion of active adversaries.

Table 2.1. Attributes of schemes for Tompa and Woll undesirable consequences [35]

Possible Attacks / **Scheme Type**		**Honest Users Learn Secret?**	**Honest Users Alerted to Cheating?**	**Adversary Learns Secret?**
Robust Schemes		Yes	Sometimes	Yes
Cheater Detection		No	Yes	Yes
Cheater Identification		No	Yes	Yes
Almost Robust (Fairness)		Sometimes	Yes	Sometimes
Cheating Immune		No	No	No

2.2.1 Classification of Secret Sharing Schemes

Secret Sharing Schemes could be classified into various categories using different criteria [75-77]. This could be in terms of the number of secrets to be shared; yielding two classes - identified as ‘single secrets’ and ‘multiple secrets’

[78, 79]. They may also be classified in terms of the share's capabilities; resulting in another two classes – tagged 'same weighted shares' and 'multi-weighted shares' [80, 81]. In this way, the secret share of a higher level user contains more information about the original secret than the share for a lower level user. Other criteria used for categorisation include the abilities of the scheme, the computational power of the participants, its robustness [74, 82, 83], and the techniques used in designing the schemes.

Generally, secret sharing schemes are classified into one of three categories [75]; namely, 'perfect', imperfect' and 'ramp' [5] schemes. Of these, the SSSS which belongs to the class of perfect secret sharing schemes is the most original, simplest, flexible and most popular [5, 75]. These categories and their authors are as illustrated below:

Perfect secret sharing schemes – Benaloh (1989), Feldman (2008), Herzberg (1995), (Pedersen (1992) and Shamir (1979).

Non-perfect secret sharing schemes - Asmuth-Bloom (1983), Brickell (1995), Ghodosi (1998), Iftene (2007) and Mignotte (1983).

Ramp secret sharing schemes – Blakley (1979), Bai (2006), Franklin (1992) and Pang (2008).

The need to consider the concept of active adversaries and the impact they may have on secret sharing schemes is highlighted in the next two sections.

2.2.2 The Issues Arising from Active Adversarial Models

A shift from the traditional passive adversarial model in favour of active adversaries for a secret sharing scheme raises a number of issues which were either not apparent previously or not important. Now that the Dealer is no longer fully trusted, shares can now be corrupted and the participants are neither fully trusted nor absolutely polarised, these issues now demand serious attention. They include answers to the following questions [35, 84, 85]:

Who should reconstruct the shares – the Dealer, one of the participants or an external third party?

Should reconstructions be open or closed; should the secret be revealed during reconstruction or not?

Are the adversaries static or dynamic?

What are the goals of the adversaries – is it just to prevent reconstruction or gain information about the secret?

2.2.3 Schemes Designed to Counter the Effects of Active Adversaries

In an effort to answer some of the questions above and neutralise the threats posed by active adversaries like the three attack models illustrated in Table 2.1, various secret sharing schemes were devised in recent time. These include:

Robust Secret Sharing Schemes

The term Robust Secret Sharing usually describes schemes that are designed to ensure successful reconstruction of the correct secret; even if some participants submit incorrect shares. The schemes in this category include:

❖ Bellare and Rogaway's Classification – Bellare and Rogaway introduced a unifying framework for secret sharing schemes whereby the traditional concepts of a trusted Dealer and polarised participants are maintained, with a relaxation of the presumption that shares can only be captured but not corrupted. Excluding their fourth category of 'no privacy', this framework identifies three meaningful levels of privacy thus [84, 86, 87]:

- Perfect Secret Sharing (PSS) - No information about the secret is revealed, independent of the computing power of the adversary; this is the traditional model of privacy.
- Statistical Secret Sharing (SSS) – A small amount of information about the secret is potentially revealed, independent of the computing power of the adversary; i.e., an imperfect scheme in the traditional model.
- Computational secret Sharing (CSS) – This protects the secret from an adversary with reasonable computing resources.

This framework goes further by identifying nine levels of recoverability.

- ❖ Robust construction

Detecting and Identifying Cheaters

Schemes that detect and/or identify cheaters comprise of the following:

Secret Sharing Schemes with Cheater Identification - These allow honest participants to detect and identify any corrupt shares submitted by an adversary [88].

Attributes of secret sharing schemes with cheater identification (detection) are [75, 82, 88]:

- Presumption of a trusted Dealer;
- Honest participants are willing to sacrifice recovery of the secret if an adversary corrupts the shares; for as long as the corrupted shares are identified (detection);
- The main recoverability goal of the adversary is to prevent the correct secret from being reconstructed while remaining unidentified (undetected);
- The schemes potentially allow the adversary to obtain the correct secret, while honest participants do not.

Other schemes include:

Almost robust secret sharing;

- ❖ Cheating immune secret sharing;
- ❖ Rotational secret sharing;
- ❖ Verifiable secret sharing (VSS);
- ❖ Information-theoretically (interactive) secure VSSs;
- ❖ Computationally secure VSSs; and
- ❖ Publicly-verifiable VSSs.

The performance assessment of various secret sharing schemes is presented in the next section.

2.2.4 Comparative Performance Analyses of Secret Sharing Schemes

The comparative performance analyses of secret sharing schemes are illustrated in Tables 2.2 – 2.4 below.

Table 2.2. Types of secret sharing schemes with their respective hurdles [52]

Type of scheme	Usage	Hurdles
Threshold Schemes.	A group of mutually suspicious individuals with conflicting interests must cooperate.	Design of access structures is difficult
General Access Structure Schemes.	Only certain specified subsets of the participants should be able to recover the secret.	To add extra functionalities is difficult.
Verifiable Secret Sharing (Interactive Proofs).	Dealer and shareholders both interact with each other. Also, shareholders can interact with each other.	Asserts a proof only to the participants of this protocol and only at the moment it is held. They cannot be legal proofs in court.
Verifiable Secret Sharing (Non-Interactive Proofs).	Only dealer is allowed to send messages, in particular, the shareholders cannot talk with each other or with the dealer when verifying a share.	Many of the proposed schemes are providing cheating verification but not cheater identification.
Publicly Verifiable Secret Sharing.	Everybody can verify the correctness of his share.	New members can"t enroll the system according to the need of actual circumstance.
Proactive Secret Sharing Schemes.	Improve security through periodic executions.	Need to be more secure and efficient of course, without any information-leak or any secret change.

Table 2.3. A matching of application type onto the required features of secret sharing schemes [52]

Application Semantics	Required feature of secret sharing
Transfer money from a bank	Threshold schemes
Launching of a ballistic missile	Threshold, General Access Structure
Communications networks	Ideal, Perfect, Low complexity
Trusted Shareholders, Untrusted Dealer	Verifiable Secret Sharing
Trusted Dealer, Untrusted Shareholders	Verifiable Secret Sharing, Periodically Renew Share
Electronic voting	Publicly Verifiable Secret Sharing
Private querying of database	Low Complexity, Threshold
Collective Control	Periodically renew shares, Enroll/dis-

	enroll shareholders, Recover lost share
escrow-cryptosystems	Publicly Verifiable Secret Sharing
Secure Storage	Ideal, Reliable, General Access Structure

Table 2.4. Comparison of secret sharing schemes on extended capabilities [52]

Authors	**Perfect**	**Ideal**	**Flexibility**	**Security**	**Multi-functionality**		**Extended Capabilities**			
			Threshold Scheme (k, n)	Computation Time Complexity	General Access Structure	Periodically Renew Shares	Enroll / Disenroll Shareholders	Verifiability of Shares	Cheater Identification	Recover lost shares
G Blakley	No	No	Yes	Low	No	No	No	No	No	No
Tang, Yao	Yes	Yes	Yes	Low	No	No	No	Yes	No	No
Chou, Lin, Li	Yes	Yes	Yes	Very Low	Yes	No	Yes	No	No	No
Shi, Zhong	Yes	Yes	Yes	Low	No	Yes	No	No	No	No
K. Srinathan	No	Yes	Yes	High	Yes	No	No	No	No	No
Staddler	Yes	Yes	Yes	High	No	No	No	No	No	No
Bai	Yes	Yes	Yes	High	No	No	No	No	No	No
Jai Yu	Yes	Yes	Yes	High	No	No	Yes	No	No	No

Tables 2.2 – 2.4 mark the end of formal reviews for the secret sharing literature. Bearing in mind that central to the idea of secret sharing is the notion of single-point vulnerability and the need to eliminate this while handling a sensitive data, it is timely that the concepts of human security perimeter and its extension mechanisms are espoused next. Other related concepts like the web of trust, human factors, human infrastructure, human trust, and trust-related human characteristics that are indispensable in the process of interpersonal human

relations would also be discussed in the next section. It would also be interesting to find out if the term ‘trust’ is quantifiable and measurable using appropriate scales.

2.3 Extending the Human Security Perimeter through a Web of Trust

Security perimeter is the boundary within which security control measures are in effect to protect assets. These measures are in three categories; physical, procedural and logic [89]. Physical security measures employ guards, weapons, dogs, safes, strong rooms, fence/barbed wire and the likes, while procedural measures deal with security management/policy related issues like vetting and password policies. Logic security is concerned with the deployment of cryptographic assets in forms of mathematical algorithms and cryptographic protocols, such as digital signatures and various encryption/decryption techniques and keys. These are designed to ensure confidentiality, integrity, availability, authenticity and non-repudiation in order to preserve mutual trust among corresponding partners. This research effort is only concerned with logic security, but with due considerations for the other two components of security measures. This is very crucial because it has become evident that, in practice, there cannot be technical hacking in a vacuum (completely independent of human hacking) [90]. For this reason, in addition to technical solutions (e.g., using Cryptography) for every security problem, there are needs for the elements of both physical and procedural measures as well. For instance, it is expected that every organisation must have procedural security policy measures or guidelines as illustrated by the sample in Appendix 4 [91].

The illustration in Figure 2.6 does shed some light on the concept of security perimeter, where the individual employee in an organisation, or a person within a given system of human interaction, only trusts himself within his individual perimeter. It is a common saying that once an item of information is disclosed to a second party; it would cease to remain a secret. This poses a problem because he/she cannot operate alone and function well as a worker; he must interact with various other individuals and entities, both within and outside the

organisation. Hence, in order for him to function effectively, he would need to extend or expand his narrow security perimeter; to do this, he needs trust- and confidence-enhancing measures such as provided by one or some of the security measures identified above. This is where technology (e.g., cryptographic algorithms and protocols) comes to play.

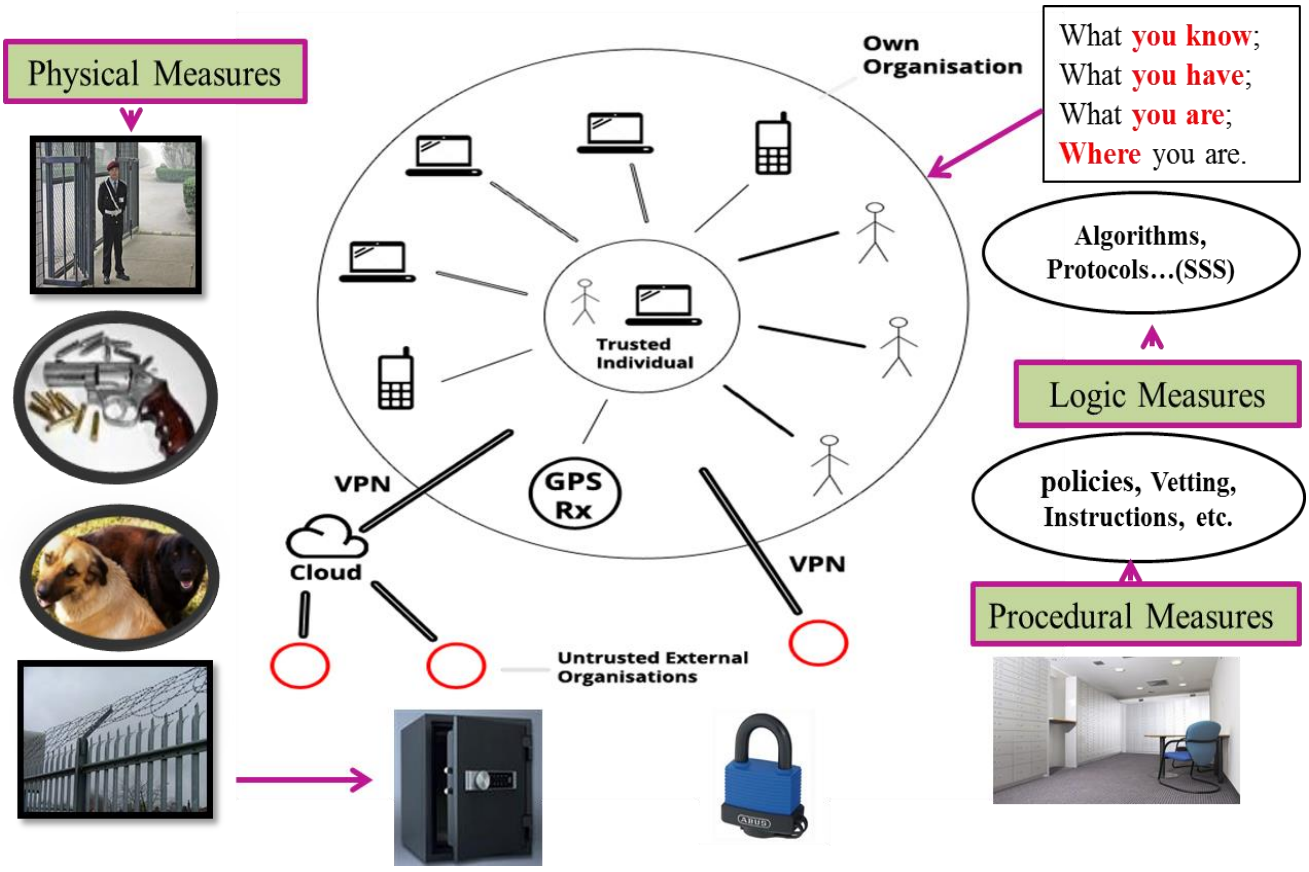


Figure 2.6. Security measures: physical, procedural and logic

At the heart of security concern is the issue of trust that is associated with the active variables in a system. Since the human factor is the most critical element in security systems [92], security perimeter could be defined in relation to the human trust level; via mutual positive identification of the correspondents/devices, using various means of authentication [93].

2.3.1 Zimmermann's Web of Trust

The web of trust is a concept used in PGP and other PGP-compliant systems to establish the authenticity of the binding between a public key and its owner. Its decentralised trust model is an alternative to the centralised trust model of a PKI, which relies exclusively on a CA or a hierarchy of CAs. As with computer networks, there are many independent webs of trust, and any user can be a part of, and a link between, multiple webs [94].

The web of trust protocol was first described by Zimmermann in 1992 in the manual for PGP version 2.0, as follows:

> “As time goes on, you will accumulate keys from other people that you may want to designate as trusted introducers. Everyone else will each choose their own trusted introducers. And everyone will gradually accumulate and distribute with their key a collection of certifying signatures from other people, with the expectation that anyone receiving it will trust at least one or two of the signatures. This will cause the emergence of a decentralised fault-tolerant web of confidence for all public keys” [95].

The scheme is flexible, unlike most public key infrastructure designs, and leaves trust decision(s) in the hands of individual users. It is not perfect and requires both caution and intelligent supervision by users. Essentially all PKI designs are less flexible and require users to follow the trusted endorsement of the PKI-generated certification authority (CA)-signed certificates. It uses self-signed certificates and third party attestations of those certificates. The term "web of trust" does not imply the existence of a single web of trust, or common point of trust, but rather one of any number of potentially disjoint "webs of trust."

Among its benefits is the fact that it can interoperate with a PKI CA fully trusted by all parties in a domain that is willing to guarantee certificates, as a trusted introducer. However, if the "web of trust" is completely trusted, its nature is such that trusting one certificate amounts to granting trust to all the certificates in that web. A PKI is only as valuable as the standards and practices that control the issuance of certificates. Thus, by including PGP or a personally instituted web of trust in a PKI scheme, it could significantly degrade the trust-ability of that enterprise's or domain's implementation of PKI [96]. Another of its drawbacks is

that, if a user loses track of a private key, he would no longer be able to decrypt messages sent to him; if the message was encrypted using the matching public key found in an Open PGP certificate. Similarly, early PGP certificates did not include expiry dates, and those certificates had unlimited lives. Users had to prepare a signed cancellation certificate against the time when the matching private key was lost or compromised.

2.3.2 Human Factors and Human Infrastructure in the Context of Trust

In this segment, effort is made to define/explain the terms trust', 'human factors' and 'human infrastructure'. Additionally, their pristine concepts and, where necessary, contexts of usage in this research work are also highlighted. This is a deliberate effort to properly situate the subtitle of this research Thesis in order to further facilitate its easy understanding by the readers.

Trust

Etymologically, the word 'trust' comes from Old Norse, a North Germanic language (Icelandic), which was spoken by the inhabitants of Scandinavia, as well as the inhabitants of their overseas settlements, from about the 9th to 13th centuries BCE [97, 98]. It either metamorphosed from 'traustr' which meant 'strong' or 'treysta' which stood for 'strengthen' or 'reinforce'. In modern English, the words generally taken as synonyms of 'trust' include faith, belief, hope, conviction, confidence, expectation, reliance and dependence. A cursory look at the dictionaries unveils the main elements of its definition as "firm belief in the reliability, truth, or ability of someone or something" (Oxford); "confidence in and reliance on good qualities, especially fairness, truth, honour, or ability" (Encarta); "to believe that someone is good and honest and will not harm you, or that something is safe and reliable" (Cambridge); "belief that someone or something is reliable, good, honest, effective, etc." (Webster); and "allow someone to have, use, or look after (someone or something of importance or value) with confidence." The value of trust in the process of all forms of human interaction is as significant as aptly described by Russell [99] in her book title: "Trust: The New Workplace Currency;" i.e., it is the medium of exchange among

humans, without which no trade, whether in kind or cash, can take place with positive results [100, 101].

The need for trust arises from the fact that, working together often involves interdependence, and people must, therefore, depend on others in various ways to accomplish their personal and organisational goals. Thus, the definition of trust adopted in this research is “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” [2, 102]. The term ‘vulnerability’ here implies the willingness to accept some measure of risk.

The significance of trust is as powerful in the process of human interactions as punctuation is in sentence construction. Consider the following illustration using a sentence - with and without punctuation marks:

Without Punctuation: “A woman without her man is nothing”

With Punctuation: (1) “A woman, without her man, is nothing.”
(2) “A woman: without her, man is nothing.”

As the respective punctuation marks turned the possible imports of the above sentence upside down, so does a message of trust – when appropriately or inappropriately communicated - turn the results of human interaction upside down. Trust is the basic infrastructure for all forms of human interactions; be it socio-economic, socio-political, ethnoreligious, interpersonal, electronic, and tele-communicative – whether locally or globally. Hence, there must be factors that enhance trust with corresponding benefits [103, 104] and factors that diminish it with corresponding detriments [99, 105]. These factors are governed by the key elements in the synonyms and definitions of trust as highlighted above. A careful examination would suggest that they include the attributes of faithfulness, hopefulness, confidence, reliability, truthfulness, ability, fairness, honour (integrity, principles, morality, honesty, probity, righteousness, rectitude, uprightness, goodness, decency, prestige, reputation, distinction, virtue, etc.), safety, effectiveness, predictability, benevolence, etc. While these factors yield

benefits, their exact opposites attract detriments. Indeed, the concept of all forms of trusteeship is a function of human trust [106].

Human Factors and Ergonomics

Human factors and ergonomics (HF&E), also known as comfort design, functional design or systems, is the practice of designing products, systems, or processes to take proper account of the interaction between them and the people who use them [107, 108]. The term 'human factor' is used mainly in the US. Its other variants include 'human factors engineering' and 'human engineering'. In Europe and the rest of the world, the term ergonomics' is more prevalent [108, 109].

'Human factors' is an umbrella term for many areas of research; including human performance, technology, design, and human-computer interaction. It is a profession that focuses on how people interact with products, tools, procedures, and any processes likely to be encountered in the modern world [101, 110, 111]. Its practitioners may come from a variety of backgrounds; though predominantly they are psychologists (cognitive, perceptual, and experimental) and engineers. Other contributors are designers (industrial, interaction, and graphic), anthropologists, and computer scientists. While ergonomics tends to focus on the anthropometrics[1] for optimal human-machine interaction, human factors is more focused on the cognitive and perceptual factors [107, 108, 112].

Human factors practitioners are particularly interested in the following areas: workload, fatigue, situational awareness, usability, user interface, learnability, attention, vigilance, human performance, control and display design, stress, visualisation of data, individual differences, aging, accessibility, shift work, human error, and working in extreme environments. In a nutshell, 'human factors' involves working to make the environment function in a way that looks

[1] Anthropometry is the study of objective measurable physical variables in humans, which impacts on architecture, industrial design and ergonomics.

natural to people by taking relevant human attributes into consideration. The terms ‘human factors’ and ‘ergonomics’ became popular only in recent times, although the origin of this field of study is traceable to the design and use of aircraft during WW2 in an effort to improve aviation safety [108].

Different sectors of human activities concentrate on slightly varying aspects of human factors and ergonomics. Although prominent among these varieties include those from professional societies, scientific literature, government agencies, industry and open sources [107], for convenience, I will take only a few samples for illustration; each from a different sector.

Human Factors and Ergonomics Society (HFES) sees HF&E as a discipline concerned with the application of what we know about people, their abilities, characteristics, and limitations of the design of equipment they use, environments in which they function, and jobs they perform [107, 113]. In the perception of WHO, HF&E refers to environmental, organisational and job factors, as well as human and individual characteristics which influence behavior at work in a way that may affect health and safety. A simple way to view human factors is to think about three aspects; the job, the individual and the organisation and how these impact on people’s health and safety-related behaviour [107]. In the scientific literature, HF&E is defined as a body of knowledge about human abilities, human limitations, and other human characteristics that are relevant to design. Human factors engineering is the application of human factors information to the design of tools, machines, systems, tasks, jobs, and environments for safe, comfortable, and effective human use. It is essentially concerned with the understanding of interactions among humans and other elements of a system, and the profession that applies theory, principles, data and methods to design in order to optimise human well-being and overall system performance [107, 108, 114]. ISO 6385 has also adopted the second scientific definition. In the industrial sector, HF&E is the study of human performance and its application to the design of technological systems. The goal of this activity is to enhance productivity, safety, convenience and quality of life. Example topics include models [115] and theories of human performance, design and analytical methodology, human-computer interface

issues, environmental and work design and physical/mental workload assessment. Human factors engineering requires input from disciplines ranging from psychology and environmental medicine to statistics [116-118] .

The concept of human factors, as employed in this research work, relates to all the trust-enhancing (beneficial) and trust-diminishing (detrimental) human attributes, as highlighted under trust above. It is then posited that the consideration of applicable elements of these attributes, both the positive and negative, is a 'sine qua non' in the design and functioning of all aspects of human endeavours in order to realise optimum output; with particular emphasis on technological systems.

Human Infrastructure

An infrastructure is the most basic level of physical and organisational structure in a complex body or system that serves as a foundation in order to enable the rest of its elements to function optimally [119]. Thus, it follows that the large-scale public systems, services, and facilities of a country or region that are necessary for economic activity, including power and water supplies, public transport, telecommunications, roads, and schools constitute the national infrastructure. When this definition is applied to the concept/context of the term 'human infrastructure' as employed in this research work, it would mean that any technological design/device/system that is emplaced without the necessary quality assurance that could only be guaranteed via requisite considerations of trust and human factors, as highlighted above, would not yield optimum results. With particular reference to any technological system, a skillful interplay between human trust and other human factors should constitute its infrastructural base. For instance, if one puts in place a gigantic state of the art industrial complex without trained workers who are capable of operating its complex systems efficiently, this would amount to a mere waste of time and resources.

2.3.3 Adeka's Web of Trust

In contrast to the Zimmermann's web of trust as a possible successor to the PKI system, which was highlighted earlier, the concept of web of trust as reflected in

the subtitle of this work has two component elements. The first element relates to a network (web) of trustees or participants in the business of secret sharing as expounded by Shamir. The second element has to do with the security which results from the web implementation of this research effort, which serves to enhance secret sharing via a secure and trusted website [120]. The same trust instruments (a web of trusted associates and secure website) that engender the emergence of such a secure and healthy business environment could also be responsible for the extension of the individual human security perimeter discussed earlier, as a consequence of increased human confidence.

Statistical Proof for the Extension of Human Security Perimeter through a Web of Trust: Estimating the Measure of Trust from the Web

In statistical contraption, the probability that a valuable item (Secret Data) that is kept by one trusted person would get lost or damaged is equal to the probability that the item would be safe or remain secure. Let the probability of loss/damage for the item being kept by one trustee be designated as $P_L T_1$ and the corresponding probability that the item would remain safe/secure be denoted as $P_S T_1$. Then, it can be deduced that:

$$P_L T_1 = 1/2 \quad (2.23)$$

$$P_S T_1 = 1/2 \quad (2.24)$$

Similarly, it can be shown that:

$$P_L T_2 = P_S T_2 = 1/4$$

$$P_L T_3 = P_S T_3 = 1/6$$

.
.
.

$$P_L T_i = P_S T_i = 1/2i \quad (2.25)$$

Where 'i' is the iterative index for trustees or trusted people sharing the Secret. In other words, Equation (2.25) is an expression of the individual probability that the fraction of the Secret that is held by each of the 'n' participants (the i^{th} participant) or trustees will be lost/damaged or remain safe/secure.

The probability that all the Shares might get lost[2] is the Joint Probability ($P_{JL}T_n$) of loss/damage for all the individual probabilities as defined above ('n' being the total number of participating trustees). In statistical notation, this is computed by taking the product of all the individual probabilities:

$$P_{JL}T_n = P_LT_1 \bullet P_LT_2 \bullet P_LT_3 \bullet \ldots \bullet P_LT_n$$

$$= \prod_{i=1}^{n} P_LT_i \qquad (2.26)$$

But

$P_LT_1 = P_LT_2 = P_LT_3 = \ldots = P_LT_n$, for all $T_{i's}$ (Shamir's assumed equal likelihood).

From Equation (2.25):

$P_LT_n = 1/2n$, thus, Equation (2.26) leads to:

$$P_{JL}T_n = \prod_{i=1}^{n} (1/2i) \qquad (2.27)$$

From Equation (2.27), it can be demonstrated that, for all 'i's' greater than '1' (i = 1,n), $P_{JL}T_i$ is much less than P_LT_1. Equations (2.25) and (2.27) may be referred to as Adeka's Twin Probability Equations on Secret Sharing (ATPESS). Consider the following illustration:

As an example, let n = 5, then, Equation (2.27) yields:

[2]It is noted that own worry is that the secret portions (Shares) being held by the trustees might get lost; not that they would be safe. Thus, henceforth, the effort to estimate the level of trust that could be associated with sharing a Secret among more than one trustee will be devoted to the probability of loss/damage only. For a (k, n)-threshold scheme, since not all the Shares are required in order to reconstruct the Secret, it follows that the concern should be about the joint probability of loss/damage.

$$P_{JL}T_5 = \prod_{i=1}^{5}(1/2i) = (1/2)\bullet(1/4)\bullet(1/6)\bullet(1/8)\bullet(1/10)$$

$$= 2.60\,x\,10^{-4}\text{ (i.e., 0.000260 for } P_{JL}T_5 \text{ compared with 0.5 for } P_LT_1)$$

But

$$P_{JS}T_n = 1 - P_{JL}T_n\text{; i.e., } P_{JS}T_5 = 1 - P_{JL}T_5$$

$$= 1 - 0.000260$$

$$= 0.99974 = 9.9974 \text{ x } 10^{-1} \text{ (i.e., } P_{JS}T_n \approx 1.0\text{), for n = 5.}$$

Where $P_{JS}T_n$ is the joint probability that all the n Shares would remain secure.

This illustration proves that mathematically and sensibly speaking, as n increases in the (k, n)-threshold secret sharing scheme, independent of 'k', the joint probability for the Secret getting lost/damaged or compromised decreases exponentially. By implication, since the joint probability of the Secret being safe is inversely proportional to that of its loss/damage, it follows that the joint probability for safety increases exponentially, as n increases. This is illustrated in Figure 2.7.

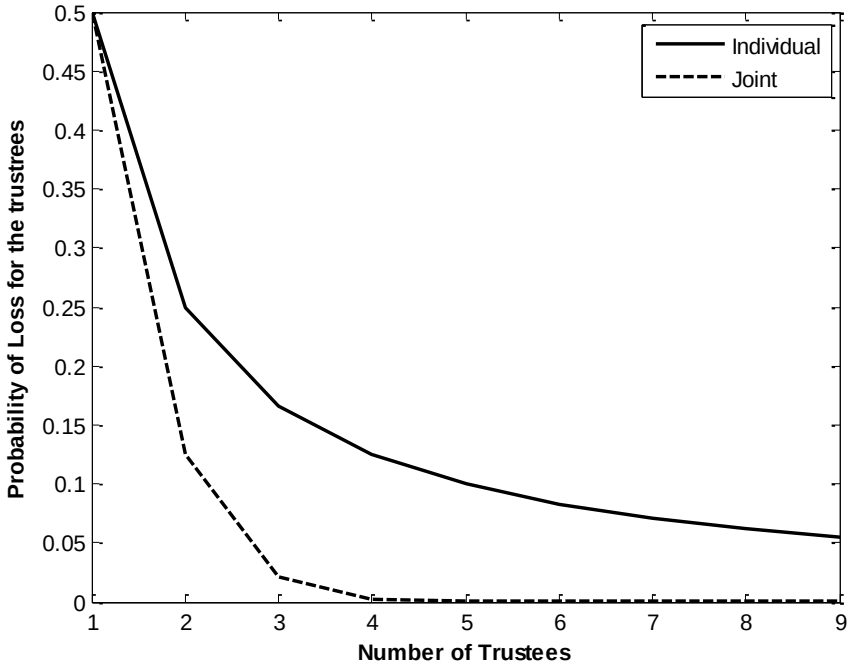


Figure 2.7. Exponential decay in the probability that a shared secret item would get lost/damaged as the number of trustees increases

Effect of (k, n)-Threshold Secret Sharing on Human Trust

Using statistical probability, as illustrated above, the lesson acquired is that secret sharing decreases the chances for the loss/damage of the Secret exponentially and, by implication, it increases the chances for the safety/security of the Secret exponentially. Therefore, it would be reasonable to posit that, secret sharing increases or extends the human confidence/trust that is to be associated with the safety/security of the Secret Data, when compared to a situation where an individual keeps the Secret all alone. The resultant increased confidence/trust, due to enhanced safety/security, is engendered by the involvement of the network (web) of 'n' trusted associates or participants/trustees in the sharing scheme; and hence, the subtitle of this Thesis – 'Extending the Human Security Perimeter through a Web of Trust. Other models for measuring human trust are briefly highlighted in the next section.

2.3.4 Other Models for Measuring the Human Trust

The subject of trust has been generating increased interest in organisational studies, most probably because many of the problems associated with organisational/system complexity have defied solutions, despite advances in technology. Cybersecurity is obviously one of such problems. Scholars have alluded to trust as a fundamental ingredient, a lubricant or an indispensable dimension of social interaction [2]. The importance of trust has been highlighted in many areas of human endeavour. These include communication, leadership, management by objectives, negotiation, game theory [121], performance appraisal, labour-management relations and implementation of self-managed work teams. In spite of the great deal of interest in trust among scholars, its study in organisations has remained problematic for a number of reasons. These include problems with the definition of trust; lack of clarity in the relationship between risk and trust; confusion between trust and its

antecedents/outcomes; lack of specificity of trust referents leading to confusion in levels of analysis; and a failure to consider both the trusting party (trustor) and the party to be trusted (trustee). Mayer et al. [2, 102] considered all these problems in varying degrees and came up with a model of trust of one individual or party for another, incorporating risk taking in the relationship. A major difficulty in previous researches on trust was a lack of clear differentiation among the factors that contribute to trust, trust itself, and its outcomes. Of particular significance is the relationship between trust and risk. Though many researchers agree that the need for trust only arises in a risky situation, there is no consensus on its relationship with trust; it is unclear whether risk is an antecedent to trust, is trust, or is an outcome of trust – and hence, the role of interpersonal trust in risk taking.

In the following subsections, the definition of trust developed by [2] is presented, and it is differentiated from similar concepts. This would be followed by the characteristics of both the trustor and the trustee, which affect the amount of trust the trustor has for the trustee. Thereafter, the relationship between trust and risk is considered. Finally, the effects of context as well as the long-term development of trust will also be highlighted. A pictorial impression of an integrative model of organisational trust [2, 102] as deduced by Mayer et al. will be presented in the process of this brief coverage.

Definition

Mayer et al. [2] began with the positions of several researchers on the concept of trust. He cited Rotter [122] who defined trust as “an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon.” His other cited opinions include the “willingness to take risks may be one of the few characteristics common to all trust situations;" and in order “to appropriately study trust there must be some meaningful incentives at stake and that the trustor must be cognisant of the risk involved.” Mayer then defined trust as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.” He applied this definition to any

relationship with another identifiable party who is perceived to act and react with volition toward the trustor. With the introduction of vulnerability, this definition parallels other definitions because being vulnerable implies that there is something of importance that could be lost, and hence, an inherent risk is also germane. It should be noted that trust is not taking risk per se; it is rather a willingness to take risk. This distinction will be further explored in a later section.

It is observed that many terms have been used synonymously with trust, thus muddling up the nature of trust. These include cooperation, confidence, and predictability. There is a need to differentiate trust from these concepts in order to correctly understand its nature [2, 102]. This is briefly attempted in the next three paragraphs.

Cooperation

Although trust and cooperation have at times been treated as synonymous, they are essentially two different concepts. One could cooperate with someone who one does not really trust for the following possible reasons: If it is known that there are control mechanisms to punish the trustee for untoward behaviour; if the situation does not make the trustor vulnerable; or where the trustee's motives coincide with the trustor's desires. Thus, cooperation without trust is possible where vulnerability is absent or minimal.

Confidence

The relationship between 'confidence' and 'trust' is not clearly defined in the available literature [2]. After citing several authors to illustrate the lack of clarity in the distinction between the two terms, Luhmann [123] proposed a distinction that helps to differentiate trust from confidence. He noted that both concepts refer to expectations that might lead to disappointments. He argued that trust differs from confidence because it requires a previous engagement on a person's part, recognising and accepting the fact that risk does exist. Although Luhmann suggested that both confidence and trust may become routine, the distinction "de-pends on perception and attribution. If you do not consider alternatives (every morning you leave the house without a weapon!), you are in

a situation of confidence. If you choose one action in preference to others in spite of the possibility of being disappointed by the action of others, you define the situation as one of trust" [123]. In this differentiation between trust and confidence, it is documented that risk must be recognised in the former and assumed; such is not the case with confidence. The trustor's explicit recognition of risk in Mayer's model [2] eliminates the conceptual ambiguity inherent in other research conclusions such as the one presented by Coleman [124].

Predictability

As with cooperation and confidence, there is clearly a relationship between predictability and trust, but the association is also vague. While it is accepted that both prediction and trust are means of reducing uncertainty as documented by Lewis and Weigert [125], much of the literature tends to equate the duo as synonyms as highlighted by Gabarro [126]. He illustrated this point by citing many definitions of trust, including "the extent to which one person can expect predictability in the other's behaviour in terms of what is 'normally' expected of a person acting in good faith." In the words of Deutsch [127], in order for the term trust to be meaningful, it must go beyond predictability. He contended that to equate the two is to suggest that a party who can be expected to consistently ignore the needs of others and act in a self-interested fashion is therefore trusted because the party is predictable. A major lacuna in such an approach is the willingness to take a risk in the relationship and to be vulnerable. One can believe such a trustee to be predictable in a situation in which the trustee influences resource distribution between the trustee and the trustor but also be unwilling to be vulnerable to that trustee. It is obvious that another party's predictability is not sufficient to make a person willing to take a risk.

Another clear illustration is that, if a person's superior always "shoots the messenger" when bad news is delivered, the superior is predictable. However, this predictability will not increase the likelihood that the individual will take a risk and deliver bad news to him. On the contrary, predictability can reduce the likelihood that the individual will trust and therefore take actions that allow vulnerability to the superior. Hence, predictability is insufficient to engender trust; and cannot be equated with trust [127]. The highlights on the factors

concerning the trustor and trustee, which lead to trust would further illustrate this point, as discussed next.

Characteristics of the Trustor

This and the next sections deal with factors concerning the trustor and then the trustee; which lead to trust. These components of the trust model are illustrated in Figure 2.8.

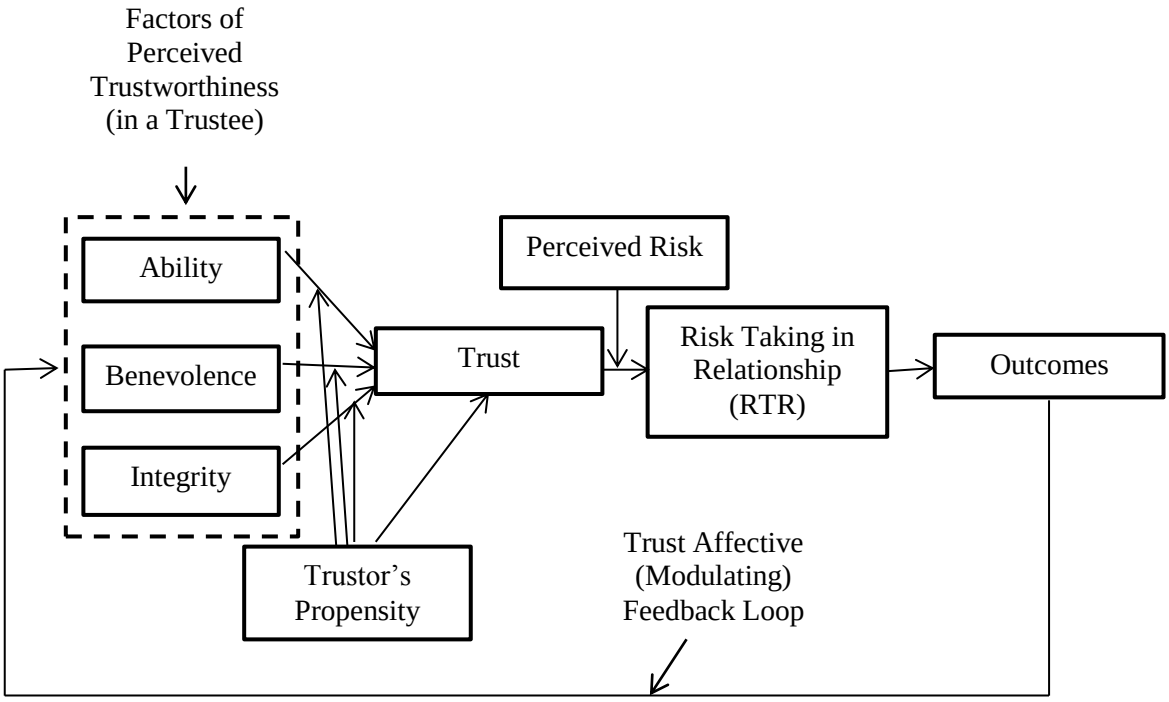


Figure 2.8. Mayer's Proposed Model of Trust [2]

One major factor which will determine the trust that one party has for another relates to the traits of the trustor; some parties are more likely to trust than are others. Many authors have considered trust from the perspective of a person's general willingness to trust others. One of the early trust theorists was Rotter [122], who defined interpersonal trust "as an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon." This definition seems to suggest that the author is

speaking of trust for a specific trustee, but his widely used trust scale focuses on a generalised trust of others; something like a personality trait that a person would presumably carry from one situation to another. For instance, typical items in his scale include: "In dealing with strangers one is better off to be cautious until they have provided evidence that they are trustworthy;" and "Parents usually can be relied upon to keep their promises." An aspect of this concept is demonstrated in the results of trust measurement using Rotter's Interpersonal Trust Scale [128]; a scale of 25-Question Graded Questionnaire whose responses measure the examinee as a trustor and then uses one's scores as a trustor to serve as a reflection of one's disposition as a trustee. That is if Mr 'A' trusts others 75% of the time as a trustor, then, there are chances that he would be 75% trustworthy as a trustee. A series of practical tests led to the following conclusion: "People who trust more are less likely to lie and are possibly less likely to cheat or steal. They are more likely to give others a second chance and to respect the rights of others" [128]. Rotter's Interpersonal Trust Scale is attached as Appendix 5

Other authors who have discussed trust in similar veins include Dasgupta, who sees generalised expectations of others as a major element in trust. For instance, "Can I trust people to come to my rescue if I am about to drown?" [129]. In the same vein, Farris et al. [130] defined trust as "a personality trait of people interacting with the peripheral environment of an organisation." That is, trust is viewed as a trait that leads to a generalised expectation about the trustworthiness of others.

In the trust model in Figure 2.8, this trait is referred to as the propensity to trust. Propensity could be thought of as the general willingness to trust others; people with different experiences, personality types, and cultural backgrounds vary in their propensity to trust [131]. Propensity will influence how much trust one has for a trustee prior to the availability of any data on that particular trustee – this is akin to what is referred to as blind trust (or bind love). Propensity is an associate of credulity, gullibility, naivety, unwariness or the tendency to do something (e.g., trust) without any cogent reason as it affects the characteristic of an individual or group.

The propensity to trust is similar to the concept of risk propensity in the model for the determinants of risk behaviour, as espoused by Sitkin and Pablo [132]. They define risk propensity as "the tendency of a decision maker either to take or avoid risks" [132]. However, this differs from the propensity to trust others as adopted by Mayer et al. [2] because risk propensity, as defined, is situation-specific and it is affected by both personality characteristics and situational factors, whereas propensity to trust is viewed as a trait that is applicable to different situations. Based on the foregoing, Mayer et al. [2] posited that:

“The higher the trustor's propensity to trust, the higher the trust for a trustee prior to the availability of information about the trustee.”

It is to be noted that, though an understanding of trust requires the consideration of the trustor’s trust propensity, a given trustor has varied levels of trust for various trustees. Thus, the trustor’s propensity alone is not sufficient. Hence, this variance is addressed in the next section by examining the characteristics of the trustee.

Characteristics of the Trustee and the Concept of Trustworthiness

An approach to understanding why a given party will trust another party more or less than others is to consider the attributes of the trustee. Ring and Van de Ven [133] argued that due to the possibility of risk in transactions, managers must concern themselves with the trustworthiness of the other party. A number of authors have considered why a party will be judged as trustworthy. Citing several authors, Mayer et al. [2] noted that credibility is affected by two factors; expertise and trustworthiness. Trustworthiness is a function of motivation (or lack of it) to lie. For example, if the trustee had something to gain by lying, he or she would be seen as less trustworthy. Generally, trust is based on expectations of how another person will behave, based on that person's current and previous implicit and explicit claims. In fiduciary relationships, trust is based on a belief in the professional's competence and integrity. A careful examination of the items in Johnson-George and Swap's [134] measure of trust reveals that they reflect inferences about the trustee. All available authors [2] have

suggested that the characteristics and actions of the trustee will make him/her more or less trustworthy. Hence, in order for researchers to understand why some parties are more trusted than others, a clear assessment of these trustee's characteristics are indispensable. A substantial number of the characteristics are highlighted in the treatment of trust under Section 2.3.2. Figure 2.8 summarises these factors of trustworthiness to three; namely, ability, benevolence, and integrity. These three characteristics of the trustee that must interplay with the trustor's propensity to trust in order to determine trustworthiness are briefly highlighted next. These variables are not trust per se, but they help to build the foundation for the development of trust.

The Factors of Trustworthiness

Some authors identify a single trustee characteristic that is responsible for trust, whereas other authors demarcate as many as ten characteristics [2, 135]. In spite of this discrepancy among the researchers, three characteristics of a trustee appear to be constant in the literature; namely, ability, benevolence, and integrity. These three appear to account for a major portion of trustworthiness. Each[3] of these contributes a unique perceptive perspective from which to assess the trustee, while the set provides a solid foundation for the empirical study of trust for another party [2].

Ability - Ability relates to that group of skills, competencies, and characteristics that enable a party to have influence within some specific domain. This area of the ability is specific because the trustee may be highly competent in some technical area, affording that person trust on tasks related to that area, having little or lacking aptitude, training, or experience in another area - for instance, in interpersonal communication. Although such an individual may be trusted to do analytic tasks related to his or her technical area, the individual may not be trusted to initiate contact with an important customer. Hence, trust is relative to the domain of competence [136, 137]. Other terms used in the literature which

[3]It is interesting to note that Aristotle's Rhetoric suggests that a speaker's ethos (Greek root for ethics) is based on the listener's perception of three things: intelligence; character (reliability, honesty); and goodwill (favourable intentions toward the listener). These bases provide an interesting parallel with the factors of ability, integrity, and benevolence, respectively.

also connote ability in a similar context include competence, perceived expertise, expertness, functional/specific competence, interpersonal competence, business sense and judgment. Whereas these terms connote a set of skills applicable to a single, fixed domain (e.g., interpersonal competence), ability highlights the task- and situation-specific nature of the construct in the model proposed by Mayer et al. [2].

Benevolence – Apart from the self-centred profit motive, benevolence is the extent to which a trustee is believed to be interested in doing good to the trustor. Benevolence suggests that the trustee has some specific attachment to the trustor; e.g., the attachment in the relationship between a mentor (trustee) and a mentee (trustor). The mentor wants to help the mentee, even though the mentor is not required to be helpful, and there is no extrinsic reward for the mentor. Benevolence is the perception of a positive orientation of the trustee toward the trustor [2]. Other researchers also used expressions that connote benevolence as a basis for trust. These include: trustee's motivation to lie (inversely proportional to high benevolence); intentions/motives; altruism; loyalty [135]; the extent to which the leader's behaviour is relevant to the individual's needs and desires of the led; and the likelihood that the trustee would give priority to organisational goals ahead of individual goals.

Integrity – Basically, the relationship between integrity and trust involves the perception that the trustee adheres to a set of principles that are appealing or acceptable to the trustor. McFall [138] and Biba [139] illustrated why not only the adherence to but also acceptability of the principles are important. She posited that mere following of a set of principles defines personal integrity. However, if that set of principles is not deemed acceptable by the trustor, the trustee's integrity would not be considered relevant for the purpose of trustworthiness; she called this moral integrity. The issue of acceptability precludes the argument that a party who is committed solely to the principle of profit seeking at all costs would be judged high in integrity, except in the unlikely event where this principle is acceptable to the trustor. Other connotations of integrity include the consistency of the party's past actions; credible communications about the trustee from other unrelated parties; the belief that the trustee has a strong sense of justice; and the extent to which the trustee's

actions are in tune with his or her words. Even though a case could be made that there are differentiable reasons why the integrity of a trustee could be perceived as higher or lower (e.g., lack of consistency is different from acceptability of principles), in the evaluation of trustworthiness it is the perceived level of integrity that is important rather than the reasons why the perception is formed [138]

From the foregoing, it is clear that the three factors of ability, benevolence, and integrity are common to most of the previous works on trust. These three factors appear to explain concisely the reasons for the variation in the level of trust that a trustor may have for trustees. Hence, Mayer et al. concluded, in line with the trust model in Figure 2.8, that:

“Trust for a trustee will be a function of the trustee's perceived ability, benevolence, and integrity and of the trustor's propensity to trust” [2].

Interrelationship of the Three Factors

Ability, benevolence, and integrity are important to trust, and each may vary independent of the others. This does not imply that the three are unrelated to one another; it only means that they are separable [2]. Consider the case of an individual and a would-be mentor. Ideally, the individual would want the mentor to be able to have the maximum positive impact on the mentee’s career and to assist/guide the mentee as much as possible. The extent to which the mentee would trust the mentor is a function of the mentee’s perception that the mentor has the ability to be helpful. This perception, alone, would not assure that the mentor would be helpful; it would only mean that the possibility exists.

As regards the mentor’s integrity, it is a function of previous positively viewed actions of the mentor in his or her relationships with others, compatibility of the mentor's statements with actions, and credible communications from others about honourable actions by the mentor. However, even if the individual is assessed to have high integrity, he or she may or may not have the knowledge and capabilities to be a helpful mentor. Hence, integrity alone will not make the individual a trusted mentor.

Consider the case of the person whose integrity is well known and whose abilities are stellar. Only these two would not guarantee that this potential mentor is trustworthy. This individual may have no particular attachment to the projected mentee. Relative to the organisational setting, the projected mentee might not trust the potential mentor enough to divulge sensitive information about mistakes or shortcomings to him. If the manager were also benevolent toward the projected mentee, he or she may try to protect him/her from the possible consequences of mistakes. A manager who is less benevolent to the focal employee may be more disposed to using the information in a way that helps the company most, even at the possible expense of the employee. However, benevolence by itself is not sufficient to engender trust. Thus, a well-intentioned person who lacks ability may not even know who in the organisation should be made aware of pertinent information. Rather than being helpful, such a person could actually do harm to the employee's career. Thus, a perceived lack of any of the three factors could undermine trust.

Ordinarily, if ability, benevolence, and integrity were all perceived to be high, the trustee would be deemed quite trustworthy. However, trustworthiness should be thought of as a continuum, rather than the trustee being either trustworthy or not trustworthy. Each of the three factors can vary along a continuum [2]. Although the simplest case of high trust presumes a high level of all three factors, there may be situations in which a meaningful amount of trust can develop with lesser degrees of the three. While it is obvious that, when all the three factors are high, it signifies a high level of trustworthiness, it would also be of interest to find out the amount by which these factors or some of them must drop before a trustee could be adjudged as untrustworthy. Similarly, the knowledge of the situations in which each of the three factors is most sensitive or critical would be of great importance and worth investigating. This leads to the pertinent interactive role of propensity in trust assessment.

Prior to the development of any relationship between two parties – when little or nothing is known about the three attributes of ability, benevolence, and integrity - the trust model in Figure 2.8 can explain trust using propensity. As a relationship begins to develop, the trustor may be able to obtain data on the trustee's integrity through third-party sources and observation, with little direct

interaction. At this stage, since there is little information about the trustee's benevolence toward the trustor, it is suggested that integrity will be important to the formation of trust early in the relationship. As the relationship develops further, interactions with the trustee allow the trustor to gain insights about the trustee's benevolence, and the relative impact of benevolence on trust starts to grow. Thus, the development of the relationship is likely to alter the relative importance of the factors of trustworthiness. Hence, Mayer et al. concluded thus:

“The effect of integrity on trust will be most salient early in the relationship prior to the development of meaningful data on benevolence, and the effect of perceived benevolence on trust will increase over time as the relationship between the parties develops” [2].

Each of these three factors captures some unique elements of trustworthiness. It was earlier posited, parsimoniously, that as a set, ability, benevolence, and integrity appear to explain a major portion of trustworthiness. Each element contributes a unique perceptive perspective from which the trustor considers the trustee. If a trustee is perceived as high on all three factors, it is argued here that the trustee will be perceived as quite trustworthy. Next is a brief explanation of risk and its relationship with trust.

Risk Taking in Relationship

It was previously emphasised that risk is an essential component of a model of trust. It is important for its role in trust-related matters to be clearly spelt out and understood by all; researchers, students and both advertent and inadvertent practitioners. There is no risk taken, per se, in the willingness to be vulnerable (i.e., to trust), but risk is inherent in the behavioural manifestation of the willingness to be vulnerable. In other words, one does not need to risk anything in order to trust; however, one must take a risk in order to engage in trusting action. The fundamental difference between trust and trusting behaviours (actions) is the same as the difference between a "willingness" to assume risk and actually "assuming" risk [2, 102]. Trust is the willingness to assume risk; behavioural trust is the assuming of risk. This critical differentiation highlights

the importance of clearly distinguishing between trust and its outcomes. It is reiterated that trust will lead to risk taking in a relationship, and the form of the risk taking depends on the situation. Even though the form of the risk taking depends on the situation, the quantum of risk that a party will take is a function of the amount of trust for the other party; a case of direct proportionality.

From the foregoing, it should be understood that the outcome of trust in the model proposed by Mayer et al. [2] is Risk Taking in Relationship (RTR). RTR as an inherent outcome of trust is different from general risk-taking actions because it can occur only in the context of a specific and clearly identifiable relationship between two parties. In addition, RTR suggests that trust will increase the likelihood that a trustor will not only form some affective link with a trustee but also that the trustor will allow personal vulnerability. The separation of trust from RTR is as illustrated in Figure 2.8 by the inclusion of a box representing each construct.

It should also be noted that trust is not involved in all risk-taking actions. A good illustration is the case of a farmer who invests time and resources into planting crops; the farmer is taking a risk with the assumption that sufficient rain will fall during the critical times of the growing season so that there will be a profitable yield. Although this action involves risk, it does not involve a trust as defined in this theory (Mayer's trust model), because there is no relationship with an identifiable "other party" to which the farmer would make himself or herself vulnerable. Nevertheless, proponents of a sociological approach might argue that this is an example of trust because there is a system that produces meteorological forecasts; Sitkin and Pablo are of the view that perceptions of meteorologists' accuracy would affect risk perception [132]. It should be remembered that the meteorologists do not control the weather; they merely provide data about the likelihood of various weather scenarios. Thus, the farmer does not trust the weather but takes a risk on what the weather will do [127]. The assessment of risk in a situation involves consideration of the context, such as weighing the likelihood of both positive and negative outcomes that might occur. If a decision involves the possibility of both negative and positive outcomes, the aggregate level of risk would be different, compared to a situation in which only the possibility of the negative outcome exists.

In summary, trust is a willingness to be vulnerable to another party, but there is no risk involved with holding such an attitude. Trust increases the likelihood of RTR, which is the behavioural manifestation of trust. Whether or not a specific risk will be taken by the trustor is determined by both the amount of trust for the trustee and by the perception of risk inherent in the behaviour. Mayer et al. then concluded that “RTR is a function of trust and the perceived risk of the trusting behaviour.” After illustrating the significance of risk in the trust model of Figure 2.8, the effect of context and the evolution of trust will be briefly highlighted in the next paragraphs.

The Role of Context

From the above, discussion on risk-taking behaviour makes a clear argument for the significance of the context in which the risk is to be taken. Even though the level of trust (as determined by ability, benevolence, integrity and propensity to trust) may be constant, the specific consequences of trust will be determined by contextual factors; the stakes involved, the balance of power in the relationship, the perception of the level of risk, and the alternatives available to the trustor. In the same vein, the assessments of the antecedents of trust (ability, benevolence, and integrity) are affected by the context. In a nutshell, the trustor’s perception and interpretation of the context of the relationship will affect both the need for trust and the evaluation of trustworthiness. Changes in the political climate and the perceived volition of the trustee in the situation can cause a re-evaluation of trustworthiness. Where there is a strong organisational control system, this could impede the development of trust, because a trustee's actions may be interpreted as responses to that control rather than signs of trustworthiness. Therefore, a clear understanding of trust for a trustee necessitates understanding how the context affects perceptions of trustworthiness.

Long-Term Effects

So far, in the trust model proposed by Mayer et al., as illustrated in Figure 2.8, trust is only described at a given point in time. There is a need to consider the

evolution of trust within a relationship in order to understand it completely [2, 140, 141]. This is necessary because the level of trust will gradually evolve as the parties interact. Available literature indicates that there are several factors that affect the process by which trust evolves. Most of these factors revolve around the fact that low trust will lead to a greater amount of surveillance or monitoring of work progress by the supervisor (trustor); since the employee (trustee) would interpret this as evidence of distrust by the supervisor, this would lead to a chain of actions and reactions whose outcomes influence how trust would evolve between the two parties. Some researchers have suggested that since reputation evolves from patterns of previous behaviour, the emergence of trust can be demonstrated in game theory [121, 142, 143].

The trust model proposed by Mayer et al. [2] incorporates the dynamic nature of trust. This is symbolised in Figure 2.8 by the feedback loop from the "Outcomes" of RTR to the perceived characteristics of the trustee. This dynamism is demonstrated by the fact that when a trustor takes a risk in a trustee that leads to a positive outcome, the trustor's perceptions of the trustee are enhanced. Similarly, perceptions of the trustee will decline when trust leads to an unfavourable outcome. Boyle and Bonacich have suggested that the outcomes of engaging in a trusting behaviour will affect trust ‘directly’ [140]. Contrary to this conclusion, Mayer et al. asserted in their conclusion that, as illustrated in Figure 2.8, the outcomes of the trusting behaviour (RTR), whether favourable or not, will influence trust ‘indirectly’ [2] at the next interaction, depending on the situation. This influence is, principally, an update of the trustor’s prior perceptions of the ability, benevolence, and integrity of the trustee.

Comparison of Trust Scales

Adeka’s statistical and graphical approaches at estimating the measure of trust in Section 2.3.3 apply only to the case of secret sharing. This merely proves that the amount of trust in the secret sharing process is directly proportional to its number of participants (trustees). Outside this domain, it is not a trust scale per se, in the strict sense of the nomenclature.

The trust model, as proposed by Mayer et al., is the first that explicitly considers both characteristics of the trustee as well as the trustor. It clearly distinguishes trust from the factors that contribute to it, and as well differentiates trust from its outcome of risk taking in the relationship. The model defines trust in such a way that distinguishes it from other similar concepts (cooperation, confidence, predictability), which have often been confused with trust in the literature. Additionally, the critical role of risk is clearly specified in this model. The model presents a versatile and dynamic definition of trust with a set of its determinants on the part of the trustee (ability, benevolence, and integrity) and the trustor (propensity to trust). It is noteworthy that the model also highlights the significance of context and long-term effects in the evolution of trust. The differentiations between factors that cause trust, trust itself, and outcomes (RTR) of trust are critical to the validation of the model; all the three component elements must be measured in order to fully test the model. The most problematic component of the model from the standpoint of measurement is trust itself; because trust is a willingness to be vulnerable, a measure that assesses that willingness is needed.

Rotter's Interpersonal Trust Scale was also highlighted, as reflected in Appendix 5; it is used to measure generalised trust of others. It estimates, quantitatively, the trusting attributes of a trustor and uses the result as a gauge for the trustor's trustworthiness. That is, using the argument that one who trusts others is likely to be trustworthy. The product of Rotter's and similar scales could serve as a veritable aid for the proposed Mayer's scale. This, to a large extent, defines the parsimony of Mayer's scale; it would rely on other means to measure most of its quantities – including trust itself.

After dealing with trust and its related concepts above, the concept of security itself will be briefly highlighted next to serve as a basis for the treatment of analysis/synthesis and the military/civil security assessment processes that follow in order to focus on the need for a risk-centred 3-factor security assessment technique.

2.4 Security Concepts and the Military Security Assessment Process

2.4.1 Security Concepts

A look up on security in dictionaries yields a general view that security is “freedom from danger, risk or loss” [144, 145]. In the context of this research work, the concern is about dangers, risks and losses associated with computers, its information/data and network transactions. Fundamentally, the need for cryptography arose in response to the requirements to secure information, whether in storage or transit. The most primary security needs it sets out to address are confidentiality, integrity, availability and authenticity [1].

While authentication is used for the symmetric (private-key) cryptography, its equivalent in asymmetric (public-key) cryptography is the digital signature. An authentication is implemented by means of a Message Authentication Code (MAC) generated by the sender, with an authentication key which is shared by the sender and the receiver. On the other hand, certification of each participant’s public key is effected via the digital signature of a Certification Authority (CA) in a Public Key Infrastructure (PKI) scheme [23].

The above concepts are vital security requirements for social interaction using computers, just as they are in face-to-face interactions: that someone is who he claims to be; that someone’s credentials, whatever type, are valid; and that a document purporting to have come from a person actually came from that person. These are the functions of authentication, integrity, and non-repudiation, respectively [146].

In assessing security problems in a system, it is important to appreciate several characteristics of the system’s security posture. These must include the threats, vulnerabilities and risks [1]. Threats are the events, issues or entities that can potentially do harm to the security of the system; these may be intentional or otherwise, including natural disasters. Vulnerabilities are the channels or means that make it possible for or engender a potential ability for harm to afflict the system; they are opportunities for harm to occur. For instance, lack of balanced diets makes a person vulnerable to diseases or leaving the gate unlocked

amounts to a vulnerability in the physical security of the house. Lastly, risks are said to exist where both threats and vulnerabilities co-exist. In other words, a threat to a system that can actually use an already existing vulnerability to compromise the security of the system creates a risk. For example, in an army that is facing a completely illiterate enemy, writing down the orders at all, in plain text, constitutes vulnerability, but there is no risk associated because there is no corresponding threat, since the enemy lacks the ability to read the message. Usually, in a systematic risk analysis to determine the potential problems in the security of a system, it is useful to create a matrix of the various threats and vulnerabilities associated with the system (Risk Assessment Matrix) [1].

2.5 Analysis, Synthesis and the Three-Factor Security Assessment

The discovery of the 3-factor security assessment process, and its revolutionary derivatives, calls for a redefinition or new understanding of the relationship between the terms ‘Analysis’ and ‘Synthesis’, as well as the intricate relationship among the security assessment factors of risk, threat and vulnerability, especially in the military.

This section is a direct consequence of the pragmatic conclusion in the last paragraph of Section 2.4.1, i.e., the object of every security assessment is the determination of possible Risk(s) relative to the asset to be protected, and that this risk could be systematically calculated quantitatively, using the Risk Assessment Matrix approach; with Threat(s) and Vulnerabilit(ies)y as inputs – hence, a 3-facor security assessment approach. Other than this approach, the security assessment process could be anything but systematic; haphazard, uncoordinated and stressful. Though this approach is not entirely new in the civil security sector of the security industry, it is contrary to the norm in most armies throughout the world. With the exception of the US military (probably, with some allies), which discovered the anomaly in 1998 and took steps to rectify it by 2006, most military establishments around the world are unaware of the inconsistency. Some armies also discovered the anomaly around the turn of the century but, rather than rectifying the situation, they adopted the Manoeuvrist Approach; a winding and rather complex approach to military appreciation, estimate process or a security assessment process which does

not really simplify the process – rather, it makes the assessment process more subjective and less quantitative.

In the search for an answer, as regards the reason (s) behind the disparity in the practice between the civil and military elements of the security industry, the researcher discovered that possible misconceptions (with the exception of Indian Army) surrounding the terms Analysis (as employed in the treatment of the Intelligence Cycle; i.e., Intelligence Analysis) and Synthesis, were most probably responsible. Hence, as a by-product or derivative of this research effort, Adeka [34] gives a detailed treatment of the security assessment/management processes and the intricate relationship that exists between the two evaluation terms/techniques of analysis and synthesis, with some revolutionary results. This section gives a synopsis of the findings with pertinent and innovative propositions.

The factual reality is that analysis and synthesis, as scientific methods, always go hand in hand; they complement each other. Every synthesis is built upon the results of a preceding analysis, and every analysis requires a subsequent synthesis in order to verify and correct its results [86]. The analysis is planned and structured so that the problems could be framed up, while synthesis is emergent and facilitates the making of connections that identify breakthrough ideas and opportunities. While analysis is a means to an end, synthesis is the actual end or resides at the end. This intricately interwoven relationship is aptly illustrated in Figure 2.9 [147]. Thus, it would not be correct to adopt one method to the exclusion of the other, even as a reductionist. Reductionism alone is not sufficient as an effective evaluation approach because it is learned from Aristotelian quotes that “the Whole is greater than the Sum of its parts” [148]]. It might be useful to pen down some definitions at this stage.

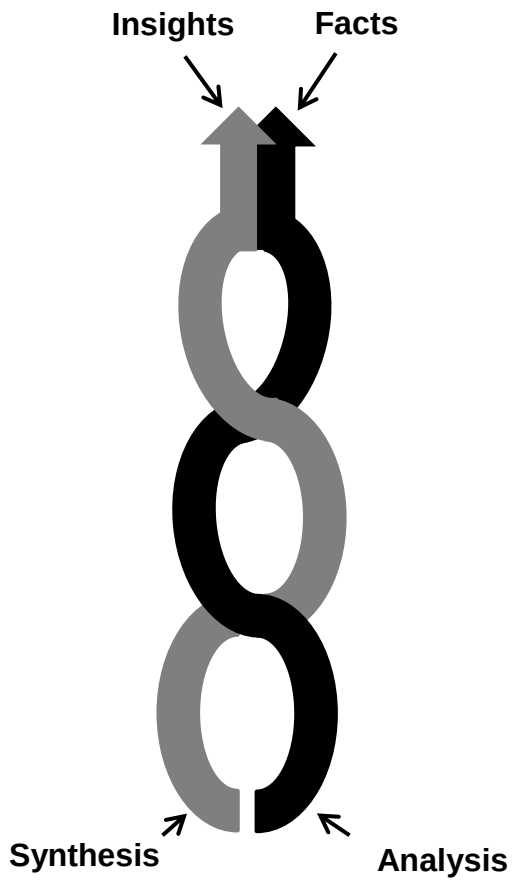


Figure 2.9. Analysis and synthesis [147]

2.5.1 Definitions

- **Analysis -** Resolution of anything complex into simple elements (opposite of synthesis); i.e., the separation of an intellectual or material whole into its constituent parts for individual study [149]. In other words, “the separation of something into its constituents in order to find out what it contains, to examine individual parts, or to study the structure of the whole” [150].

- **Syn- and Thesis -** The prefix **‘**syn-’ is of Greek origin, meaning ‘together’, ‘together with’ or ‘united’ [119]. Similarly, the word ‘thesis’ comes from tithenai, which is Greek for ‘to put or lay down’ [150].

- **Synthesis -** The combining of the constituent elements of separate material or abstract entities into a single or unified entity (opposite of analysis); i.e., a complex whole is formed by combining individual pieces [150]. In Greek, it is

called suntithenai, which means place together or put together [151]]. In other words, a new unified whole resulting from the combination of different ideas, influences, or objects [150], is formed to facilitate a study of the complete entity. Hence, the Aristotelian quotes: “The Whole is greater than the Sum of its parts” [148]**.**

- **Threat -** The potential for a threat-agent to exploit or accidentally trigger a specific vulnerability [152]; i.e., a potential that an event, process, activity, or substance can be perpetuated by one or more threat agents that have an adverse effect on an organisation, via a specific vulnerability [152]. Thus defined, it implies that a threat is not significant unless a specific vulnerability corresponding to it can be identified [1, 153].

- . The US military uses hazard, mostly, in place of threat or interchangeably, and danger for vulnerability [154]. The military’s Composite Risk Management (CRM) process “does not differentiate between the sources of the hazard,” [154], thus, vulnerabilities are usually treated as hazards or threats (leading to Equation (2.29)); vulnerability is not mentioned in its 5-step CRM process. However, this is not without some measure of apparent inconsistencies; sometimes threat and hazard are used to differentiate between threats emanating from the enemy and natural disasters respectively [154].

- **Intelligence Analysis -** Intelligence analysis establishes the significance and implications of processed information, integrates it by combining disparate pieces of information to identify collateral information and patterns, then interprets the significance of any newly developed knowledge [155]. In other words, intelligence analysis is the interpretation of the significance and implications of integrated processed bits of information.

- **Threat Analysis -** The examination of threat-agents against system vulnerabilities to determine the threats for a particular system in a particular operational environment. Threat analysis is synonymous to threat assessment [152].

❖ **Vulnerability -** A flaw or weakness in system security procedures, design, implementation, or internal controls which, if exploited or accidentally triggered, could result in a security breach or a violation of the system's security policy [1].

❖ **Risk -** Risk refers to the likelihood that vulnerability will be exploited or triggered; that a threat may become harmful [1]. Inherent in this definition are two possible deductions. The first is that risk is not a function of the action to be taken as viewed by many; rather, it is strictly dependent on the degree of match or mismatch between threats and vulnerabilities, to the advantage of the adversary or threat-agent. Secondly, the two most conspicuous components of risk are the threat and vulnerability; both must correspondingly co-exist for risk to exist [1]. In other words, as far as the identification of risk is concerned, a threat carries no significance unless it has a co-existing or potential vulnerability that corresponds to it, and vice versa. The tripartite relationship among the trio is such as to mathematically satisfy Equations (2.28) and (2.29) [34]; Equation (2.29) applies to the US military model only.

$$r = t \wedge v \tag{2.28}$$

$$r = \tau, (\tau = t \vee v) \tag{2.29}$$

Where r denotes Risk, t denotes Threat, v stands for Vulnerability, τ is as defined and the symbols '$\wedge$' and '$\vee$' represent the logic operators 'AND' and 'OR' respectively. Equation (2.28) is the substantive formula for determining the existence of risk in the risk assessment process, while Equation (2.29) specifically applies to the US military approach as a variant of Equation (2.28); this is a consequence of the apparent inconsistency in its concepts of threat as illustrated in the above definition. These two equations were originally derived by the author as a consequence of his understanding of the tripartite relationship among the three concepts; risk, threat, and vulnerability. They may be referred to as Adeka's Twin Risk Equations (ATREs); for the 3-factor security assessment process. The curve of Equation (2.28) is as plotted in Figure 2.10. It depicts the existence of Risk on the graph of Threat

against Vulnerability; i.e., risks exist only if, and only if, corresponding threats and vulnerabilities co-exist.

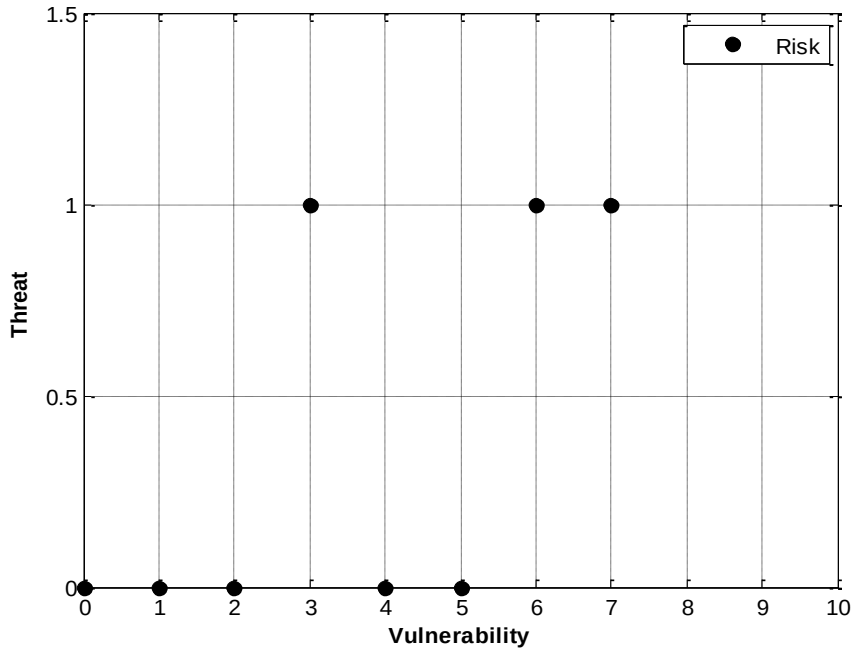


Figure 2.10. Risk exists iff corresponding threat and vulnerability co-exist.

2.5.2 Security Assessment Procedure in the Nigerian Defence and National Security Agencies

The security agencies strictly covered by this section are those established by the National Security Agencies Act of 1986; these are the Defence Intelligence Agency (DIA), State Security Service (SSS or DSS) and National Intelligence Agency (NIA). It is noted that, currently, the DIA has operatives outside its headquarters, in addition to the Services intelligence establishments; the Nigerian Army Intelligence Corps (NAIC), Directorate of Naval Intelligence (DNI) and the Directorate of Air Intelligence (DAI). Appropriate examples will be cited from the Nigerian Army (NA), where necessary, to reflect the case in the Armed Forces of Nigeria (AFN), and NAIC to reflect the practice in the Defence Intelligence. Where there is divergence, examples would also be cited from the other agencies within the national intelligence community. References could be made to cases outside Nigeria. The affected establishments are illustrated in Figure 2.11.

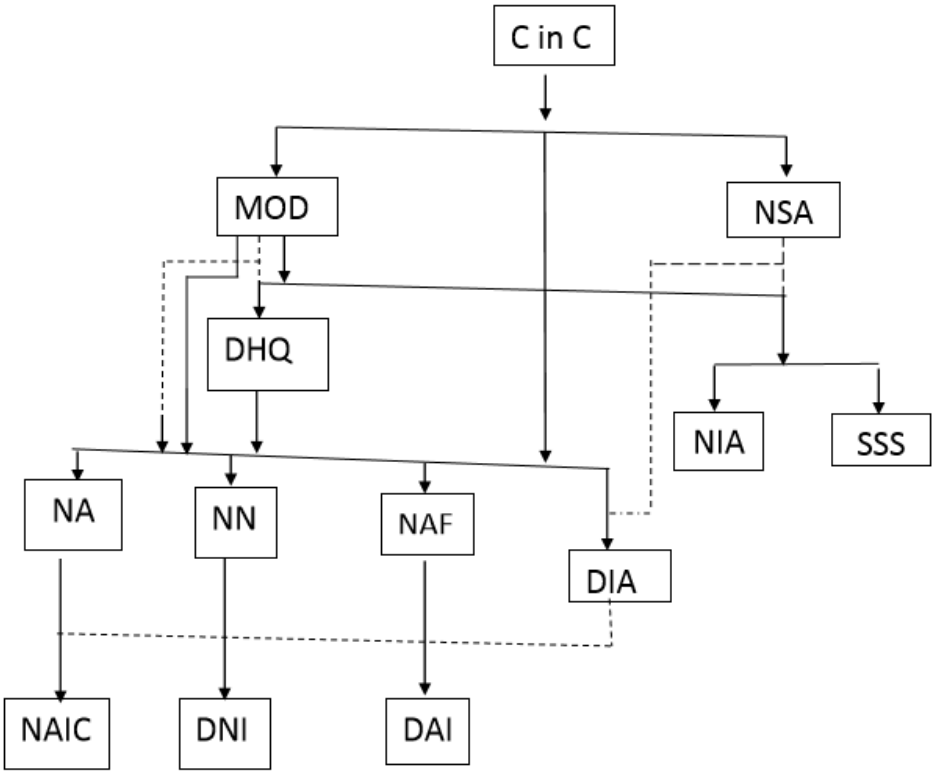


Figure 2.11. Nigerian Armed Forces and national security agencies: operational and administrative/supervisory chains of command.

LEGEND

————	...	Operational Chain of Command
– – – – – – –	...	Administrative/Supervisory Chain of Command
C in C	...	President & Commander in Chief
MOD	...	Ministry of Defence
DHQ	...	Defence Headquarters
NA	...	Nigerian Army
NN	...	Nigerian Navy
NAF	...	Nigerian Airforce
DIA	...	Defence Intelligence Agency
NAIC	...	Nigerian Army Intelligence Corps
DNI	...	Directorate of Naval Intelligence
DAI	...	Directorate of Air Intelligence
NSA	...	National Security Adviser
NIA	...	National Intelligence Agency
SSS	...	State Security Service (Department of State Service (DSS))

It is not intended to discuss the mechanical details of security operations or the evaluation process by the affected organisations. Rather, the general assessment concept, approach and the target of the assessment constitute the focus of this segment.

The concern of this section is a case of a security assessment practice whereby threat analysis is usually overemphasised to the detriment of vulnerability; in fact, the phrase vulnerability analysis is never heard of. The threat is usually given the boldest heading in security evaluations, with its details and characterisation, while vulnerability, if mentioned at all, is accorded a mere casual reference. The term risk suffers the same fate as a does vulnerability. This is not to say that the security assessments have been useless all through, no; rather, the issue is that even when experts engage in security evaluations which unconsciously involves threat analysis, vulnerability analysis, risk analysis and, even, risk management - all these have always been tagged with the label of threat analysis alone. The great possibility here is that it is either the terms are individually not critically understood or their technical inter-relationships have never been carefully weighed. In the case of the US military, where vulnerability could be synonymous to threat [154], it means that threat would be equal to risk, for Equation (2.28) to hold; they use only the two terms of threat and risk (since v could be synonymous to t); due to their rather awkward but unique concept, where t and v are lumped up together as one and the same quantity [154] and they would specify when the entity is called threat (prior to risk assessment), distinctive from when it is referred to as risk (after risk assessment). That is, when v is synonymous to t in Equation (2.28), $r = t$, and vice versa; $r = \tau$ in Equation (2.29), with τ as defined. In Nigerian case (Nigerian military and others not aligned with the US military), the notion is that at all times and in all situations, $t = t$ (with $r = 0$; $v = 0$); this is an impossible arithmetic, which is not in accord with reality. This is why the very bulky and complex security evaluations done quarterly or annually by the DMI for the Chief of Army Staff's (COAS) conferences are simply tagged 'DMI THREAT ANALYSIS.'

Heritage

The fore-runner of the NAIC (DMI) was the Field Security Section (FSS) of the Royal Nigerian Army, which was established on 1st November 1962 under the command of Captain PG Harrington (BR) of the British Army as General Staff Officer Grade 2 Intelligence (GSO2 Int) [156]. Major CK Nzeogwu was the first Nigerian officer to hold that appointment from November 1962 to 1964 [157]. Evidence abound to prove that the NAIC took an active part in the training of officers and personnel of the DNI, DAI, the Nigeria Police (NP) and, especially, the SSS. In general, it could be argued that the entire Nigerian military derived its heritage from the British Armed Forces; Nigeria being a former British colony.

Effect of Heritage and Association

Whatever is said about the DMI above, in respect of its security assessment process, is also representative of the other military security agencies (DNI, DAI). This is also true of the other security agencies (NIA, DSS); the only difference might be that, while in one instance 'Threat Analysis or Threat Assessment' would be the main title heading of the assessment report itself, in another instance the same phrase may be a centre or group heading towards the end of the report in the analysis or assessment segment. In virtually all cases, the entire assessment is on threats, without mentioning vulnerability or risk; not to talk of measuring or calculating risk.

The above contagious phenomenon is also true about the sister Services of the AFN {NA, Nigerian Navy (NN) and Nigerian Air Force (NAF)} represented by the NA. There were no provisions for risk, threat and vulnerability in the template for the military decision-making process (military appreciation) which the NA used up to March 2003. An individual expert might make casual references to some of these terms here and there in the appreciation process, but definitely without any papered calculations. In an apparent effort to improve the existing system, the British Army introduced what is termed the Manoeuvrist Approach in warfare to the NA in 2003. In the 6-step estimate process employed by this new approach, critical vulnerability (without threat and risk) is mentioned in Step 1, while risk (without threat and vulnerability) is mentioned in Steps 4 and 5. In all the instances, there is no provision for calculating risk.

A disturbing aspect of this evaluation process is that it is non-systematic, non-quantitative and its quality is entirely dependent on the initiative, ingenuity and dexterity of the security 'analyst'. Apart from some orderly arrangement of headings, it is essentially a haphazard process, as far as the contents and thought process are concerned. Most probably, what could be perceived as the most important shortcoming of the process is its target, which is a threat, instead of risk. It is clear from Equation (2.28) that threat is only one of two equally important components that make up a risk, and the significance of threat cannot be determined without an analysis on a correspondent vulnerability. Thus, if the focus of the evaluation process is on the threat, instead of risk, then it is not only misdirected but also significantly narrowed down to not more than about 50% of what ought to have been considered as inputs. In other words, if what the reports claim to have been done on paper is actually what is done on the ground, then, an appreciable work would have been left undone.

Possible Geographical Spread of the Nigerian Practice

In the US military, the concept of risk calculation was not used until April 1998, when the first Army doctrinal publication on risk management was made in the Field Manual (FM) 100-14 [154]. The doctrine was not fully integrated into the Military Decision Making process (MDMP) and the army training management system until 2006, when FM 100-14 was revised, expanded and re-designated 'FM 5-19, Composite Risk Management (CRM);' a fall-out of the global war on terrorism [154]. The CRM, perceived as a significant cultural change for the US Army, is "not a stand-alone process, a "paperwork" drill, or an add-on feature. … This milestone manual outlined a framework that leaders could use to make force protection a routine part of planning, preparing, and executing operational, training, and garrison missions [154]."

The fact that the US Army knew nothing about risk management as part of MDMP, until 1998, is a comfortable indication that the culture of neglect in the incorporation of risk evaluation and management into the military security assessment, appreciation or estimate process, is global. This position, which is also re-enforced by the fact that the Nigerian military might not have been alone, having derived its heritage from the British Armed Forces (BAF), is,

unfortunately, contrary to the military strategic reasoning that is as old as Sun Tzu (about 500 BCE) [26]. Possible reasons behind this anomaly and its major implications are highlighted below.

Possible Reasons and Implications

It is recalled that most military security operatives/analysts started their career as intelligence operatives/analyst, and the first thing any intelligence operative learns on his mission to become a spy is the intelligence process, as illustrated in the Intelligence Cycle [155]. The most crucial stage in the intelligence process is the "intelligence analysis," as defined above. Unfortunately, the military tradition of learning on the job, with few or no questions and as little room for prior theoretical knowledge as the situation permits, encouraged most amateur intelligence "analysts" to progress into "analytical experts" without adequately appreciating the meaning of the term analysis. Thus, while in actuality, they engage in more of synthesis than analysis, everything is lumped up together under intelligence analysis, to the detriment of synthesis. With time, the word analysis became bastardised in its usage, without regard to the fact that synthesis is the direct opposite of analysis; this anomaly is not exclusively limited to the military and intelligence organisations.

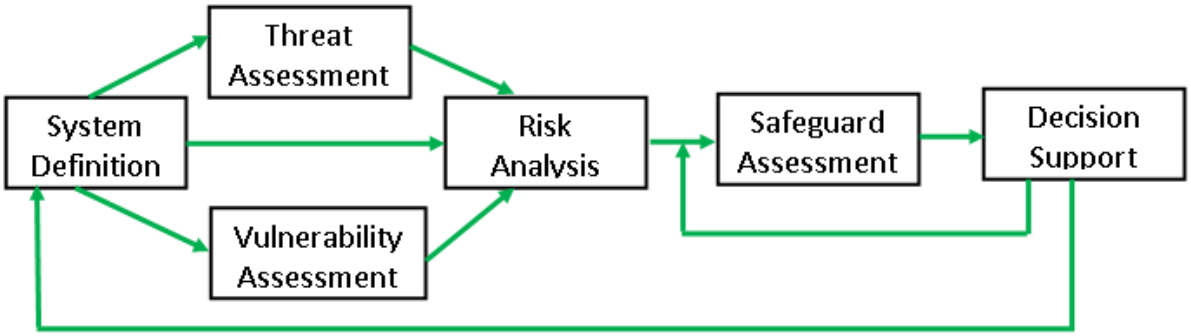
As at today, it would seem as if analysis is the only evaluation and examination tool in existence. Thus, virtually, evaluators have all become unconscious reductionists. It is common to hear of data analysis, political analysis, security analysis, scientific analysis, economic analysis, and demographic analysis, etcetera; while, in fact, all these evaluation processes involve both analysis and synthesis. Of all the literature search for this work [34], examining about 200 Intelligence Cycle models [155, 158-160], the word synthesis never appeared in any of them, except for the Indian Army [161], while analysis appeared in all of them; either as a heading or at least in the explanations. In the researcher's entire life (at 53), he has never come across the noun synthesist (the same is true of his computer, which rejects it as an English word: thanks to Encarta and Oxford dictionaries; otherwise, he would have been lost). On the other hand, hardly does a day pass by without one seeing or hearing the noun analyst. This original misconception in the assessment skill of the intelligence officer, which resulted in referring to the function of synthesis as analysis, and having no idea

about synthesis at all, was progressively transferred and inherited from generation to generation. Some of the intelligence officers might have never been conscious of the technical meaning of the term analysis, standing alone, without any linkage as in the phrase intelligence analysis. In other words, they might know what the phrase intelligence analysis means, as part of a professional heritage, but they might not even understand what the operating term analysis, itself, stands for.

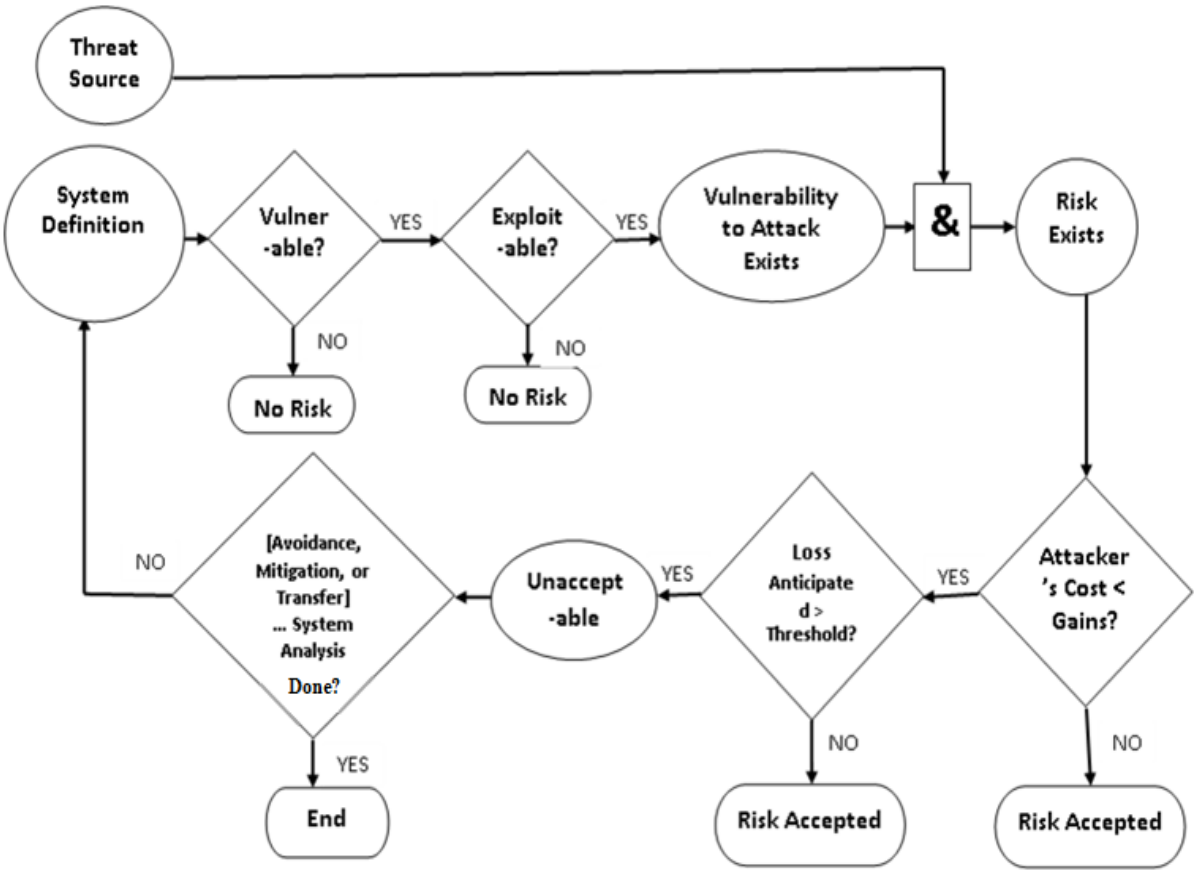
In the process, this evolved a culture of non-systematism and haphazardness in the perception and attitude of most of the intelligence officers in relation to assessment processes. Since there is a very thin or no dividing line between the intelligence operative/analyst and security operative/analyst, this culture was transmitted in situ; from intelligence analysis to security analysis/assessment. Thus, the terms vulnerability and risk in security assessment have suffered the fate that is almost identical to that of synthesis in intelligence assessment, while threat in security assessment enjoys the undeserved dominance of analysis in intelligence assessment. This appears to be the crux of the matter with all public defence, intelligence and security heritages around the world, except for some of those aligned with the US and who are amenable to quick adaptation [34]. It is the same reason that is most probably responsible for the divergence in the security assessment practices between the two segments of the security industry.

2.5.3 Security Assessment Practice in the Private Security Industry

The security assessment procedure in the private security sector of the security industry is governed by the relationship established in Equation (2.28), as illustrated in Figures 2.10 and 2.12 (a, b) [152, 162]. It is highly systematised, with a very clear sequence of actions, and a check-back procedure which enhances review. It focuses on risk as the output, with threat and vulnerability as inputs. The risk assessment and management processes are similar for all organisations, though implementation may depend on the nature of the risks in question [163]. Consider the following:



(a)



(b)

Figure 2.12: (a) Risk management overview (b) A flow chart for risk mitigation action points [152, 162]

Approaches

The US approach employs the Military Standard (MIL-STD-1629) procedure for performing Failure Modes Effects and Criticality Analysis (FMECA) [164]. This is an evaluation technique which charts the probability of failure modes within a

system against the severity of their consequences in a Risk Assessment Matrix [165]. The key objective of FMECA is to systematically evaluate and document the potential impact of each functional or hardware failure on mission success, personnel and system safety, system performance, maintainability and maintenance requirements. The UK approach, on the other hand, uses the Risk Priority Number (RPN) methodology [163]. This is a method for evaluating the risk associated with potential problems identified during a Failure Mode and Effects Analysis (FMEA). An FMEA can be performed to identify the potential failure modes for a product or process. The RPN method then requires the assessment team to use past experience and engineering judgment to rate each potential problem according to the following rating scales[165]:

- Severity - which rates the severity of the potential effect of the failure.
- Occurrence - which rates the likelihood that the failure will occur.
- Detection - which rates the likelihood that the problem will be detected before it reaches the end-user/customer.

2.5.4 The Risk Assessment Matrix

In a systematic risk analysis to determine the potential problems in the security of a system, it is useful to create a matrix of the various threats and vulnerabilities associated with the system (Risk Assessment Matrix).

Before Using the MIL-STD-1629 procedure, two attributes are required to carry out a risk assessment using the risk assessment matrix. Kara-Zaitri [164] enumerated these as follow:

- The Severity, Effect or Impact of the event; if it occurs.
- The Likelihood of each event in terms of a probabilistic value or class.

In this approach, the probabilities that risks would result from certain events are assigned for each event (i.e., the likelihood that a given threat would exploit a particular vulnerability) and the effect of the impact of the occurrence is also defined. For instance, for a 3 x 3 Risk Assessment Matrix in Table 2.5, let the probability levels, with corresponding values, be High (1.0), Medium (0.5) and Low (0.1); and the corresponding threat impact levels be High (100), Medium (50) and Low (10). Depending on the organisation's requirements and

the granularity of risk assessment desired, a 4 x 4 or 5 x 5 matrix may be used [152]. In which case, Very Low/Very High threat probability and a Very Low/Very High threat impact to generate a Very Low/Very High risk level can be incorporated into the matrix. The resultant matrix for this example is in Table 2.5 [152, 154].

Table 2.5. Risk assessment matrix [149]

PROBABILITY	SEVERITY (IMPACT)		
	Low (10)	Medium (50)	High (100)
High (1.0)	(10 x 1.0) = 10	(50 x 1.0) = 50	(100 x 1.0) = 100
Medium (0.5)	(10 x 0.5) = 5	(50 x 0.5) = 25	(100 x 0.5) = 50
Low (0.1)	(10 x 0.1) = 1	(50 x 0.1) = 5	(100 x 0.1) = 10

Risk Scale: High (50+ to 100); Medium (10+ to 50); Low (1 to 10)

Having assessed the risk, one of the following risk management decisions or mitigation options will have to be considered. Risk mitigation, the second process of risk management, involves prioritising, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process [152]. Kara-Zaitri [166] stated that these mitigation options include:

- Avoid - Redesign the process to avoid particular risks with the plan of reducing overall risk.
- Diversify - Spread the risk among numerous assets or processes to reduce the overall risk of loss or impairment.
- Control - Design activities to prevent, detect or contain adverse events or to promote positive outcomes.
- Share - Distribute a portion of the risk through a contract with another party, such as insurance.

- Transfer - Distribute all of the risks through a contract with another party, such as outsourcing.
- Accept - Allow minor risks to exist to avoid spending more on managing the risks than the potential harm.

The goals and mission of an organisation should be considered in selecting any of these risk mitigation options. Since it may not be practicable to address all identified risks, priority should be given to the threat and vulnerability pairs that have the potential to cause a more severe impact on the organisation. In addition, due to peculiarities of different organisations, the option used to mitigate the risk and the methods used to implement controls may vary [163]. Usually, the best approach is to have a mix of appropriate technologies from among the various vendor security products, along with the appropriate risk mitigation option and nontechnical, administrative measures [152].

2.5.5 Findings and Innovative Propositions

A culture of non-systematism, haphazardness and lack of accountability in the perception and attitude of most intelligence officers, in relation to assessment processes, has persisted for long [34]. This most probably resulted from the original misconception surrounding the opposite functions of analysis and synthesis, which was facilitated by the tradition of ‘learning on the job’ with few or no questions (the copycat syndrome inherent in military regimentation); thus virtually obliterating the term synthesis/synthesist from the professional dictionary, and over-emphasising analysis/analyst out of proportion in the process. Since there is a very thin or no dividing line between the intelligence operative/analyst and security operative/analyst, this culture was transmitted, in situ, from intelligence analysis to security analysis/assessment. Thus, the terms vulnerability and risk in security assessment have suffered the fate that is almost identical to that of synthesis in intelligence assessment, while threat in security assessment enjoys the undeserved dominance of analysis in intelligence assessment. This appears to be the crux of the matter with all public defence, intelligence and security heritages around the world, with probable exceptions of Indian Army and the armies of those aligned with the US; those amenable to quick adaptation.

In an effort to resolve this anomaly, the following suggestions would be advanced, based on an analysis of the implications enumerated by Adeka [34], as follows:

- In the intelligence process, the function usually referred to as intelligence analysis is actually a synthesis function; it should be renamed intelligence synthesis, which would be carried out by synthesists, and accorded a definition similar to that of the Indian Army. (The Indian Army's Combat Intelligence Précis defines the concept of synthesis in its model of Intelligence Cycle as, 'the process of putting together all intelligence (that is, evaluated and interpreted information, including the intelligence staff's assessment) pertaining to a combat area; to analyse the strengths/weaknesses of the enemy and predict the manner in which he is likely to conduct his operations').

- Intelligence products should be amenable to re-evaluation and accountability. This is in line with the current thought, as from the 1970s, necessitated by scandalous revelations mostly characterised by high-handedness on the part of intelligence agencies or treacherous manipulations by political leaders, globally [167].

- In military and security operations, the object of security assessment should be the risk, which is quantitatively measured via the Risk Assessment Matrix approach, using threat and vulnerability as inputs; threat and vulnerability should be uniquely defined and differentiated, contrary to the practice in the US military. Thus, where there is presently Threat Analysis or Threat Assessment as a heading in an estimating process or security report, it should be replaced with Risk Analysis or Risk Assessment; and where there is none, one should be created as necessary. In other words, the highest security assessment heading in an estimating process or security report (whether it is a main, group, paragraph, sub or sub-sub-paragraph heading) should discuss the risk, with threat and vulnerability as sub headings or considerations under it.

- ❖ A risk assessment security report should reflect the process that produced it; both should agree. Depending on the extent of complexity or level at which the assessment is made, there may be a need to attach a risk assessment worksheet as an annexure or appendix to the reports.

Thesis, Synthesis and Innovative Propositions

As a ripple effect of this investigation, it has become necessary to devise some new terminologies and adjust the context of others to cater for some of the problems identified. It is recalled that analysis and synthesis ought to go hand in hand for optimum results, and that one technique may predominate in certain instances. Thus, instead of lumping up everything together, calling it Data Analysis, and then be accused of suffering from the hangover of the intelligence officers' culture of complacency, it should be possible to communicate the exact technique being employed: such as data analysis; data synthesis; data analysis and synthesis; and in what relative proportions, if necessary.

It would not be satisfactory if this effort is concluded without taking a second look at the word thesis in the context that it is a synonym of dissertation. As defined, etymologically, the prefix 'syn-' is of Greek origin, meaning 'together', 'together with' or 'united.' Similarly, the word 'thesis' comes from 'tithenai', which is Greek for 'to put or lay down.' A careful examination of the research process reveals that it would pass through some or all of the following stages and more [147]:

- ❖ Data Collection/Organisation - Make data manageable.
- ❖ Data Mining - Identify what you see.
- ❖ Data Sorting and Clustering - Manipulate or reframe and integrate data as necessary.
- ❖ Identification of Insights - Discuss, articulate, incubate and socialise the insights.

All of the above stages in the research process, and other minor processes would precede the final process; which is the harmonisation of all the bits into a single report which is popularly referred to as thesis or dissertation. However, even before the research proposal is completed, the process of putting down (thesis) notes of different lengths and forms would have already commenced. So, whether on a board/wall as in Figure 2.13 or in notebooks, digital data repositories of all kinds - including the computer, as well as in the researcher's brain, there would have been theses all over the place already. Hence, it would be more meaningful to distinguish the final dissertation from all the other pieces of theses. Thus, the synonym of dissertation ought to be termed a Synthesis, rather than a Thesis.

Figure 2.13**.** Open card sort arrayed on a wall; showing some Theses [147]

2.5.6 Neologies

The neologies, which emerged as a consequence of the risk assessment discoveries outside the main research focus, are as proposed and defined below:

- **Analosynthesis** - A data evaluation method which employs both analysis and synthesis, but it is analysis-heavy or the analysis approach predominates.
- **Synthonalysis** - A data evaluation method which employs both synthesis and analysis, but it is synthesis-heavy or the synthesis approach predominates.
- **Equisynalysis** - A data evaluation method which employs both analysis and synthesis, where both techniques are almost equally employed; about fifty-fifty.
- **Synthesis**[4] - This term should replace analysis in the Intelligence Cycle; the phrase 'Intelligence Analysis' now becomes 'Intelligence Synthesis'.
- **Socio-cryptanalysis** - This refers to social or human hacking, using social engineering techniques.
- **Implications – N.B:** It should be noted that the ripple effects of the above propositions would also apply; i.e., other terms corresponding to the above terminologies are also inherently proposed. For instance: analyst, analytic and analytical correspond to analysis, similarly, synthesist, synthetic and synthetical are also assumed to have been catered for (where they never existed), corresponding to synthesis as defined herein; and ditto for all the other terminologies.

The proposed shift in nomenclature, from a threat to risk, would not only facilitate a better understanding of the entire processes but also propel the need to employ relevant evaluation tools, as expected of professionals. Again, risk is a function of the likelihood that a given threat-source would exploit a particular existing/potential vulnerability, and the resulting impact of that adverse event on the target of interest. Threat and vulnerability, as defined, do not belong to the same environment and are generally of different characterisation. Threats come from the usually unknown/known adversary or accident which may be artificial or natural, all of which are external to the asset that is being protected, and are meant to harm it, either intentionally or otherwise. Vulnerabilities, on the other hand, are faults/weaknesses due to a failure or inadequacy which are inherent

[4]Etymologically, a very close and careful examination of the above definitions might even suggest that the word **Thesis,** as a synonym of **Dissertation**, should be replaced with **Synthesis.** This becomes evident, if it is accepted that what the Greeks refer to as thesis is as reflected in Figure 2.13.

to the asset that is being protected. A threat would remain a threat distinct from vulnerability, and it would remain insignificant unless there exists a relevant vulnerability that corresponds to it. The two concepts should never be grouped together as one concept (as employed in the US military doctrine), as this would compound the assessment process; since it would be difficult to eliminate all the risks, where a threat lacks a corresponding vulnerability, it would cancel out naturally and simplify the risk assessment process.

It should be noted that this proposal does not eliminate threat analysis, but it will bring into pragmatic focus the relevance of threat itself, by highlighting its natural and indispensable relationship with vulnerability in the security assessment context. Similarly, it compels the threat to take its proper place, at a lower level, as one of two equally important inputs in the security assessment process.

After going through the concept of security and its assessment procedures in the last two segments, cyber/cyberspace and its threat landscape are discussed in the next segment. This will underscore the significance of cryptography, cryptanalysis and social engineering concepts that are treated immediately afterwards. It is an appreciation of this significance that instigated the measures proposed in Chapter 6 to drive home the danger inherent in the apparent negligence of exploitation of trust by confidence artists with negative implications on cybersecurity.

2.6 The Concepts of Cyber and Cyberspace

As a prefix, ‘cyber-’ is used in an increasing number of terms to describe new things that are being made possible by the spread of computers. For instance, cyber-phobia means an irrational fear of computers [168]. The term originated from kybernetes, the Greek word for steersman or governor [169]. Its contemporary usage dates back to 1948 when it was first used in cybernetics, a word coined by Norbert Wiener and his colleagues [15]. ‘Cyber’ is mostly used as a prefix to describe a person, thing, or idea as part of the computer and information age. Thus, the word ‘cyber’, almost a synonym of the computer, could be defined as something of, relating to or involving computers/computer

networks [144]. It is in this context that the Internet is described as the cyber marketplace.

Closely related to cyber is the concept of cyberspace, a metaphor for describing the non-physical terrain (a virtual world) created by computer systems [170]. For instance, online systems create a cyberspace within which people can communicate with one another (via e-mail), do research, or simply window-shop. Like physical space, cyberspace contains objects (which include files, mail messages, and graphics) and different modes of transportation and delivery. Unlike real space, however, exploring cyberspace does not require any physical movement other than pressing keys on a keyboard or moving a mouse. Defined as “the online world of computer networks and especially the Internet” [144], the term cyberspace was coined by William Gibson. He first used it in his story "Burning Chrome", in 1982 [171], [172], and it appeared in his science-fiction novel, Neuromancer, in 1984 [173]. The US National Military Strategy for Cyberspace Operations defines cyberspace as “the domain characterised by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures.” This leads to a brief highlight on network security.

2.6.1 Network Security

In computer networking, network security [174] consists of the measures taken by the network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of the computer network and network-accessible resources. It is the granting of access to data in a network for authorised users and denial of same for unauthorised users, as determined by the network administrator. Users are assigned an ID and password that allows them access to information and programmes within their authority. A glossary of cyber-network and Internet-related terminologies is in Appendix 1; network security is in the third transport layer as illustrated in the appendix – Figure 1-2.

2.6.2 Constituents of Cyber Warfare

It is difficult to come by a globally accepted definition of cyber warfare, since the UN has none [175]. It is even being debated as regards the correctness of the

term cyber warfare. Instead of calling it a form of warfare, some believe that all politically motivated cyberattacks are merely sophisticated versions of three activities that are as old as warfare itself. Thus, what should really be talked about are cyber-sabotage, cyber-espionage, and cyber-subversion, instead of cyber warfare [176]. However, in line with the opinions of other experts, Pentagon has formally recognised cyberspace as a new domain in warfare; the 5th Domain, after land, sea, air and space [177-179].

In view of the above, cyber warfare may be defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" [180]. This seems to situate cyber warfare as a form of cybercrime which includes an activity crossing international borders and involving the interests of at least one nation-state [181]. This concept seems to be in tune with the two historical standards for warfare doctrine [175]: “War is nothing but a duel on an extensive scale. … war, therefore, is an act of violence to compel our opponent to fulfill our will,” [26] and “One hundred victories in one hundred battles is not the most skillful. Seizing the enemy without fighting is the most skillful” [182].

2.6.3 The Threat Landscape in Cyber Warfare

Whether it was under Sun Tzu, Napoleon Bonaparte, Alexander the Great or own contemporary world, no analysis of war can be made without an understanding of the enemy forces and their composition, disposition, strength, centres of gravity and terrain [175]. In this virtual warfare, the battle space consists of the cyberspace as defined in Section 2.6, while the weapons consist of the various cyber tools, especially the computer/Internet, employed in cybercrimes. These crimes include hacking, botnet, phishing, cyberbullying, cyber stalking, virus attacks, malware/spyware attacks, fraudulent websites, denial-of-service attacks, ID theft (impersonation to commit fraud), cyber terrorism, and cyber war.

The threats are classified into the most active threats (in terms of actors) and the most dangerous threats (in terms of impact) [175]. In descending order, the threat landscape in terms of the number of cyber activities is dominated by the

script kiddy, criminal, hacker groups, insider, political/religious groups and APT/Nation-state (Advanced Persistent Threat; military and affiliated groups that may receive support from the government). Of these, the malicious insider is adjudged to be the most dangerous group; they are estimated to represent only about 20% of the threat but cause about 80% of the damage [175]. Researchers have shown that, in terms of damages caused, the impact of the activities is almost in reverse order, compared to the prevalence of activities. Thus, in descending order, the threat landscape in terms of the impact of cyber activities is dominated by APT/Nation state, insider, terrorism, physical/environmental attacks (both natural and man-made), criminal/phishing attacks, hacker groups, unintentional actions, hacktivism and Noob/Script kiddy. The motivations for cyberattacks are varied. They are however influenced by the number of activities in descending order as follows: money, espionage, skills for employment, fame/status, entertainment, hacktivism, terrorism, and war.

2.6.4 National Cyber Threats

This section will briefly discuss the national cyber threats, vulnerabilities, motivations for cybercrimes, and the DDoS attacks. In the US, the concept of having a programme for the protection of national or critical infrastructure against cyberattacks has been in place since 1996. In 2001, the Patriot Act defined critical infrastructure as those “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

Any of the common security concerns of modern computer security, as highlighted in Section 2.7, threatens mostly cyber-based national infrastructure. These include confidentiality, integrity, availability, authenticity, non-repudiation and identity theft [1, 183, 184]. These are the primary considerations or pillars in modern computer communications security. They manifest via an ever-growing list of cybercrimes, as highlighted in Sections 2.6 and 2.6.4, the worst of which is the DDoS attack [15].

In addressing these pillars of security concerns, which may involve both technical and nontechnical measures, the following means would also need to be provided: identification – who does the client claim to be; authentication – how could it be established that the client is actually who he claims to be; authorisation – now that the client has been verified, what is he/she allowed to do; accountability – who did what, and, perhaps, who pays the bill? Measures aimed at addressing some of these concerns are discussed in Section 2.7.

National Cyber Vulnerabilities

Unlike threats, vulnerabilities are not easily amenable to grouping in taxonomy. Howev er, the national infrastructure would need to address obvious problems like improperly configured equipment, poorly designed LANs, unpatched system software, exploitable bugs in application code, and locally disgruntled employees. It is recalled that of all the malicious actors, the malicious trusted insiders are the most dangerous. The most fundamental vulnerability in national infrastructure is the pervasive complexity underlying the system. The staggering complexity is such that, many times, it is unpalatable security incidents that uncover aspects of computing functionality that were not previously known to anyone; including the system designers, at times [183, 185]. In addition, it is most discomforting to note that, in some cases, the optimal security solution requires the simplification and cleaning up of poorly conceived infrastructure; most large organisations are not amenable to this approach.

In most cases, the best way to ensure a comprehensive assessment of vulnerabilities associated with national infrastructure is to take care of their relative exploitation points. In order to appreciate this approach, an abstract national infrastructure cybersecurity model is illustrated in Figure 2.14. It comprises of the external adversary (hackers on the Internet), the internal adversary (trusted insiders), and supplier adversary (vendors and partners). The model also shows three exploitation points, namely; remote access (Internet and telework), system administration and normal usage (management and use of software, computers, and networks), and supply chain (procurement and outsourcing). The three exploitation points and types of adversaries could

be associated with different types of possible motivations, for either a full or test attack on national infrastructure, as highlighted in the next segment.

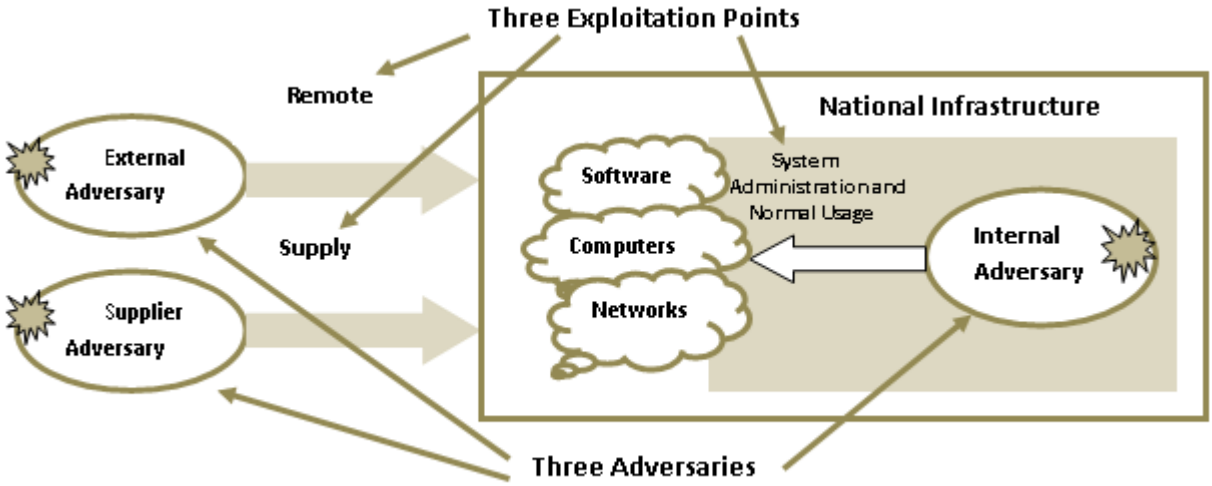


Figure 2.14. Adversaries and exploitation points in national infrastructure [16]

Whenever vulnerability is identified within an organisation, it is necessary for an appropriate authority to make a public vulnerability advisory if the benefits of notifying the system maintenance engineers outweigh the risk of alerting the intruders. This cost-benefit calculation is particularly important where many other organisations can directly benefit from the information by taking immediate remedial actions. The timing and manner of issuing a vulnerability risk advisory, or whether it should not be issued at all, must be determined on a case-by-case basis, depending on the threat and situation [183].

Motivations for Cyber Attacks

Possible motivations for cyberattacks on an infrastructure may include the following [183]:

- **Country-sponsored Warfare** - A cyberattack that is sponsored and funded by enemy countries and directed at the national infrastructure ought to be considered as the most important potential motivation. This is because the willingness and intensity of such an adversary's capacity to

deal a deadly blow are potentially unlimited. The Estonian case of April 2007 provides a good example for this category.

- **Terrorist Attack -** The terrorist motivation is also significant because terrorist groups can easily acquire sufficient capability and funding to conduct dangerous attacks on infrastructure. From experience, a terrorist motivation may decompose into ethnoreligious and socio-cultural components.
- **Commercially Motivated Attack -** When a company chooses to employ cyberattacks to secure a commercial advantage, it could become an incident of national infrastructure dimension if the target constitutes a national asset.
- **Financially Driven Criminal Attack -** Identity theft is the commonest example of a financially motivated criminal attack. However, other cases may include the intimidation and extortion of companies to avoid cyber incidents.
- **Hacking -** It is instructive to note that many types of attacks are still driven by the motivation of hackers, who are usually mischievous youths trying to learn or build a reputation for themselves among hackers. This is a much less sinister motivation which national leaders can find better ways to tap this boundless energy that is characteristic of youthful exuberance.

Distributed Denial of Service Attack

A Denial-of-Service (DoS) attack is effected by bombarding the target (e.g. website) with such a volume of requests that it cannot cope with the quantum rise in demand. The website will be slowed down, and, in extreme cases, it will be overwhelmed to the point where it simply stops working [16]. This results in complete service denial for the clients using the website; hence, the term DoS.

The DoS attack is usually carried out by a remotely controlled network of compromised or possessed computers (bots, zombies; in a botnet) which are distributed (scattered) across geographic, political and service provider boundaries; hence, the term DDoS. The end-users whose machines (PCs) are employed are innocent of the attack, as their machines are remotely

programmed to attack a target that is designated by the botnet controller. These machines are usually broadband-connected. This cyber traffic jam, considered as the most insidious type of attack that exists today [15, 183], is virtually unstoppable because of the ineffective administration of the end-user machines and ubiquity of the botnet coverage. This is further compounded by the fact that bots are programmed to take commands from multiple controller systems. Thus, any successful attempts to destroy a given controller result in the bots simply homing to another controller.

The bot recruitment is implemented by using Trojan horses or viruses, sent to the user in e-mail. The email content automatically forwards itself to all the destinations that are stored in the victim's address book. This attack will continue by the virus propagating itself throughout a system, and subsequently, infect one organisation after the other. Examples of this kind are the 'I Love You' and 'Internet Worm' viruses [178]. The five entities that may constitute a botnet attack are [183]:

- **Botnet Operator -** This is the individual, group or country that creates the botnet, including its setup and operation. It is the operator that benefits from financial gains when used for the purpose. Evidence-backed identification of botnet operators has been very difficult for both the law enforcement and cybersecurity initiatives.
- **Botnet Controller -** The set of servers that command and control botnet operations. Usually, this is a server that has been maliciously compromised for this purpose, without the knowledge of the real owner. Controller activities include all recruitment, setup, communication and attack. Typical botnets include a handful of controllers distributed across the globe in a non-obvious manner.
- **A Collection of Bots -** These are the end-user broadband-connected PCs infected with botnet malware. They are usually owned and operated by bona fide citizens who are unconsciously used as instruments in a botnet attack. When a botnet includes a concentration of PCs in a given region, observers often incorrectly attribute the attack to that region. It is projected that the use of smart mobile devices in a botnet will grow as upstream capacity and device processing power increase.

- **Botnet Software Drop -** Most botnets include servers that are designed to store software that might be useful for the botnets during their life-cycle; this is akin to a military arsenal. Like controllers, botnet software drop points are usually servers that have been compromised for this purpose; often unknown to the normal server operator.
- **Botnet Target -** This is the location that is targeted in an attack. It is usually a website, but, in practice, it can be any device, system or network that is visible to the bots. Mostly, the targets are prominent and controversial websites, simply because they are visible via the Internet and have a great deal at stake in terms of their availability.

The victims of cyberattacks via the DDoS mechanism are countless and their heterogeneous list is endless. Examples include attacks against Iranian nuclear facilities in 2009/10 and the planned cyber war against Iran ("Olympic Games") published by New York Times in February 2016, the compromised computers of the Climate Research Unit (CRU) at the East Anglia University (2009) and the nearly 4,000 individual victims of the defunct British tabloid, the News of the World (2002- 2011; about 11,000 documents). Other high-profile victims are NATO (2011), CIA (2011) and Nigerian Army Education Corps Website (2011).

Recent attacks include the DDoS attacks against JANET (UK) in February and April 2016, Israel's CCTV Systems (February 2016), University of Central Florida (February 2016), Ex-Israeli Army Chief of Staff (February 2016), South Africa's Department of Water Affairs (DWA) (February 2016) and the Hillary Clinton Campaign, as part of attacks on Democrats (June 2016). These are in addition to thousands of botched/successful hacking attempts/attacks against various other critical national infrastructural facilities in the US, UK, Europe and other countries [19-21]. Yet, the latest and one of the most significant DDoS attacks in recent years, covering both the US and Europe simultaneously, is the one which occurred on Friday, 21st October 2016, as reported by 'The Guardian' under the heading: "Major cyberattack disrupts Internet service across Europe and US" [186]. The list of popular sites affected by the attacks includes Netflix, Twitter, Spotify, Reddit, CNN, PayPal, Pinterest, AirBnB, Github Fox News, The Guardian, New York Times, Wall Street Journal and the Amazon.

The attacks seemed to have been mainly directed at ‘Dyn’, one of the companies that run the Internet’s Domain Name System (DNS); it is headquartered in Manchester, New Hampshire (US). Millions of IP addresses were affected. Its unique significance lies in the fact that it occurred at a time when the US Presidential campaign of 2016 was at its climax amid reinvigorated rhetoric about allegations of electoral rigging by one of the major candidates. It is possible that these widespread DDoS attacks could have been part of an ongoing rehearsal for a possible plot to rig the US Presidential elections which would be due in about eighteen days; the FBI and other US security agencies were still investigating the incidence as at the time of this report. Details of cyberattacks timeline are available in Hackmageddon [187]. The statistics for February 2016 highlighted above represents only a tip of the iceberg for that month alone.

In the Global Risk Report 2015, it is highlighted that large-scale cyberattacks, characterised by DDoS bombardment, were among the prominent risks in 2015 [16, 188]. With the successful attacks on JANET(such an elitist infrastructure; twice within three months at attacker’s own prime chosen time), the successes against NATO and Pentagon, the ease with which Iranian nuclear facilities were diminished by some 20% and the glamorous US “Olympic Games” lying in wait for the total incapacitation of the nuclear programme, should diplomacy fail, coupled with the alleged dabbling into the US democratic process by an antagonistic foreign power, it is clear that the 5^{th} warfare domain (the cyberspace warfare) has become a reality – it is the most likely candidate that would replace the defunct Cold War.

The security and financial implications of these compromises can only be best imagined. That is, given the growing sophistication of cyberattacks, the rise of hyper-connectivity with a growing number of physical objects connected to the Internet, and increasing quanta of sensitive personal data being stored by companies in the cloud, it is obvious that the risk of large-scale cyberattacks remains high; with respect to both impact and probability. For instance, in the United States, the economic cost of cybercrime is estimated at $100 billion each

year [188]. According to the first official government estimate on the issue, published in February 2011, cybercrime costs the British economy some £27.00 billion ($35.902 billion) a year [189]. As at June 2015, this estimate rose to £34.00 billion ($45.20 billion) [190].

From the foregoing, any serious present study on cybersecurity must acknowledge the unique threat posed by botnets, because virtually every Internet-connected system is vulnerable. The arithmetic of the situation is especially intimidating [183]; a botnet that might steal about 500 Kbps of upstream capacity from each bot would only need three bots to collapse a targeted T1 connection. Thus, only 16,000 bots would be required, theoretically, to fill up a 10-Gbps connection [183]. The threat is obvious since most of the thousands of botnets that have been observed on the Internet are at least of this size; many prominent botnets like Storm and Conficker have several million bots. Thus, the national infrastructure faces a severe threat; especially with the threats posed by DDoS at a time when IP traceback mechanism is not yet a market reality. These two concepts are illustrated below.

- Illustration of DDoS

As an example, consider a hypothetical gateway which allows for 1.5 Gbps of inbound traffic, and a botnet creates an inbound stream much larger than 1.5 Gbps. It is obvious that a logjam would result at the inbound gateway, and a DoS condition would occur as illustrated in Figure 2.15 [183].

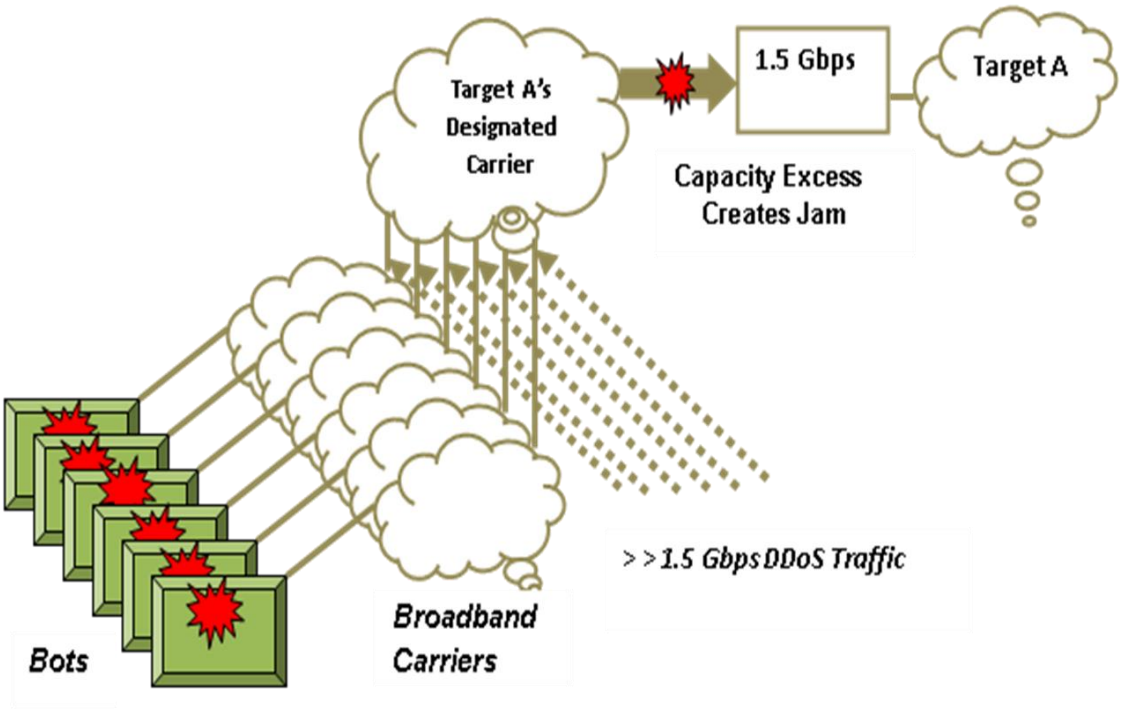


Figure 2.15. A sample DDoS attack from a botnet [183]

❖ IP Mechanism

The problem of finding the source of a transmission packet is called an IP Traceback problem. Thus, IP traceback is a means or method for "reliably determining the origin of a packet on the Internet" [191]. The relevance of IP Traceback technology can only be fully appreciated if the prevalence of the variety of active cyberattacks on the Internet is reflected upon. Specifically, operators of every Internet Services Provider (ISP) consider the Distributed Denial of Services (DDoS) attacks as the most potent in this regard [15]. The detection and countering of a DDoS attack source is particularly difficult because the IP network is basically stateless with multi-management domains, and the source IP spoofing (camouflaging or faking) is easy. Thus, the IP Traceback Technology is designed to trace and locate the source(s) of packet transmissions with a focus on countering DDoS attacks [15, 191].

As illustrated in Figure 2.16, in the IP traceback mechanism, the user (victim) at a linked terminal unit first issues a tracking request for a packet that is considered to be an attack. A piece of packet data is encoded with a

unidirectional hash function and transferred to a trace-back system within an Autonomous System (AS) to which the user belongs. The requested trace-back system examines each packet to determine whether it is coming in from an external source or from its own system. When the issued packet is coming from a neighbouring AS, a trace request is queried to the AS. This process is repeated recursively until the trace-back system identifies an actual AS to which the attack source belongs [15]. Although practical tests have demonstrated that tracing the original source of Internet communications is feasible, there are still loose ends to be tied up before the technology becomes a market reality [15].

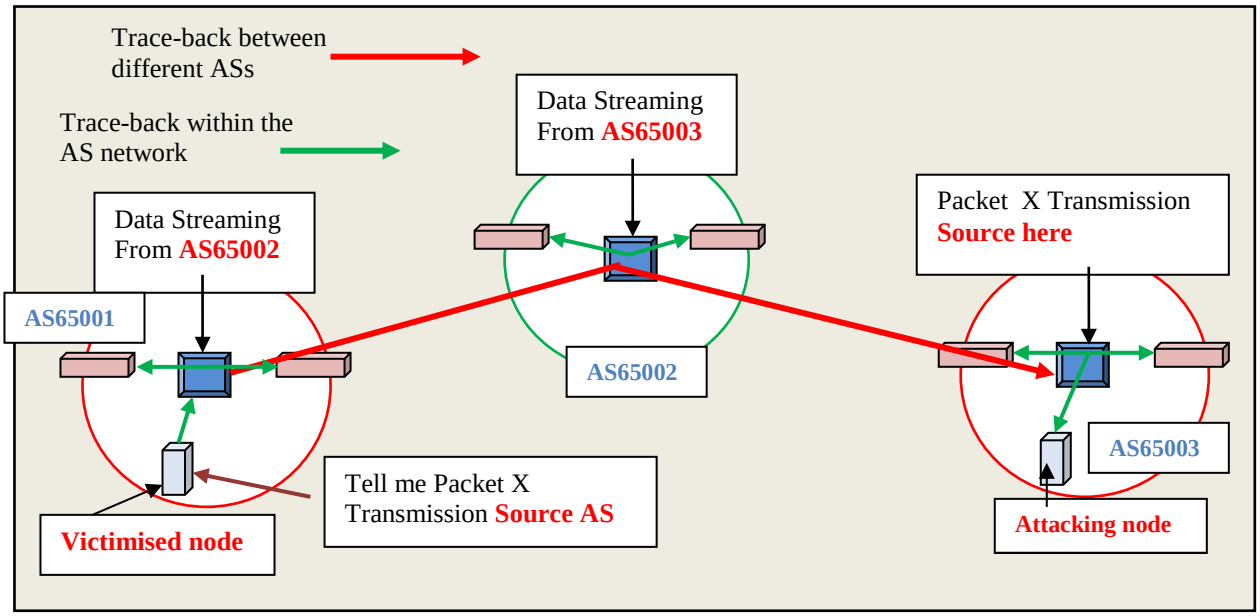


Figure2.15. Mechanism of IP traceback technology [23]

2.7 Cryptographic Solutions for the Technical Threats to Cybersecurity

This section highlights cryptographic solutions for the technical threats to communication security. Obviously, as soon as the first literate human realised that it was necessary to write down a piece of information, either for storage or transmission/ transportation, and there would be undesirable consequences should that bit of information be exposed to his antagonists, the challenge of

cryptology became manifest. As people started figuring out ways of encoding information or trying to understand others' encoded messages, the field kept on developing until it reached the current level of complexity; and the development continues [1]. The common technical problems that have been identified in the course of this development relate to the threats of eavesdropping, modification, replay, masquerading (impersonation, identity theft), penetration and repudiation, as well as their highly sophisticated techniques of accomplishment. From inception, cryptography has been struggling to find solutions to these problems. The cryptographic countermeasures designed to meet these challenges include mechanisms aimed at ensuring confidentiality, integrity, availability and authenticity, as discussed herein [178].

2.7.1 Confidentiality

The confidentiality of a message in any form is guaranteed by encryption with a secret key, as long as only the legitimate users have access to that key. Thus, symmetric encryption can provide confidentiality of a message. An eavesdropper would not be able to read the plaintext without the key, even if he acquires the ciphertext. Although asymmetric encryption could also be used to achieve the same objective, it is strongly argued that, for the purpose of confidentiality, symmetric encryption is favoured over its asymmetric counterpart. This is mainly because of its relative advantage in the speed of execution. However, as the characteristics of both methods are useful in message protection, hybrid systems are often employed to combine their relative advantages.

2.7.2 Integrity

Messages and files require protection against surreptitious modification. While confidentiality procedures offer protection against eavesdroppers, they give little protection against modification and integrity of the message or file. This is critical for text and data messages which are vulnerable to this form of attack. This is particularly instructive in the banking and other financial arenas, where an intruder may be able to change monetary values and account numbers, in a standard transaction form, without the need to actually read it (except for non-

malleable encryption algorithms). The solution to integrity threat is to employ digital signatures, MACs or some other redundancy scheme in the plaintext prior to encryption. In summary, digital signatures serve the following purposes:

- **Public Verifiability -** Anybody in possession of the authentic public key can verify the signature.
- **Authenticity and Integrity -** Modification of a message or its replacement can be detected.
- **Non-repudiation -** The signatory of a message cannot deny having signed the document.

2.7.3 Availability

A basic but very fundamental essential in communication security is the control of availability and access to the medium, sensitive data, and cryptographic equipment. This involves mainly the issues of physical access control, PINs, and passwords. While physical access control is beyond the scope of this discussion, password is reserved for a special attention in Chapter 3.

2.7.4 Authentication

In voice transmission using high-quality transceivers, voice recognition is the obvious authentication method, where the receiver is familiar with the voice of the sender. However, if the two parties are not familiar with each other or the voice quality of the transmission medium is not reliable, other measures would be required to ensure mutual authentication. Using symmetric or asymmetric encryption and suitable key management, the basic problem of message authentication can be resolved. The employment of digital signatures is one approach. However, the problems associated with replay or spoofing, where a third party taps into the medium, records the transmitted message and retransmits it at a later time or date, remain unresolved. Just imagine the confusion that would arise at Station B, Figure 2.17, if Station A sends the encrypted message “ENEMY ATTACKING YOUR LOCATION NOW!” by 8:00 AM and Station Z (an eavesdropper), who could not even understand the message due to lack of key, records it and retransmits it to Station B at 8: PM

on the same day; note that Station B would receive this as an authentic message, since it has not been modified. This highlights the need for time authentication to be included in the security package, such that replayed messages would not be decode-able.

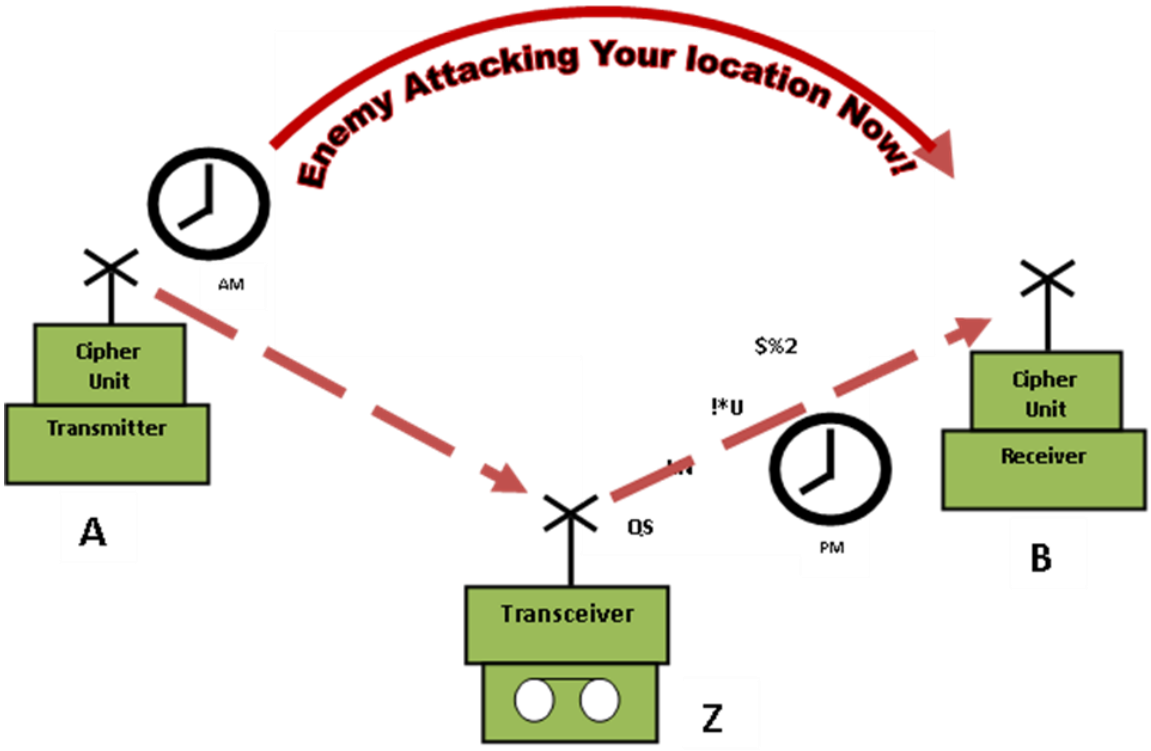


Figure 2.17. The need for time authentication [151]

Time authentication as a method of message authentication is often associated with voice and fax encryption equipment. The protection is achieved by either introducing a time slot of typically 5 min after the original encryption or modifying the key generator process so that the generator at the receiver will not synchronise with the original generator position at the transmitter. That is, all equipment within the network must have the same ±5 min time setting to be able to decode the ciphertext. The use of time slot is, however, tricky, in the sense that the receiver must have the capacity to check several time slots at the same time since two stations with very similar times can be in different time slots. Other authentication methods include the use of time stamps and mutual key agreement.

2.8 Security Engineering in Context

Security engineering deals with the building of systems that would remain dependable in the face of malice, error, and mischance. It concentrates on the tools, processes and methods required to design, implement and test complete systems, as well as to adapt existing systems as their environment changes. These require cross-disciplinary expertise covering cryptography, computer security, hardware temper-resistance, knowledge of economics, applied psychology, organisations and the law [192]. On its own, modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Thus, a good security engineering requires an amalgamation of four elements [192]. There is a need for the policy**;** the objectives set out for achievement. Then the mechanism; such as the ciphers, access controls, hardware tamper-resistance, and other machinery that would be gathered in order to implement the policy. Another requirement is the assurance; the degree of reliance to be placed on each mechanism. Lastly, there is the incentive; the motives which the people protecting and maintaining the system have to enhance optimum performance, as well, as the motives that the attackers have in trying to defeat the policy. All of these elements must interact as illustrated in Figure 2.18

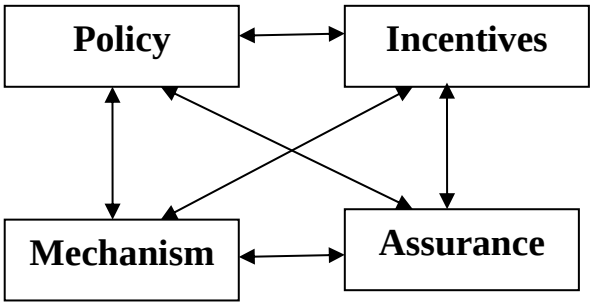


Figure 2.18. Security engineering analysis framework [175]

There is always the tendency to build security around technology, thereby neglecting the most important factor of any security system; the human factor. Security revolves around people; both the people who attack the systems, as

well as the trusted ones who defend those systems. The people, who must be trusted, in order for the system to function, constitute the most critical element of any security system. This is because they are the most resilient and the only ones endowed with real initiatives. They take decisions, they improvise and they are the most skilled at detecting attacks. However, as components of a security system, human beings are double-edged swords. They suffer from fatigue and can be distracted, tricked and even compromised. Due to their privileged access, when trusted people become compromised they can carry out attacks that outside criminals might find difficult to even contemplate. Therefore, the best trick is to design security systems that maximise the positive aspects of people, while minimising their negative aspects [193].

2.9 Context of Cryptography

Cryptography is the art and science of keeping messages secured [146]; encryption is its original goal [23]. It is the science of using mathematics to encrypt and decrypt data, thereby making it possible to store sensitive information or transmit it across insecure networks (e.g. Internet), such that it cannot be read by anyone except the intended recipient; with the appropriate decryption key. It is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects of information security, such as data confidentiality, data integrity and authenticity [56]. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering [25]. There are several ways of classifying cryptographic algorithms. Figure 2.19 shows 3 categories [25] based on the number of keys that are employed for encryption and decryption. Basically, as illustrated in Figure 2.19, cryptography is the conversion of information from a readable state (plaintext) to an apparent nonsense (ciphertext) with the aid of an encryption key at the source.

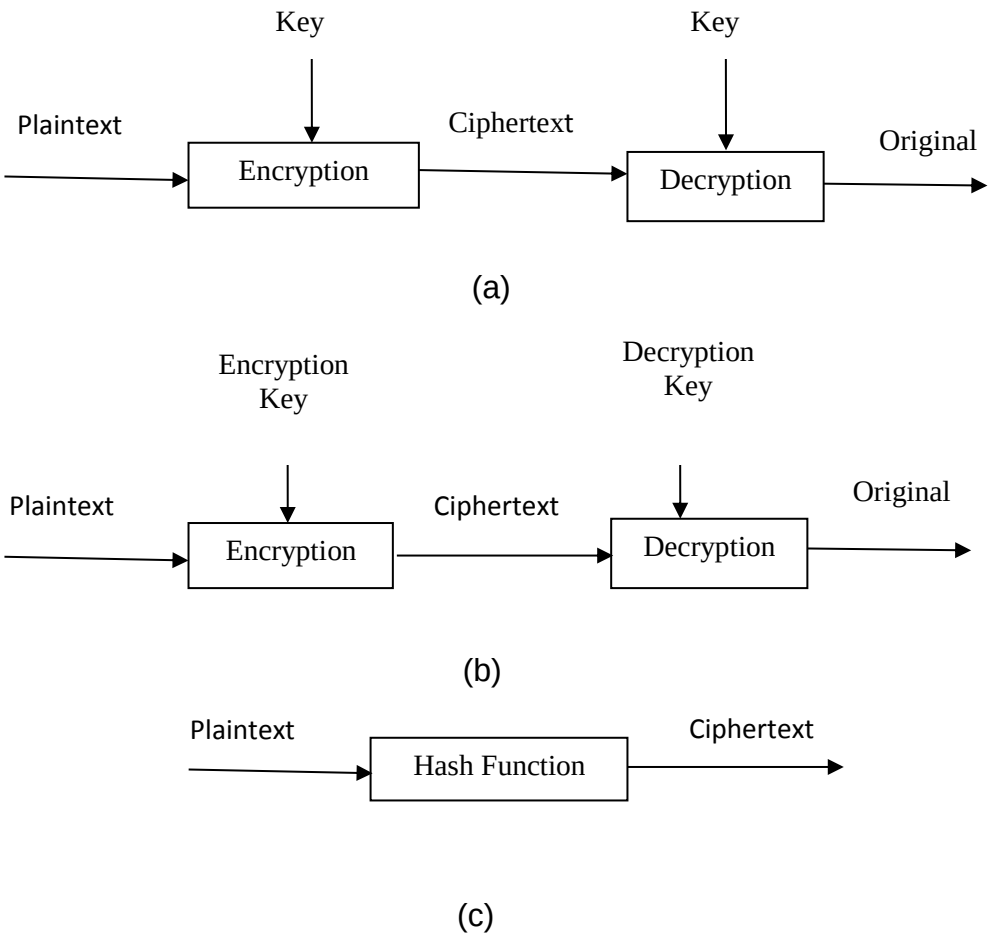


Figure 2.19. Cryptographic settings for secret key, public key, and hash function (a, b and c respectively) [184]

The resultant ciphertext is converted back to the original plaintext with the aid of a decryption key (which may or may not be the same as the encryption key) at the sink. Depending on the strength of the encryption key, some ciphertexts may be easily broken, such as some mono-alphabetic substitution ciphers (e.g. the Caesar Cipher). Others may appear unbreakable, at least within the relevant timeframe. For instance, the Necronomicon of Al-Hirra, or Book of the Dead (The Voynich Manuscript) has remained unbroken since 730 CE [194].

Cryptography could be likened to a lock in the physical world. A lock, on its own, is useless until it is part of a larger physical system, such as a door on a building, a chain, a safe, a car, and etcetera. This larger system also includes the people whose roles are crucial in order for the lock to function at all, and to do so effectively. Similarly, cryptography on its own is useless until it forms part

of a larger security system; and it is only a very small part of it. As illustrated in Section 2.8, it is only one item under the security mechanism, while the entire mechanism itself is only one out of four major areas of security engineering concerns. However, though it is a small part, cryptography is nonetheless a very important part because, unlike the lock which only denies or grants access to all, cryptography also performs the sensitive function of distinguishing between good access and bad access [23].

From the foregoing, it is obvious that the effectiveness of a cryptosystem can only be assessed within the context of the entire security system, of which the human factor is the weakest link. Again, it must be noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that encompasses all the other elements of the entire system. This underscores the significance of social engineering in every security arrangement.

2.9.1 General Model of Cryptosystems

Figure 2.20 illustrates the flow of information in a general cryptosystem. Given the following denotations:

M	=	P = Plaintext (Message)
E	=	Encryption Function
D	=	Decryption Function
K_1	=	Encryption Key
K_2	=	Decryption Key
C	=	Ciphertext (Encrypted Message)

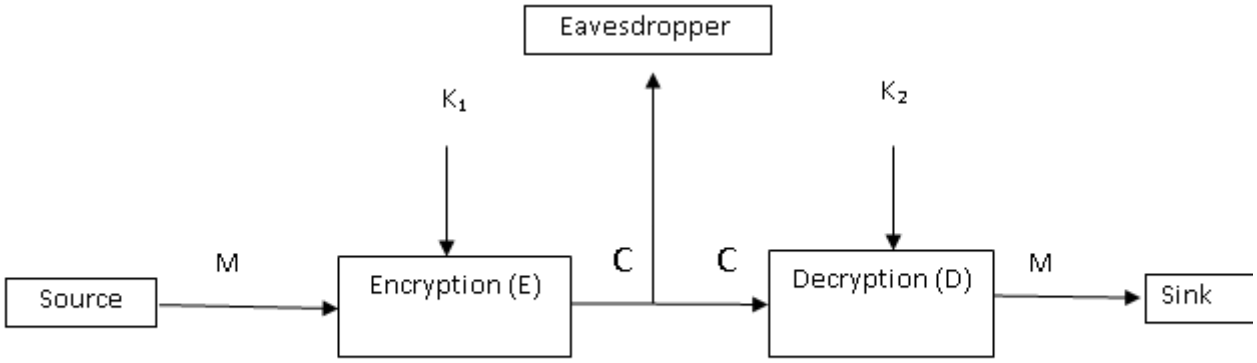


Figure 2.20. Characterisation of a General Cryptosystem

The encryption and decryption operations are respectively governed by the equations:

$$E_{K_1}(M) = E_{K_1}(P) = C \quad (2.30)$$

$$D_{K_2}(C) = D_{K_2}\{E_{K_1}(M)\} = M = P \quad (2.31)$$

Where K_1 may or may not be the same as K_2; for Symmetric and Asymmetric Cryptography respectively [146]. Where $K_1 = K_2$ for a symmetric operation

$$E_K(M) = E_K(P) = C \quad (2.32)$$

$$D_K(C) = D_K\{E_K(M)\} = M = P \quad (2.33)$$

For symmetric cryptography, the key, which is kept secret, is known only to the sender and receiver. Thus, for 'n' users, the number of keys required is [195]]:

$$^{n}C_2 = \frac{n(n-1)}{2} \quad (2.34)$$

For asymmetric cryptography, however, the encryption key K_1 is publicised while the decryption key K_2 is kept secret by the owner [23].

Eavesdropping or wiretapping is the interception of an information data by an unauthorised third party monitoring a communication channel [195]. The traditional practice in cryptographic analysis is to depict Alice as the sender at the Source, Bob as the receiver at the Sink and Eve as the intruder or eavesdropper between the source and the sink [23].

A cryptographic algorithm is a mathematical function used for encryption and decryption [146, 196] The decryption algorithm is usually the reverse of its encryption counterpart; for instance, addition and subtraction. As an illustration, assume the number 786 is to be sent using a cryptosystem, and both parties have agreed on a key value of 019. Using an encryption algorithm, which is the addition of the message (786) and the key (019), the ciphertext is 805. Since the recipient knows the key (019) and the encryption algorithm (addition), the message can be decrypted from the ciphertext by doing the reverse operation; subtracting 019 from 805 to get the plaintext message 786. Anybody intercepting the communication should have some difficulty in figuring out the plaintext from the ciphertext without the key, even if the encryption technique is known [196, 197].

2.9.2 Cryptographic Key Management

The most secure cryptographic algorithm/protocol is virtually useless without an efficient and effective key management system. It is understood that key management is the Achilles heel of most secure communication systems [182]. Available records indicate that the most effective way to attack a secure communications system is to influence the system's personnel and exploit weaknesses in its management; this again underscores the importance of human trust and other human factors in cybersecurity. It is clear from Table 2.6 that, even for a known algorithm, in order to break a key by brute force, an incredible amount of effort, in both time and logistics, is required. Thus, rather than spending a stupendous amount of money on analytical tools to gain information on a 128-bit key, which is statistically impossible within a useful time frame, it is much easier and less expensive to exploit the weaknesses in the human infrastructure; the weakest link in the security system (due to operational

deficiencies and compromise reasons). The purpose of key management is to reduce the risk associated with these threats/vulnerabilities to the barest minimum and to process secret keys in such a manner that it is transparent to both the user and the network. The issues that relate to key management include key generation, distribution/installation, activation/use, expiration/revocation and destruction.

Table 2.6. Estimates of time required to break keys by brute force [178]

Key Length (bits)	Key Variety	Tests/Sec/ Computer	Number of Computers	Time Used
40	1.1×10^{12}	10^9	10^3	1.1 s
56	7.2×10^{16}	10^9	10^3	20 h
80	1.2×10^{24}	10^9	10^3	38,000 years
128	3.3×10^{38}	10^9	10^3	1.1×10^{19} years
128	3.4×10^{38}	10^9	$7 \times 10^{9*}$	1.5×10^{12} years

*World population

2.9.3 Cryptanalysis

It is recalled that the main purpose of cryptography is to keep the plaintext and/or key secret from eavesdroppers (adversaries, attackers, interceptors, interlopers, intruders, opponents, or enemies). Eavesdroppers are assumed to have complete access to the messages in the communication channels, as well as having complete knowledge of the algorithm. The science of recovering an encrypted message without having the decryption key is called cryptanalysis. For cryptanalysis to be adjudged as successful, it may recover the plaintext or the key. It may also find sufficient weaknesses that could lead to the breaking of the cryptosystem. If the key is lost through a non-cryptanalytic means, this is termed a compromise, while an attempted cryptanalysis is known as an attack. There are four general types of cryptanalytic attacks; namely, ciphertext-only attack, known plaintext attack, chosen-plaintext attack and adaptive-chosen-

plaintext attack. Other types of attacks include chosen-ciphertext attack, chosen-key attack, and robber-hose cryptanalysis [195, 196, 198].

2.10 Social Engineering: the Art of Human Hacking

Social engineering is the act of influencing people's behaviour through the manipulation of their emotions; this is used as a means to gain and betray their trust in order to have access to their system. This is done over the phone, via an email, through social media or in person and a variety of other methods. The major difference between social engineering and other attack methods is the use of human beings as a vector for the attack; the wetware in hackers' parlance. Some people are naturally gifted in the science of social hacking, but the art could also be taught and learned. The use of wetware, which has grown rapidly in recent years, is said to be the dominant technique in attacking some target sets [18, 175]. Most modern attacks employ a blend of technical and social engineering techniques. Social engineering covers what is popularly called '419' (advance fee fraud), a unique form of confidence artistry, whose antidote is proposed in Chapter 5. Hence, conceptual clarifications relevant in the treatment of Chapter 5 are highlighted next.

2.10.1 Conceptual Clarifications

The term cyberspace does not have a standard and objective definition [199, 200]. Generally, it is used to describe the virtual world of computers. In other words, while the term 'cyber' denotes the computer and anything that relates to it, cyberspace refers to the notional environment in which communications over computer networks occur [201]. It is "the domain characterised by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures" [202].

Computerisation is to cause certain operations or processes to be performed by a computer, particularly, as a replacement for human labour. Digitisation is the

process of converting real-world analogue quantities (texts, images, audio, video, etc.) into a digital format [203]. In this format, information is organised into discrete small units of data (bits) which are grouped into bytes. This is the binary data that computers and several devices with computing capacity can process. Thus, digitisation involves a process that results in the breaking down of a given whole into its smaller parts.

Miniaturisation is the continuous reduction in the sizes of manufactured items, regardless of whether they are mechanical, optical/electronic products and devices; e.g., mobile phones, computers, vehicle engine downsizing, etc. [204]. This trend is made possible by the emergence of micro and nanotechnologies. Authentication is the process of establishing the true identity of a user or an entity [205]; i.e., to prove that a person/an entity is indeed the one whom he/that it claims to be.

Tele-density used to be computed as the number of fixed telephone lines per hundred inhabitants. With the advent of GSM, where mobile cellular subscribers outnumber the fixed line connections in some countries, the term Mobi-density is preferred in such countries; i.e., mobile cellular subscribers per hundred inhabitants. Since the two terms may lead to mutual disadvantages for countries with well-established fixed lines and those whose GSM network is still at the initial stage of development, ITU has proposed the use of Effective Tele-density; defined as either fixed line connections or mobile subscribers per hundred inhabitants – whichever of the two is higher [206, 207].

Advance fee fraud (alias 419), which is also known as the Nigerian Scam, has grown into an epidemic [24]. The term ‘419’ was coined from Section 419 of the Nigerian Criminal Code (part of Chapter 38: Obtaining Property by False Pretences; Cheating) [208]. Basically, 419 is a form of confidence trick which the confidence artists use to defraud unassuming innocent business partners, both locally and globally. An example of a 419-transaction is illustrated in Figure 2.21, where Caller 2 gives his fake location as KANO (Location E; circled in Red) in his mobile phone conversation with Caller 1 at IBADAN (Location B), while he is actually speaking from LAGOS (Location A). Please note that Caller

2 could have given his fake location as KUMASI (Location C) in Ghana or NIAMEY (Location D) in Niger or anywhere in the world, claiming to have roamed his mobile service. This necessitates some discussions on LBA in Chapter 5 and underscores the significance of trust-centred human attributes in cybersecurity designs.

These conceptual clarifications under social engineering, which serve as a prelude for tackling the confidence artists in Chapter 5, bring the extensive literature review to a close. The lessons learned from the review on trust in Sections 2.3.2 – 2.3.4 of this chapter will be invaluable in the study, understanding and practical implementation of the antidote against the 419 style of fraud in Chapter 5. Before then, the relevance of password security, as the first line of defence in cyberspace, within the context of human factors is treated in Chapter 3 immediately after the deductive summary for the literature review in the last section of this chapter. This would have provided sufficient background for the presentation of the main research design and implementation with result analyses in Chapter 4, prior to Chapter 5. Next is the deductive summary of the literature review.

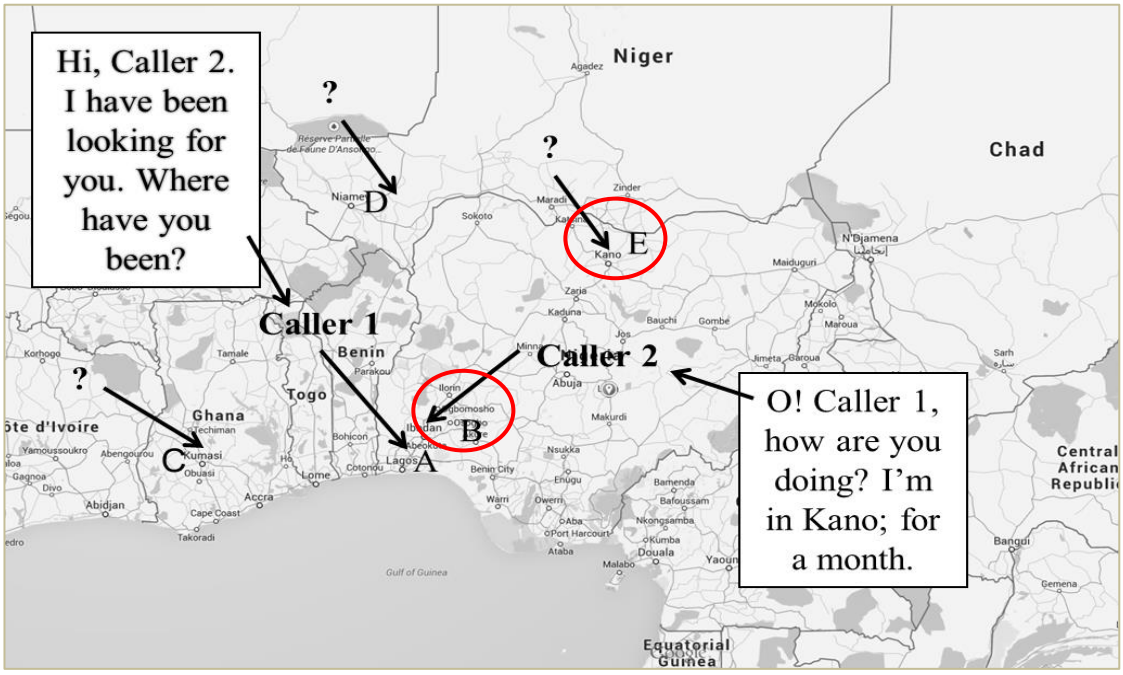


Figure 2.21. A 419 mobile phone conversation: giving a fake caller's location

2.11 Deductions

Chapter 2 covers literature review. It discussed secret sharing schemes, the concepts of trust and the extension of human security perimeter through a web of trust. It also discusses the concept of security and the military security assessment process, a 3-factor security assessment process (risk-centred security assessment technique) and analysis/synthesis. This is followed by the concepts of cyber/cyberspace with its threat landscape and national cyber threats/vulnerabilities. The chapter ended with highlights on cryptography/cryptanalysis and social engineering before deductions. The deductions hereunder are given sequentially.

2.11.1 Secret Sharing Schemes

This segment covers reviews on the theories of secret sharing schemes. It highlighted the theoretical basis for SSSS, a global overview of Secret Sharing Schemes and cryptographic key management, with a focus on key recovery schemes. The chapter undertook this review in search of an appropriate technological model or algorithm that could use technology in conjunction with trust-centred human factors to enhance cybersecurity, and thus extend the human security perimeter. The perception resulting from the theoretical analysis in this chapter prepares ground for a web design and development to practically implement a multi-authentication web-based secret sharing scheme - the CDRSAS-PT.

The SSSS is hereby chosen, as a guide for implementation in this work, because of its originality, simplicity, flexibility, security, and popularity, after examining the three main categories of secret sharing schemes: namely, perfect, non-perfect and ramp secret sharing schemes. This choice also comes after reviewing other (k, n)-threshold schemes, including those of Blakley, Asmuth/Bloom, and Mignotte. The SSSS was also selected and used as one of the cryptographic primitives in the implementation of the CDRSAS-PT, the main research design.

The main theory behind the SSSS is based on polynomial interpolation. The polynomials could be replaced by any other functions which are easy to evaluate and to interpolate. This idea is rooted in the notion that two points are enough to define a line, three points are required to define a quadratic expression and four points are needed to define a cubic function, etc. In other words, it requires ‘k’ points to define a polynomial of order ‘k-1’.

With the theoretical background relating to secret sharing schemes and cryptographic key recovery techniques covered in this chapter, the research effort appears set for its main design and implementation, as would be presented in the next chapter; i.e., devising or adapting an appropriate technological scheme that would use technology in conjunction with the human factor of trust to enhance cybersecurity; and thus extend the human security perimeter.

2.11.2 Trust, Human Factors Human infrastructure

The value of trust in the process of all forms of human interaction is as significant as aptly described by Russell [99] in her book titled: “Trust: The New Workplace Currency;” i.e., it is the medium of exchange among humans, without which no trade, whether in kind or cash, can take place with positive results. Trust may be defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” [2, 102].

Human infrastructure refers to those inherent requisite human inputs (e.g., trust and other human attributes) without which any technological design/device/system that is emplaced would not attain necessary quality assurance and would not yield optimum results.

The concept of human factors, as employed in this research work, relates to all the trust-enhancing (beneficial) and trust-diminishing (detrimental) human attributes. It is then posited that the consideration of applicable elements of these attributes, both the positive and negative, is a ‘sine qua non’ in the design and functioning of all aspects of human endeavours in order to realise optimum

output; with particular emphasis on technological systems.

After introductory discussions on trust, human factors, human infrastructure and the web of trust, this section covers a number of issues related to the study of trust in an organisational setting. Each is considered and dealt with, leading to the adoption of a model of dyadic trust in an organisational context. This trust model, as proposed by Mayer et al. (Figure 2.8) is the first that explicitly considers both characteristics of the trustee as well as the trustor. It clearly distinguishes trust from the factors that contribute to it, and as well differentiates trust from its outcome of risk taking in the relationship. The model defines trust in such a way that distinguishes it from other similar concepts (cooperation, confidence, predictability), which have often been confused with trust in the literature. Additionally, the critical role of risk is clearly specified in this model. The model presents a versatile and dynamic definition of trust with a set of its determinants on the part of the trustee (ability, benevolence, and integrity) and the trustor (propensity to trust). It is noteworthy that the model also highlights the significance of context and long-term effects in the evolution of trust. The differentiations between factors that cause trust, trust itself, and outcomes (RTR) of trust are critical to the validation of the model; all the three component elements must be measured in order to fully test the model. The most problematic component of the model from the standpoint of measurement is trust itself; because trust is a willingness to be vulnerable, a measure that assesses that willingness is needed.

Rotter's Interpersonal Trust Scale was also highlighted; it is used to measure generalised trust of others. Lastly, Adeka's statistical and graphical approaches at estimating the measure of trust in Section 2.3.3 apply only to the case of secret sharing. This merely proves that the amount of trust in the secret sharing process is directly proportional to its number of participants (trustees).

2.11.3 The Three-Factor Security Assessment Process

The discovery of the 3-factor security assessment process, and its revolutionary derivatives calls for a redefinition or new understanding of the relationship between the terms 'Analysis' and 'Synthesis', as well as the intricate

relationship among the security assessment factors of risk, threat, and vulnerability, especially in the military.

A look up on security in dictionaries yields a general view that security is “freedom from danger, risk or loss.” In the context of this research work, the concern is about dangers, risks, and losses associated with computers, its information/data and network transactions. Fundamentally, the need for cryptography arose in response to the requirements to secure information, whether in storage or transit. The most primary security needs it sets out to address are confidentiality, integrity, availability, and authenticity.

In assessing security problems in a system, it is important to appreciate several characteristics of the system’s security posture. These must include the threats, vulnerabilities, and risks. Usually, in a systematic risk analysis to determine the potential problems in the security of a system, it is useful to create a matrix of the various threats and vulnerabilities associated with the system (Risk Assessment Matrix).

The object of every security assessment is the determination of possible Risk(s) relative to the asset to be protected, and that this risk could be systematically calculated quantitatively, using the Risk Assessment Matrix approach; with Threat(s) and Vulnerability (ies)y as inputs – hence, a 3-facor security assessment approach. This position is a direct consequence of the pragmatic conclusion in the last paragraph of Section 2.4. Other than this approach, the security assessment process could be anything but systematic; haphazard, uncoordinated and stressful. Though this approach is not entirely new in the civil security sector of the security industry, it is contrary to the norm in most armies throughout the world, with the exception of the US military (probably, with some allies), which discovered the anomaly in 1998 and took steps to rectify it by 2006.

As regards the reason (s) for the disparity in the practice between the civil and military elements of the security industry, the researcher discovered that

possible misconceptions (with the exception of Indian Army) surrounding the terms ‘Analysis’ (as employed in the treatment of the Intelligence Cycle; i.e., Intelligence Analysis) and ‘Synthesis’, were most probably responsible. This, in turn, is most probably a direct consequence of the military tradition of learning on the job, with few or no questions and as little room for prior theoretical knowledge as the situation permits. Hence, as a by-product or derivative of this research effort, Adeka [34] gives a detailed treatment of the security assessment/management processes and the intricate relationship that exists between the two evaluation terms/techniques of analysis and synthesis, with some revolutionary results which led to about five neologies listed in Section 2.6.6. The synopsis on the 3-factor security assessment process, as presented in Section 2.6.1., incorporates the novel Adeka’s Twin Risk Equations (ATREs) – Equations (2.28) and (2.29). Equation (2.28), the substantive equation, is illustrated in Figures 2.10 and 2.12.

The factual reality is that analysis and synthesis, as scientific methods, always go hand in hand; they complement each other. Every synthesis is built upon the results of a preceding analysis, and every analysis requires a subsequent synthesis in order to verify and correct its results. While analysis is a means to an end, synthesis is the actual end or resides at the end. This intricately interwoven relationship is aptly illustrated in Figure 2.9.

In an effort to resolve the anomalous disparity between the public and private segments of the security industry, it is posited that the public security industry should borrow a leaf from its private counterpart, by adopting the risk-based 3-factor security assessment process; as already done by the US Army.

The concepts of the human security perimeter and Adeka’s Web of Trust, as contained in the subtitle of this Thesis, “Extending the Human Security Perimeter through a Web of Trust”, are expounded in Section 2.4.3. At the heart of security concern is the issue of trust that is associated with the active variables in a system. Since the human factor is the most critical element in security systems, security perimeter could be defined in relation to the human trust level; via mutual positive identification of the correspondents/devices, using various means of authentication.

Adeka's concept of the web of trust has two component elements. The first element relates to a network (web) of trustees or participants in the business of secret sharing as expounded by Shamir. The second element has to do with the security which results from the web implementation of this research effort, which serves to enhance secret sharing via a secure and trusted website. The same trust instruments (a web of trusted associates and secure website) that engender the emergence of such a secure and healthy business environment could also be responsible for the extension of the individual human security perimeter, as a consequence of increased human confidence that the secret would be better secured.

A statistical proof for estimating the measure of human trust from the web is presented in Section 2.6.1. As illustrated in Figure 2.7, it could be proved that mathematically and sensibly speaking, as n increases in the (k, n) threshold secret sharing scheme, independent of 'k', the joint probability for the Secret getting lost/damaged or compromised decreases exponentially. By implication, since the joint probability of the Secret being safe is inversely proportional to that of its loss/damage ($P_{JL}T_n + P_{JS}T_n = 1.0$), it follows that the joint probability for safety increases exponentially, as n increases. Therefore, it would be reasonable to posit that, secret sharing increases or extends the human confidence/trust that is to be associated with the safety/security of the Secret Data, when compared to a situation where an individual keeps the Secret all alone. The resultant increased confidence/trust, due to enhanced safety/security, is engendered by the involvement of the network (web) of 'n' trusted associates or participants/trustees in the sharing scheme; and hence, the subtitle of this Thesis– 'Extending the Human Security Perimeter through a Web of Trust.

2.11.4 Cyber Threats Landscape

In the global village, the cyberspace, characterised by the prevalence of computer/Internet, is synonymous to ubiquity. In such a system, dominated by sundry criminals, where the IP traceback technology to every individual host is not yet a practical reality due to the ease with which IPs can be spoofed, the

turbulence in the cyberspace, given the prevailing threat landscape, could only be best imagined. Putting cryptography and the entire concept of security in proper perspectives, it must be noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. Due to its importance, the human factor could serve as a barometer for defining security perimeter. This underscores the significance of social engineering in every facet of security arrangement. As components of a security system, human beings are double-edged swords. They suffer from fatigue and can be distracted, tricked and even compromised. Due to their privileged accesses, when trusted people become compromised they can carry out attacks that outside criminals might find difficult to even contemplate. It is thus not surprising to discover that malicious insiders who represent only about 20% of actors in the cyber world are responsible for some 80% of the damages caused. This might spell doom for the prospect of a successful defence against socio-cryptanalysis (social hacking) when the trade becomes perfected.

It is noteworthy that, while technical means continue to improve in technical cyber defence, a lot needs to be done in social engineering to checkmate the rising trend of socio-cryptanalysis. The need to step up efforts at improving the security of passwords and pass-phrases, as it affects human attitude, cannot be over-emphasised.

2.11.5. Advance Fee Fraud (419)

Advance fee fraud (alias 419), which is also known as the Nigerian Scam, has grown into an epidemic [24]. The term ‘419’ was coined from Section 419 of the Nigerian Criminal Code (part of Chapter 38: Obtaining Property by False Pretences; Cheating) [208]. Basically, 419 is a form of confidence trick which the confidence artists use to defraud unassuming innocent business partners, both locally and globally. An example of a 419-transaction is illustrated in Figure 2.21, where Caller 2 gives his fake location as KANO (Location E; circled in Red) in his mobile phone conversation with Caller 1 at IBADAN (Location B),

while he is actually speaking from LAGOS (Location A). Please note that Caller 2 could have given his fake location as KUMASI (Location C) in Ghana or NIAMEY (Location D) in Niger or anywhere in the world, claiming to have roamed his mobile service. This necessitates some discussions on LBA in Chapter 5 and also underscores the significance of trust-centred human attributes in cybersecurity designs.

Chapter 3

PINs, Passwords and Password Security Purgatory

This brief treatment of password security will cover definition, significance, history, categories of access control tools, factors in the security of a password System, multiplicity of passwords with associated problems (storage, length, composition, and attitude), password repositories, security guidelines on password usage, security versus human factors and training/security awareness education. Deductions will close the chapter after an analytical presentation of a password survey on Africa, using Nigeria as a case study.

3.1 Definition and Significance

A summary of definitions indicate that a password or passphrase is a secret word/phrase, a string of characters, or some form of an interactive message or signal that is used for authentication; to prove identity or gain access to a resource/place [209, 210]. Thus, in a nutshell, a password is a basic method of access control. The main function of an access control system is to restrict the use of the resources to authorised users alone. In addition, it limits or defines the degree of access granted to every authorised user [211]. The word purgatory, in the context of this chapter, denotes a miserable situation that is of critical, complex and/or unusual difficulty [209].

3.2 History

From Polybius' description of the system for the distribution of watchwords in the Roman military [212], it is obvious that passwords or watchwords have been used since ancient times. In the military tradition, the password system operates as a pair of secret words or phrases; a challenge and response. For instance, in the opening days of the Battle of Normandy, paratroopers of the US 101st Airborne Division used the password flash, which was presented as a challenge, and answered with the correct response, thunder. The challenge and response were changed every three days. Similarly, the US paratroopers also used a device known as a "cricket" on 'D-Day', in place of a password system, as a temporarily unique method of identification; one metallic click given by the

device in lieu of a password challenge was to be met by two clicks in response [210].

Passwords have been used with computers since the earliest days of computing. MIT's Compatible Time-Sharing System (CTSS), one of the first time-sharing operating systems, was introduced in 1961. It had a login command that requested a user password. When the user typed in a password, the system would turn off the printing mechanism, so that the user might type in his password with privacy" [213]. The idea of storing login passwords in a hashed form as part of the Unix operating system was invented by Robert Morris in the early 1970s [214]. The system was based on a simulated Hagelin rotor crypto machine and first appeared in 6th Edition Unix in 1974. A later version of his algorithm, known as crypt (3)[5], used a 12-bit salt[6] and invoked a modified form of the DES algorithm 25 times to reduce the risk of pre-computed dictionary attacks [213].

3.3 Categories of Access Control Tools

Citing Furnell et al. [215], Jeslet et al. [118] noted that the means of user authentication include the following:

- Smart card or other tokens
- Fingerprint, Retinal image, {Iris & retinal identification and vein patterns [83]}, Voice and Facial pattern
- Password or PIN (Personal Identification Number)

Each approach has its strong and weak points. Regardless of the approach that is selected by an organisation, there is a trade-off between the value of the resources and the effectiveness and cost of implementation and maintenance. It

[5] In Unix computing, crypt is the name of both a utility program and a C programming function. Though both are used for encrypting data, they are otherwise essentially unrelated. To distinguish between the two, writers often refer to the utility program as crypt(**1)**, because it is documented in section 1 of the Unix manual pages, and refer to the C library function as crypt**(3)**, because its documentation is in manual section 3. [Online]. Available: http://en.wikipedia.org/wiki/Crypt_(Unix). [Accessed: 21 Oct. 2012].

[6] In cryptography, a ***salt*** consists of random bits, forming one of the inputs to a one-way function. The other input is usually a password or passphrase. The output of the one-way function can be stored with the salt rather than the password, and still be used for authenticating users ("ISC Diary – Hashing Passwords". www.Dshield.org). [Accessed: 24 Sep.,2012].

is also noteworthy that, despite significant advances in graphic-based approaches, the password remains the most common means of authentication [211], as well as the first line of defence against intrusion into a computer system [216].

3.4 Factors in the Security of a Password System

The security of a system that is protected using passwords depends on several factors. Among these is the need for the overall system to be designed for sound security, with protection against viruses, eavesdroppers and similar threats. Physical security against threats like shoulder surfing, video camera and keyboard sniffers should also be taken care of. Passwords should also be chosen such that they are hard to guess and also hard for an attacker to discover using any of the available automatic attack schemes. It is now common practice for the computer to hide passwords as they are being typed as a measure against bystanders reading the passwords. Since this practice may lead to errors and stress, thereby encouraging users to choose weak passwords, experts are now of the view that the system should be designed such that users have the option to show or hide the passwords as they are being typed [217].

Password strength is a measure of how effective is a password in resisting guessing and brute-force attacks. Usually, this is an estimate of how many trials an attacker who does not have direct access to the password would need, on average, to guess it correctly. The strength of a password is a function of length, complexity and unpredictability [218]. There are two main factors to consider in determining password strength. These are the number of guesses to find the correct password and the ease with which an attacker can check the validity of each guessed password. The first factor is determined by password length and its measure of randomness; this factor is under users' control. The second factor is determined by how the password is stored and used; this factor is determined by the password system design and beyond the control of the user. Effective access control may force extreme measures on criminals seeking to acquire a password or biometric token [219]. Less extreme measures may include extortion, rubber hose cryptanalysis, and side channel attack.

3.5 Multiplicity of Passwords and Associated Problems

The measure of carelessness associated with the use of passwords is amazing. However, studies have shown that most of the problems associated with the users' care-free attitude in respect of password usage have a lot to do with the multiplicity of passwords used by an individual [179]. Experience has shown that an active Internet user could have over 60 passwords and PINs for various applications and services; of these, those with the best memories might not be able to memorise up to 25% [220]. Thus, the resultant problems include storage, password length, and composition. As a result, in order to relieve the brain of undue stress, password users resort to attitudes that are inimical to the security of the passwords, and, by extension, security of the system they were designed to protect. These negative attitudes include:

- Writing all passwords in a diary
- Using the same password for all applications
- Relating the password to the particular application, e.g., using the room number and occupant's initials as access to the office door.
- Using very simple configurations such as 12121212, 12345678, or 1a2b3c4d.
- Pasting passwords on the wall, board or computer, etcetera.

The security risk associated with this practice is widespread, as a study showed that 50% of users wrote their passwords down [216].

3.6 Password Repositories

The multiplicity of passwords has engendered the problem of password storage. This has given rise to many software applications designed to facilitate password management. These are collectively called wallets and are in two different varieties. The first is a username/password repository; an encrypted file kept in one's computer that holds information which one needs to log into one's various accounts. The most prominent of these is Darn! Passwords! [220, 221]. It has a password generator that can make up passwords for various applications and allows one to drag one's passwords into the application or Web site that one is using. It allows one to remember only one password

instead of many. Similar applications are Password Safe [222] and QWallet [223], both for windows. Selznick PassWallet [224] provides similar functionality on the Macintosh and Palm OS. Apparently, no similar product exists for Unix or Linux.

In addition to a password, the other type of wallet programme holds other information that a user might need in accessing a Web site, and also aims at moving from one site to the other without re-entering the information [220]. The most prominent application in this category is Microsoft's Passport [225] which is targeted at consumer-oriented shopping sites. The Passport server maintains personal information about the customer (e.g., credit-card numbers, shoe size, etcetera) and passes on this information, with permission, to the sites that the customer visits. Passport works only with participating merchant site, so the user still needs to keep track of passwords and usernames to other sites. Note that in an effort to make the service as general as possible, Microsoft did not protect the re-direction at the beginning of a Passport session by SSL [226], this is one of the several risks in its protocol [220]. From the foregoing, the problem of password storage remains unresolved, since the computer itself could be stolen, damaged or hacked.

3.7 Security Guidelines on Password Usage

It is usually better to have passwords centrally controlled, if possible. Whatever the case, in order to improve the strength of access security, the following guidelines should be followed in the use of passwords [179]:

- It should be kept absolutely secret; not divulged to any other user
- It should not be written down or recorded where it can be accessed by other users.
- It must be changed if there is the slightest indication or suspicion of a compromise.
- It must be changed when a member of the organisation leaves the group or changes task
- It should be at least eight characters long (alpha-numeric with mixed case/symbols) [210].

- ❖ It should not be formed from any obvious source; e.g. username or group/company/project name, family name or initials or partner's name, months of the year or days of the week, car number plate registration, nicknames/pet names, telephone numbers, all numeric or all alphabetic characters and more than one consecutive identical characters).
- ❖ It must be changed monthly or at least bi-monthly.
- ❖ It must be changed more frequently the greater the risk or more sensitive the assets being protected.
- ❖ It must not be included in an automated log-in procedure, i.e. not stored in a macro function.
- ❖ It should not be a dictionary word [210].

3.7.1 Guidelines for Strong Passwords

Guidelines for choosing good passwords are designed to make passwords less easily discovered by intelligent guessing. Common guidelines include [227], [228]:

- ❖ A minimum password length of 12 to 14 characters if permitted
- ❖ Generating passwords randomly where feasible
- ❖ Avoiding passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., ID numbers, ancestors' names or dates).
- ❖ Including numbers and symbols in passwords if allowed by the system
- ❖ If the system recognises case as significant, using capital and lowercase letters
- ❖ Avoiding using the same password for multiple sites or purposes
- ❖ Avoid using something that the public or workmates know you strongly like or dislike
- ❖ Use acronyms of mnemonic words/phrases
- ❖ Providing an alternative to keyboard entry (e.g., spoken passwords, or biometric passwords).

- ❖ Requiring more than one authentication system, such as 2-factor authentication (something you have and something you know).
- ❖ Write Down Passwords

From the above, it is clear that experts are now divergent as regards whether it is better to write down the passwords or not. Some guidelines advise against writing passwords down, while others, noting the large numbers of password protected systems users must access, encourage writing down passwords as long as the written password lists are kept in a safe place, such as a wallet or safe, not attached to a monitor or in an unlocked desk drawer. Schneier [228] noted that:

> "Simply, people can no longer remember passwords good enough to reliably defend against dictionary attacks and are much more secure if they choose a password too complicated to remember and then write it down. We're all good at securing small pieces of paper. I recommend that people write their passwords down on a small piece of paper, and keep it with their other valuable small pieces of paper: in their wallet."

In addition, some even argue that the concept of password expirations is obsolete [229]**,** for the following reasons:

- ❖ Asking users to change passwords frequently encourages simple and weak passwords.
- ❖ If one has a truly strong password, there is little point in changing it. Changing passwords which are already strong introduces the risk that the new password may be less strong.
- ❖ A compromised password is likely to be used immediately by an attacker to install a backdoor, often via privilege escalation. Once this is accomplished, password changes won't prevent future attacker access.

- ❖ Mathematically it does not gain much security at all.

    - Moving from never changing one's password to changing the password on every authenticate attempt (pass or fail attempts) only doubles the number of attempts the attacker must make on average before correctly guessing the password in a brute force attack; one gains much more security by just increasing the password length by one character than changing the password on every use.

However, Password expiration serves two purposes [230]:

- ❖ If the time to crack a password is estimated to be 100 days, password expiration times fewer than 100 days may help ensure insufficient time for an attacker.
- ❖ If a password has been compromised, requiring it to be changed regularly should limit the access time for the attacker.

3.7.2 Guidelines on Password Management

A password management system is an administrative arrangement aimed at providing an effective interactive resource that ensures the quality of the passwords and enforces their use in tune with the security manager's policy. In general, password management should enable secure login procedures and protect passwords against unauthorised use and access [179]. This includes measures which ensure that passwords are stored in files that are separate from the main application system data, using a one-way encryption algorithm. These measures offer some protection against password cracker programs and dictionary attacks.

As part of the separation process between the client and the producer, the initial (default) passwords from the manufacturer must be replaced after equipment installation. The management must ensure that no protected asset is accessed without submission of the correct password. Where users are allowed to choose their own passwords, a re-confirmation, by re-typing a new password definition, should be made compulsory. Password changes should be enforced at

predetermined intervals and a record of the changed passwords should be kept to prevent recycling [179].

While users may be allowed the choice of password data, password policy and implementation should be centrally controlled and formally managed as follow:

- Users should sign a declaration, undertaking to keep personal passwords confidential
- Passwords should be conveyed in a secure manner, and avoid distribution by telephone, third parties, e-mail and normal internal mail; receipt of the password should be acknowledged by users.
- Initial passwords should be forcibly changed after the first usage
- Temporary passwords should be issued, in the event that a user forgets his password.

Apart from gaining intrusion through the access indiscipline of security personnel, there are many logic approaches of gaining unauthorised access to security equipment and protected data. The challenge and response procedure is an accepted way of dealing with the logic intruders. This is discussed in the next section [179].

3.7.3 Logic Challenge and Response Procedure

The challenge/response control is a form of access control which is designed to resist the threats to user authentication by such activities as spoofing [179]. The procedure is based on something known to the user (password, PIN, etc.) and something possessed by the user (a chip card, dongle, etc.). As illustrated in Figure 3.1, the user starts an entry procedure by inserting a smart card into an encryption device or a remote computer function to access files. The destination unit generates a random number which is transmitted to the user's terminal as a challenge. In response, the user enters his password, and the two values are presented to a cryptographic algorithm, such as a hash function, which generates a response result to the inputs of the challenge and password. The resulting username response is transmitted back to the source security module where the remote username response is verified by comparing it with the

expected value stored in the source module. Upon successful verification, the user is allowed access to the desired function; otherwise, access is denied.

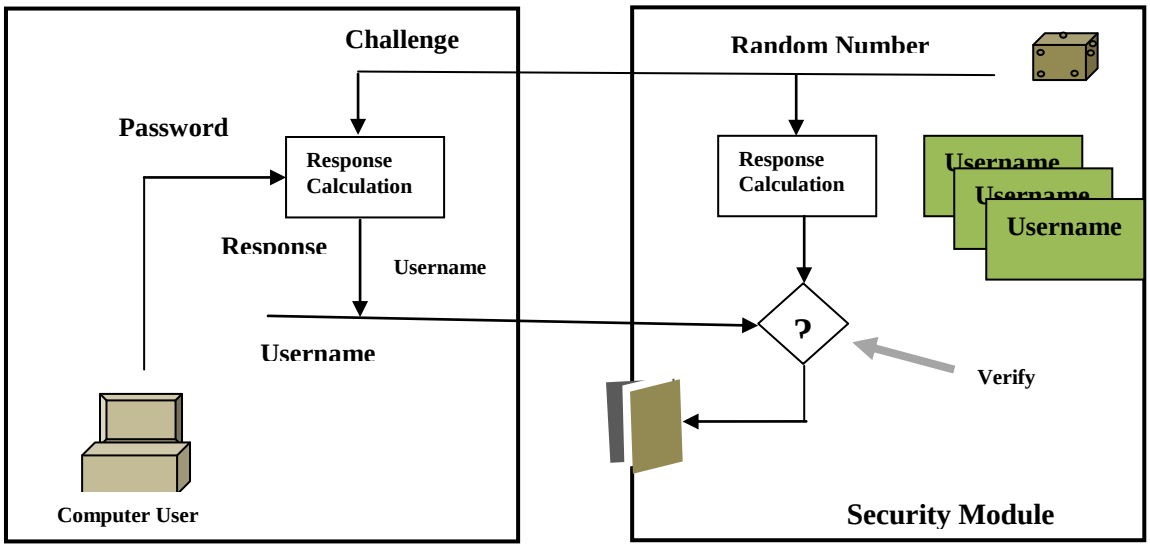


Figure 3.1. Challenge/response method of access control [1]

3.7.4 Password Security versus Human Factors

A synthesis of security guidelines for password usage shows that there is no common standard for passwords; different systems have different requirements. If this situation is analysed against the backdrop of the fact that an average user has several passwords, all of which are expected to be strong, in conjunction with unavoidable human fallibility, it is obviously impracticable for any human being to combine all the conditions associated with the password system. Thus, since it is the security of the total system (online, offline, physical, procedural and logic) that is important, it is necessary to think of passwords that would take both human and security factors into consideration [216]. Therefore, in order to ensure password security, there is a need to strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions that would, in turn, compromise security.

The above conclusion buttresses the significance of social engineering in security designs and the fact that security is indeed a function of both technology and social engineering. Unfortunately, most of the literature materials are only concerned with having strong enough rules; only three articles encountered in this research process focused on the pitfalls of having too stringent password regulations [216, 231, 232].

3.7.5 Training and Security Awareness Education

Every organisation should have a security awareness training policy which ensures that organisations are responsible for not only training their own personnel but also their agents and contractors that have access to their facilities. Initial training will need to include a review of the requirements and tailored training needs to specific security policies, processes and technology of one's organisation based on the level of security responsibilities for different segments of users.

A security training program should include awareness education covering the organisational security policy, password maintenance, incident reporting, and viruses; periodic security reminders conducted as updates to the basic security education; user education concerning virus protection, including identification, reporting and prevention measures; user education in importance of monitoring log-in success/failure, and how to report discrepancies, including employee responsibility for ensuring security of information; and user education in password management, including organisational rules to be followed in creating, changing and ensuring confidentiality of passwords [233]. Personnel should also be informed of the need for the various techniques employed in the organisation's password security architecture, which are highlighted herein, as an important means of checkmating social hackers (socio-cryptanalysts).

3.7.6 Password Security Architecture

Common techniques used to improve the security of computer systems protected by a password include:

- ❖ Not displaying the password on the display screen as it is being entered or obscuring it as it is typed by using asterisks (*) or bullets (•).
- ❖ Allowing passwords of adequate length.
- ❖ Requiring users to re-enter their password after a period of inactivity (a semi log-off policy).
- ❖ Enforcing a password policy to increase password strength and security.
- ❖ Using encrypted tunnels or password-authenticated key agreement to prevent access to transmitted passwords via network attacks.
- ❖ Limiting the number of allowed failures within a given time period (to prevent repeated password guessing). After the limit is reached, further attempts will fail (including correct password attempts) until the beginning of the next time period. However, this is vulnerable to a form of denial of service attack.
- ❖ Introducing a delay between password submission attempts to slow down automated password guessing programs.

Some of the more stringent policy enforcement measures can pose a risk of alienating users, possibly decreasing security as a result.

The survey on password security is discussed next. This is designed to gauge the attitude of computer users towards password security as a major vulnerability point in cyber defence.

3.8 A Survey on Password Security Awareness in Developing Countries

Internet world statistics [181] show an increase in the number of Internet users across the world. This is illustrated by six global statistics as follow: December 31, 2000 – 360,985,492 (Africa: 4,514,400; i.e., 1.25%); March 31, 2011 - 2,095,006,005 (Africa: 118,609,620; i.e., 5.66%); December 31, 2011 - 2,267,233,742 (Africa: 139,875,242; i.e., 6.17%); June 30, 2012 - 2,405,518,376 (Africa: 167,335,676; i.e., 6.96%); June 30, 2014 - 3,035,749,340 (Africa: 297,885,898; i.e., 9.81%); and June 30, 2016 – 3,631,124,813 (Africa: 340,783,342; i.e., 9.38%). These statistics show that the use of Internet by the developing world, using Africa as a case study, is not only increasing by population, but also by global percentage. Hence, this research

effort [234] became interested in finding out the state of Internet security awareness by conducting a survey between February and August 2012, in an African country. The target population was the organisational executives from the level of Senior Enterprise Officer and above. Altogether, 66 officials aged 30 upwards responded; all these responses were used to plot Figures 3.2 and 3.3, while 26 responses, picked at random, were used to plot Figures 3.4 and 3.5. Figures 3.2 and 3.3 covered responses from 3 organisations, while Org. 4 is the grand total of responses from all the three organisations, to reflect the national statistics. Figures 3.4 and 3.5 analyse the responses by rank (and age; to some extent). Only three of the eleven questions in the questionnaire were used in this analysis; Questions 2, 4 and 5. The questionnaire is attached as Appendix 2.

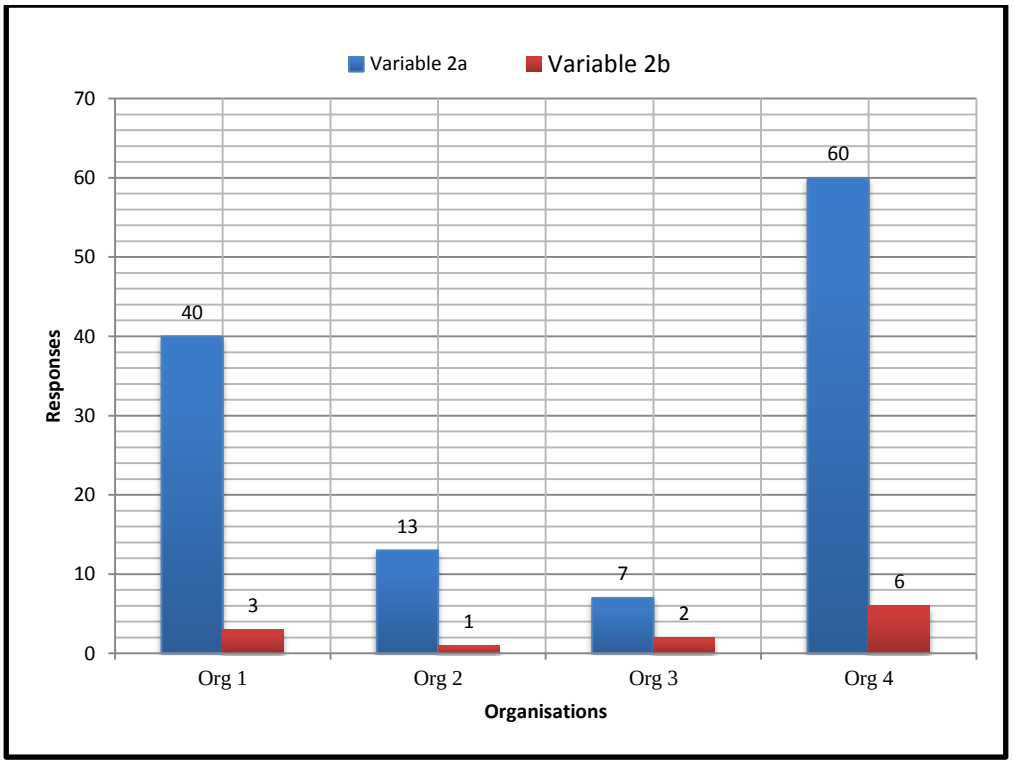


Figure 3.2. Level of password awareness (2a = Yes; 2b = No)

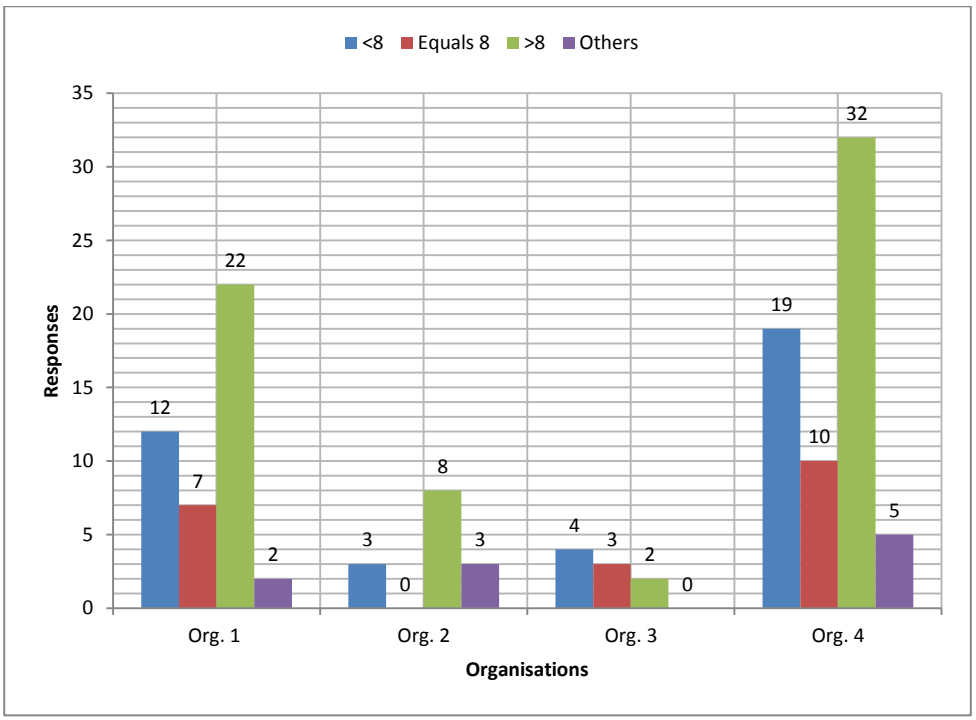


Figure 3.3. Significance of password length awareness

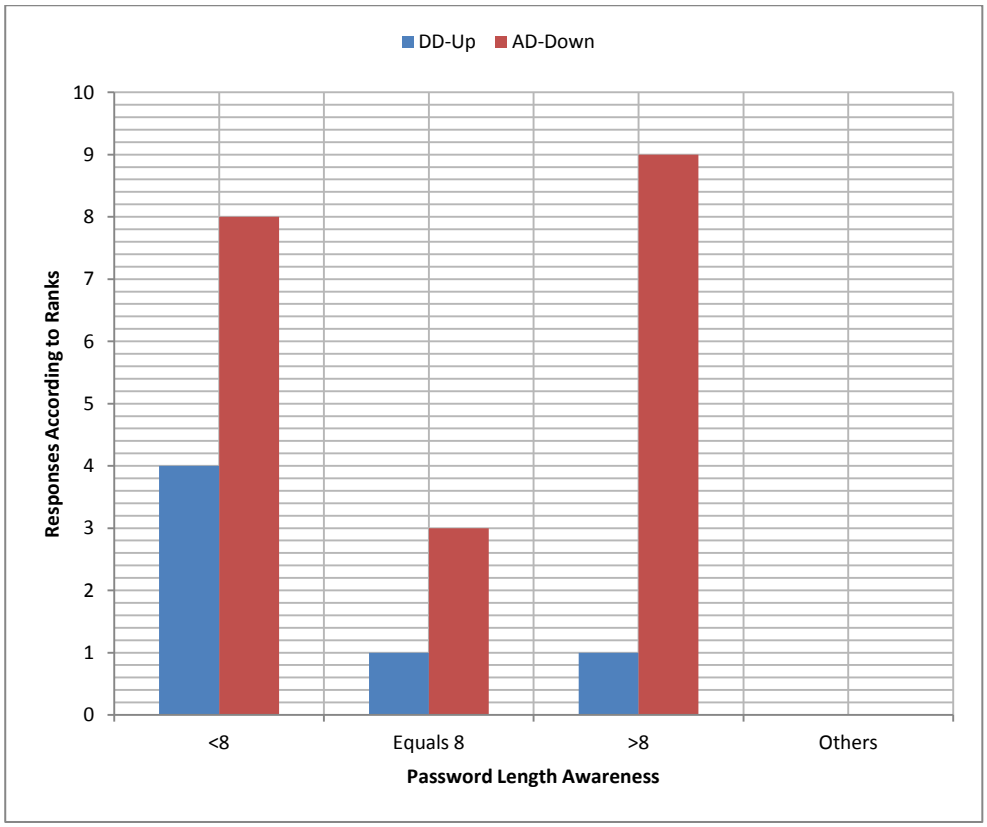


Figure 3.4. Significance of password length awareness

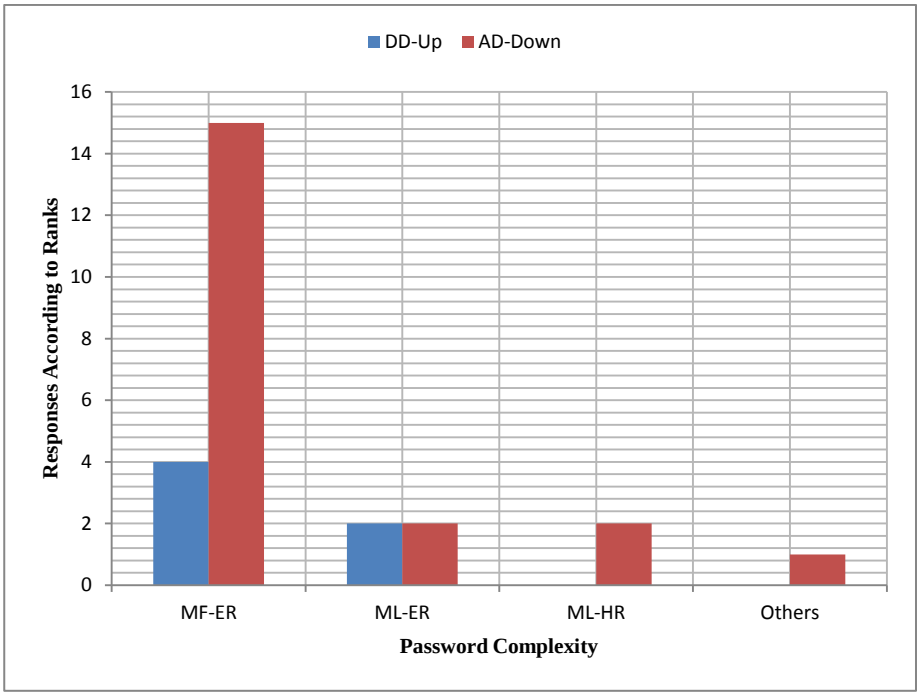


Figure 3.5. Significance of password complexity awareness

Figure 3.2 reflects the answers to Question 2: “Do you have a password for granting or denying access to your computer?” - answer Yes or No. The bar labelled Variable 2a represents Yes, while the maroon-coloured bar represents No. Figure 3.3 reflects the answers to Question 4 by the organisation: “What is the length of your email password?” – Answers: Less than eight characters; eight characters; more than eight characters; and others (please describe). Figure 3.4 analyses responses to Question 4, by rank, seniority or appointment: DD-Up means from Deputy Directors upwards; AD-Down means from Assistant Directors downwards. Figure 3.5 reflects responses to Question 5: “What is the nature of your passwords?” – Answers: Meaningful/easily remembered (MF-ER); Meaningless/easily remembered (ML-ER); Meaningless/hard-to-remember (ML-HR); Others (please describe).

Looking at the national statistics from this survey, Figures 3.2 and 3.3 show that the levels of awareness are generally okay, but the percentage of users with passwords less than eight characters in Figure 3.3 is too high for comfort. Figure 3.5 also shows a satisfactory result with the same caveat as in Figure 3.3. This result also illustrates the possibility that organisational administrators from AD-Down (about the age of 40 downwards) are not only more active on

the Net but also more security-conscious; the implication is that they take instructions from their less security-conscious superiors. Lastly, Figure 3.5 confirms the fear that most Internet users are inclined to choosing passwords that are both meaningful and easily remember-able.

3.8.1 The Password Security Problem

It is posited in this work that destitution of requisite balance between the factors of technology and factors of 'humanity', as defined by Spinellis [235], is responsible for the purgatory posture of password security related problems.

This is because security countermeasures mostly focus on partial security in favour of technology, using various cryptographic encryption techniques, to the detriment of total security incorporating humanity; bearing in mind the prevalence of social engineering realities. This is contrary to the criminal cyberattack strategy which is mostly social engineering based.

Fundamentally, the need for cryptography arose in response to the requirements to secure information, whether in storage or transit. The most primary security needs it sets out to address are confidentiality, integrity, availability, authenticity, theft and non-repudiation [236]. In the case of social engineering (SE), a taxonomy of user vulnerabilities include dishonesty, honesty, vanity, compassion, gullibility, curiosity, courtesy, diffidence, apathy, irresponsibility, naivety and greed [16, 17]. Thus, SE could be seen as a glorified nomenclature for what is popularly referred to as 419 in Nigeria.

Most existing security arrangements, both in theory and practice, seem to underplay the significance of the social aspect of cyber defence. Examples include the ITU's blueprint for ensuring a global culture of cyber-security (Table 1.1), which failed to assign the responsibility for the social culture of cyber-security to any group of professionals [19-21]. This underestimate of the significance of social engineering input in cyber defence is also indicative of the current UK National Cybersecurity Programme (NCSP) which has allocated only one percent to education [20]; out of the £650 million ($1.01 billion) earmarked for cyber-security in the next five years (2011-2015).

3.8.2 Proposal for a Suggested Solution

In an effort to minimise the password security purgatory phenomenon, it is noted that the human factor is the most critical factor in the security system for at least three possible reasons: it is the weakest link; it is the only factor that exercises initiatives; and the factor that transcends all the other elements of the entire system. This underscores the significance of social engineering in every security arrangement. It is thus recommended that, in the handling of password security issues, human factors should be given priority over technological factors.

It is realised that most of the password security-related problems have linkages with the lack of secure storage system; thus encouraging users to choose weak passwords and compelling security engineers and managers to insist that passwords must not be written down and must be changed frequently. Hence, in an effort to make a contribution towards resolving this problem, this research [8] will explore the use of the (k,n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of password repository. This presupposes an inclination towards writing down the password: after all, gold and silver are not memorised; they are stored.

This brings the discussions on password security to a close, except for the deductive summary which follows immediately in the next section. This also completes all requisite background components for the implementation of the main research design on secret sharing in Chapter 4.

3.9 Deductions

As a basic method of access control, passwords constitute the first line of defence in most computer-based information security systems. However, the measure of user's carelessness relative to password security is amazing. Studies have shown that most of the problems associated with the users' care-free attitude have a lot to do with the multiplicity of passwords required of every user. Experience shows that an active Internet user has over 60 passwords and PINs for various applications and services; of these, those with the best memories might not be able to memorise up to 25%. Thus, the resultant

problems include storage, password length, and composition. As a result, in order to relieve the brain of undue stress, password users resort to attitudes that are inimical to password security. The security risk associated with such attitudes is widespread, as a study showed that 50% of users wrote their passwords down.

Experts are now divided as regards whether it is better to write down the passwords or not. Due to a large number of password protected systems that users must access, some experts encourage writing down passwords as long as the written password lists are kept in a safe place, such as a wallet or safe; not attached to a monitor or in an unlocked desk drawer. Similarly, some even argue that the concept of password expirations is obsolete because mathematically, the practice of changing passwords frequently does not gain much security at all; one gains much more security by just increasing the password length by one character than changing the password on every use.

A synthesis of security guidelines for password usage shows that there is no common standard for passwords; different systems have different requirements. If this situation is analysed against the backdrop of the fact that an average user has several passwords, all of which are expected to be strong, in conjunction with unavoidable human fallibility, it is obviously impracticable for any human being to observe all the conditions associated with the password system. Thus, since it is the security of the total system that is important, it is necessary to think of passwords that would take both human and security factors into consideration. Hence, in order to ensure password security, there is a need to strike a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. This conclusion buttresses the significance of social engineering in security designs and the fact that security is indeed a function of both technology and social engineering.

As part of security training and security awareness education, organisational personnel should also be acquainted with the need for the various techniques employed in the organisation’s password security architecture, as an important

means of checkmating social hackers (socio-cryptanalysts). From the foregoing, the security of passwords remains a purgatory issue. Thus, the significance of continual security training and awareness education in all organisations cannot be over-stressed.

Chapter 4

Cloud Data Repository Secure Access Prototype Design, Implementation, Practical Results and Discussions

Chapter 4 discusses the Cloud Data Repository Secure Access Scheme Prototype (CDRSAS-PT), which is a web-based authentication system. It is primarily designed to implement the sharing, distribution and reconstruction of a sensitive secret data; e.g., a combination key for firing a nuclear missile, the access code for a flow station, the Coca-Cola formula or any highly sensitive data that could compromise the functioning of an organisation, if leaked to unauthorised person (s), and the loss of which spells doom for the organisation. This is carried out in a secure web environment, globally. It is a threshold secret sharing scheme, designed to extend the human trust security perimeter. Though primarily designed as a secret-sharing system, it could be adapted to serve as a cloud data repository and secure data communication scheme.

A secret sharing scheme is a method by which a dealer (appointed by an organisation) distributes pieces (shares) of a secret data to a group of people (trustees), such that only authorised subsets of the trustees can reconstruct the secret. Secret sharing schemes are important tools in cryptography which are used as a building block in many secure protocols; e.g., a general protocol for multiparty computation, Byzantine agreement, threshold cryptography, access control and attribute-based encryption.

This chapter highlights the web design concept, the design/implementation and presents its performance characteristics, practical results and discussions. In a nutshell, the chapter is a brief summary of the layout and functions of the 15-page secure server website prototype. This is the main focus of the PhD research effort titled, ‘Cryptography and Computer Communications Security: Extending the Human Security Perimeter through a Web of Trust.’ These include the Admin, Login, Secure Share, and Secret Data web pages. Apart from issues relating to connectivity and database, some of the prototype functions are also represented in the Use Case Diagram, Sequence Diagram

and State Diagram, as contained in Figures 6.5 – 6.8, which also illustrate the design steps. It also highlights the novelties or areas of new knowledge that have been accomplished in the secret sharing scheme as at date. This chapter ends with a basic comparison of the CDRSAS-PT and the SSSS algorithm, using security and four QoS metric parameters; namely, server bandwidth, system scale, service capacity ratio and real-time performance (time delay).

4.1 Web Design and Implementation

The design concept envisaged the engineering and development of a web-based system that displays a real-time digital clock (showing the GMT or UTC timing), with some form of authentications (password, username, SMS code, GPS location data and share code) prior to access authorisation, for security purposes. It should also display a timer (down counter). Supposing that a secret item (e.g., a password) is shared among five participants who are scattered around the world; say one each in Russia, China, Nigeria, USA, UK, etc., and each of them has only a fraction of the Secret, which is grossly insufficient to determine the whole secret. It is required that at least three or more fractions of the password domiciled in any three or more of the above countries must be assembled in order to reconstruct the whole password. In the event that the password in use by the rightful owner or authority is missing or gets destroyed, some of the participants with fractions of it would be required to recombine or reconstruct it from their different locations around the world. Each of them would be required to enter his/her own fraction of the password on the website within a specified period of time (say a 5-minute time window; e.g., between 1420 and 1425 hours GMT of a given date) so that the entire password would be reconstructed at a designated GPS location, as may be directed or configured by the Dealer (share coordinator or administrator of the website).

The website, as conceived above, was designed and implemented using HTML5, PHP, Java, Servlets, JSP, Javascript, MySQL, JQuery and CSS. It was also launched and successfully tested for various performances. The codes are written in Eclipse IDE. These are running on Tomcat and Apache databases using XAMPP Server. For the prototype, the input data (the Secret to be shared) is generated by the computer and divided into ‘n’ Shares (n = 5), and at

least ‘k’ or more Shares (k =3) are required to reconstruct the secret data; each of the three Shares is logged into the prototype web page using a different web browser window, to simulate different locations. If the computer hosting the server can be port-forwarded, the CDRSAS-PT utilises Shamir’s Secret Sharing Algorithm, MD5 encryption and user registration methods to securely create and share data through a web browser in a Wi-Fi configuration; or using the local host in a wired LAN. Such transmitted shares could be received anywhere in the world, provided there is Internet accessibility. A summary of the detailed functions of the CDRSAS-PT is in Appendix 6, while its JUnit test results are in Appendix 7.

Screenshots of real web pages from the CDRSAS-PT are also displayed in this chapter. In order to run the server via the localhost: start up the Tomcat server (Java) in Eclipse, Apache (PHP) and MySQL (database). Point the browser to http://localhost:8080/secretshare/ (‘secretshare’ being the appropriate file name; this could be changed). Each user must be registered to access the system. When the user registers, the password and GPS coordinates could be encrypted using MD5.

The pictorial impression of the layout for the CDRSAS-PT, when in operation, is as presented in Figure 4.1. Its geographical coverage is depicted in Figure 4.2, while its equipment components and requisite input data necessary to enable a user to gain access to the system are as shown in Figure 4.3. All the components used in building the system are open-source.

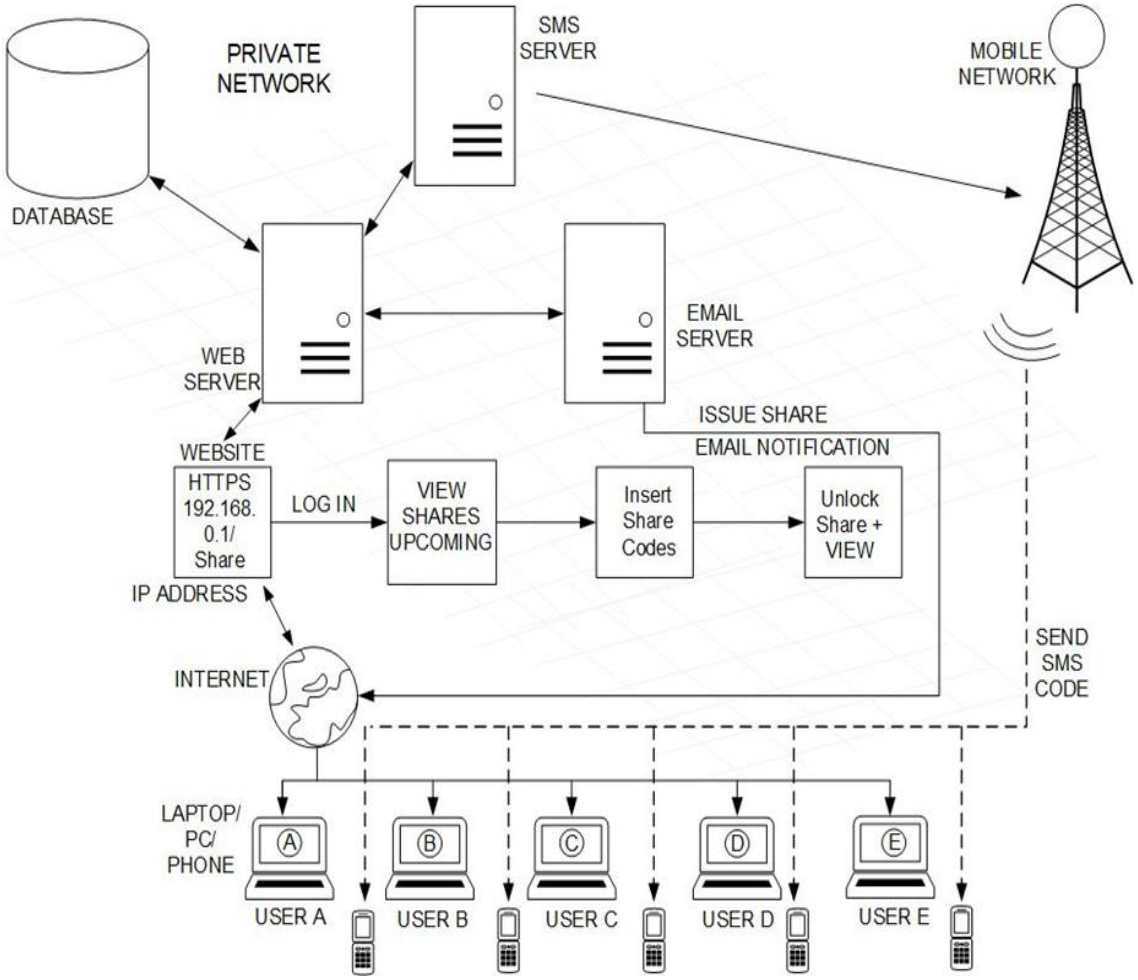


Figure 4.1. Pictorial impression of the layout for the CDRSAS-PT; when in operation

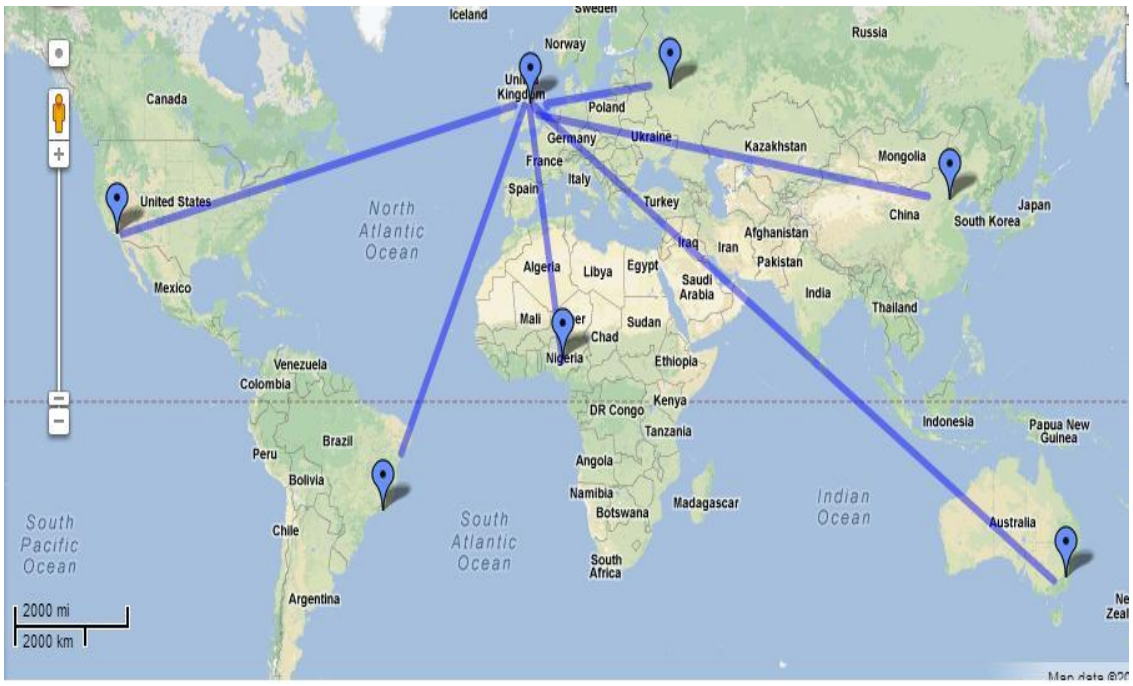


Figure 4.2. CDRSAS-PT employing a secure server at the School of Electrical Engineering and Computer Science, Faculty of Engineering and Informatics, University of Bradford, United Kingdom, with a client each at Los Angeles, USA; Rio de Janeiro, Brazil; Abuja, Nigeria; Canberra, Australia; Beijing, China; and Moscow, Russia.

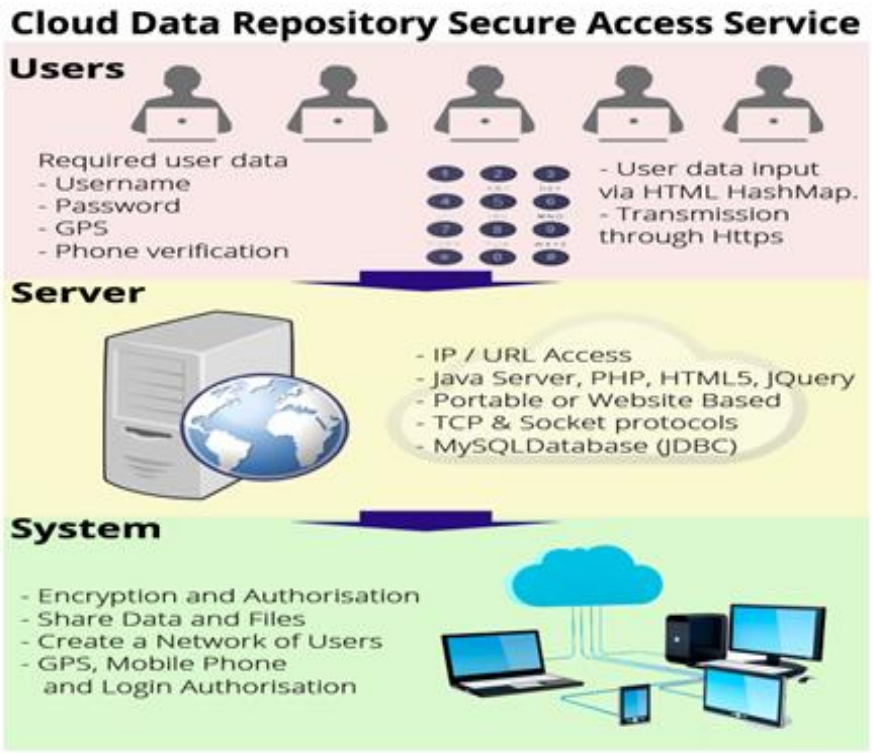


Figure 4.3. Equipment components and requisite input data necessary to enable a user to gain access to the CDRSAS-PT

4.2 Connectivity

The system currently runs on a laptop via local host within a typical home router, using Wi-Fi. Remote access to this system can be achieved by setting up port forwarding on the router. This is required because the IP address in the home environment is usually dynamic. The laptop running the server will have an internal IP address: 192.168.x.x (which can be viewed in the command prompt by typing ipconfig). This IP needs to be registered in the router settings for port forwarding. Once this is set, the router will forward any requests on port 8080 (port could be different) to the local host on 192.168.x.x:8080/secretshare/ - which is the login page. The next stage is to find the external IP address of the local router, which can be obtained via a simple Google search. Then any remote users can point their browsers to <router-ip-address>:8080/secretshare/ and start using the sharing system. The server can also be remotely accessed through a wired LAN with an appropriate switch. The prototype has been successfully demonstrated using both techniques. Using port forwarding as described above, the server can be accessed from anywhere in the world.

4.3 Database

The database, Java class structure, has the main class DB_SecureShare that extends the MYSQLDB connection class. It also implements the UserDAO interface to allow for extension and maintainability. The Apache database currently stores prototype trial personal information for five users; Username, Password and GPS data. The setting is illustrated in Figure 4.4.

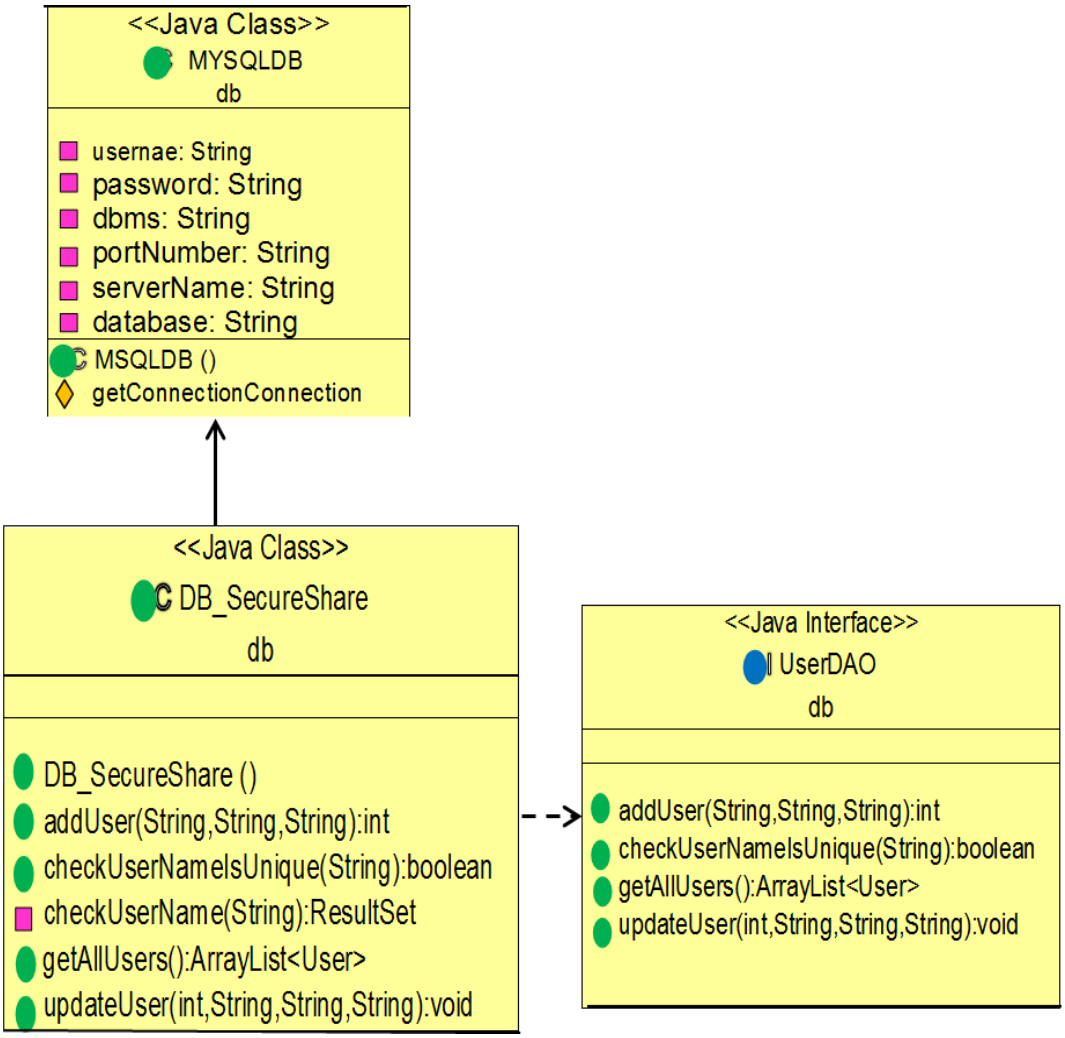


Figure 4.4. Java class structured database

4.4 Summary of Design Steps

Generally, the design steps follow the Waterfall model, which is illustrated in Figure 4.5.

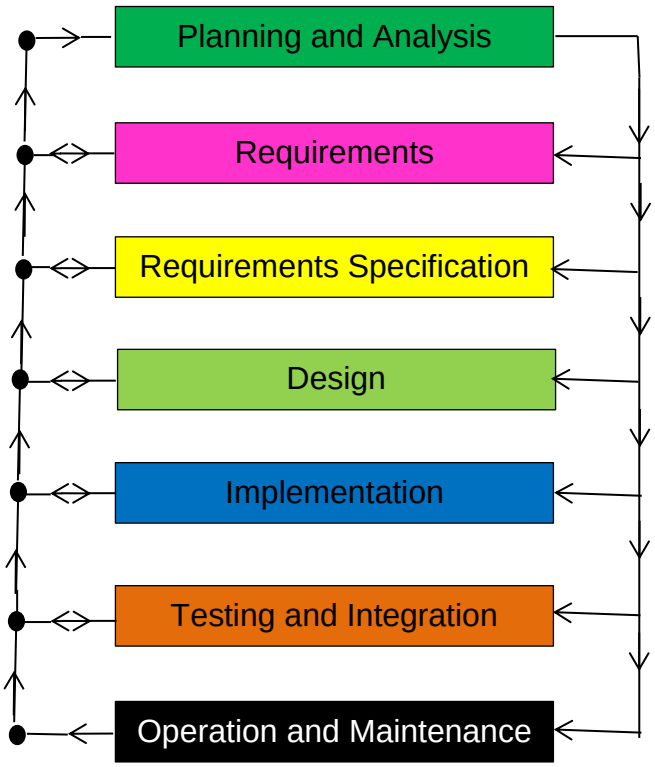


Figure 4.5. Web design steps: the waterfall model

Figures 4.6 – 4.8 show the Use Case Diagram, Sequence Diagram and the State Diagram for the CDRSAS-PT, respectively. It is clear from these illustrations that, the prototype algorithm requires three security data entries to accomplish a successfully authenticated entry by every user. These are in addition to the usual login details, such as passwords and username.

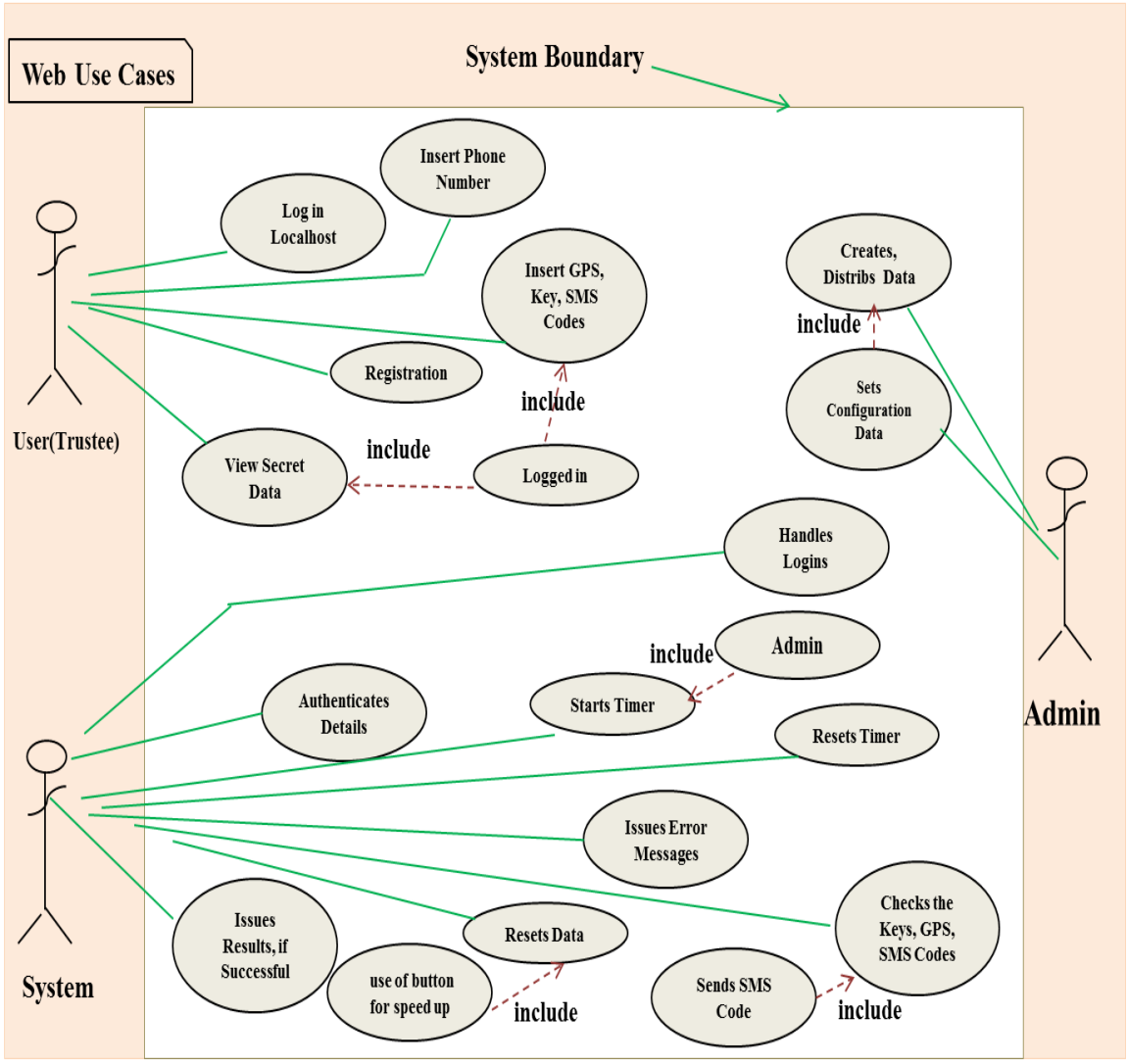


Figure 4.6. Use case diagram

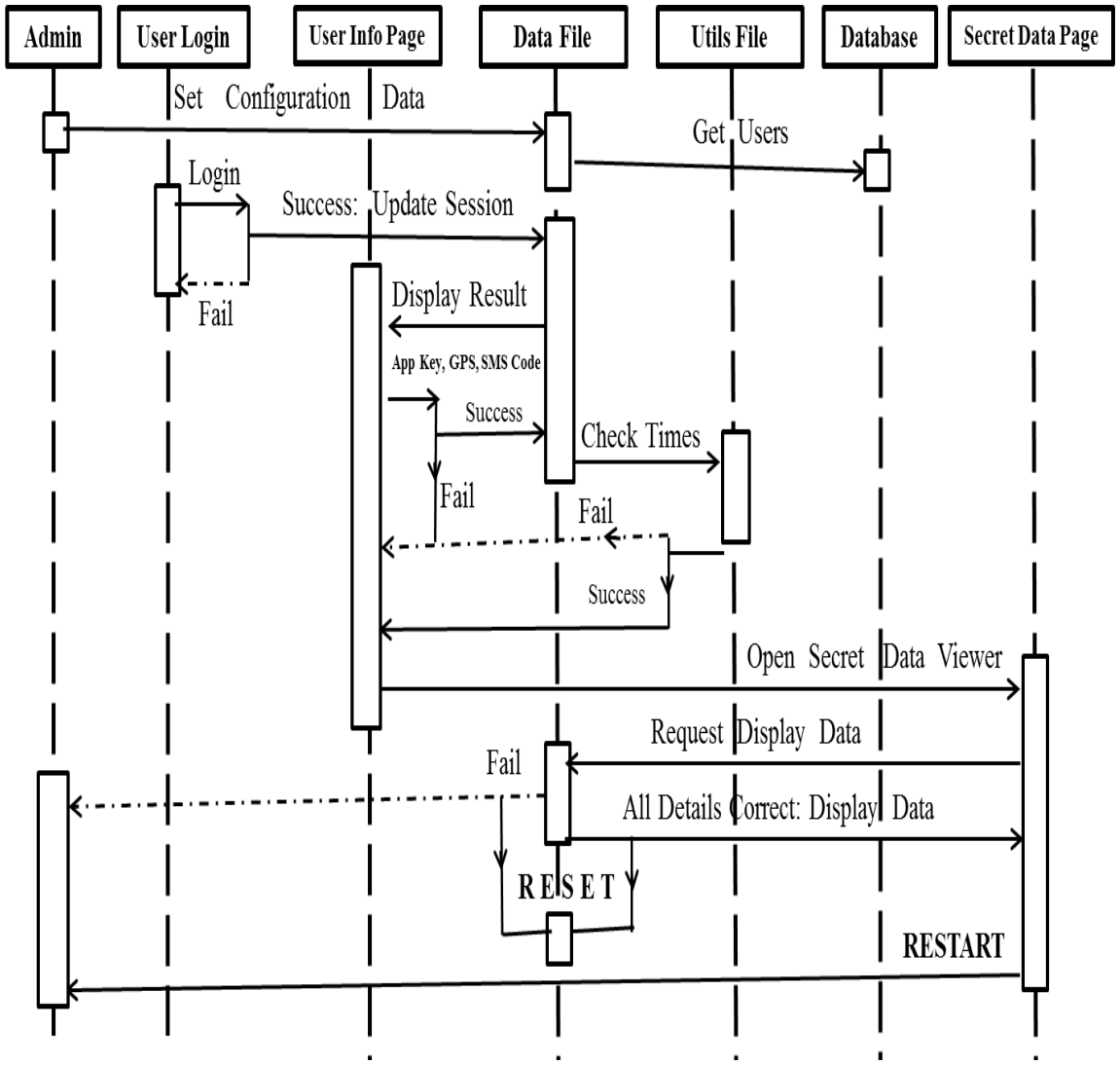


Figure 4.7. Sequence diagram (nb: 'restart' is a default after the recovered data has been shown, following the submissions of all keys, GPS and SMS codes)

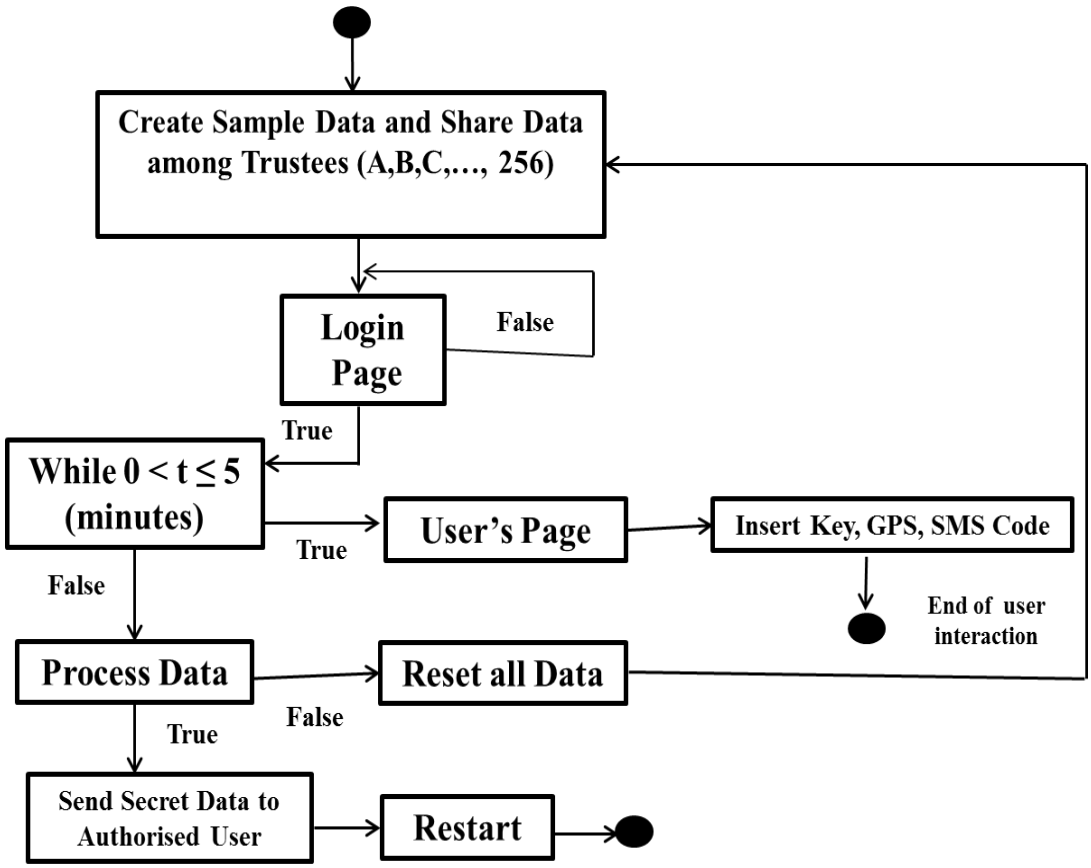
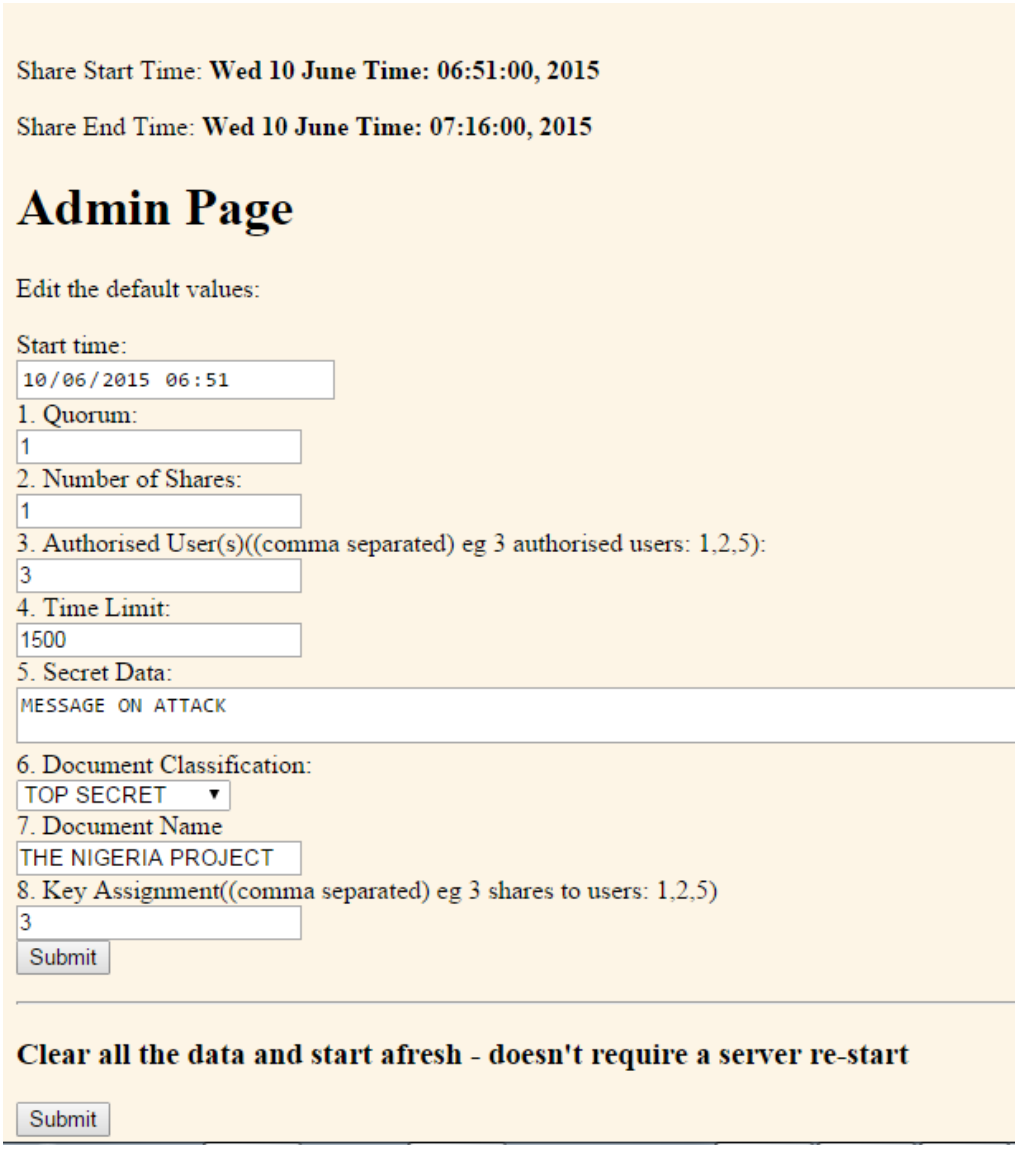


Figure 4.8. State diagram

4.5 Admin Web Page

The Admin web page can only be viewed by the user on the server side within the local host; any external connections are denied. This page must be fully configured before a session can commence. For instance, if the start time on the Admin page has not been set, then the user cannot log in. When the Admin sets the start time and the time duration is specified, the end time which is automatically calculated from these is also displayed. The default format for HTML5 date-picker is used for the date and user display time. All the values can be set as in Figure 4.9 (a); illustrating a quorum of one out of one shares (this is a default setting for testing purpose; the setting may also be used when an individual wishes to adapt the system for use as a cloud data repository scheme). It is also on this page that the sharing process can be restarted to begin another session, after a successful recovery of a secret data in the previous session, or to repeat the previous session in the event of a failure.

Point 3 allows the user who is authorised to view the data to be selected. Point 8 allows the keys to be assigned to specific users; in a given situation where not all registered users participate, and the shares are not serially assigned according to the database serialisation. Page 2 of the Admin web page (Master Share Details) displays part of the results of the settings configured in Figure 4.9 (a), as shown in Figure 4.9 (b); this is to assist while testing the prototype. Once the form in Figure 4.9 (a) is submitted, the system sends the information to Shamir's Secret Sharing Algorithm.



(a)

Figure 4.9: (a) Part of page 1 of Admin page; (b) Part of page 2 of Admin page

This encrypts the data and returns a number of keys based on the setting above. The system uses HTTP GET request to use SSSS API. The system uses the GSON library to parse the data into a DTOSecret object. A sample JSON is:

{“timeStart”:”1368221578”,”secretKeys”:[“0101596f75”],”numberOfShares”:”1”,”quorum”:”1”}

As part of the user data displayed in Figure 4.9 (b), this is a sample response from the SSSS algorithm, where it has split the secret data into a single key; as set in the Admin. In the illustrated example herein, only the first two lines of these sample data, assigned to the first user ‘a’, are shown at the bottom of Figure 4.9 (b). After this stage, all the data needed for a session is set and the system is ready to handle users and share secret data.

Share Start Time: **Wed 10 June Time: 06:51:00, 2015**

Share End Time: **Wed 10 June Time: 07:16:00, 2015**

Master Share Details

Secret keys

[0101454e454d59204c4f434154494f4e20415420415241524541204b4e4f4c4c2057494c4c2

Number of shares

1

Quorum

1

TimeLimit

1500

Authorised users:

Id: 3 - User name: c

Assignment:

User [id=1, userName=a, password=cc175b9c0f1b6a831c399e269772661, gpsAssigne
phoneNumber=07753209018, loggedIn=false, timeRemaining=0, timeLogeedIn=null,
smsCodeUser=null]

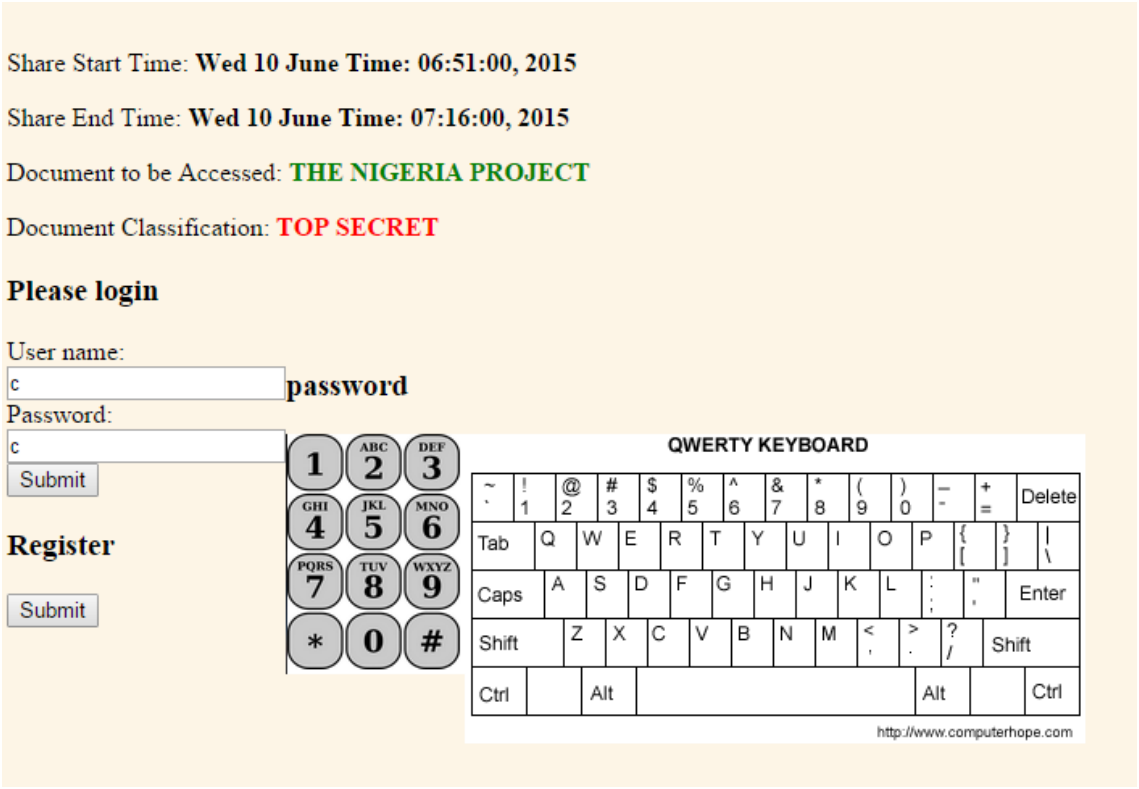
(b)

4.6 Login Web Page

The opening web page (home page) on the client side allows the user to log in and register; he registers only for the first time, which could be edited afterward if he wishes. Here the user input is entered through the hashed keypad. Once the login has been submitted, using a POST request through HTTP, it gets passed through the MD5 function and compared with the MD5 value stored in the database. In order to prevent an SQL Injection Attack, the system uses prepared statements [160]. In logging in, for example, security verification checks are carried out to prevent security breaches: e.g., does the entered name exist and does the md5 password match? A 'Yes' leads to the opening of the next web page; the Secure Share page. The Login page uses a hashed map keypad, where JQuery is used to get the keypad values and input them into the text box when the text field is clicked. The registration and login forms are shown in Figures 4.10 (a) and 4.10 (b) respectively.

(a)

Figure 4.10: (a) Page 2 of Login page (Registration Form); (b) Part of page 1 of Login page (Login Form)



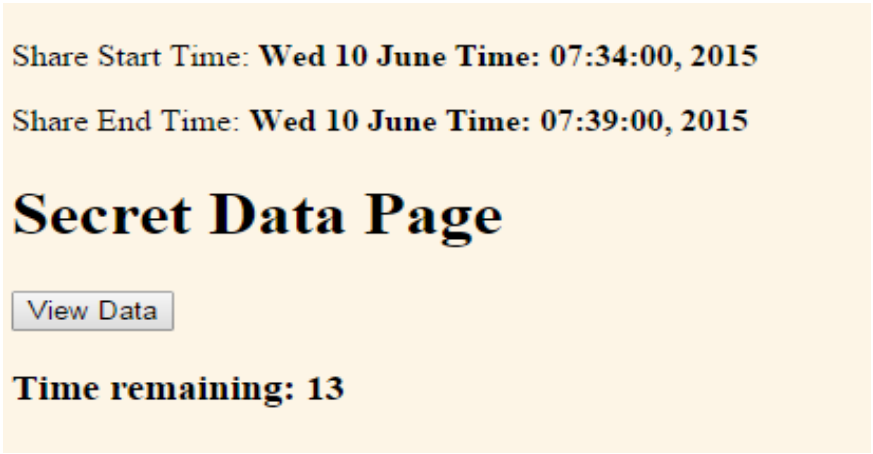
(b)

4.7 Secure Share and other Web Pages

Secure Share page is where the users log into to add their keys, GPS data, and mobile authentication code. Similar verification checks are again carried out, using MD5 hashes and other data in the database, as done in the login page, to ensure that the data added meet the criteria. That is, does the GPS match; has the correct user entered the correct key assigned to him; and does the verification code sent to the user match? The page also makes provision for editing of personal data, if the user wishes to do so. Part of the Secure Share web page is shown in Figure 4.11 (a). The result of a successfully authenticated entrance by a user into a share/reconstruction session for all users, except the authorised user, is also shown in Figure 4.11 (a) – where 'c' is the username of the Client; that of the authorised user is as in Figure 4.11 (b). The prototype system generates a Universally Unique Identifier (UUID) and sends it to the

mobile number registered by the user for additional authentication purposes. The SMS message contains the passcode for the data share.

(a)



(b)

Figure 4.11: (a) Secure share page; (b) Secret data viewing page

This is implemented using a built-in java UUID generator. The Secure Share page has a countdown clock, which expires based on the share duration set in the Admin page. Once all the shares (or the required threshold) have been added, the data can be unlocked. The authorised user gets to see a page with a countdown and a button to reveal the secret data. Once the authorised user clicks the View Data Button (which appears only on his own screen), various checks are carried out; to ensure that each user has added the key and code assigned to him correctly, his GPS data is correct, the quorum (threshold) has been met and if within the time limit; i.e., the countdown clock is still counting as at the time the last user successfully enters his data. Finally, the keys are sent back into the SSSS algorithm for a final check.

4.8 Secret Data Web Page

If all went well without any error, a successful sharing process will display the Secret Data page when the authorised user clicks the View Data Button; otherwise, an appropriate error message is displayed on the page. If the display shows success, the system is restarted, ready for the next share session; if it shows a message that indicates failure, the system is restarted, ready to repeat the failed session. The authorised user can view the reconstructed secret data one time only. The system gets wiped out as soon as the secret data has been unlocked and displayed. Any page refreshment or re-attempt will result in an error message. A sample result of this page is shown in Figure 4.12 – where ‘b’ is the username of the authorised Client (Authorised User).

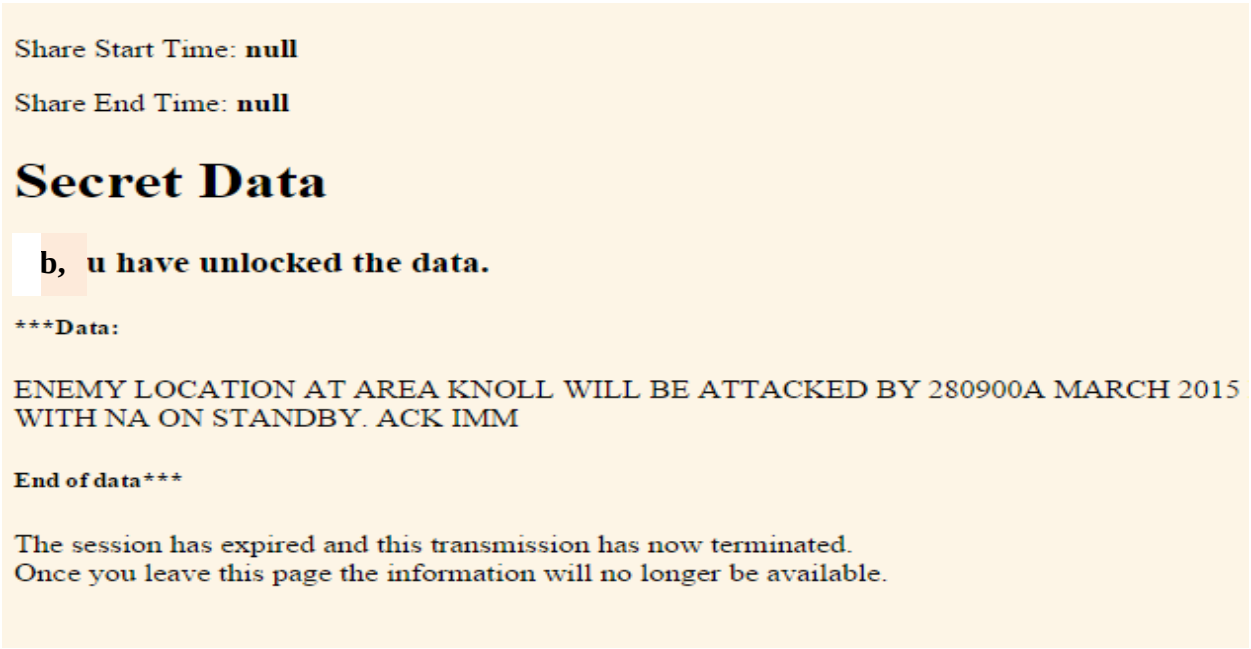


Figure 4.12. Secret data page displaying success

Next is the identification of novelties in this research implementation, followed by a quantitative analysis of the results compared with the SSSS. The Thesis also highlights the challenge encountered in the research process and suggests the scope for future work.

4.9 Areas of New Knowledge (Novelties)

❖ The CDRSAS-PT has modified the SSSS algorithm by sharing a much shorter (than most secret data) randomly generated key that is used to lock up the secret data; as opposed to encrypting/sharing the secret data itself. This would be extremely significant in cloud computing, especially if homomorphic encryption becomes a reality. In a nutshell, it costs more in terms of bandwidth and delay in a typical communication link to encrypt the data and share the resulting information among servers (as done in SSSS) compared to sharing the keys only (as proposed in the CDRSAS). Theoretically, the strong points of this modification are demonstrated in Section 4.10, using four QoS metric parameters; namely, server bandwidth, system scale, service capacity ratio and real-time performance (time delay).

❖ Other novelties associated with the CDRSAS-PT include the following:

- The geographical spread of participants (trustees) which is now global in nature as against a one-location based recombination process envisaged in previous secret sharing schemes. This revolution in the science of secret sharing is illustrated in Figure 4.2.
- As a consequence of globalisation, location-based user authentication techniques are introduced. These are the employment of the GPS coordinates and SMS text mobile authentication codes; thus greatly enhancing the security of the system.
- Inherent capability for location-based automatic mutual authentication; a novelty in the public civil domain.
- In an effort to minimise the chances of hacking, a dynamic time window is introduced within which secret sharing and recombination processes must be accomplished. Consequently, a digital clock and timer (down counter) are incorporated into the system, since time restriction is among the logic tests in the greatly enhanced Shamir's secret sharing algorithm.
- Other long-standing unresolved issues in relation to secret sharing, which have now been resolved in the Cloud Data Repository Secure Access Scheme (CDRSAS), include the following:

    - Who is the Combiner;
    - Where should the recombination take place; and
    - Who is entitled to have access to the reconstructed secret?

    These questions have now been resolved with the designation of an Authorised User (non-permanent) in the scheme, to be programmed by the Admin for every secret sharing session, as would be dictated by particular circumstances.

❖ It is also instructive to note that the practical implementation of a web-based authentication secret sharing scheme, with all the complements of the CDRSAS, has no precedence.

4.10 Quantitative Assessment Relative to the SSSS Algorithm

In making this comparative analysis, the main difference in the technical approach between the SSSS and CDRSAS-PT should be borne in mind. As highlighted earlier, the CDRSAS-PT has modified the SSSS algorithm by sharing a much shorter (than most secret data) randomly generated key that is used to lock up the secret data. This is contrary to the approach employed in the SSSS, which encrypts the secret data itself, and shares the encrypted output as keys.

4.10.1 Real-Time Performance and Server Bandwidth Cost

Consider a peer-to-peer network in which there exists some data, D, sharing for instance. The servers holding the data must be explored in terms of bandwidth and the data propagation delay over the network in real-time. In such case, the scalability (i.e. number of peers in the system) problem in the sharing of the secret data is considered useful in evaluating the Quality of Service (QoS) of the concerned network. Four QoS metrics are involved, namely, server bandwidth, system scale, service capacity ratio and real-time performance (time delay) [237].

Here, real-time performance refers to the average delay of all the peers in a system between the time a data was sent from a source and when it finally arrives its destination.

Consider some data “D” divided into chunks of the form

$$P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \tag{4.1}$$

having a constant bit rate (CBR) of R. If the time length of each of the data is T_c, then the whole data from which the chunks are obtained is $T_c R$. Note that each of the data chunks in the polynomial of Equation (4.1) can be described as a vector-matrix of the form

$$a_{j,k} = \begin{bmatrix} a_{j,1} & a_{j,2} & \cdots & a_{j,k} \end{bmatrix} \quad \forall j = 0, 1, \cdots, n \text{ and } k = 1, 2, \cdots, K \tag{4.2}$$

Thus, the data chunks can be formed into a matrix of the form

$$D_{j,k} = \begin{bmatrix} a_{0,1} & a_{0,2} & \cdots & a_{0,K} \\ a_{1,1} & a_{1,2} & \cdots & a_{1,K} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,K} \end{bmatrix} \quad \forall j = 0, 1, \cdots, n \text{ and } k = 1, 2, \cdots, K \tag{4.3}$$

In a typical communication system, the data chunk $a_{j,k}$ is transmitted at each time instant from which the data processing cost/implications can be discussed; metrics of discussion may include bandwidth, delay and channel capacity.

Consider a case of many storing repositories, as is the case of Shamir Secret sharing formula. Let these repositories be servers that can be used to store the data chunks. On the other hand, these data chunks are the secret keys obtained by splitting the randomly generated key, which is used to lock up the secret data.

It is assumed that each server receives only one chunk of the data, which could form a vector matrix, for instance. Let the propagation delay between server peers (where the data chunks can be stored) be T_t. Next, define the average service capacity ratio (SCR) as β; the ratio of a peer's upload-bandwidth to the streaming bitrate. Define $t(b,n)$ as the average delay of all peers in the system, then the relationship between real-time performance and server bandwidth cost can be expressed as [161]:

$$t(b,n) = \begin{cases} \dfrac{n}{b} T_c + T_t & b \geq n \\ \min\left\{ \dfrac{i}{b} T_c + T_t + \dfrac{n-i}{b} t(b_i, n-i), \quad i = 1, 2, \cdots, b \right\} & b < n \end{cases} \tag{4.4}$$

where b is the ratio of server bandwidth cost to streaming ratio, n is the scale of the system.

The first relation in Equation (4.4) can be explored in cases where there are equivalent bandwidth and number of participating secret data repositories. For instance, consider a case where there are 5 participating servers (as it has been used in this thesis); 5 servers have been used for the feasibility of practical real-life implementation. On the other hand, as short as the data length is, the security strength in the length of such data chunks is quite vulnerable (a corollary is in a password whose length is 5 characters). Thus, for scalability and better security strength, a consideration is therefore given to a case where there are much more peers than the bandwidth (that is the second case in Equation (4.4)). This is a minimisation problem. Hence, the solution to the minimisation problem of Equation (4.4) reduces to [237]:

$$t(b,n) = \log_{\beta}\left(\frac{n}{b}\right) \tag{4.5}$$

As an example and typical of the proposal in this Thesis, suppose that the cryptographic encryption keys are divided into 1000 (i.e. n = 1000), then Figure 4.13 describes the effects of the system scale (i.e. number of peers) on delay and the bandwidth cost over a communication link/network.

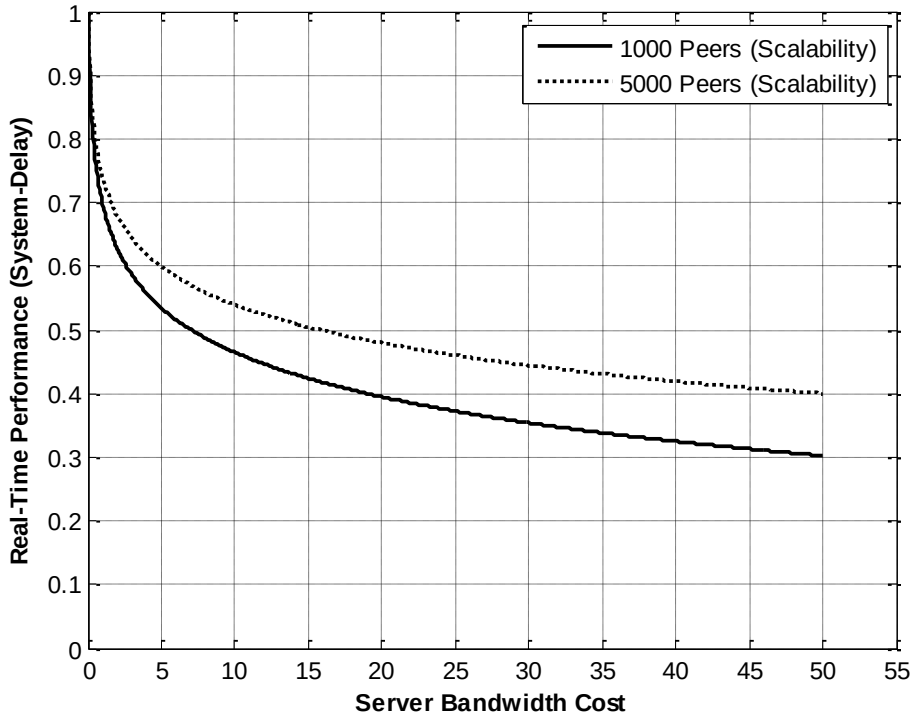


Figure 4.13. Impact of system scale on delay and server bandwidth

From Figure 4.13, it can be observed that the bandwidth involved increases with increasing number of server peers (i.e. the scale). For instance, considering a case where there are 1000 peers (servers) to which the data chunks (i.e. the shared keys) will be shared at 0.4 real-time performance and where there are 5000 peers (servers); it costs 50% of the bandwidth in the case of 5000 peers while it costs only 20% of the bandwidth when there are 1000 peers. The variation provides 30% bandwidth saving in favour of the smaller data chunks. Also, at constant bandwidth cost, for instance, 50%, the delay incurred for sharing the data into 5000 is 0.4 while that of 1000 peers is 0.3. Thus, it costs more in terms of bandwidth and delay in a typical communication link to encrypt the data and share the resulting information among servers (as done in SSSS) compared to sharing the random key only (as proposed in the CDRSAS). Ordinarily speaking, the SCR is the base of the logarithmic function described in Equation (4.5). The SCR reveals the allowable downloadable data bits per chunk; measured in bits/chunk. It translates that using higher SCR saves both the bandwidth and real-time performances; as illustrated in Figure 4.14.

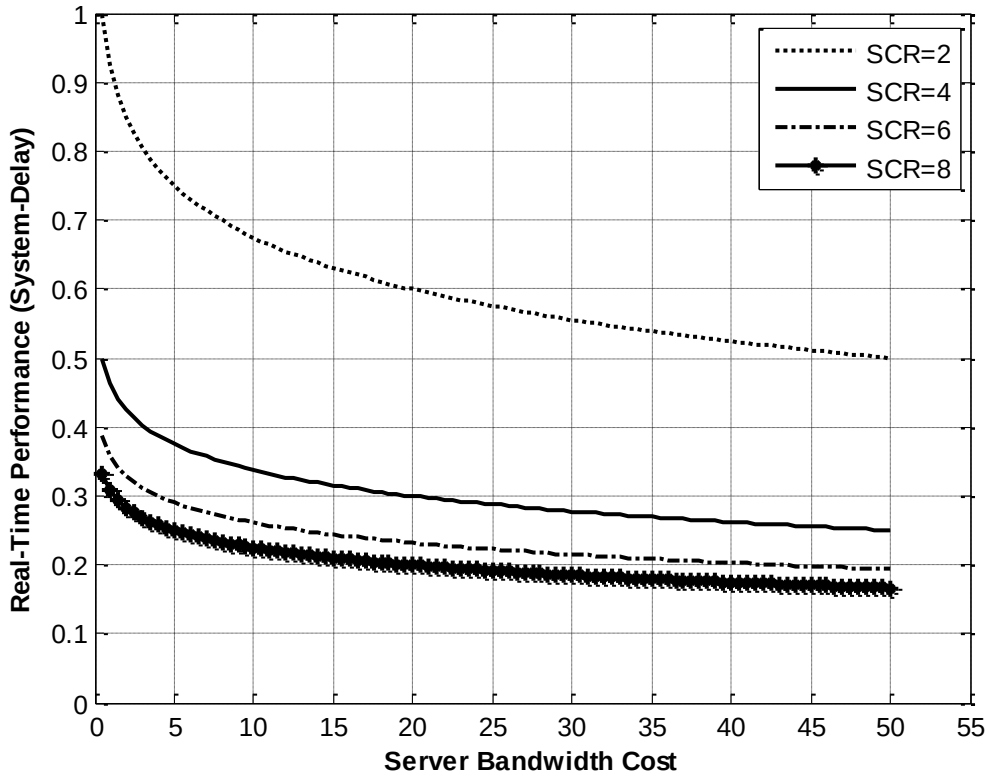


Figure 4.14. Impact of service capacity ratio on delay and server bandwidth

4.10.2 Channel Capacity Performance

From information theory, it is well-known that the channel capacity of a communication link can be described as [238, 239]:

$$C = B\log_2(1+SNR) \qquad \text{in bits/second} \tag{4.6}$$

where C is the channel capacity that is measured in bits/second and B is the bandwidth measured in Hz. SNR represents the ratio of signal to noise powers measured in dB.

Now, consider the data chunks as binary data. For the two data lengths discussed in Section 4.10.1, namely, 1000 and 5000 bits; if they are transmitted over channel bandwidths of 1000 Hz and 5000Hz respectively, then for varying SNR values the channel capacities can be represented as in Figure 4.15.

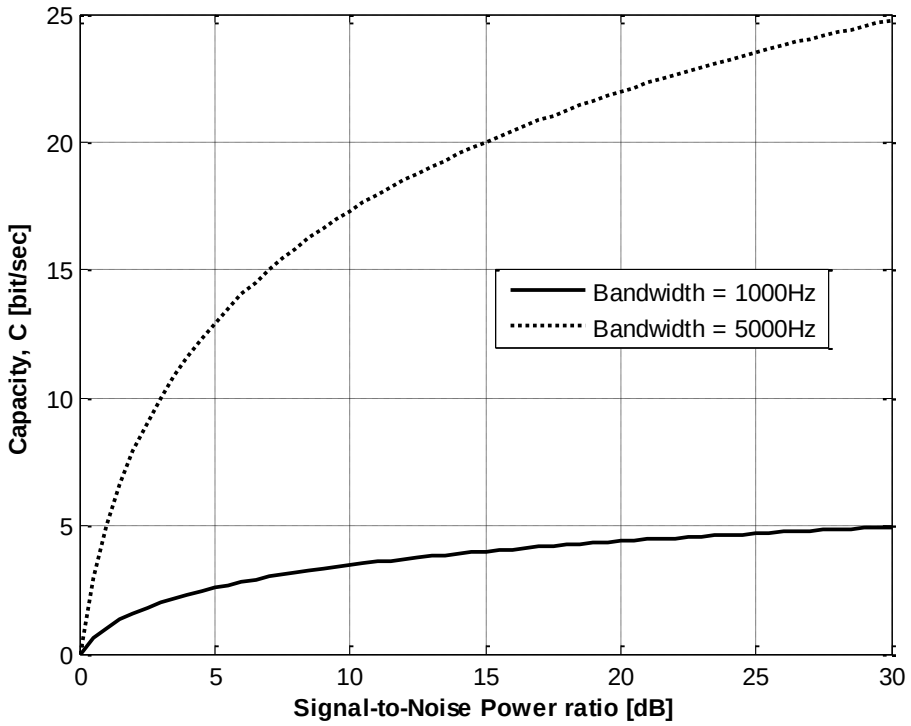


Figure 4.15. Capacity performance at different bandwidth allocations

The results shown above imply that the system with larger bandwidth (5kHz) requires the reservation of more communication resources than the system with

a smaller bandwidth. If both data chunks are expected to be transmitted over fair (equal) resource allocation, the 5000 data chunks will be starved thus leading to delay, data loss and overall slow communication. In essence, over the 5kHz bandwidth, the 1000 data chunks will consume only 20% of the bandwidth resources. On the other hand, over the 1kHz bandwidth, the 5000 data chunks will require 500% of the bandwidth resources.

The expression in Equation (4.6) can be used to discuss the spectral efficiency which is measured in bits/second/Hz as (dividing both sides by B):

$$\frac{C}{B} = \log_2(1 + SNR) \qquad \text{in bits/second/Hz} \tag{4.7}$$

Again, consider the data chunks as binary data; over a 1 kHz bandwidth. Then for varying signal to noise power ratio (in dB), the maximum channel spectral efficiencies are shown in Figure 4.16.

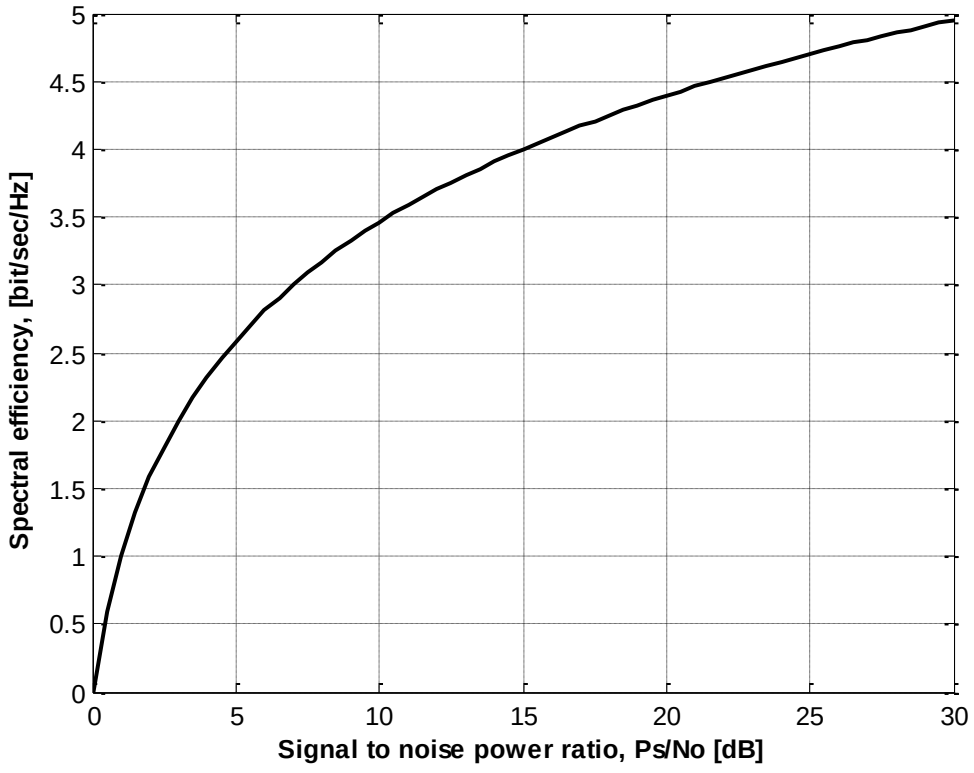


Figure 4.16. Variation of spectral efficiency with bits-(signal)-to-noise power ratio

The plot divides the area into two interesting regions; the upper region shows where data transmission is not possible while the lower region represents where data transmission is possible. The graph itself exemplifies maximum spectral allowance for data transmission under the Shannon criteria.

4.10.3 A Unique Advantage in the CDRSAS-PT

The CDRSAS-PT has a unique advantage compared to the SSSS. In both schemes, the length of the shared keys is proportional to the size of the secret data and the random key respectively. This is considered a unique advantage in the CDRSAS-PT because there is liberty to make the random key as short or long as possible (much shorter than the secret data) independent of the secret data to be secured. Thus, the CDRSAS can handle a much larger secret data than the SSSS; it can attach a whole file as a secret data, while the SSSS cannot. Similarly, this advantage has another connotation. As analysed in Sections 3.4 and 3.7.1, the strength of a password is directly proportional to its length. Therefore, since the length of the stream of random characters that is shared as secret keys in the CDRSAS-PT can be pre-determined by design, it follows that, when above fact is applied to the secret keys, a longer key would be more secure than a shorter one. In this way, the designer of CDRSAS-PT is at liberty to generate a short or long key (independent of the size of the secret data that is to be protected); depending on the security sensitivity of the application. This flexibility, which is not possible with the Shamir's algorithm, becomes an added advantage in the CDRSAS-PT. In this way, the designer is then at liberty to decide on a trade-off between security demands and other performance metric parameters.

4.11 Technical Challenge

In the process of implementing the research design, one technical challenge that took time to overcome was how to accurately determine the distance in kilometres between two GPS coordinates. This was very crucial because, without it, the CDRSAS-PT would not be able to test for the satisfaction of a location boundary condition by comparing the registered GPS data with the real login GPS data that would be keyed in by Clients for location-based authentication; the system is designed to permit location errors within a

maximum tolerance of 30 metre radius only. The search for a solution led to the discovery of the Haversine Law and Haversine Formula [240].

The Law of Haversines

For a unit sphere, a triangle on the surface of the sphere is defined by the great circles connecting three points; u, v and w on the sphere, as illustrated in Figure 4.17 [241].

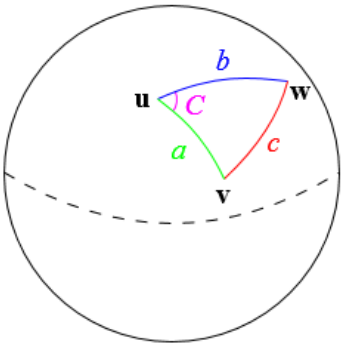


Figure 4.17. Measuring a distance between two GPS coordinates [241]

If the lengths of the three sides are a, b and c as shown, and the angle of the corner opposite c is C, then the law of haversines states that:

$$hav(c) = hav(a-b) + \sin(a)\sin(b)hav(C) \qquad (4.8)$$

Where ‘hav’ is the haversine function

Since this is a unit sphere, the lengths a, b and c are equal to the angles (in radians) subtended by those sides from the centre of the sphere {for a non-unit sphere, each of these arc lengths is equal to its central angle (in radians) multiplied by the radius of the sphere)}.

The Haversine Formula

Given any two points on a sphere, the haversine of the central angle between them is given by:

$$hav\left(\frac{d}{r}\right) = hav\left(\phi_2 - \phi_1\right)\cos\left(\phi_1\right)\cos\left(\phi_2\right)hav\left(\lambda_2 - \lambda_1\right) \tag{4.9}$$

where:

$$hav\left(\theta\right) = \sin^2\left(\frac{\theta}{2}\right) = \frac{1-\cos(\theta)}{2}$$

- d is the distance between the two points (along a great circle of the sphere; using spherical distance)
- r is the radius of the sphere
- ϕ_1, ϕ_2: Latitudes of Point 1 and Latitude of Point 2, respectively
- λ_1, λ_2: Longitude of Point 1 and Longitude of Point 2
- $\left(\frac{d}{r}\right)$ is the central angle, assuming angles are measured in radian (NB: ϕ and λ can be converted from degrees to radians by multiplying by $\frac{\pi}{180}$ as usual).

The solution for d can be found by applying the inverse haversine (if available) or by using the arcsine (inverse sine) function:

$$d = r\ hav^{-1}(h) = 2r\arcsin\left(\sqrt{h}\right) \tag{4.10}$$

Where h is haversin (d/r), or more explicitly:

$$d = 2r\arcsin\left(\sqrt{hav\left(\phi_2 - \phi_1\right) + \cos\left(\phi_1\right)\cos\left(\phi_2\right)hav\left(\lambda_2 - \lambda_1\right)}\right)$$

$$= 2r\ \arcsin\left(\sqrt{\sin^2\left(\frac{\phi_2 - \phi_1}{2}\right) + \cos(\phi_1)\cos\left(\phi_2\right)\sin^2\left(\frac{\lambda_2 - \lambda_1}{2}\right)}\right), \text{ QED.}$$

With this result, it is now possible to test and find out if a particular GPS location data entered into the system satisfies the limit imposed by the system or not, and hence, decide whether access should be granted or not; location-based authentication/authorisation.

Apart from the foregoing, the only challenge worth mentioning is a general one; i.e., how to cope with the rate of increase in cybercrimes - both in frequency and intensity – with world powers like the US, Russia, China, UK, North Korea, Iran, etc., being perceived as both victims and aggressors. In the Global Risk Report 2015, a baby of the World Economic Forum based in Geneva, it is highlighted that large-scale cyberattacks are among the prominent risks in 2015. That is, given the growing sophistication of cyberattacks, the rise of hyper-connectivity with a growing number of physical objects connected to the Internet, and increasing quanta of sensitive personal data being stored by companies in the cloud, it is obvious that the risk of large-scale cyberattacks remains high; with respect to both impact and probability. For instance, in the United States, the economic cost of cybercrime is estimated at $100 billion each year [188].

4.12 Limitation

The main limitation of secret sharing is the presumption that all participants are equally trustworthy; in practice, this may not be the case. George Orwell observed that “some animals are more equal than others” [65]. Similarly, some participants would be more equal than others. In other words, in most circumstances, some participants are trusted more than others. For instance, in a network of computers, where each computer represents a participant, a higher security threshold might be required for the computers that are more likely to be corrupted, like those connected to the Internet, and a lower threshold for the more trusted computers. That is, it might be necessary or better to define differently sized subsets of the participants needed to reconstruct the secret. The structure consisting of all these sets is called an access structure.

4.13 The Way Forward

Practically speaking, the CDRSAS-PT has gone beyond meeting the full requirements of the research design as conceived. However, it remains a prototype and would require further work to make it viable for practical deployment in the market. Further work could focus on the following:

- ❖ Having a managed area to set up future shares at a given period;
- ❖ Having more than one different share sessions happening simultaneously;
- ❖ Capturing all the user interactions in a database;
- ❖ Other incorporations aimed at making the system more robust and versatile;
- ❖ Further practical system performance tests for high volume traffic, when adapted and adopted for public deployment.

This, in effect, completes the full implementation of the PhD research design with a fully tested functional scheme – the CDRSAS. However, there is still scope for future work to further enhance the performance and security of the system. The details of the scoped items are as suggested in Appendix 8 (every item asterisked therein is a projected future characteristic for the envisaged CDRSAS-DT). The deductive summary for this chapter now follows prior to Chapter 5. Chapter 5 employs the lessons learned from this research effort to focus on the possible measures designed to checkmate the confidence artists' use of technology to manipulate human trust in their perpetration of fraudulent crimes.

4.14 Deductions

The web-based authentication CDRSAS prototype employs various building blocks, including the SSSS algorithm, MD5 and various libraries. Its programming elements include HTML5, PHP, Java, Servlets, JSP, MySQL, JQuery, and CSS. These are running on Tomcat and Apache databases using XAMPP Server. The source code is object oriented and adheres to software engineering tools and principles [242], [243].

The prototype system does work and the data can be shared across the globe through a web page; using a secure server. It passed all the JUnit tests but has

not been tested under heavy traffic. The phone number is registered during the registration process but the user is allowed to edit it along with other existing user details; these are potential areas of security concern subject to modifications. The Admin page can be used to easily reset and create shares for users, and reconstruct same. The share settings are easily configurable. The Admin page (accessible with local access only) can be refreshed to display the data in the system; who has logged in and has entered what.

Hacking into the system to illegally access the data would be a very tough task. There are many checks to ensure that every condition has been met before the data is unlocked. SMS-text-verification-based authentication gives an added level of security and a modern touch. The same is true of GPS coordinates.

As regards novelty, the CDRSAS-PT has modified the SSSS algorithm by sharing a much shorter (than most secret data) randomly generated key that is used to lock up the secret data; as opposed to encrypting/sharing the secret data itself. This would be extremely significant in cloud computing [244], especially if homomorphic encryption becomes a reality [244]. In a nutshell, it costs more in terms of bandwidth and delay in a typical communication link to encrypt the data and share the resulting information among servers (as done in SSSS) compared to sharing the keys only (as proposed in the CDRSAS).

The CDRSAS Prototype has also expanded the secret sharing system by incorporating a dynamic time window, digital clock/timer (down counter), GPS data authentication and SMS text mobile authentication into the secret sharing process. The difference between the SSSS algorithm and the CDRSAS prototype secure server is akin to the difference between the vacuum tube diode/semiconductor transistor and a radio transceiver system. Similarly, the design has resolved some long-standing issues by answering the questions: Who is the Combiner; Where should the recombination take place; and Who is entitled to have access to the reconstructed secret? It does this by designating an Authorised User in the scheme, to be programmed by the Admin for every sharing session, as would be dictated by particular circumstances. Lastly, this scheme has globalised the practical implementation of secret sharing for the first time.

Further work would focus on the following: having a managed area to set up future shares at a given period; having more than one different share sessions happening simultaneously; capturing all the user interactions in a database; other incorporations aimed at making the system more robust and versatile; and subjecting the system to various practical performance tests, for high volume traffic, when adapted for public deployment. Details of future work to enhance the performance and security of the system are in Appendix 8 (every item asterisked therein is a projected future characteristic).

Chapter 5

Location-Based Authentication as an Antidote against GSM-Dependent Advance Fee Fraud in the Cyberspace

The degree of cyber-related insecurity occasioned by fraudulent practices in Africa has been an issue of great concern economically, especially as it relates to foreign direct investments and dealings with other international partners. Apart from the economic costs to the nations, corporate organisations and individuals, it has also been an image problem for some of the countries in various international fora. It was in an effort to find ways of using technology, within the context of its interplay with human trust and other trust-centred human attributes, to mitigate the negative effects of this state of insecurity that this chapter was designed. Although it was tailored, specifically, for the West African environment, using Nigeria as a case study, the results are applicable to all countries with similar situations in Africa, with global implications.

Based on a survey involving two field trips to Nigeria (in November 2013 and December/January 2015/16) and the knowledge acquired via the implementation of CDRSAS-PT in Chapter 4, among other resources, this chapter begins by examining the general security situation in the sub-regional environment, with a focus on cyber-security, especially as it relates to the use of Global System for Mobile Communications (GSM). The cybersecurity aspect of the survey facilitated the discussions in Section 5.4; using data from official security agencies (NP, SFU, NFIU, EFCC and NCC). Details of the GSM roaming aspect of the survey will be discussed (Section 5.6.2), after highlighting Location-Based Authentication (LBA), advance fee fraud (419), digitisation and teledensity. The survey data primarily affect the sub-Saharan nations, with Nigeria as the hub of activities. It is recalled that some requisite conceptual clarifications relevant to this chapter were treated in Section 2.10.1; including cyberspace, computerisation, miniaturisation, 419, digitisation and teledensity. Next, both the forward and backward effects of these technological developments are then assessed vis a vis the national security posture with a focus on the security of cyberspace. This would be followed by discussions on

identifiable measures aimed at countering or mitigating possible security threats in the cyberspace. These would include the possibility of using LBA and further digitisation of the GSM Mobile country codes down to City/Area codes along with GSM Mobile/Global Positioning System (GPS) authentications. Where necessary, these could be combined with the use of a web-based Secret Sharing Scheme for services with very high security demands. Possible challenges to the suggested mitigating measures would also be considered. The LBA techniques are discussed next. This will be followed by the basics of GPS techniques and its capabilities /limitations.

5.1. Location-Based Authentication Techniques

Due to the ubiquity of wireless communication systems, culminating in the global Internet, modern technology dictates that reliable means for explicit identification be emplaced between/among interacting entities. The process of user identification is generally called authentication. To 'authenticate' is to establish the validity of the claim of a user or an entity. In the cyber world, it means positive verification of a user, device, or other entity in a computer system, often as a prerequisite for granting access to resources in a system [245]. According to Jaros and Kuchta [93], it is referred to as message origin validation, while Zhen et al. [3] defines it as an affirmation of the identity of an object in centralised systems. Authentication is among the three processes of AAA (Authentication, Authorisation, and Accounting) [3, 4], as illustrated in Figure 5.1.

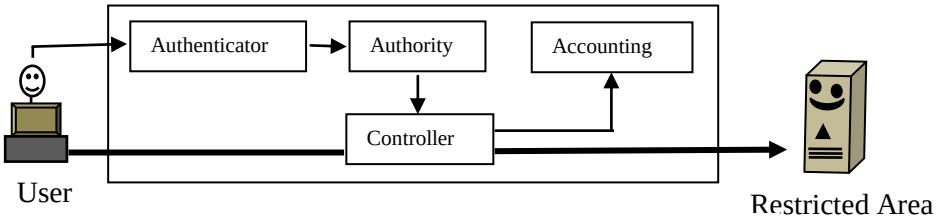


Figure 5.1. A General AAA system [3, 4]

When a user requests for access to the restricted area, he is first authenticated, based on which access is granted or denied. Where access is granted, the controller establishes a connection between the user and the restricted area;

whether access is granted or not, an account which records the information concerning the user's actions is created.

These days, authentication techniques are divided into four main categories, based on related authentication factors. These respectively employ the following [246]: what the user knows - this is based on knowledge of confidential information (e.g. password); what the user has - techniques using tokens, smart cards, RFID (Radio Frequency Identification Device), hardware keys, etc.; what (or who) the user is – these deal with biometric techniques that are limited to a human authentication, using parameters like the eyes, fingerprints, etc; and where the user is located – this technique is based on the user's physical location; it is a new authentication factor [246, 247].

Location-Based Authentication (LBS) encourages new service concepts in tracking applications, with the potential to make many messaging and mobile Internet services more relevant to customers as information is adjusted to context. In this way, location information can considerably improve service usability. Due to the multidimensional benefits of location information, operators now consider it as their third asset besides voice and data transmission, with important investment opportunities [248]. These include services related to directions, emergency, transportation of sensitive goods/asset tracking and personal/car navigation; where accuracy is high [248]. A brief review of some location-based authentication techniques now follows.

5.1.1 N-Kerberos Protocol

The N-Kerberos protocol is basically a location-based Kerberos protocol. This is a cryptographic protocol where it is imperative for users to use a very secure location signature created using the P(Y) code (derived from the GPS signal). This is used in an authentication technique to reduce the possibility of replay attacks. In order for this technique to function well, the server must have a list of the physical addresses of the legitimate participants in its database. Possible disadvantages here would relate to the fact that a fraudulent user could give a false location after reading it from the GPS receiver which he carries about all

the time. In addition, the GPS signals are not available indoor without costly installation of appropriate sensor networks [247].

5.1.2 STAT I and STAT II Schemes

STAT I (Space-Time Authentication Technique I) and STAT II are multifactor location-based authentication schemes. Both employ an authentication terminal (a pocket device that is connected to user's terminal via USB) which acts the most key roles in these techniques. The user himself must be authenticated first, via his fingerprints, followed by his space-time information authentication. STAT I technique uses GPS system to determine the user's position, while STAT II uses active infrastructure {proprietary communication technology IQRF(Information Query Radio Frequency)} to provide space-time information. Some of the limitations of these techniques are inherently obvious from their mechanisms [93].

5.1.3 Main Location Technique Principles

Basically, the location of a mobile user can be determined in one of two ways; tracking and positioning. If a sensor network determines the location, the mechanism is termed tracking; in which case the user must wear a tag or badge to enable the sensor network track his position. The location information is first stored in the sensor network; it is sent to the mobile user on request, via wireless communication. On the other hand, if the mobile system determines the location itself, the mechanism is called positioning. In this case, a system of transmitters or beacons sends out radio, infrared, or ultrasound signals. Location information is directly available on the mobile system and does not have to be transferred wirelessly. Similarly, location information is not readable for other users, thus privacy issues do not arise [248].

Tracking and positioning systems are based on the following basic techniques [248]:

Cell of Origin (COO)

A technique used if the positioning system has a cellular configuration. Wireless transmitting technologies have a restricted range; in the sense that a radiated

signal is available only in a certain area, called the cell. Thus, if the cell has certain identifying characteristics, it can be used to determine a location.

Time of Arrival (TOA) and Time Difference of Arrival (TDOA)

Electromagnetic signals move with the speed of light, assumed to be relatively constant at approximately 300,000 km/s. Thus, using the principle of Doppler Effect, the time difference between sending and receiving a signal (TDOA) can be used to compute the spatial distance between the transmitter and receiver. A similar principle can be used with ultrasound, where the signals take a longer time and the measurement is simpler; though ultrasound can only reach low distances. In GSM networks, although the term Enhanced Observed Time Difference (E-OTD) is often used instead of TDOA, the principle is the same.

Angle of Arrival (AOA)

If antennas with direction characteristics are used, the direction from which a given signal arrives can be determined. Given two or more directions from fixed positions to the same object, the location of the object can be computed.

Measuring the Signal Strength

The intensity of electromagnetic signals decreases with the inverse square of the distance from their source, even in a vacuum. Given specific signal strength, the distance to the sender can be computed; this technique is prone to inaccuracies due to obstruction-induced attenuations.

Processing Video Data

Significant patterns in a video data stream from video cameras can be used to determine the user's location; if users wear badges with conspicuous labels. Thus, positioning systems use techniques from image processing to detect and interpret image data. In principle, video positioning systems are based on the AOA technique; a specific pixel in an image represents a certain angle relative to the camera's optical axis.

Triangulation, Trilateration, and Traversing

Generally, precise positioning methods have their roots in land surveying, where geometric techniques are employed to determine locations using angles and distances. Any positioning system that provides geographic coordinates is still based on these geometric principles [248]. Figure 5.2 (a-c) illustrates how to compute the coordinates of a location u, using triangulation, trilateration, and traversing respectively:

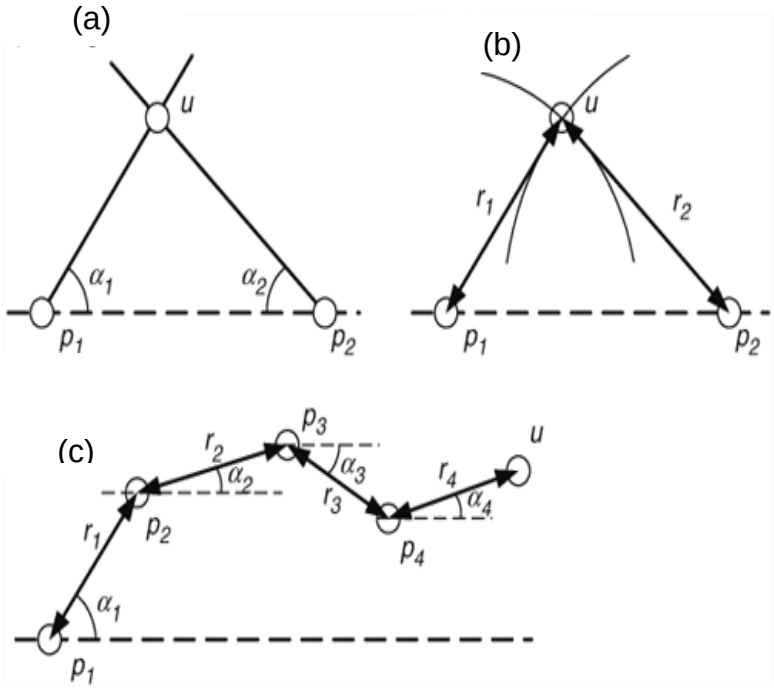


Figure 5.2. (a) Triangulation; (b) Trilateration; and (c) Traversing. [248].

❖ Triangulation

This needs two fixed positions (p_1 and p_2). From each position, the angle to the location u is measured. The location u can be determined by the intersection of two lines. With the help of trigonometric functions, the coordinates of u can be easily worked out.

❖ Trilateration

This also needs two fixed positions but uses two distances to the unknown location. The location u is obtained by the intersection of two circles. Usually,

there exist two intersection points. Thus, one of the points is eliminate using additional information. In contrast to triangulation, trilateration leads to nonlinear equation systems, which have no closed solution for 3-dimensional positioning. Numeric methods are employed to solve the resultant equations [248].

❖ Traversing

This uses several distance–angle pairs. Starting with a known point p_1, the distance and direction to another point p_2 are measured. After a few steps, the unknown point u is determined. It should be noted that, in principle, a single step could be used to move from a known point to the unknown point.

It should be noted that triangulation is the generic term for any kind of geometric approaches for location, even though its original meaning is as described above. Similarly, Figure 5.2 assumes a positioning in two dimensions. For 3-dimensional positioning, similar mechanisms are used, but with three parameters (angles, distances and altitudes) in order to calculate 3-dimensional coordinates.

In general, positioning systems are divided into three classes; satellite positioning systems, indoor positioning systems and systems that use an existing network infrastructure [248]. Of these, satellite positioning system, in the form of GPS, has the widest coverage, most secure and most accurate, where it is available; it is available everywhere except indoors and locations where it is screened from view by obstacles [93, 247, 248]. It is also capital intensive in launching/supervision. The GPS is discussed with more details in the next section.

5.2 The Basics of GPS Techniques

The GPS is a radio navigation system that enables land, sea and airborne users to determine their exact location, velocity and time 24 hours a day, in all weather conditions, anywhere in the world [249]. The capabilities of the modern system render its predecessors impractical and obsolete; e.g., magnetic

compass, sextant, chronometer and other radio-based devices. The GPS supports a variety of military, commercial and consumer applications [248].

Basically, the satellite is a self-contained communications system with the ability to receive signals from earth and to retransmit those signals back with the use of a transponder; an integrated receiver and transmitter of radio signals [249]. There are 24 satellites in orbit. The orbital distance from earth is about 17,700 to 20, 200 km, taking about 12 hours for a complete orbit. At least 5 and at most 11 satellites are mostly visible over the horizon from every point on the earth's surface [248]. The GPS satellite constellation and triangulation process are shown in Figure 5.3 (a, b), respectively.

Figure 5.3: (a) The 24 satellites in orbit; (b) GPS triangulation process [250]

Each satellite has a computer, an atomic clock and a radio. Atomic clocks are integral parts of the GPS because extreme accuracy in timing is necessary for the triangulation involved in the positioning system. The satellite continually broadcasts its position and time; once a day, each satellite checks its own time and position with a ground station and makes corrections. On earth, every GPS receiver has a computer that triangulates its own position using bearings from three of the four visible satellites. The result is displayed in form of a geographic position; longitude and latitude. This is correct, for most receivers, within a few meters (10m for Google Nexus 7 Tablet). The receiver may also display maps. Data from the fourth satellite is used to figure out the altitude of the geographic position. When on the move, it may also display navigation data; speed, the direction of travel, and estimated times of arrival. Some specialised GPS receivers can also store data for use in Geographic Information System (GIS) and map making [250]. Nowadays, most smartphones and tablets are GPS-compliant; e.g., Google Nexus 7 and 10 tablets – ‘Google Now’ [251].

Using the GPS, it is difficult to fake location in the cyberspace. Hence, cracking user's position is a very complicated endeavour [247], [252].

The GPS is the most prominent example of a satellite navigation system. It is owned, operated and maintained by the US. In 1984, the first GPS satellites were launched, and 12 satellites were operational by 1990. A first operational status was achieved with 21 system satellites and three reserve satellites on December 8, 1993. The full operation capability was declared on July 17, 1995 [248].

The GPS system is divided into three segments; the user segment, the space segment, and the control segment. The user segment consists of the devices of the mobile user, the space segment consists of the satellites which are powered by solar cells, while the control segment (Earth Station) is used for administration of the satellites as well as for correction of the satellite internal data. The GPS signals are of two components; the encrypted Precise Positioning Service (PPS) exclusively for military purposes, and Standard Positioning Service (SPS) which is freely available for civilian users. Satellites use two frequencies; L1 (1575.42 MHz) for PPS and SPS, and L2 (1227.6 MHz) exclusively for PPS.

The Russian counterpart of the GPS is GLONASS (Globalnaya Navigationnaya Sputnikovaya Sistema), while the EU system in the making is called Galileo (otherwise called Global National Satellite System- GNSS); first launching started in October 2011, and the 30-satellite Galileo system is expected to be completed by 2019 [253]. The Chinese system consists of two separate satellite constellations; a limited test system that has been operating since 2000, and a 35-satellite system full-scale global navigation system that is currently under construction is expected to be completed by 2020. It is called the BeiDou Satellite Navigation System (BDS) or the COMPASS [254].

5.2.1 Basic GPS Positioning Calculations

If a user wants to determine a position with the help of satellites, he needs the exact positions of the satellites (s_i) as well as the exact distances to the satellites (r_i). At least three satellites are needed to determine the user's location u in three dimensions. Since satellites move on fixed orbits, a mobile user can easily compute his or her exact position at a certain time. An almanac contains a list of all working satellites and their orbits. It is updated when satellites are shut down or new satellites start functioning in new orbits. It should be noted that the precision of the values s_i directly influences the precision of the location u. In order to compute the distances, r_i, every satellite sends a signal, which exactly specifies the current satellite time. A receiver compares this time with its internal clock. The distance r can be determined from the time difference Δt with the formula r = c Δt; where, c ≈ 300,000 km/s [248].

5.3 GPS Capability and Location-based Authentication

It is clear from the foregoing that, as at date, the satellite positioning technique is the most reliable locating technique in terms of accuracy, coverage and costs (relative to the user). This is important because, for a location-based authentication technique to be effective, it ought to be user-centred, otherwise, evasive actions would render it useless. The current capability of the GPS dictates that positioning must be based on own location only; i.e., an entity 'A' cannot use his GPS receiver data to determine the position of another entity 'B' in a different location. That is, using the GPS in location-based authentication necessitates that the user must be the one to supply the own space-time information to the server and vice versa. Thus, a fraudulent user could supply fake information at will, and vice versa. This has a negative implication on the trust level that authentication is designed to achieve. In order to resolve this problem, it is either a way is found to enable the authenticator to use own GPS data to determine the location of the client or transceiver devices are equipped with GPS capabilities to facilitate automatic mutual authentication; as demonstrated by the Cloud Data Repository Secure Access Service – Prototype in Chapter 4.

After discussing the LBA techniques and GPS capabilities in the preceding sections, an area assessment of the state of cyber insecurity in Africa is presented in the succeeding sections. This leads to a proposal to harness both technology and human factors to counter or mitigate criminality in the cyberspace.

5.4. The State of Cyber Insecurity in Africa, Using Nigeria as a Case Study

Every society has its bad eggs; research estimates show that about 4% of Nigerians engage in cybercrimes [255]. Regardless of the magnitude of this percentage, Nigerian 419 Scam is a major concern, not only for the African Governments and their citizens but the entire global community [208].

Cybercrime refers to any unlawful act perpetrated using the computer, electronics and ancillary devices as tools within the cyberspace [256]. It involves disruption of network traffic along with virtually an endless list of major and sundry crimes including terrorism and outright warfare [202]. It targets individuals, individual properties, corporate organisations, governments, the entire nation and the global community at large [202, 256]. Discussions with and statistics from the Economic and Financial Crimes Commission (EFCC), Abuja, and the Special Fraud Unit (SFU) of the NP, Lagos, Nigeria, indicate that cybercrimes that are prevalent in Nigeria include [257, 258]: fishing and spoofing activities targeting bank customers; skimming of standard issue magnetic-stripe ATM (Automated Teller Machine) cards; cloning and/or defacing of government and business websites; spamming activities involving 419 Scam solicitations (for lottery, inheritance, charity, romance, crude oil, fund transfer, employment, contracts, etc.); fraudulent online purchases from e-commerce sites made with fake foreign financial instruments and stolen credit card information; online investment scams targeting local victims; deployment of malicious programmes – mostly off-the-shelve spyware, keystroke loggers, Trojans and extractors on target systems; targeting of emotionally vulnerable persons on free social networking sites; and the use of free email services (especially g-mail, yahoo-mail and hotmail) in cybercrime related communications.

Cybercrimes are very common in Nigeria. Statistics reveal that these crimes are mostly committed by males between the ages of 20–35, and mostly based in University towns [257]. Nigeria currently ranks first in Africa, and third in the world, after the US and UK, with 5.7% cybercrime perpetrators (down by 0.2% from 2006), as illustrated in Table 5.1 [256].

Table 5.1. Top ten countries by count (cybercrime perpetrators) [256]

Country	Percentage
1. United States	63.2%
2.United Kingdom	15.3%
3. Nigeria	5.7%
4. Canada	5.6%
5. Romania	1.5%
6. Italy	1.3%
7. Spain	0.9%
8. South Africa	0.9%
9. Russia	0.8%
10. Ghana	0.7%

From Table 5.2, all the indices for the incidence of cybercrime in Nigeria are on the increase for the three years; some astronomically, bearing in mind that the indicators for 2014 are incomplete. Virtually all researchers agree that globalisation occasioned by the revolution in Information and Communication Technology (ICT) has greatly contributed to the rise in cybercrimes in Nigeria. However, this does not explain why Nigeria should be far ahead of South Africa, for instance, with 5.7% against 0.9%, given that the Internet usage in South Africa is about 50% compared to Nigeria [259]. Many researchers agree that it is Nigerian 419 Scam that has sharply differentiated from South Africa, and this was enhanced by miniaturisation of communication devices among other factors, especially the mobile phone which is very portable and more amenable to deception in respect of callers' location information [208, 255, 257].

Table 5.2. Statistics of fraudulent cybercrimes in Nigeria [257, 258]

Year	Description	Quantity
2012	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	89 100 2.4 Billion
2013	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	99 188 8.4 Billion
2014*	No of Cases Reported No of Suspects Arrested Financial Recoveries (Naira)	93 - 630 Million
2014* … For the First Quarter Only		

The implication of this finding would be fully appreciated only if it is realised that the annual statistics for mobile phone subscribers in Nigeria indicates a leap from 266,461 to 135,253,599 between 2001 and 2012, respectively. The teledensity for the corresponding periods also witnessed a quantum leap from 0.73 to 80.85 respectively [260]. Nigerian Governments have been fighting fraudulent crimes for long without much result. This led to the establishment of various outfits, in addition to the Nigerian Criminal Code Act. Thus, it could be said that while globalisation has enhanced the socio-economic life of the people, it has also come along with insecurity problems that have so far defied solutions. The solutions designed to counter feigned-location based fraud related crimes will be treated next.

5.5 Countering Feigned-location Based Fraud Related Crimes Using the Digitised (Split) Cells of Origins

It is noteworthy that most of the measures so far employed in Nigeria to counter the cyber and other fraud-related crimes are mostly based on legal instruments; in terms of enactments and enforcements. Since the most valuable tool for the 419 fraudsters is the mobile phone, it seems reasonable to approach the problem from a technological angle as one of the most optimistic ways forward. It is hereby proposed that location-based authentication be employed in two versions in Nigeria. While one version is to actually detect the exact physical location of the fraudster, the other is to deter him/her from committing the crime.

For actual detection, there would be a need to make all transceivers GPS-compliant, with inherent capabilities for location-based automatic mutual authentication as advocated by Adeka et al. [205]. This would be able to detect the locations of both static and mobile cyber criminals; please note that a mobile phone is being treated here as a computer – smartphones are computers with phone capabilities.

The deterrence approach would be realised by a further digitisation of the country codes for the GSM cellular phone systems, as explained in the next segment. This could be very effective against 419 fraudsters who use the mobile phone as their main tool. Where necessary, the two approaches could be combined with the use of a modified web-based secret sharing scheme for services with very high security demands. These would then be augmented with an administrative approach; which may take the form of good governance by way of mitigating corruption and job creation for the teaming idle youth populations in Africa.

5.5.1 Background to the Deterrence Approach

In the evolution of cellular phones, two major reasons for dropping certain standards stemmed from security limitations and incompatibility of diverse standards. Researches were heated up to solve these challenges. Breakthroughs yielded the Long Term Evolution (LTE) today [261, 262]. Since then, subsequent cellular standards have become more mobile, secure and compatible with earlier standards across different national boundaries. Aside from these improvements, security challenges still abound such as location identification of a mobile user. Recently, the 3GPP (3rd Generation Partnership Project) working group proposed the inclusion of the Time Difference of Arrival (TDOA) algorithm [263] in the LTE-Advanced (LTE-A) Release 10 and beyond (which has been revised to inherit Rel-8/9 features) to identify the location of a mobile caller [264, 265]. In cellular phone networks, although the term Enhanced Observed Time Difference (E-OTD) is often used instead of TDOA, the principle is the same [266], except that the former involves the broadcast of cell-ID [265].

In contrast to mobile phones, fixed telephones are more secure and mostly preferred in official involvements, since they are trackable more accurately. Its address can be easily traced since the address (including the city codes) assigned to a user is known. This feature makes it more dependable to transact businesses using fixed telephones than mobile phones. This proposal considers mapping the security advantage of the fixed telephones on to the mobiles (with a variety of modifications) such that it can be more dependable than it has been. Of course, most business organisations would benefit, should the mobile lines provide a dependable security trust-head.

In the meantime, area codes are known to be common and are defined differently for different countries [267, 268]; e.g., three digits for USA, Canada and Nigeria, two digits for Brazil and one digit for Australia and New Zeeland. Similarly, there are variable lengths for the United Kingdom, Germany, Austria, etc. Sometimes, and in some countries also, these area codes are part of caller's mobile number. It is hoped that another variety can be exploited as the proposed would travel with the permanent caller mobile number. Being the first of its kind, it is possible that this research may revolutionise area/city coding for mobile nodes and that the security breaches volunteered by the cellular telecommunication security orifice will be solved permanently, within the context of current technology.

This proposal does not suggest any change in the numbering plan or hardware of any telecommunication network operator, but integration into the software configuration of the radio routeing elements of the network operator's systems – base station (Node-B, evolved-Node B or Home-eNB). It does not affect the traditional design of the mobile handsets nor would the handsets be reconfigured for the purpose.

5.5.2 Benefits to the Nations

From experience, the duo of location-based identification and mobility has always been a confidence-inspiring pair of factors for criminals; the mobile communication technology is no exception. This is because prompt identification of the geographical position of the mobile phone users is still a

technology challenge, which is consequent upon mobility and positioning. Most crimes in Nigeria are therefore aided and/or perpetrated using mobile phones. Such crimes include kidnapping, robbery, impersonation, terrorism and all shades of '419'. Sometimes, family members masquerade to defraud own family. Debtors pretend to reside in Abuja while physically being in Lagos. The ban on the use of GSM/Thuraya services in North Eastern Nigeria (Borno, Yobe and Adamawa States) [25, 269, 270], in the wake of the State of Emergency (SoE) declared in May 2013, is a robust illustration of the argument being canvased in support of this proposal. Hence, this proposal means a solution for reducing the tendency to commit the crimes associated with the use of mobile phones to enhance confidence in the committing of such crimes in the country [186]. It is instructive to note that the deterrence effect, of the technological solution envisaged in the proposal, is even more than its enhancing practical reality in tracking down the criminals with a view to subjecting them to justice. This proposal could serve as an effective obituary for '419 and Associates,' not only in Nigeria and Africa but the world at large.

5.5.3 The Proposed Technology

In the meantime, a mobile phone caller can be traced to the country of origin using the country calling code. It makes it very possible that fraudulent activities can thrive since the exact location of the mobile caller cannot be estimated by the ordinary users. In LTE-A Release 10 and beyond, mobile phones are proposed to incorporate the TDOA in determining the location of the mobile caller [264, 265]. This tracking functionality permits that only the network operators and/or the security agencies such as the police would be able to trace the origin of a mobile caller, depending on the TDOA parameters [263] extracted from the caller. It can be reasoned that this still makes the acquisition of the space-time information of a mobile caller vague, perilous, tedious, and expensive. The proximity of a caller's location characteristics to the parameters extracted from the TDOA algorithm cannot define the position of a caller closer than 10 meters. In addition, the time it takes to compute and then trace the origin of the caller can as well leverage fraud. The proposed initiative can be combined with the TDOA to improve the identification of a mobile user's geographical location faster. In fact, at least four cells are required to perform

Observed Time Difference of Arrival (OTDOA) [263, 271], and the disadvantages cannot be overstressed.

Just like the landlines wherein a caller location can be easily identified, a similar situation is being advocated for a mobile user. This could be achieved by a further digitisation (splitting) of the GSM country code into city/area codes, corresponding to the emergent Cells of Origins, as illustrated in Figure 5.4 (c).

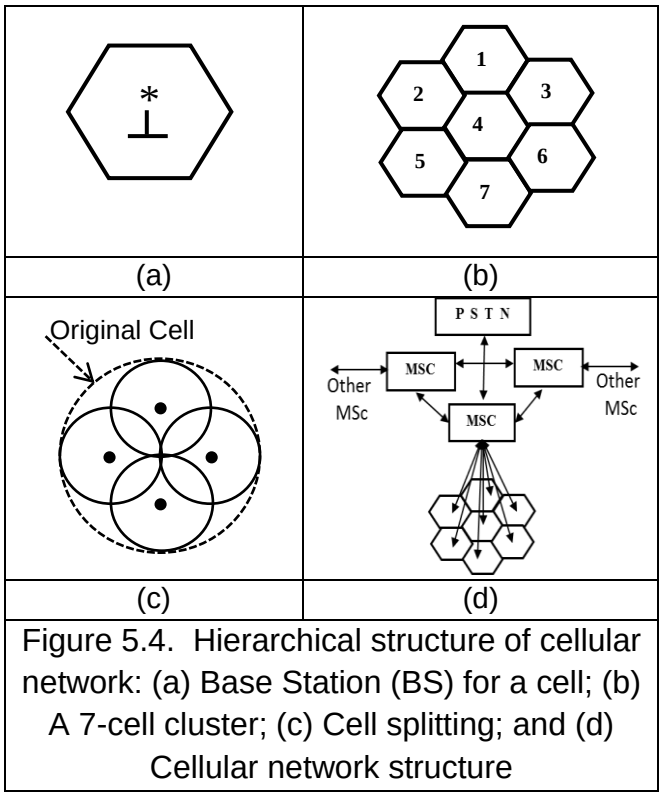


Figure 5.4. Hierarchical structure of cellular network: (a) Base Station (BS) for a cell; (b) A 7-cell cluster; (c) Cell splitting; and (d) Cellular network structure

Thus, the caller ID travels with the city/area codes as well, instead of country code alone. With proper public awareness education, it would become clear to all users that such phones would no longer be safely used in defrauding people by falsifying the city location of the caller. The exact city location can be extended to a mobile phone user to reduce and also discourage fraudulent activities among mobile phone users. The city/area codes will be incorporated in the base stations within an area. Each base station will bear a code of the area within which it is domiciled; i.e., its cell. The radio signal originating from such base stations will be routed with city/area code parameters to disclose the

origin of a call via the Cell of Origin (COO). Further binning of the available area codes, as defined by the Nigerian Communications Commission (NCC) [272], like in the case of USA [267], can be made to ensure discrete proximity to the COO of a mobile phone radio information. Thus, for each call placed by a user, the trunk prefix in the trunk code [272] (i.e. the '0' in '043' of 043-805123456, for example) will remain, but the trunk code will be modified to characterise the discrete area in the city from where a call originated.

The hierarchical structure of a cellular network is illustrated in Figure 5.4 [273]. The structure is formed by connecting the major components like mobile phones, Base stations (BS) and Mobile Switching Centres (MSC). The BS serves a cell which could be a few kilometres in diameter as shown in Figure 5.4 (a); instead of using a circle to depict an ideal situation, the hexagon is used for convenience. When the cells are grouped together, they form a Cluster as shown in Figure 5.4 (b). Usually, the number of cells in a cluster is limited by the requirement that the clusters must fit together like jig-saw pieces. The possible cell clusters are the 4-,7-,12- and 21-cell clusters [273]. The size of a cell can be changed or reduced by splitting the original cell. Figure 5.4 (c) illustrates how a cell can be split into four; this involves reducing the radius of the original cell by half [273]. As illustrated in Figure 5.4 (d), all BSs in a cluster are connected to the MSC using land lines. Each MSC of a cluster is then connected to the MSC of other clusters and a Public Switched Telephone Network (PSTN) main switching centre. The MSC stores information about the subscribers located within the cluster and is responsible for directing calls to them [273].

The advantage of these codes is that it will be relative to the specific geographical location of a mobile phone; for instance, if a user leaves Gwarimpa for Nyanya (two different areas in Abuja, Nigeria), the area code would change and would identify where the caller resides at the time of the call. This is also the case for interstates. Genuine privacy issues may not be relevant since, as in the current situation, users would be at liberty to either activate or de-activate the Caller ID facility [266]. In addition, it would be correct to posit that national/public security should take priority over the personal security/privacy of an individual.

In security related terminologies, this proposal is inherently a location-based authentication initiative; though it does not comprise all the ingredients of AAA (Authentication, Authorisation and Accounting) [4, 93, 267]. However, all the processes of AAA [266] would be a security requirement for the operations of special security agencies. These security agents and some designated top government functionaries could be permitted by the NCC and the network operators, at the instance of necessary legislations, to operate special mobile numbers and phones that would not reveal these city/area codes.

After the treatment of the state of cyber insecurity in Africa which led to a proposed technological solution as presented above, the most likely challenge to this proposal, which is a human factor index, is catered for via a survey that is presented in the next section; with encouraging results.

5.6 Anticipated Challenges

Every technology evolves with its challenges; this is no exception. In this section, the possible challenges that may evolve with this proposal are enumerated, with possible countermeasures spelt out.

5.6.1 Roaming

Most times, the mobile phone user travels abroad for conferences, training, workshops, businesses, health, etc. Some of these users prefer to roam their calling IDs. This technology (if operated in Nigeria only) cannot provide the city codes of the foreign countries (unless it is adopted there or globally). However, except for the case of roaming, the proposed city codes provide well-binned space-time information of a mobile phone user based on city/area codes. The possible effect of roaming on the reliability of the proposed system was investigated in the course of implementing this proposal; the result is presented in the next section. The survey showed that users who roam their mobile voice communications and use the service effectively throughout their overseas travels are in the region of 10% for the upper-class citizens and less than 2% for the lower class citizens. Statistics also shows that most of those involved in 419 Scam, as operatives, belong to the lower class.

5.6.2 Survey: Effect of Roaming on Location-Based Authentication

Using the questionnaires attached as Appendix 3, two surveys were conducted, with field trips to Nigeria; partially in November 2013 and December/January 2015/2016. The approaches included the use of questionnaires, structured interviews and examination of official records; using direct personal contact, email and phone calls. The data obtained from the security agencies (NP, SFU, NFIU, EFCC and NCC), among others, facilitated the discussions on cybersecurity in Section 5.4. Details of the survey on GSM roaming are now presented in this section.

Due to lack of cooperation by Mobile Service Providers (MSPs) which frustrated the completion of the survey in 2013, it was decided that random samples of individuals be used from a population of (about 250) Nigerians of all designations from all parts of the country and beyond. The data was mainly generated using Question 18 in the structured interview sample questions for GSM mobile services in Appendix 3. The compiled data is as presented in Table 5.3 (with a legend), while the annual statistics and roaming frequency are plotted in Figures 5.5 and 5.6, respectively.

Table 5.3. Grand total of the number of subscribers who roam their GSM calls in Nigeria with associated statistics

YEARS	**NUMBER OF ROAMING SUBSCRIBERS PER YEAR**								**Remarks**
	0	1	2	3	4	5	Above 5	Total	Digits 0-5 represent the no. of times the users against each year roamed their calls.
2006	228	20	1	1	0	0	0	22	Out of 250 Samples (8.8%); < 2% under 30.
2007	223	10	12	2	1	1	1	27	Out of 250 Samples (10.8%); < 2% under 30.
2008	229	13	5	1	0	0	2	21	Out of 250 Samples (8.4%); < 3% under 30.
2009	229	14	0	3	1	0	3	21	Out of 250 Samples (8.4%); < 2% under 30.
2010	226	20	1	1	0	2	0	24	Out of 250 Samples (9.6%); < 2.5% under 30.
2011	227	22	0	0	0	1	0	23	Out of 250 Samples (9.2%); < 2.5% under 30.
2012	223	21	1	0	2	0	3*	27	Out of 250 Samples (10.8%); < 2.5% under 30.
2013	221	19	1	3	4	1	1	29	Out of 250 Samples (11.6%); < 2% under 30.
2014	197	30*	5*	4*	1*	3*	10*	53*	Out of 250 Samples (21.2%); < 10% usage; < 2% under 35.
2015	212	35(30*)	0	0	1	0	2	38	Out of 250 Samples (15.2%); < 10% usage; < 2% under 35.
Grand Total	2,215	204(60*)	26(5*)	15(4*)	10(1*)	8(3*)	22(13*)	285	Out of 2,500 Cumulative Samples (11.4%); < 10% usage; < 2.25% under 35.
Average No. of Roaming Subscribers Per Annum								28.5	Out of 250 Samples (11.4%); < 2.25% under 35. This represents the annual average over the ten years for the 250 samples considered

LEGEND

* - This implies automatic roaming by MSPs; this is usually the case if the subscriber's credit level is high (about ₦5,000.00; $16.67.00; £12.50; using the Bureau de Change (BDC) exchange rate of 300 Naira to a US Dollar and 400 Naira to a Pound Sterling) as at the time of embarking on overseas travels - where the phone setting gives the MSP a leeway to manipulate the system to own advantage.

< x % Under 35 - This means that less than x % of subscribers in the random sample were under 35 years of age. This information is relevant

because the NP/EFCC records show that most cyber offenders in Nigeria are young (between the ages of 20 and 35 years).

< 10% Usage - This means less than 10% of subscribers actually use the roamed service (usually voice calls) throughout the period of their overseas journeys. Though the cost for SMS roaming is relatively cheaper than that of voice calls, some of the MSPs do not allow the use of SMS facility for automatic roaming – apparently, designed to leave the subscriber with no option other than to make voice calls at relatively high rates.

Result Analysis

From the computations in Table 5.3 (especially the remark column which is based on both the recorded data and personal interactions with the target population) and the illustrations in Figure 5.5, it is obvious that the members of the targeted population who roam their mobile services are in the region of 10%.

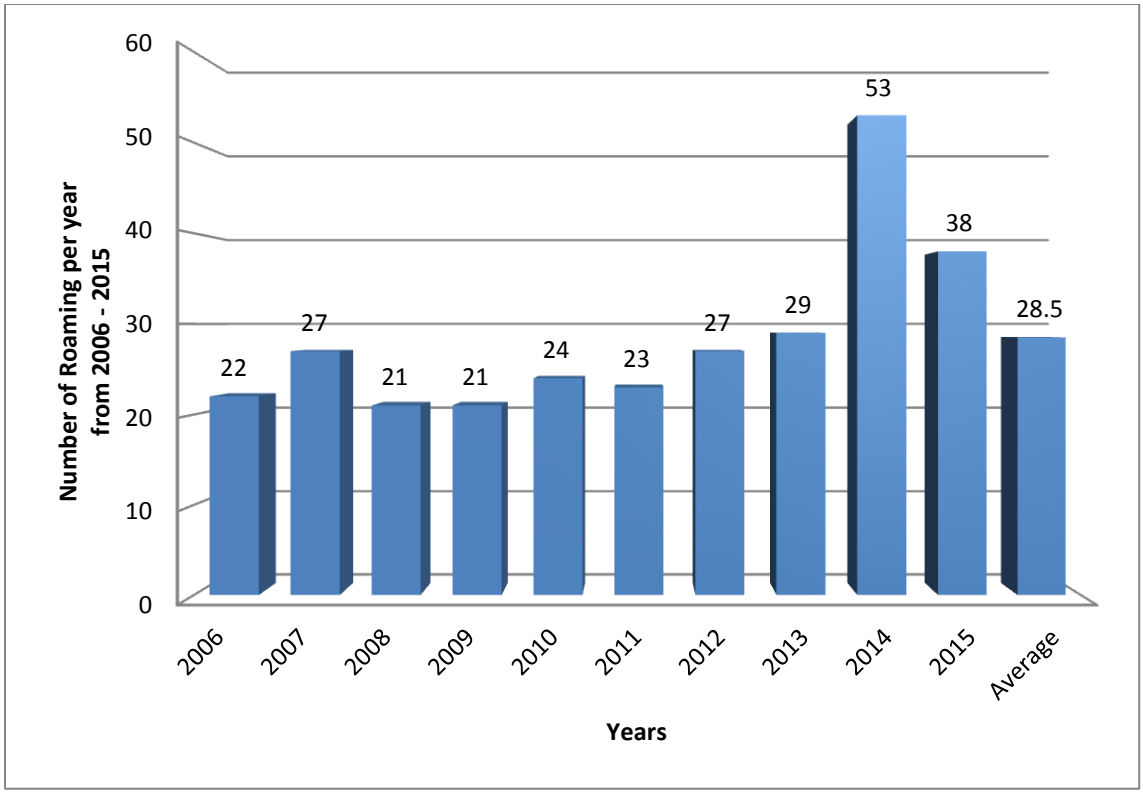


Figure 5.5. Total and average annual roaming statistics in a decade

Bearing in mind the fact that part of the roaming incidence is at the discretion of the MSPs rather than the subscribers, personal interactions also authenticated that the roaming subscribers are not only less than 10% of the population, their actual usage of the roamed services is also much less than 10% of their communication needs (i.e., 10% of 10% = 0.1 x 0.1 = 0.01 = 1% of the population). This is not an exaggeration because, in practice, most of those who roam their mobile services only use them to view calls; to enable them to use other facilities to contact their callers in the case of important calls. This is due to the factual belief that roamed services are extravagantly costly. Table 5.3 and Figure 5.6 illustrate the fact that the number of those who roamed their mobile services only once in a year is conspicuously much higher than those who roamed twice or more.

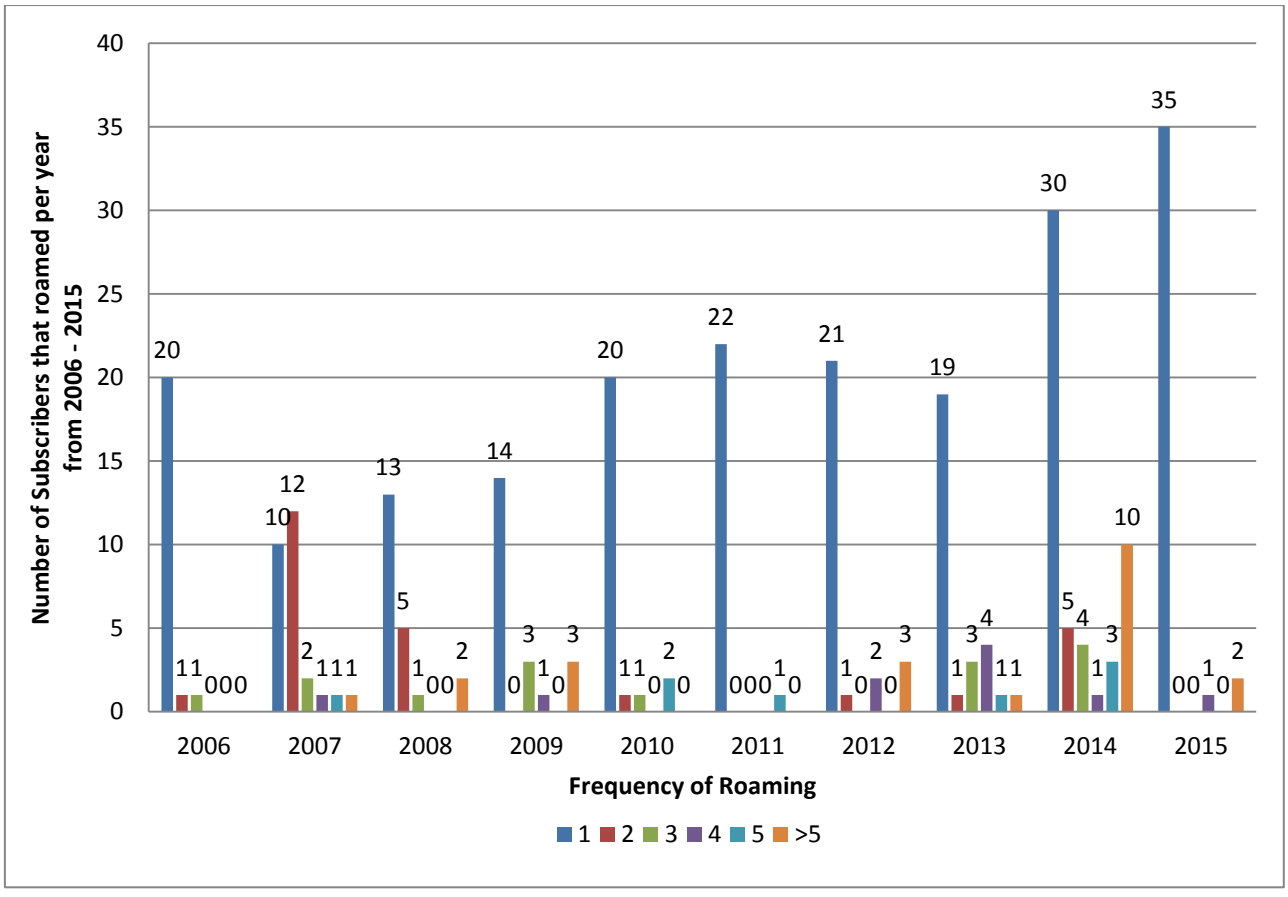


Figure 5.6. Annual roaming frequency

From the above statistics, it cannot be safely posited that the incidence of effective roaming is on the rise because, of recent, more roaming is done at the instance of the MSPs. It is noteworthy, that there were abrupt hikes in the number of roaming subscribers in 2014 and 2015. These could be explained by two possible reasons: Firstly, there were more roaming at the instance of the MSPs as a marketing strategy to make more money at all costs; secondly, these might be connected with the uncertainties associated with the general elections earlier scheduled for 14th February 2015 – it was postponed and later held on 28th March 2015. This second reason is informed by the fact that most of the roaming within the time frame were concentrated in the last quarter of 2014 and the first quarter of 2015; with a good number of the affected individuals being politicians.

From the above, it could be deduced that there remained a culture of lukewarm attitude towards roaming among Nigerians, throughout the decade under review. It is also very impressing to observe that about less than 2.25% of the roaming subscribers were under the age of 35; data from and discussions with the SFU/EFCC indicate that the effective age bracket for most cyber offenders in Nigeria is from 20 – 35 years. Thus, it could be concluded that, in pragmatic terms, about 1.0% of the targeted population roam their mobile services, and less than 2.25% are under the age of 35. Hence, it would be safe to posit that the likely negative effect of GSM roaming on the proposed LBA as a means of mitigating the incidence of 419 advance fee fraud, and related cyber offences in the world, would be negligible.

5.6.3 Awareness Education

In Nigeria, most users tend to believe that all telecommunications caller numbers not starting with the trunk prefix (zero) are an international call. This has been used to swindle victims most often than not. When this proposal is implemented, most users will face the challenge of adjusting to recognise that all numbers not beginning with the zero prefix are not foreign numbers. It is hoped that a sensitisation campaign will be carried out to educate the general public about the change using Newspapers, radio, TV stations, posters, etc.

The Government at all levels, NCC, MSPs and security agencies would have an important role to play in this regard.

5.6.4 Cloning Fraud

This is a high-tech problem that can be perpetrated only by some experts who are capable of knowingly, wittingly or fraudulently obtaining the factory details of a mobile-phone or by monitoring the radio characteristics of a particular mobile phone for a long time. Cloning fraud occurs when the factory-set Electronic Serial Number (ESN) and telephone Mobile Identification Number (MIN) have been dubbed and used to programme a different phone, such that when the legal, as well as illegal (cloned), user places a call, the ESN/MIN of the legitimate mobile will be transmitted [274, 275]. The transmission of similar ESN/MIN from different mobile nodes is already known [275] and described as Sybil attack in, for example, wireless sensor networks [272, 274, 276-278], and several solutions have been suggested [279-283]. It will be easy to identify the location from which the fraudulent user calls when the proposed method is adopted since the city/area codes would be different. This can easily isolate the legitimate user from the illegitimate user. Meanwhile, for cell phone cloning fraud, the cellular equipment manufacturing industry has deployed authentication systems that have proven to be a very effective countermeasure [274].

5.6.5 Immunity/Security of Special Security Agencies and Authorised Government Functionaries

It may be delicate to always reveal the space-time information of a security professional, such as agents of the State Security Service (SSS). These security agents and some designated top government functionaries could be permitted by the NCC and the MSPs, at the instance of necessary legislations, to operate special mobile numbers and phones that would not reveal these city/area codes.

5.6.6 Man-in-the-middle and Rogue Base-station Attacks

The man-in-the-middle (MitM) attack involves intercepting a call and re-routing it through a third party to the receiver at the other end, such that both the original

source and the sink do not know that the link is mutilated. This can be tackled by authenticating the Mobile User (MU) and a Home e-Node B (HeNB or LTE Femtocell) from a contractual proxy-signature already established between the HeNB and OAM (Operation, Admission and Maintenance) [284]. A rogue base station may lead to a Denial of Service (DoS). Meanwhile, DoS due to a rogue base station has been discovered and solution proffered in [285], including impersonation [286].

5.6.7 Compatibility with future evolutions

LTE-A Rel-10 and beyond, is not a new radio access technology but the evolution of LTE to further improve the performance [287]. This evolution inherited all the Rel-8/9 functionalities with additions such as carrier aggregation, enhanced multi-antenna support, improved support for heterogeneous deployments, and relaying [287]. The Rel-9 uses OTDOA for uplink and E-CID (Enhanced-Cell ID) for both uplink and downlink [271]. The E-CID positioning algorithm, in addition to the serving eNB (in other words the radio cell) and the broadcast cell ID which was defined in LTE Rel.8, the information such as propagation delay calculated from the difference in timing of signal transmission and reception and the Angle of Arrival (AoA), are utilised to estimate the position of the MU [271]. For other lower standards, the proposed technology would comfortably fit in.

5.6.8 Replacement for other positioning algorithms

This algorithm may rather be seen as the primary algorithm to which any other possible geographical positioning algorithm can be appended. For instance, the use of GPS can be added to the city code algorithm. After all, the Rel-9 was defined to involve assisted-GPS (A-GPS), OTDOA and E-CID [271].

5.7 The Way Forward

An assessment of the possible solutions to the problem identified in Section 2.10.1 (as illustrated in Figure 2.21) seems to be in favour of the solution by manufacturers. That is, since a fraudulent user (Client) could supply fake own location data at will, and vice versa, there is an urgent need to make all

transceiver devices GPS-compliant, with inherent capabilities for location-based automatic mutual authentications. This would go a long way in facilitating successful socio-technological countermeasures against feigned-location based advance fee fraud related crimes. This recommendation is in congruence with [247], which posited that the P(Y) code signature should be injected into the user's device to avoid carrying the GPS receiver every time.

However, privacy issues might arise to oppose this recommendation. This would be a weak argument, given the fact that such devices could be enhanced with enabling/disabling capabilities at the user's discretion; similar to the Bluetooth technology. In addition, privacy considerations should not be at the expense of the emergence of a fault-tolerant web of confidence, that is inherent in Zimmermann's web of trust proposed some 20 years ago [94]. Similarly, it would be more proper for national/public security to take precedence over issues that relate to personal security/privacy of any individual.

This brings to a close, the discussions on the need to employ the interplay among human trust, other trust-related human characteristics, and technology to mitigate the dangers posed by confidence artists in the cyberspace. A concise global conclusion for the entire Thesis and the PhD research effort will follow immediately after the deductive summary for this chapter.

5.8 Deductions

The main concern of this chapter is to devise a means for maximising the benefits of the GPS technology in optimising the effectiveness of location-based authentication techniques, in an effort to extend the security perimeter relative to human trust. The chapter reviewed the concepts/techniques associated with this authentication scheme and explained the current technological capabilities of the GPS, with some illustrations. It was observed that the effectiveness of a GPS-derived location-based authentication technique is being hampered by the fact that the user must be the one to supply the own space-time information (own location data) to other correspondents, and vice versa, to facilitate authentication; given the possibility that a fraudulent user (Client) could supply fake own location data at will. It recommends the urgent need to make all

transceiver devices GPS-compliant, with inherent capabilities for location-based automatic mutual authentication; as achieved by the Cloud Data Repository Access Service Prototype (a novelty in the public civil domain). This would go a long way in facilitating successful socio-technological countermeasures against feigned-location based fraud related crimes, especially if combined with cell-splitting of the Cell of Origin and further digitisation of the GSM country codes into area/city codes.

This recommendation is against the backdrop of the fact that, privacy issues should not be allowed to hinder the emergence of a fault-tolerant web of confidence that is inherent in Zimmermann's web of trust. In addition, it would be more proper for national/public security to take precedence over issues that relate to personal security/privacy of any individual. This would be a plausible argument since such devices could be enhanced with enabling/disabling capabilities at the user's discretion; similar to the Bluetooth technology.

As this technological solution is proposed herein to check 419 and other related cybercrimes, let the attention of all stakeholders be drawn to the fact that, although security solutions have a technological component, security is fundamentally a people-centred problem. Hence, there would be a need to combine technical efforts with administrative efforts to chart a way forward; this could be in form of good governance by way of mitigating corruption and job creation for the idle youth populations in Africa.

Chapter 6

Conclusions and Recommendations

6.1 Summary of Conclusions

This research was motivated by a strong belief that, solving for insecurity in cyber networks is more of a human-centred problem than a technology-centred one. In other words, pragmatically speaking, for instance, there could be no technical hacking in a vacuum (completely devoid of human compromise). Thus, the apparent lack of adequate attention on human-factor-oriented cyber defence inspired its conduct in the chosen topic 'Cryptography and Computer Communications Security: Extending the Human Security Perimeter through a Web of Trust.' This is with a view to devising a new or adapted technological scheme that would combine the capabilities of technology with the human factor of trust in order to enhance the effectiveness of cyber defence; in an effort to answer the main research question. This was accomplished by increasing or expanding the security perimeter relative to human trust, via a network of trustees and secure web environment in conjunction with the SSSS.

In general terms, it is optimistic that the outcome of this study would be of great benefit to governments, corporate organisations and individuals who have one thing or the other to do with the ICT industry. The work is also aimed at stimulating interest in this subject area among the upcoming generation of engineers in the developing countries, especially Nigeria – the author's home country, where cryptography is not a popular subject.

In specific terms, the results attained in this work have uncovered many areas of new knowledge. The main novelties that have been accomplished in this work relate to modifications, in form of addition, subtraction or substitution in the SSSS algorithm, in an effort to resolve some of the identified weaknesses in the (k, n) - threshold schemes. The contributions made in the research effort are in two main categories – novelties and risk assessment discoveries. The key contributions are highlighted in the next two paragraphs.

The novelties include modification of the SSSS algorithm by sharing a randomly generated key which is used to lock up the secret data; rather than sharing the secret data itself. This results in improved performances in QoS metrics; which include server bandwidth, system scale, service capacity ratio, real-time performance (time delay) and enhanced security with a higher human trust threshold for the emergent system (CDRSAS). Other novelties in this category include globalisation of the science of secret sharing, application of location-based authentication in secret sharing, inherent capability for location-based automatic mutual authentications, and security-enhanced secret sharing through the use of time window. In addition, the work has also resolved the following long-standing questions in the science of secret sharing: Who is the Combiner; Where should Recombination take place; and Who is entitled to have access to the Reconstructed Secret Data?

The risk assessment discoveries consist of two main areas: discovering the need for a 3-factor (risk, threat and vulnerability) security assessment process and proposing the necessity for same in the military; and derivation of two new pairs of equations - Adeka's Twin Risk Equations and Adeka's Twin Probability Equations on Secret Sharing.

Using social engineering, the confidence artists have contributed a great deal in perverting the cyberspace with an overwhelming negative impression on cybersecurity. Defeating socio-cryptanalysis in the cyberspace would require a combination of strategies that are centred on the interplay among human trust, trust-related human attributes, and technology. In this connection, there would be needs for the following: Making all transceiver devices GPS-compliant with inherent capabilities for location-based automatic mutual authentication in the public civil domain; further cell-splitting of the existing Cells of Origin in the GSM technology; further digitisation of the existing GSM country codes into area/city codes; and deliberate efforts at public awareness education on the significance and efficacy of the employment of trust and trust-related human attributes in countering socio-cryptanalysis in the cyberspace.

The above innovations are discussed in Sections 2.3 – 2.5, 4.9 and 4.10. Detailed chapter summaries are at the end of each chapter in the form of deductive summaries under the heading ‘Deductions’.

6.2 Challenges

In the process of implementing the research design, one major technical challenge that took the time to overcome was how to accurately determine the distance in kilometres between two GPS coordinates. This was very crucial because, without it, the CDRSAS-PT would not be able to test for the satisfaction of a location boundary condition, by comparing the registered GPS data with the real login GPS data that would be keyed in by Clients for location-based authentication; within a maximum of 30-metre radius. The search for a solution led to the discovery of the Haversine Law and Haversine Formula, which facilitated the mathematical calculations, as illustrated in Section 4.11.

The second challenge relates to the fluidity of happenings in the cyberspace; i.e., how to cope with the rate of increase of cybercrimes; both its frequency and intensity. Apart from individual and organisational targets, the rate at which apparently organised attacks are perpetrated against both national security and economic interests seems to buttress the fact that the Fifth Domain in warfare is already a reality; with the US, UK, Russia, China, North Korea, Iran, etc., being both perceived as victims and aggressors. In the Global Risk Report 2015, released by the World Economic Forum, it is highlighted that large-scale cyberattacks are among the prominent risks in 2015. In the US alone, cybercrime already costs an estimated $100 billion each year.

Administrators of secret sharing should always remember to carefully define the access structure, in order to partially offset the limitation inherent in the fact that all participants are not equally trustworthy.

6.3 Recommendations for Future Work

This marks the completion of both the Thesis and the PhD research effort, except for the suggested scope for future work herein. The likely scope items for future work would focus on the need to adapt the CDRSAS-PT for high-

volume traffic operation for possible deployment at the organisational level. The effort will focus on the following:

- ❖ Having a managed area to set up future shares at a given period;
- ❖ Having more than one different share sessions happening simultaneously;
- ❖ Capturing all the user interactions in a database;
- ❖ Other incorporations aimed at making the system more robust and versatile;
- ❖ Subjecting the system to high-volume traffic performance tests, when adapted for public deployment; and
- ❖ The upgraded system will be PHP-based, instead of a Java server, to make it more cost effective for hosting on the website instead of a computer-based server.

The CDRSAS-PT originally used the Shamir's key that is derived from the encrypted output of the original message itself. This would make the system less secure when homomorphic encryption takes off in earnest; hence, the Shamir's key has now been replaced with a randomly generated key. Details of future work to further enhance the performance and security of the system are in Appendix 8 {every item asterisked therein is a projected future characteristic of the Deployment System Type (CDRSAS-DT) which is currently unavailable in the prototype (CDRSAS-PT)}.

This ends the Thesis, with bibliography, eight appendices and the list of the author's contributions attached.

Bibliography

[1] C. Swenson, *Modern Cryptanalysis: techniques for advanced code breaking*: John Wiley & Sons, 2012.

[2] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of management review,* vol. 20, pp. 709-734, 1995.

[3] S. Zhen, L. Zhoujun, and D. Wenhua, "Different approaches for the formal definition of authentication property," *Communications,* pp. 854-858, 2003.

[4] R. He, M. Yuan, J. Hu, H. Zhang, Z. Kan, and J. Ma, "A novel service-oriented AAA architecture," in *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, 2003, pp. 2833-2837.

[5] L. Csirmaz, "Ramp secret sharing and secure information storage," 2009.

[6] D. McQuail, *McQuail's mass communication theory*: Sage publications, 2010.

[7] M. M. Spada, "An overview of problematic Internet use," *Addictive behaviors,* vol. 39, pp. 3-6, 2014.

[8] C. Mendelson, "Recruiting participants for research from online communities," *Computers Informatics Nursing,* vol. 25, pp. 317-323, 2007.

[9] P. B. Gove, *Webster's third new international dictionary of the English language, unabridged* vol. 1: Merriam-Webster, 1993.

[10] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*. Indianapolis: Wiley Publishing Inc., 2000/2004.

[11] E. Site, R. Cuts, and S. In, "Security Engineering: A Guide to Building Dependable Distributed Systems," *2ed Editio,* pp. 239-274, 2008.

[12] R. Moore, *Cybercrime: Investigating high-technology computer crime*: Routledge, 2010.

[13] W. G. Kruse II and J. G. Heiser, *Computer forensics: incident response essentials*: Pearson Education, 2001.

[14] D. Mann and M. Sutton, ">> NETCRIME More Change in the Organization of Thieving," *British Journal of Criminology,* vol. 38, pp. 201-229, 1998.

[15] D. Miyamoto, "Development of Practical IP Trace-back Technology," *NICT News, No. 396,* September, 2010.

[16] S. Ridley and J. Bird, *Cybercrime*. London: Franklin Watts, 2010.

[17] ITU. (2010). *Global Cybersecurity Agenda (GCA)*. Available: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/chapter_5.html [Accessed: 16 Nov. 2012].

[18] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*: indianapolis: John Wiley & Sons, 2011.

[19] T. Vaidya, "2001-2013: Survey and Analysis of Major Cyberattacks," *arXiv preprint arXiv:1507.06673,* 2015.

[20] T. Rid, "Cyber war will not take place," *Journal of Strategic Studies,* vol. 35, pp. 5-32, 2012.

[21] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Internet of things (iThings/CPSCom), 2011 international conference on and 4th international conference on cyber, physical and social computing*, 2011, pp. 380-388.

[22] ITU. (2005, 2 October). *World Summit on Information Society*. Available: http://www.itu.int/wsis/index.html

[23] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*: Indianapolis: John Wiley & Sons, 2011.

[24] C. Hadnagy, *Social engineering: The art of human hacking*: Indianapolis: John Wiley & Sons, 2010.

[25] G. C. Kessler, "An overview of cryptography," ed: Gary C. Kessler, 2015.

[26] S. Tzu, *The art of war*: Orange Publishing, 2013.

[27] T. Espiner. (2010). *Whitehall official outlines cybersecurity funding plan*. Available: http://www.zdnet.co.uk/news/security/2010/11/17/whitehall-official-outlines-cybersecurity-funding-plan-40090898/ [Accessed: 29 Sep. 2011].

[28] M. Easterby-Smith, R. Thorpe, and P. R. Jackson, *Management research*: Sage, 2012.

[29] R. B. Johnson, A. J. Onwuegbuzie, and L. A. Turner, "Toward a definition of mixed methods research," *Journal of mixed methods research,* vol. 1, pp. 112-133, 2007.

[30] J. W. Creswell, *Research design: Qualitative, quantitative, and mixed methods approaches*: Sage publications, 2013.

[31] R. E. Glasgow, "What does it mean to be pragmatic? Pragmatic methods, measures, and models to facilitate research translation," *Health Education & Behavior,* vol. 40, pp. 257-265, 2013.

[32] G. Badley, "The crisis in educational research: a pragmatic approach," *European educational research journal,* vol. 2, pp. 296-308, 2003.

[33] E. D. Brod, *The Essence of Ethical Pragmatism: The Common Sense Philosophy*. Raleigh (NC): Lulu Publishing Services, 2016.

[34] M. I. U. Adeka, "Threat Analysis versus Risk Analysis in Intelligence and Security Assessment " in *Nigerian Defence and Security: Essays in Commemoration of Nigerian Defence Academy Golden Jubilee*, O.E. Tangban, Ed., ed Kaduna: Nigerian Defence Academy, 2014, pp. 705-744.

[35] K. M. Martin, "Challenging the adversary model in secret sharing schemes," *Coding and Cryptography II, Proceedings of the Royal Flemish Academy of Belgium for Science and the Arts,* pp. 45-63, 2008.

[36] A. M. Joshi, D. M. Jadhav, N. A. Kazi, A. N. Suryawanshi, and J. Katti, "Authentication of grayscale forensic image using visual secret sharing," in *Emerging Devices and Smart Systems (ICEDSS), Conference on*, 2016, pp. 56-60.

[37] R. Jurca and B. Faltings, "An incentive compatible reputation mechanism," in *E-Commerce, 2003. CEC 2003. IEEE International Conference on*, 2003, pp. 285-292.

[38] A. Shamir, "How to share a secret," *Communications of the ACM,* vol. 22, pp. 612-613, 1979.

[39] F. M. Reza, *An introduction to information theory*: Courier Corporation, 1994.

[40] F. Miao, Y. Fan, X. Wang, Y. Xiong, and B. Moaman, "A (t, m, n)-Group Oriented Secret Sharing Scheme," *Chinese Journal of Electronics,* vol. 25, pp. 174-178, 2016.

[41] Y. Miura and Y. Watanabe, "Security of (n, n)-threshold audio secret sharing schemes encrypting audio secrets," in *Statistical Signal Processing Workshop (SSP), 2016 IEEE*, 2016, pp. 1-5.

[42] K. Muthukumar and M. Nandhini, "Modified secret sharing algorithm for secured medical data sharing in cloud environment," in *Science Technology Engineering and Management (ICONSTEM), Second International Conference on*, 2016, pp. 67-71.

[43] A. Parakh and S. Kak, "Space efficient secret sharing for implicit data security," *Information Sciences,* vol. 181, pp. 335-341, 2011.

[44] C. L. Liu, *Introduction to combinatorial mathematics* vol. 181: McGraw-Hill New York, 1968.

[45] G. R. Blakley, "Safeguarding cryptographic keys," *Proc. of the National Computer Conference1979,* vol. 48, pp. 313-317, 1979.

[46] C. A. Neff, "A verifiable secret shuffle and its application to e-voting," in *Proceedings of the 8th ACM conference on Computer and Communications Security*, 2001, pp. 116-125.

[47] V. Nikov, S. Nikova, B. Preneel, and J. Vandewalle, "Applying General Access Structure to Metering Schemes," *IACR Cryptology ePrint Archive,* vol. 2002, p. 102, 2002.

[48] V. Nikov, S. Nikova, B. Preneel, and J. Vandewalle, "On distributed key distribution centers and unconditionally secure proactive verifiable secret sharing schemes based on general access structure," in *Progress in Cryptology—INDOCRYPT 2002*, ed: Springer, 2002, pp. 422-435.

[49] R. Cramer, I. Damgård, and U. Maurer, "General secure multi-party computation from any linear secret-sharing scheme," in *Advances in Cryptology—EUROCRYPT 2000*, 2000, pp. 316-334.

[50] D. J. Pohly and P. McDaniel, "Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols," in *Dependable Systems and Networks (DSN), 2016 46th Annual IEEE/IFIP International Conference on*, 2016, pp. 371-382.

[51] M. Mortensen, "Secret Sharing and Secure Multi-party Computation," *University of Bergen,* 2007.

[52] S. Patil and P. Deshmukh, "An Explication of Multifarious Secret Sharing Schemes," *International Journal of Computer Applications,* vol. 46, 2012.

[53] M.W. Inc., "Webster's third new international dictionary... unabridged: With seven language dictionary.(3 vols)," ed: Merriam-Webster, 1993.

[54] P. Paillier, "On ideal non-perfect secret sharing schemes," in *International Workshop on Security Protocols*, 1997, pp. 207-216.

[55] D. R. Stinson, *Cryptography: theory and practice*: CRC press, 2005.

[56] A. J. Menzies, P. C. van Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," ed: CRC Press, 1997.

[57] Y. Sun, G. Li, Z. Lin, F. Xiao, and X. Yang, "A completely fair secret sharing scheme without dealer," in *Consumer Electronics-Taiwan (ICCE-TW), 2016 IEEE International Conference on*, 2016, pp. 35-36.

[58] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE transactions on information theory,* vol. 30, pp. 208-210, 1983.

[59] M. Mignotte, "How to share a secret," in *Cryptography*, ed: Springer, 1983, pp. 371-375.

[60] S. C. Kothari, "Generalized linear threshold scheme," in *Advances in Cryptology*, 1985, pp. 231-241.

[61] Y. Wang, Z. Liu, and Q. Xu, "New rational parties relying on reputation," *Security and Communication Networks,* vol. 7, pp. 1128-1137, 2014.

[62] P. Feldman, "A practical scheme for non-interactive verifiable secret sharing," in *Foundations of Computer Science, 1987., 28th Annual Symposium on*, 1987, pp. 427-438.

[63] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology—CRYPTO'91*, 1992, pp. 129-140.

[64] Z. Wang, M. Karpovsky, and L. Bu, "Design of Reliable and Secure Devices Realizing Shamir's Secret Sharing."

[65] G. Orwell, *Animal farm*: Random House, 2010.

[66] M. Ito, A. Saito, and T. Nishizeki, "Secret sharing scheme realizing general access structure," *Electronics and Communications in Japan (Part III: Fundamental Electronic Science),* vol. 72, pp. 56-64, 1989.

[67] M.-Y. Wu, "Improving Security and Privacy of Images on Cloud Storage by Histogram Shifting and Secret Sharing," 2015.

[68] M. A. Blaze, "Escrow key management system for accessing encrypted data with portable cryptographic modules," ed: Google Patents, 1998.

[69] N. Zhang, Y. Chen, H. Tian, T. Wang, and Y. Cai, "A Novel Connection Correlation Scheme Based on Threshold Secret Sharing."

[70] T. Okamoto, "Authenticated key exchange and key encapsulation in the standard model," in *Advances in Cryptology–ASIACRYPT 2007*, ed: Springer, 2007, pp. 474-484.

[71] M. T. Arafin and G. Qu, "Secret Sharing and Multi-user Authentication: From Visual Cryptography to RRAM Circuits," in *Proceedings of the 26th edition on Great Lakes Symposium on VLSI*, 2016, pp. 169-174.

[72] B. G. Banik and S. K. Bandyopadhyay, "Secret Sharing Using 3 Level DWT Method of Image Steganography Based on Lorenz Chaotic Encryption and Visual Cryptography," in *Computational Intelligence and Communication Networks (CICN), 2015 International Conference on*, 2015, pp. 1147-1152.

[73] R. Bitar and S. E. Rouayheb, "Staircase codes for secret sharing with optimal communication and read overheads," *arXiv preprint arXiv:1512.02990,* 2015.

[74] M. Tompa and H. Woll, "How to share a secret with cheaters," *journal of Cryptology,* vol. 1, pp. 133-138, 1989.

[75] S. Sarma, "A Review of Secret Sharing Schemes," *Research Journal of Information Technology,* vol. 5 (2), pp. 67-72, 2013.

[76] M. Cheraghchi, "Nearly optimal robust secret sharing," IACR Cryptology ePrint Archive, 2015: 9512015.

[77] S. J. De and S. Ruj, "Failure Tolerant Rational Secret Sharing," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 925-932.

[78] C. Blundo, A. De Santis, and U. Vaccaro, "Efficient sharing of many secrets," in *Annual Symposium on Theoretical Aspects of Computer Science*, 1993, pp. 692-703.

[79] M. Deshmukh, N. Nain, and M. Ahmed, "An (n, n)-Multi Secret Image Sharing Scheme Using Boolean XOR and Modular Arithmetic," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 690-697.

[80] T. Tassa, "Hierarchical threshold secret sharing," *Journal of Cryptology,* vol. 20, pp. 237-264, 2007.

[81] M. Fukumitsu, S. Hasegawa, J.-Y. Iwazaki, M. Sakai, and D. Takahashi, "A Proposal of a Password Manager Satisfying Security and Usability by Using the Secret Sharing and a Personal Server," in *2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA)*, 2016, pp. 661-668.

[82] W. Ogata, K. Kurosawa, and D. R. Stinson, "Optimum secret sharing scheme secure against cheating," *SIAM Journal on Discrete Mathematics,* vol. 20, pp. 79-95, 2006.

[83] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed-Solomon codes," *Communications of the ACM,* vol. 24, pp. 583-584, 1981.

[84] P. Rogaway and M. Bellare, "Robust computational secret sharing and a unified account of classical secret-sharing goals," in *Proceedings of the 14th ACM conference on Computer and communications security*, 2007, pp. 172-184.

[85] V. Harish, N. R. Kumar, and N. Raajan, "New visual secret sharing scheme for gray-level images using diamond theorem correlation pattern structure," in *Circuit, Power and Computing Technologies (ICCPCT), 2016 International Conference on*, 2016, pp. 1-5.

[86] W. Huang, M. Langberg, J. Kliewer, and J. Bruck, "Communication efficient secret sharing," *arXiv preprint arXiv:1505.07515,* 2015.

[87] S. Jarecki, A. Kiayias, H. Krawczyk, and J. Xu, "Highly-Efficient and Composable Password-Protected Secret Sharing (Or: How to Protect Your Bitcoin Wallet Online)," in *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 276-291.

[88] Y. Liu, Y. Wang, L. Zhu, J. Jiang, and X. Hei, "(k, n) Secret Sharing Scheme against Two Types of Cheaters," in *Networking and Network Applications (NaNA), 2016 International Conference on*, 2016, pp. 284-287.

[89] F. Farahmand, S. B. Navathe, P. H. Enslow, and G. P. Sharp, "Managing vulnerabilities of information systems to security incidents," in *Proceedings of the 5th international conference on Electronic commerce*, 2003, pp. 348-354.

[90] J. Long, *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*: Syngress, 2011.

[91] InstantSecurityPolicy.com. *Custom Security Policies*. Available: http://www.Instantsecuritypolicy.com/index-uk.html?gclid=CKrV1vr8zbYCFaTItAodsTAAvA. [Accessed: 3 Jun. 2015].

[92] M. Adeka, S. Shepherd, and R. Abd-Alhameed, "Resolving the password security purgatory in the contexts of technology, security and human factors," in *Computer Applications Technology (ICCAT), 2013 International Conference on*, 2013, pp. 1-7.

[93] D. Jaros and R. Kuchta, "New Location-Based Authentication Techniques in the Access Management," in *Wireless and Mobile Communications (ICWMC), 2010 6th International Conference on*, 2010, pp. 426-430.

[94] B. Schneier and N. Ferguson, "Practical cryptography," *Wiley Dreamtech India Pvt Ltd,* 2003.

[95] N. Ferguson and B. Schneier, *Practical cryptography* vol. 141: Wiley New York, 2003.

[96] E. Gerck, "Overview of Certification Systems: X. 509, PKIX, CA, PGP & SKIP," *The Bell,* vol. 1, p. 8, 2000.

[97] A. Torp and L. S. Vikør, *Hovuddrag i norsk språkhistorie*: Ad Notam Gyldendal, 1993.

[98] E. V. Gordon, "An Introduction to Old Norse," 1981.

[99] N. S. Russell. (July 2012). *"10 Simple Behaviors That Diminish Trust" in Trust - The New Workplace Currency. [Online]. Available:* . Available: https://www.psychologytoday.com/blog/trust-the-new-workplace-currency/201207/10-simple-behaviors-diminish-trust. [Accessed: 4 Oct 2016].

[100] P. B. Forsyth, C. M. Adams, and W. K. Hoy, *Collective Trust: Why Schools Can't Improve without It*: ERIC, 2011.

[101] I. Kompatsiaris, D. Gatica-Perez, X. Xie, and J. Luo, "Special section on social media as sensors," *IEEE Transactions on Multimedia,* vol. 15, pp. 1229-1230, 2013.

[102] F. D. Schoorman, R. C. Mayer, and J. H. Davis, "An integrative model of organizational trust: Past, present, and future," *Academy of Management review,* vol. 32, pp. 344-354, 2007.

[103] A. Kydd, "Trust, reassurance, and cooperation," *International Organization,* vol. 54, pp. 325-357, 2000.

[104] R. Chen. (July 2012). *101 Simple Ways to Build Trust. [Online]. Available:* http : //www.embracepossibility.com/blog/ways-to-build-trust/#comments. [Accessed: 4 Oct. 2016]

[105] P. A. Hancock, D. R. Billings, K. E. Schaefer, J. Y. Chen, E. J. De Visser, and R. Parasuraman, "A meta-analysis of factors affecting trust in human-robot interaction," *Human Factors: The Journal of the Human Factors and Ergonomics Society,* vol. 53, pp. 517-527, 2011.

[106] A. S. Sweet and T. L. Brunell, "Trustee Courts and the Judicialization of International Regimes," *Trustee,* vol. 1, 2013.

[107] D. M. Licht, D. J. Polzella, and K. R. Boff, *Human factors, ergonomics and human factors engineering: An analysis of definitions*: Crew System Ergonomics Information Analysis Center, 1989.

[108] HFES. *Definitions of Human Factors and Ergonomics*. Available: http://www.hfes.org/Web/EducationalResources/HFEdefinitionsmain.html#profsoc. [Accessed: 4 Oct. 2016].

[109] C. D. Wickens, S. E. Gordon, Y. Liu, and J. Lee, "An introduction to human factors engineering," 1998.

[110] X. Liu, A. Nourbakhsh, Q. Li, R. Fang, and S. Shah, "Real-time rumor debunking on twitter," in *Proceedings of the 24th ACM International on Conference on Information and Knowledge Management*, 2015, pp. 1867-1870.

[111] S. Papadopoulos, K. Bontcheva, E. Jaho, M. Lupu, and C. Castillo, "Overview of the Special Issue on Trust and Veracity of Information in Social Media," *ACM Transactions on Information Systems (TOIS),* vol. 34, p. 14, 2016.

[112] B. Shneiderman, *Software psychology: Human factors in computer and information systems (Winthrop computer systems series)*: Winthrop Publishers, 1980.

[113] A. Chapanis, "To Communicate the Human Factors Message, You Have to Know What the Message Is and How to Communicate It " *Human Factors Society Bulletin,* vol. 34, Number 11, pp. 1-4, November 1991.

[114] J. B. Walther, "Computer-mediated communication impersonal, interpersonal, and hyperpersonal interaction," *Communication research,* vol. 23, pp. 3-43, 1996.

[115] L. Z. N. Y. J. Liu and R. Wang, "Collusion detector based on GN algorithm for trust model," 2016.

[116] R. P. Gordon, "The contribution of human factors to accidents in the offshore oil industry," *Reliability Engineering & System Safety,* vol. 61, pp. 95-108, 1998.

[117] A. Chapanis, *Human factors in systems engineering*: John Wiley & Sons, Inc., 1996.

[118] C. P. Nemeth, *Human factors methods for design: Making systems human-centered*: CRC press, 2004.

[119] E. Dictionary, "Encarta Dictionary," ed: English: UK, 2008.

[120] J.H. Cho, A. Swami, and R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys & Tutorials,* vol. 13, pp. 562-583, 2011.

[121] M. Paul and R. John, "Economics, organization and management," ISBN 0-13-223967-1, Prentice Hall, New Jersey1992.

[122] J. B. Rotter, "A new scale for the measurement of interpersonal trust1," *Journal of Personality,* vol. 35, pp. 651-665, 1967.

[123] N. Luhmann, "Familiarity, confidence, trust: Problems and alternatives," *Trust: Making and breaking cooperative relations,* vol. 6, pp. 94-107, 2000.

[124] J. S. Coleman and J. S. Coleman, *Foundations of social theory*: Harvard university press, 1994.

[125] J. D. Lewis and A. Weigert, "Trust as a social reality," *Social forces,* vol. 63, pp. 967-985, 1985.

[126] J. J. Gabarro and A. Althos, "Interpersonal behavior: Communication and understanding in relationships," *Interpersonal behavior: communication and understanding in relationship,* 1978.

[127] M. Deutsch, "Trust and suspicion," *Journal of conflict resolution,* pp. 265-279, 1958.

[128] J. B. Rotter, "Interpersonal trust, trustworthiness, and gullibility," *American psychologist,* vol. 35, p. 1, 1980.

[129] P. Dasgupta, "Trust as a commodity," *Trust: Making and breaking cooperative relations,* vol. 4, pp. 49-72, 2000.

[130] G. F. Farris, E. E. Senner, and D. A. Butterfield, "Trust, culture, and organizational behavior," *Industrial Relations: A Journal of Economy and Society,* vol. 12, pp. 144-157, 1973.

[131] G. Hofstede, "Motivation, leadership, and organization: do American theories apply abroad?," *Organizational dynamics,* vol. 9, pp. 42-63, 1980.

[132] S. B. Sitkin and A. L. Pablo, "Reconceptualizing the determinants of risk behavior," *Academy of management review,* vol. 17, pp. 9-38, 1992.

[133] P. S. Ring and A. H. Van de Ven, "Structuring cooperative relationships between organizations," *Strategic management journal,* vol. 13, pp. 483-498, 1992.

[134] C. Johnson-George and W. C. Swap, "Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other," *Journal of personality and social psychology,* vol. 43, p. 1306, 1982.

[135] J. K. Butler, "Toward understanding and measuring conditions of trust: Evolution of a conditions of trust inventory," *Journal of management,* vol. 17, pp. 643-663, 1991.

[136] D. E. Zand, "Trust and managerial problem solving," *Administrative science quarterly,* pp. 229-239, 1972.

[137] R. W. Boss, "Trust and managerial problem solving revisited," *Group & Organization Management,* vol. 3, pp. 331-342, 1978.

[138] L. McFall, "Integrity," *Ethics,* vol. 98, pp. 5-20, 1987.

[139] K. J. Biba, "Integrity considerations for secure computer systems," DTIC Document1977.

[140] R. Boyle and P. Bonacich, "The development of trust and mistrust in mixed-motive games," *Sociometry,* pp. 123-139, 1970.

[141] H. W. Kee and R. E. Knox, "Conceptual and methodological considerations in the study of trust and suspicion," *Journal of Conflict Resolution,* pp. 357-366, 1970.

[142] L. H. Strickland, "Surveillance and trust1," *Journal of personality,* vol. 26, pp. 200-215, 1958.

[143] A. W. Kruglanski, "Attributing trustworthiness in supervisor-worker relations," *Journal of Experimental Social Psychology,* vol. 6, pp. 214-232, 1970.

[144] M. W. Inc. *Cyber Defined*. Available: http://www.merriam-webster.com/dictionary/cyber?show=0&t=1335771267. [Accessed: 07 Oct. 2011].

[145] R. House. (2006). *Definitions from Dictionary.com: Based on the Random House Unabridged Dictionary*. Available: http://www.dictionary.com. [Accessed: 10 May 2015].

[146] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*: john wiley & sons, 2007.

[147] L. Ellerby. (2009). *Analysis, Plus Synthesis: Turning Data into Insights* Available: http://uxmatters.com/mt/archives/2009/04/analysis-plus-synthesis-turning-data-into-insights.php. [Accessed: 05 Jun. 2015].

[148] S. McLeod. (2008). *Reductionism and Holism*. Available: http://www.simplypsychology.org/reductionism-holism.html . [Accessed: 07 Jun. 2015].

[149] U. A. HQ TRADOC. (2008). *Pamphlet 525-5-500: Glossary, Commander's Appreciation and Campaign Design, Version 1.0*. Available: http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf . [Accessed: 01 Jul. 2012].

[150] G. McColm. *Analysis, Synthesis, and Doing Homework*. Available: http://shell.cas.usf.edu/~mccolm/pedagogy/HWanalysissynthesis.html . [Accessed: 07 Jun. 2015].

[151] A. S. Hornby, "Oxford advanced learner's dictionary," 2005.

[152] G. Stoneburner, A. Goguen, and A. Feringa, "Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology, retrieved November 25, 2009," ed, 2002.

[153] TRADOC (US Army), "Pamphlet 525-5-500: Glossary, Commander's Appreciation and Campaign Design, Version 1.0," ed, 2008.

[154] F. Manual, "Composite Risk Management," 2005.

[155] R. Dunne. (2010). *The intelligence cycle*. Available: http://ukcrimeanalysis.Blog spot.co.uk/2010/11/intelligence-cycle.html. [Accessed: 25 Feb. 2016] .

[156] HQ Intelligence (Nigerian Army), "Chronicle of Command," ed, 2012.

[157] GlobalSecurity. (1986). *National Security Organization (NSO: Nigeria).* . Available: http://www.globalsecurity.org/. [Accessed: 8 July 2012].

[158] IOSS, *1 - Interagency OPSEC Support Staff. Compendium of OPSEC Terms*: Greenbelt, MD, 1991.

[159] A. Nagorski, *The Greatest Battle: Stalin, Hitler, and the Desperate Struggle for Moscow that Changed the Course of World War II*: Simon and Schuster, 2007.

[160] W. Gortney, "Department of Defense Dictionary of Military and Associated Terms," *Joint Publication,* pp. 1-02, 2014.

[161] A. T. Umaru, "An Answer to the Question: Should it be 'Intelligence Synthesis' or 'Intelligence Analysis'? ," ed, 27 July 2012.

[162] C. Kara-Zaitri, "Asset risk management. Risk Management Module: A lecture on Risk Management delivered at the SoEDT, University of Bradford," ed, 2012a.

[163] V. Nikonov, "General risk management concepts " presented at the International Conference on Risk Assessment and Management, 2011.

[164] C. Kara-Zaitri, "Risk assessment tools. Risk Management Module: A lecture on Risk Management delivered at the SoEDT, University of Bradford," ed, 2012b.

[165] Dept of Defence, "MILITARY STANDARD: PROCEDURES FOR PERFORMING A FAILURE MODE EFFECTS AND CRITICALITY ANALYSIS," ed: United State Of America, 1980.

[166] C. Kara-Zaitri, "Summary Lecture. Risk Management Module: A lecture on Risk Management delivered at the SoEDT, University of Bradford," ed, 2012c.

[167] H. Born and I. Leigh, *Democratic Accountability of Intelligence Services*: Geneva Centre for the Democratic Control of Armed Forces (DCAF), 2007.

[168] Webopedia. *Cyber Terms*. Available: http://www.webopedia.com/TERM/C/ cyb er.html. [Accessed: 07 Oct. 2011

[169] Amazon. *Answer Viewer*. Available: http://askville.amazon.com/word-cyber-older-modern-eaning/AnswerViewer.do?requestId=4086267. [Accessed: 07 Oct. 2011].

[170] Webopedia. *Cyberspace*. Available: http://www.webopedia.com/TERM/C/cyb erspace.html. [Accessed: 07 Oct. 2011].

[171] T. Bradley, et al.,, *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security*: Rockland, MA (US): Syngress Publishing, Inc., 2006.

[172] W. Gibson. *Cybepunk*. Available: http://project.cyberpunk.ru/idb/williamgibson. htm. [Accessed: 07 Oct. 2011].

[173] W. Gibson. *Study Guide for William Gibson: Neuromancer (1984)*. Available: http://www.webring.org/l/rd?ring=williamg;id=8;url=http%3A%2F%2Fpublic%2E wsu%2Eedu%2F~brians%2Fscience_fiction%2Fneuromancer%2Ehtml. [Accessed: 04 May 2015]

[174] A. Simmonds, P. Sandilands, and L. Van Ekert, "An ontology for network security attacks," in *Applied Computing*, ed: Springer, 2004, pp. 317-323.

[175] J. Andress and S. Winterfeld, *Cyber warfare: techniques, tactics and tools for security practitioners*: Elsevier, 2013.

[176] W. J. Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs,* pp. 97-108, 2010.

[177] M. Murphy, "Cyberwar: War in the fifth domain," *Economist, July,* vol. 3, 2010.

[178] R. Sutton, *Secure communication: applications and management*: John Wiley & Sons, 2002.

[179] R. A. Clarke and R. K. Knake, *Cyber war*: Tantor Media, Incorporated, 2014.

[180] C. Bassford, "The Clausewitz Homepage," *Online on the internet: http://www.clausewitx.com/readings/OnWar1873/TOC.htm;2010. [Accessed 30 April 2012].* 2008.

[181] J. A. Ophardt, "Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield," *Duke L. & Tech. Rev.,* p. i, 2010.

[182] A. Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis,* vol. 34, pp. 62-73, 2010.

[183] E. Amoroso, *Cyber attacks: protecting national infrastructure*: Burlington (US): Elsevier, 2012.

[184] R. Lehtinen and G. Gangemi Sr, *Computer security basics*: " O'Reilly Media, Inc.", 2006.

[185] N. Kshetri, *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*: Springer, 2016.

[186] C. Johnston, "Major cyber attack disrupts Internet service across Europe and US," in *The Guardian*, ed. London, Aval: https://www.theguardian.com/technology/2016/oct/21/ddos-attack-dyn-internet-denial-service . [Accessed: 22 Oct 2016].

[187] Hackmageddon. *Cyber Attacks timeline*. Available: http://www.hackmageddon.com/category/security/cyber-attacks-timeline/page/2/. [Online]. [Accessed: 3 Sep. 2016].

[188] W. E. Forum, "Technological Risks: Back to the Future, in Part 1 – Global Risks Report, 2015".

[189] M. Lesk, "Cybersecurity and economics," *Security & Privacy, IEEE,* vol. 9, pp. 76-79, 2011.

[190] A. Tovey, "Cyber attacks cost British industry £34bn a year," in *The Telegraph*, ed, 2015.

[191] C. Jiayong, "IP Traceback Technology and its Standardization," *ZTE Corporation,* 15 April 2007.

[192] R. Anderson, "Security engineering: A guide to building dependable distributed systems. 2008," 2nd ed: Wiley.

[193] B. Schneier, *Beyond fear: Thinking sensibly about security in an uncertain world*: Springer Science & Business Media, 2003.

[194] S. J. Shepherd, *Cryptography: Diffusing the Confusion*: Research Studies Press Limited, 2001.

[195] M. Y. Rhee, *Cryptography and secure communications*: McGraw-Hill, Inc., 1993.

[196] D. Kahn, "The Codebreakers: History of Secret Communication," ed: New York: MacMillan Publishing Co., 1967.

[197] D. Kahn, "The Codebreakers: The Comprehensive History Of Secret Communication From Ancient Times To The Internet Author: David Kahn," 1996.

[198] R. E. Blahut, *Cryptography and Secure Communication*: Cambridge University Press, 2014.

[199] R. Ottis and P. Lorents, "Cyberspace: Definition and implications," in *Proceedings of the 5th International Conference on Information Warfare and Security*, 2010, pp. 267-270.

[200] M. N. M.I. Adeka, E. Ibrahim, S.J. Shepherd, I. Elfergani, A.S. Hussaini, F. Elmegri and R.A. Abd-Alhameed, "Africa: cyber-security and its mutual impacts with computerisation, miniaturisation and location-based authentication " *EAI Journal (Submitted for Publication),* 2015.

[201] S. Thomas, *Technobiophilia: Nature and Cyberspace*: A&C Black, 2013.

[202] M. Adeka, "Cryptography and computer communications security: Extending the human security perimeter through a web of trust," MPhil-PhD Transfer Report, School of Electrical Engineering and Computer Science, University of Bradford, Bradford (UK). 2013.

[203] M. ROUSE. (2007). *Peripherals Glossary*. Available: http://whatis.techtarget.Com/definition/digitization. [Accessed: 01 Jun. 2015].

[204] I. PRESENT, "Cramming more components onto integrated circuits," *Readings in computer architecture,* p. 56, 2000.

[205] M. Adeka, M. Ngala, M. Bin-Melha, E. Ibrahim, S. J. Shepherd, I. T. Elfergani, A. S. Hussaini, F. Elmegri, and R. Abd-Alhameed, "Nigeria: Cyber Space Security Vis a Vis Computerisation, Miniaturisation and Location-Based Authentication," in *Wireless Internet*, ed: Springer, 2015, pp. 322-334.

[206] H. D. Aslam, M. S. Azhar, K. Yasmeen, H. M. Farhan, M. Badar, and A. T. Habib, "Effects of globalisation on developing countris," *Journal of American Science,* vol. 8, 2012.

[207] I. Core, "Indicators ITU. pdf http://www. itu. int/ITU-D/ict/partnership/material [Accessed: 28 Sep. 2014]." *CoreICTIndicators. pdf*.

[208] M. Chawki, "Nigeria Tackles Advance Free Fraud," *Journal of Information Law & Technology,* 2009.

[209] E. Dictionary, "Encarta Dictionary," ed: English: UK, 2004.

[210] M. Bando, *101st Airborne: The Screaming Eagles in World War II*: Zenith Press, 2007.

[211] D. S. Jeslet, G. Sivaraman, M. Uma, K. Thangadurai, and M. Punithavalli, "Survey on Awareness and Security Issues in Password Management Strategies," *IJCSNS,* vol. 10, p. 19, 2010.

[212] D. W. Baronowski, "Roman military forces in 225 BC (Polybius 2.23-4)," *Historia: Zeitschrift fur Alte Geschichte,* pp. 181-202, 1993.

[213] P. Crisman, "CTSS Programmer's Guide," ed: MIT Press, Cambridge, Mass, 1965.

[214] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM,* vol. 22, pp. 594-597, 1979.

[215] S. M. Furnell, P. Dowland, H. Illingworth, and P. L. Reynolds, "Authentication and supervision: A survey of user attitudes," *Computers & Security,* vol. 19, pp. 529-539, 2000.

[216] E. F. Gehringer, "Choosing passwords: security and human factors," in *Technology and Society, 2002.(ISTAS'02). 2002 International Symposium on*, 2002, pp. 369-373.

[217] R. Reyes. (2009). *Do We Need to Hide Passwords?* Available: http://www.lyquix.com/search?q=password. [Accessed: 11 May 2015].

[218] M. McDowell, J. Rafail, and J. Hernan, "Choosing and Protecting Passwords," ed: Carnegie Mellon University. http://cns. esf. edu/Sec_Rec/PW_rec1. htm, 2004.

[219] J. Kent, "Malaysia car thieves steal finger," *BBC News,* vol. 31, 2005.

[220] S. Farrell, "Password policy purgatory," *IEEE Computing Society,* pp. 84-87, 2008.

[221] EmmaSoft. (2002). *Darn! Reminder Software!* Available: http://www.ordarn.com. [Accessed : 20 September, 20012].

[222] B. Schneier. (1999). *Password safe*. Available: http://www.counterpane.com/passsafe.html. [Accessed: 15 Oct. 2012].

[223] N. Mead. *QWallet: Save and protect your valuable informartion*. Available: http://qwallet.en.softonic.com/ . [Accessed: 16 May 2015].

[224] Selznick. *Password Wallet: Your Solution to Password Confusion*. Available: http://www.selznick.com/products/passwordwallet/ . [Accessed: 16 May 2015].

[225] R. Oppliger, "Microsoft. net passport and identity management," *Information Security Technical Report,* vol. 9, pp. 26-34, 2004.

[226] A. D. Rubin, *White-hat security arsenal: tackling the threats*: Addison-Wesley Longman Ltd., 2001.

[227] Microsoft. *Safety & Security Centre: Check your password—is it strong?* Available: https://www.microsoft.com/en-gb/security/pc-security/password-checker.aspx. [Accessed: 16 May 2015].

[228] B. Schneier. (2005). *Schneier on Security: Write down your password*. Available: https://www.schneier.com/blog/archives/2005/06/write_down_your.html. [Accessed: 16 May 2015].

[229] E. Spafford. (2006). *Spafford On Security Myths and Passwords*. Available: http://slashdot.org/story/06/04/25/0033238/spafford-on-security-myths-and-passwords. [Accessed: 21 May 2015].

[230] Unicityd. (2006). *In Defence of Password Expiration*. Available: https://lopsa.org/node/295. [Accessed: 21 May 2015].

[231] A. Adams and M. A. Sasse, "Users are not the enemy," *Communications of the ACM,* vol. 42, pp. 40-46, 1999.

[232] W. Rash. (2002). *Password chaos threatens e-commerce*. Available: http://techupdate.znet.com/techupdate/stories/main/0,14179,28,47895,00html. [Accessed: 12 Oct. 2012].

[233] N. Snip, *Security Manual: Chapter 1*. Available: http://www.nesnip.org/security chapter1.htm#Section%20I. [Accessed: 22 May 2015].

[234] S. F. Midkiff, "Network (computer science)," *Microsoft Student,* 2008.

[235] D. Spinellis, "The Antikythera mechanism: A computer science perspective," *Computer,* vol. 41, pp. 22-27, 2008.

[236] D. Wall, "1 Cybercrimes and the Internet," *Crime and the Internet,* p. 1, 2003.

[237] Y. Lu, H. Ren, and J. Wang, "Real-time performance vs. server bandwidth cost in peer-to-peer streaming system," in *Computer and Electrical Engineering, 2008. ICCEE 2008. International Conference on*, 2008, pp. 286-290.

[238] V. Garg, *Wireless Communications & Networking*: Morgan Kaufmann, 2010.

[239] A. Goldsmith, *Wireless communications*: Cambridge university press, 2005.

[240] R. W. Sinnott, "Sky and telescope," *Virtues of the Haversine,* vol. 68, p. 159, 1984.

[241] W. Gellert, *The VNR concise encyclopedia of mathematics*: Springer Science & Business Media, 2012.

[242] M. Rouse. *Object-Oriented Programming (OOP)*. Available: http://searchsoa.te chtarget.com/definition/object . [Accessed: 11 Jun. 2015]

[243] I. Jacobson, "Object oriented software engineering: a use case driven approach," 1992.

[244] K. M. Khan and Q. Malluhi, "Trust in cloud services: providing more controls to clients," *Computer,* vol. 46, pp. 0094-96, 2013.

[245] TSLAC. *Computer and Network Security in Small Libraries*. Available: https://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html. [Accessed: 26 May 2015].

[246] G. Lenzini, M. S. Bargh, and B. Hulsebosch, "Trust-enhanced security in location-based adaptive authentication," *Electronic Notes in Theoretical Computer Science,* vol. 197, pp. 105-119, 2008.

[247] N. Abdelmajid, M. A. Hossain, S. Shepherd, and K. Mahmoud, "Location-Based Kerberos Authentication Protocol," in *Social Computing (SocialCom), 2010 IEEE Second International Conference on*, 2010, pp. 1099-1104.

[248] J. Schiller and A. Voisard, *Location-based services*: Elsevier, 2004.

[249] V. Labrador. *Satellite communication: How satellites work*. Available: http://www.britannica.com/EBchecked/topic/524891/%20satellite-communication%20/288217/How-satellites-work. [Accessed: 26 May 2015].

[250] gis2gps. *What is GPS: It is a Global Positioning System*. Available: http://www.gis2gps.com/GPS/GPSDEF/gpsdef.html. [Accessed: 26 May 2015].

[251] C. J. Johnston. *My Google Nexus 7 and Nexus 10: Google Now andNavigation* .Available: http://www.quepublishing.com/articles/article.aspx?p=2018196. [Accessed: 26 May 2015].

[252] H. Wen, P. Y.-R. Huang, J. Dyer, A. Archinal, and J. Fagan, "Countermeasures for GPS signal spoofing," in *ION GNSS*, 2005, pp. 13-16.

[253] R. Prasad and M. Ruggieri, *Applied satellite navigation using GPS, GALILEO, and augmentation systems*: Artech House, 2005.

[254] S. Dong, H. Wu, X. Li, S. Guo, and Q. Yang, "The Compass and its time reference system," *Metrologia,* vol. 45, p. S47, 2008.

[255] O. Ehimen and A. Bola, "Cybercrime in Nigeria," *Bus Intelligence J,* vol. 3, pp. 93-98, 2010.

[256] D. D. Ashaolu, "Combating Cybercrimes and Nigeria," *Basic Concepts in Cyberlaw, Ashaolu et al Ed., Velma Publishers,(Abuja, 2012),* 2011.

[257] EFCC, "EFCC Annual Report," September 2013.

[258] Nigeria Police(SFU), "Statistics for Crimes in Relation to Fraud in Nigeria " Police Annual Reports, 2012 - 2014.

[259] E.D. Argaez. *Internet World Statistics 2014*. Available:http://www.internetworldstats.com/af/ng.htm. [Accessed: 26 May 2015].

[260] N. C. Commission. *Statistics for Tele-density in Nigeria*. Available: http://ncc.gov.ng/index.php?option=com_content&view=article&id=125:subscriber-statistics&catid=65:industry-information&Itemid=73. [Accessed: 28 Sep. 2014].

[261] M. Rinne and O. Tirkkonen, "LTE, the radio technology path towards 4G," *Computer Communications,* vol. 33, pp. 1894-1906, 2010.

[262] I. F. Akyildiz, D. M. Gutierrez-Estevez, and E. C. Reyes, "The evolution to 4G cellular systems: LTE-Advanced," *Physical Communication,* vol. 3, pp. 217-244, 2010.

[263] A. H. Sayed, A. Tarighat, and N. Khajehnouri, "Network-based wireless location: challenges faced in developing techniques for accurate wireless location information," *Signal Processing Magazine, IEEE,* vol. 22, pp. 24-40, 2005.

[264] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE-advanced: next-generation wireless broadband technology [Invited Paper]," *Wireless Communications, IEEE,* vol. 17, pp. 10-22, 2010.

[265] S. Abeta, "Toward LTE commercial launch and future plan for LTE enhancements (LTE-Advanced)," in *Communication Systems (ICCS), 2010 IEEE International Conference on*, 2010, pp. 146-150.

[266] M. Adeka, S. Shepherd, and R. Abd-Alhameed, "Extending the security perimeter through a web of trust: The impact of GPS technology on location-based authentication techniques," *in Proceedings of the Fifth International Conference on Internet Technologies and Applications (ITA 13),* pp. 465-473, 2013.

[267] Z. Song, Z. Li, and W. Dou, "Different approaches for the formal definition of authentication property," in *Communications, 2003. APCC 2003. The 9th Asia-Pacific Conference on*, 2003, pp. 854-858.

[268] *Cell Phone Fraud*. Available: http://www.fcc.gov/guides/cell-phone-fraud (Accessed on 27/09/2013)

[269] N. MUSA, "JTF bans Thuraya handsets, recharge cards in Borno," in *The Guardian*, ed. Nigeria, June 19, 2013.

[270] O. Audu, "JTF bans Thuraya phones in Borno, others, says Boko Haram use them for attacks," in *Premium Times*, ed, June 19, 2013.

[271] M. John, "Location Services Part 2: LTE Release 9 Features," *LTE University,* 2011.

[272] K.-F. Ssu, W.-T. Wang, and W.-C. Chang, "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information," *Computer Networks,* vol. 53, pp. 3042-3056, 2009.

[273] W. C. Lee, *Mobile cellular telecommunications: analog and digital systems*: McGraw-Hill Professional, 1995.

[274] Q. Zhang, P. Wang, D. S. Reeves, and P. Ning, "Defending against sybil attacks in sensor networks," in *Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on*, 2005, pp. 185-191.

[275] Y. Kou, C.-T. Lu, S. Sirwongwattana, and Y.-P. Huang, "Survey of fraud detection techniques," in *Networking, sensing and control, 2004 IEEE international conference on*, 2004, pp. 749-754.

[276] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*, 2006, pp. 564-570.

[277] J. R. Douceur, "The sybil attack," in *Peer-to-peer Systems*, ed: Springer, 2002, pp. 251-260.

[278] J. Yin and S. K. Madria, "Sybil attack detection in a hierarchical sensor network," in *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, 2007, pp. 494-503.

[279] H. Yu, M. Kaminsky, P. B. Gibbons, and A. D. Flaxman, "SybilGuard: Defending against sybil attacks via social networks," *Networking, IEEE/ACM Transactions on,* vol. 16, pp. 576-589, 2008.

[280] I. Khalil, S. Bagchi, C. N. Rotaru, and N. B. Shroff, "UnMask: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks," *Ad hoc networks,* vol. 8, pp. 148-164, 2010.

[281] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the sybil attack," *University of Massachusetts Amherst, Amherst, MA,* 2006.

[282] S. Lv, X. Wang, X. Zhao, and X. Zhou, "Detecting the sybil attack cooperatively in wireless sensor networks," in *Computational Intelligence and Security, 2008. CIS'08. International Conference on*, 2008, pp. 442-446.

[283] G. Danezis and P. Mittal, "SybilInfer: Detecting Sybil Nodes using Social Networks," in *NDSS*, 2009.

[284] J. Cao, M. Ma, H. Li, and Y. Zhang, "A Survey on Security Aspects for LTE and LTE-A Networks."

[285] M. Barbeau and J.-M. Robert, "Rogue-base station detection in WiMax/802.16 wireless access networks," in *Annales des télécommunications*, 2006, pp. 1300-1313.

[286] M. Barbeau, J. Hall, and E. Kranakis, "Detecting impersonation attacks in future wireless and mobile networks," in *Secure Mobile Ad-hoc Networks and Sensors*, ed: Springer, 2006, pp. 80-95.

[287] S. Parkvall, A. Furuskär, and E. Dahlman. Evolution of LTE towards IMT-Advanced [Online]. Available: http://www.ericsson.com/res/docs/2013/evolution-of-lte-towards-imt-advanced.pdf

Appendix 1

Glossary of Cyber-Network and Internet-Related Terms

1. Introduction

This glossary covers computer communications protocols, computer network, network programming and network topology, as well as basic hardware components, network performance and the transport layers.[7] [8] [9]

2. Communications Protocols

A communications protocol is a set of rules for exchanging information over a network. It is usually a protocol stack, that is, a stack of protocols, in which each protocol uses the protocol below it. A good example of a protocol stack is the Hypertext Transfer Protocol (HTTP), an application protocol for distributed, collaborative, hypermedia information systems.[10] HTTP is the foundation of data communication for the World Wide Web (WWW). Hypertext is a multi-linear set of objects, building a network by using logic links (hyperlinks) between the nodes (for example, text or words). HTTP is the protocol to exchange or transfer hypertext. The standards development of HTTP was coordinated by the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C), resulting in the publication of a series of Requests for Comments (RFCs), most notably RFC 2616 (June 1999), which defines HTTP/1.1, the version of HTTP in common use. HTTP runs over TCP over IP over IEEE 802.11 (TCP and IP are members of the Internet Protocol Suite, and IEEE 802.11 is a member of the Ethernet protocol suite). This stack is used between the wireless router and the home user's personal computer when the user is surfing the web. Communication protocols have various properties, such as whether they are connection-oriented or connectionless, whether they use circuit mode or packet switching, or whether they use hierarchical or flat addressing. Of the several communication protocols, a few are described below:

- **Ethernet -** Ethernet is a family of protocols used in LANs, described by a set of standards together called IEEE 802. This is published by the Institute of Electrical and Electronics Engineers (IEEE). It has a flat addressing scheme and is mostly situated at levels 1 and 2 of the OSI model.[11] For home users today, the most well-known member of this protocol family is IEEE 802.11, otherwise known as Wireless LAN (WLAN). However, the complete protocol suite deals with a multitude of networking aspects not only for home use, but especially when the technology is deployed to support a diverse range of business needs. MAC bridging (IEEE 802.1D) deals with the routing of

[7] http://en.wikipedia.org/wiki/Computer_network
[8] http://www.petri.co.il/osi_concepts.htm
[9] New global standard for fully networked home, ITU-T, 2008-12-12, retrieved 2012-10-01
[10] Fielding, Roy T.; Gettys, James; Mogul, Jeffrey C.; Nielsen, Henrik Frystyk; Masinter, Larry; Leach, Paul J.; Berners-Lee (June 1999). "RFC 2616: Hypertext Transfer Protocol -- HTTP/1.1".
[11] OSI - Open Systems Interconnection: See the transport layers at the end of this appendix.

.

Ethernet packets using a Spanning Tree Protocol, IEEE 802.1Q describes VLANs, and IEEE 802.1X defines a port-based Network Access Control protocol, which forms the basis for the authentication mechanisms used in VLANs, but it is also found in WLANs – it is what the home user sees when the user has to enter a "wireless access key".

- **Internet Protocol Suite -** The Internet Protocol Suite (IPS), often called TCP/IP, is the foundation of all modern internetworking. It offers connectionless as well as connection-oriented services over an inherently unreliable network traversed by datagram transmission at the Internet protocol (IP) level. At its core, the protocol suite defines the addressing, identification, and routing specification in form of the traditional Internet Protocol Version 4 (IPv4) and IPv6 (the next generation of the protocol with a much enlarged addressing capability).
- **SONET/SDH -** Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardised multiplexing protocols that transfer multiple digital bit streams over optical fibre using lasers. They were originally designed to transport circuit mode communications from a variety of different sources, primarily to support real-time, uncompressed, circuit-switched voice encoded in PCM (Pulse-Code Modulation) format. However, due to its protocol neutrality and transport-oriented features, SONET/SDH was also the obvious choice for transporting Asynchronous Transfer Mode (ATM) frames.
- **Asynchronous Transfer Mode -** ATM is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing and encodes data into small, fixed-sized cells. This differs from other protocols such as the Internet Protocol Suite or Ethernet that use variable sized packets or frames respectively. ATM has similarity with both circuit and packet switched networking. This makes it a good choice for a network that must handle both traditional high-throughput data traffic, and real-time, low-latency content such as voice and video. ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins. While the role of ATM is diminishing in favour of next-generation networks, it still plays a role in the last mile, which is the connection between an Internet service provider and the home user.[12]

3. Computer Network Programming

Computer network programming involves writing computer programs that communicate with each other across a computer network. Different programs must be written for the client process, which initiates the communication, and for the server process, which waits for the communication to be initiated. Both endpoints of the communication flow are implemented as network sockets; hence network programming is basically socket programming.

- **Network Socket –** A network socket is an endpoint of an inter-process communication flow across a computer network. Today, most communication between computers is based on the Internet Protocol; therefore most network sockets are Internet sockets. A socket API is an Application Programming Interface (API), usually provided by the operating system that allows

[12] Martin, Thomas. "Design Principles for DSL-Based Access Solutions". Retrieved 18 June 2011.

application programs to control and use network sockets. Internet socket APIs are usually based on the Berkeley sockets standard. A socket address is the combination of an IP address and a port number, much like one end of a telephone connection is the combination of a phone number and a particular extension.[13] Based on this address, internet sockets deliver incoming data packets to the appropriate application process or thread. There are several Internet socket types available:

- **Datagram Sockets -** Also known as connectionless sockets, which use User Datagram Protocol (UDP).
- **Stream Sockets -** Also known as connection-oriented sockets, which use Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP).
- **Raw Sockets -** Also called Raw IP sockets, typically available in routers and other network equipment. Here the transport layer is bypassed, and the packet headers are made accessible to the application.

There are also non-Internet sockets, implemented over other transport protocols, such as Systems Network Architecture (SNA).[14] We also have Unix Domain Sockets (UDS), for internal inter-process communication.

4. Types of Computer Networks

Networks are often classified by their physical or organisational extent or their purpose. Usage, trust level, and access rights differ between these types of networks. Thus, we have the following types of computer networks:

- **Personal Area Network -** A Personal Area Network (PAN) is a computer network used for communication among computer and different information technological devices close to one person. Some examples of devices that are used in a PAN are personal computers, printers, fax machines, telephones, PDAs, scanners, and even video game consoles. A PAN may include wired and wireless devices. The reach of a PAN typically extends to 10 meters.[15] A wired PAN is usually constructed with USB and Firewire[16] connections while technologies such as Bluetooth and infrared communication typically form a wireless PAN.
- **Local Area Network -** A Local Area Network (LAN) is a network that connects computers and devices in a limited geographical area such as home, school, computer laboratory, office building, or closely positioned group of buildings. Each computer or device on the network is a node. Current wired LANs are most likely to be based on Ethernet technology, although new standards like ITU-T G.hn also provide a way to create a wired

[13] Cisco Networking Academy Program, CCNA 1 and 2 Companion Guide Revised Third Edition, P.480, ISBN 1-58713-150-1

[14] www-306.ibm.com - AnyNet Guide to Sockets over SNA.

[15] "Personal Area Network (PAN)". Retrieved September 30, 2012.

[16] FireWire is Apple Computer's version of a standard, IEEE 1394, High Performance Serial Bus, for connecting devices to your personal computer. FireWire provides a single plug-and-socket connection on which up to 63 devices can be attached with data transfer speeds up to 400 Mbps (megabits per second). The standard describes a serial bus or pathway between one or more peripheral devices and your computer's microprocessor. Many peripheral devices now come equipped to meet IEEE 1394. Available at: http://searchnetworking.techtarget.com/definition/FireWire

LAN using existing home wires (coaxial cables, phone lines and power lines).[17] The defining characteristics of LANs, in contrast to WANs (Wide Area Networks), include their higher data transfer rates, smaller geographic range, and no need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at data transfer rates up to 10 Gbit/s. IEEE has projects investigating the standardisation of 40 and 100 Gbit/s.[14] LANs can be connected to WAN by using routers.

- **Home Area Network -** A Home Area Network (HAN) is a residential LAN which is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices. An important function is the sharing of Internet access, often a broadband service through a cable TV or Digital Subscriber Line (DSL) provider.
- **Storage Area Network -** A Storage Area Network (SAN) is a dedicated network that provides access to consolidated, block level data storage. SANs are primarily used to make storage devices, such as disk arrays, tape libraries and optical jukeboxes, accessible to servers so that the devices appear like locally attached devices to the operating system. A SAN typically has its own network of storage devices that are generally not accessible through the local area network by other devices. The cost and complexity of SANs dropped in the early 2000s to levels allowing wider adoption across both enterprise and small to medium sized business environments.
- **Campus Area Network -** A Campus Area Network (CAN) is a computer network made up of an interconnection of LANs within a limited geographical area. The networking equipment (switches, routers) and transmission media (optical fibre, copper plant, Cat5 cabling etc.) are almost entirely owned (by the campus tenant/owner: an enterprise, university, government etc.). In the case of a university campus-based campus network, the network is likely to link a variety of campus buildings including, for example, academic colleges or departments, the university library, and student residence halls.
- **Backbone Network -** A backbone network is part of a computer network infrastructure that interconnects various pieces of network, providing a path for the exchange of information between different LANs or sub networks. A backbone can tie together diverse networks in the same building, in different buildings in a campus environment, or over wide areas. Normally, the backbone's capacity is greater than that of the networks connected to it. A large corporation which has many locations may have a backbone network that ties all of these locations together, for example, if a server cluster needs to be accessed by different departments of a company which are located at different geographical locations. The equipment which ties these departments together constitutes the network backbone. Network performance management including network congestion are critical parameters taken into account when designing a network backbone. A specific case of a backbone network is the **Internet backbone, which is the set of WAN connections and core routers that interconnect all networks connected to the Internet.**
- **Metropolitan Area Network -** A Metropolitan Area Network (MAN) is a large computer network that usually spans a city or a large campus.

[17] New global standard for fully networked home, ITU-T, 2008-12-12, retrieved 2012-10-2

- **Wide Area Network -** A WAN is a computer network that covers a large geographic area such as a city, country, or spans even intercontinental distances, using a communications channel that combines many types of media such as telephone lines, cables, and air waves. A WAN often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.
- **Enterprise Private Network -** An enterprise private network is a network built by an enterprise to interconnect various company sites, e.g., production sites, head offices, remote offices and shops, in order to share computer resources.
- **Virtual Private Network -** A Virtual Private Network (VPN) is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g., the Internet) instead of by physical wires. The data link layer protocols of the virtual network are said to be tunnelled through the larger network when this is the case. One common application is secure communications through the public Internet, but a VPN need not have explicit security features, such as authentication or content encryption. VPNs, for example, can be used to separate the traffic of different user communities over an underlying network with strong security features. VPN may have best-effort performance, or may have a defined service level agreement (SLA) between the VPN customer and the VPN service provider. Generally, a VPN has a topology more complex than point-to-point.
- **Virtual Network -** Not to be confused with a VPN, a Virtual Network defines data traffic flows between virtual machines within a hypervisor in a virtual computing environment. Virtual Networks may employ virtual security switches, virtual routers, virtual firewalls and other virtual networking devices to direct and secure data traffic.
- **Internetwork -** An internetwork is the connection of multiple computer networks via a common routing technology using routers. The Internet is an aggregation of many connected internetworks spanning the Earth.
- **Organisational Scope -** Networks are typically managed by organisations which own them. According to the owner's point of view, networks are seen as intranets or extranets. A special case of network is the Internet, which has no single owner but a distinct status when seen by an organisational entity; that of permitting virtually unlimited global connectivity for a great multitude of purposes.
- **Intranets And Extranets -** Intranets and extranets are parts or extensions of a computer network, usually a LAN.
    - An **intranet** is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications that are under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorised users. Most commonly, an intranet is the internal network of an organisation. A large intranet will typically have at least one web server to provide users with organisational information.

- An **extrane**t is a network that is limited in scope to a single organisation or entity and also has limited connections to the networks of one or more other usually, but not necessarily, trusted organisations or entities—a company's customers may be given access to some part of its intranet—while at the same time the customers may not be considered trusted from a security standpoint. Technically, an extranet may also be categorised as a CAN, MAN, WAN, or other type of network, although an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

❖ **Internet -** The Internet is a global system of interconnected governmental, academic, corporate, public, and private computer networks. It is based on the networking technologies of the IPS. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the US Department of Defence. The Internet is also the communications backbone underlying the World WWW. Participants in the Internet use a diverse array of methods of several hundred documented, and often standardised, protocols compatible with the IPS and an addressing system (IP addresses) administered by the Internet Assigned Numbers Authority (IANA) and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

5. Computer Network Topology

❖ **Common Layouts -** A network topology is the layout of the interconnections of the nodes of a computer network. Common layouts are:

- **Bus Network -** All nodes are connected to a common medium along this medium. This was the layout used in the original Ethernet, called 10BASE5 and 10BASE2.
- **Star Network -** All nodes are connected to a special central node. This is the typical layout found in a WLAN, where each wireless client connects to the central wireless access point.
- **Ring Network -** Each node is connected to its left and right neighbour node, such that all nodes are connected and that each node can reach each other node by traversing nodes left- or rightwards. The Fibre Distributed Data Interface (FDDI) made use of such a topology.
- **Mesh Network -** Each node is connected to an arbitrary number of neighbours in such a way that there is at least one traversal from any node to any other.
- **Fully Connected Network -** Each node is connected to every other node in the network.

Note that the physical layout of the nodes in a network may not necessarily reflect the network topology. As an example, with FDDI, the network topology is a ring (actually two counter-rotating rings), but the physical topology is a star, because all neighbouring connections are routed via a central physical location.

6. Overlay Network

An overlay network is a virtual computer network that is built on top of another network. Nodes in the overlay are connected by virtual or logic links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. The topology of the overlay network may (and often does) differ from that of the underlying one. A sample overlay network is shown in Figure 1-1 below. The sample shows IP over SONET over Optical. This sample overlay network shows IP over SONET over Optical. For example, many peer-to-peer networks are overlay networks because they are organised as nodes of a virtual system of links run on top of the Internet. The Internet was initially built as an overlay on the telephone network.[18] The most striking example of an overlay network, however, is the Internet itself: At the IP layer, each node can reach any other by a direct connection to the desired IP address, thereby creating a fully connected network; the underlying network, however, is composed of a mesh-like interconnect of sub networks of varying topologies (and, in fact, technologies). Address resolution and routing are the means which allows the mapping of the fully connected IP overlay network to the underlying ones.

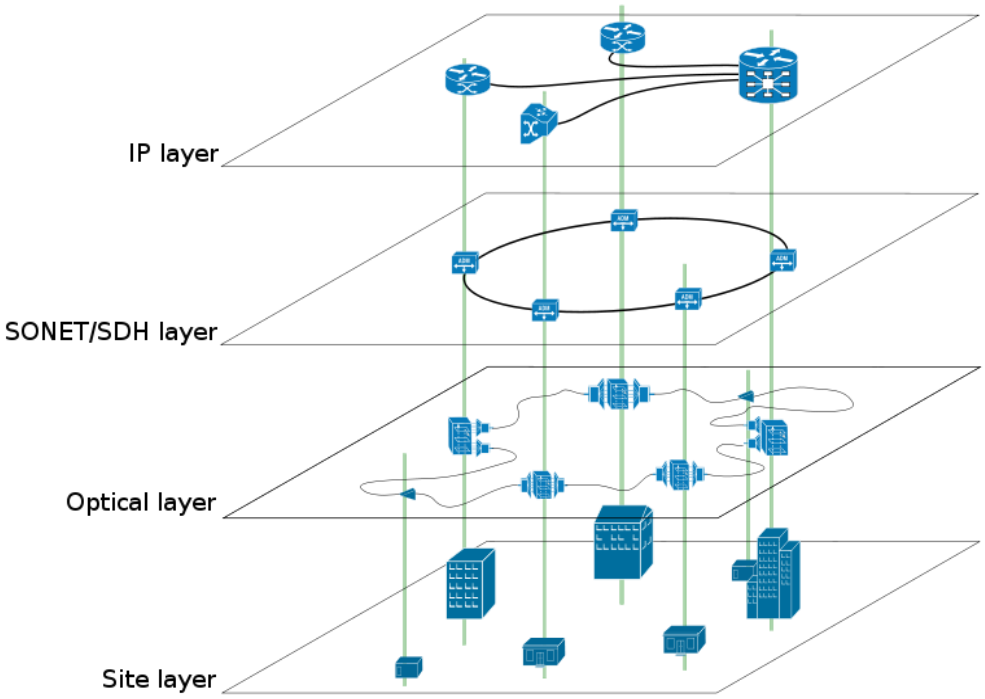


Figure 1-1. Overlay Network Broken-up into Logic Layers [Ft. Note 20]

7. Networking Hardware: Basic Hardware Components

Apart from the physical communications media themselves, networks comprise additional basic hardware building blocks interconnecting their terminals. These include network interface cards (NICs), hubs, bridges, switches, and routers.

[18] D. Andersen; H. Balakrishnan; M. Kaashoek; R. Morris (10-2001), Resilient Overlay Networks, Association for Computing Machinery, http://nms.lcs.mit.edu/papers/ron-sosp2001.html, retrieved 2012-10-12

- **Network Interface Cards** - A network card, network adapter, or NIC is a piece of computer hardware designed to allow computers to physically access a networking medium. It provides a low-level addressing system through the use of MAC addresses. Each Ethernet network interface has a unique MAC address which is usually stored in a small memory device on the card, allowing any device to connect to the network without creating an address conflict. Ethernet MAC addresses are composed of six octets. Uniqueness is maintained by the IEEE, which manages the Ethernet address space by assigning 3-octet prefixes to equipment manufacturers. The list of prefixes is publicly available. Each manufacturer is then obliged to both use only their assigned prefix (es) and to uniquely set the 3-octet suffix of every Ethernet interface they produce.

- **Repeaters and Hubs -** A repeater is an electronic device that receives a signal, cleans it of unnecessary noise, regenerates it, and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable that runs longer than 100 meters. A repeater with multiple ports is known as a hub. Repeaters work on the Physical Layer of the OSI model. Repeaters require a small amount of time to regenerate the signal. This can cause a propagation delay which can affect network communication when there are several repeaters in a row. Many network architectures limit the number of repeaters that can be used in a row (e.g. Ethernet's 5-4-3 rule). Today, repeaters and hubs have been made mostly obsolete by switches.

- **Bridges -** A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges broadcast to all ports except the port on which the broadcast was received. However, bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address to that port only. Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived. There are three types of bridges:
  - **Local Bridges -** Directly connect LANs.
  - **Remote Bridges -** Can be used to create a WAN link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced with routers.
  - Wireless bridges: Can be used to join LANs or connect remote stations to LANs.
- **Switches -** A network switch is a device that forwards and filters OSI layer 2 datagrams (chunks of data communication) between ports (connected cables) based on the MAC addresses in the packets.[19] [20] A switch is distinct

[19] "Define switch.". WWW.Wikipedia.com. Retrieved September l 8, 2012.
[20] Teletraffic Engineering Handbook, ITU-T Study Group 2, archived from the original on 2012-10-01

from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.[21] Some switches are capable of routing based on Layer 3 addressing or additional logic levels; these are called multi-layer switches. The term switch is used loosely in marketing to encompass devices including routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier).

- **Routers -** A router is an internetworking device that forwards packets between networks by processing information found in the datagram or packet (IP information from Layer 3 of the OSI Model). In many situations, this information is processed in conjunction with the routing table (also known as forwarding table). Routers use routing tables to determine what interface to forward packets (this can include the "null" also known as the "black hole" interface because data can go into it, however, no further processing is done for said data).
- **Firewalls -** A firewall is an important aspect of a network with respect to security. It typically rejects access requests from unsafe sources while allowing actions from recognized ones. The vital role firewalls play in network security grows in parallel with the constant increase in cyberattacks for the purpose of stealing/corrupting data, planting viruses, etcetera.
- **Network Performance -** Network performance refers to the service quality of a telecommunications product as seen by the customer. It should not be seen merely as quantum of message or data through the network. Two illustrations using circuit-switched network and one type of packet-switched network(ATM) are:
  - **Circuit-Switched Networks -** In circuit switched networks, network performance is synonymous with the grade of service. The number of rejected calls is a measure of how well the network is performing under heavy traffic loads.[14] Other types of performance measures can include noise, echo and so on.
  - **Asynchronous Transfer Mode -** In an ATM network, performance can be measured by line rate, Quality of Service (QoS), data throughput, connect time, stability, technology, modulation technique and modem enhancements.[22]

  There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modelled instead of measured; one example of this is using state transition diagrams to model queuing performance in a circuit-switched network. These diagrams allow the network planner to analyse how the network will perform in each state, ensuring that the network will be optimally designed.[23]

[21] Basic Components of a Local Area Network (LAN)". NetworkBits.net. Retrieved September 8, 2012.
[22] Telecommunications Magazine Online, Americas January 2003, Issue Highlights, Online Exclusive: Broadband Access Maximum Performance, Retrieved on September 20, 2012.
[23] State Transition Diagrams". Retrieved July 13, 2003.

8. Network Security

In the field of networking, the area of network security[24] consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorised access, misuse, modification, or denial of the computer network and network-accessible resources. Network security is the authorisation of access to data in a network, which is controlled by the network administrator. Users are assigned an ID and password that allows them access to information and programs within their authority. Network Security covers a variety of computer networks, both public and private that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals.

9. The Seven Transport Layers

The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) is a product of the Open Systems Interconnection effort at the International Organisation for Standardisation. It is a prescription of characterising and standardising the functions of a communications system in terms of abstraction layers. Similar communication functions are grouped into logic layers. A layer serves the layer above it and is served by the layer below it. For example, a layer that provides error-free communications across a network provides the path needed by applications above it, while it calls the next lower layer to send and receive packets that make up the contents of that path. Two instances at one layer are connected by a horizontal connection on that layer.

The OSI model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, and proceeding to the bottom layer, over the channel to the next station and back up the hierarchy. These layers are:

- **Layer 1 (Physical)** - This layer conveys the bit stream - electrical impulse, light or radio signal through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.
- **Layer 2 (Data Link)** - At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronisation. The data link layer is divided into two sub layers: The Media Access Control (MAC) layer and the Logic Link Control (LLC) layer. The MAC sub layer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronisation, flow control and error checking.
- **Layer 3 (Network)** - NFS uses IP as its network layer interface. IP is responsible for routing, directing datagrams from one network to another.

[24] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.

The network layer may have to break large datagrams, larger than MTU, into smaller packets and host receiving the packet will have to reassemble the fragmented datagram. The Internetwork Protocol identifies each host with a 32-bit IP address. IP addresses are written as four dot-separated decimal numbers between 0 and 255, e.g., 129.79.16.40. The leading 1-3 bytes of the IP identify the network and the remaining bytes identify the host on that network. The network portion of the IP is assigned by Inter-NIC Registration Services, under the contract to the National Science Foundation, and the host portion of the IP is assigned by the local network administrators. For large sites, the first two bytes represents the network portion of the IP, and the third and fourth bytes identify the subnet and host respectively. Even though IP packets are addressed using IP addresses, hardware addresses must be used to actually transport data from one host to another. The Address Resolution Protocol (ARP) is used to map the IP address to its hardware address.

- **Layer 4 (Transport)** - Transport layer subdivides user-buffer into network-buffer, sized datagrams and enforces desired transmission control. Two transport protocols, Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), sit at the transport layer. Reliability and speed are the primary difference between these two protocols. TCP establishes connections between two hosts on the network through sockets which are determined by the IP address and port number. TCP keeps track of the packet delivery order and the packets that must be resent. Maintaining this information for each connection makes TCP a stately protocol. UDP on the other hand provides a low overhead transmission service, but with less error checking. NFS is built on top of UDP because of its speed and statelessness. Statelessness simplifies the crash recovery.
- **Layer 5 (Session) -** The session protocol defines the format of the data sent over the connections. The NFS uses the Remote Procedure Call (RPC) for its session protocol. RPC may be built on either TCP or UDP. Login sessions use TCP whereas NFS and broadcast use UDP.
- **Layer 6 (Presentation**) - This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.
- **Layer 7 (Application)** - This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.

Understanding how the OSI Model works is not only useful for theoretical purposes, but also for real life scenarios. The graphical representation of the 7-layer OSI model is shown in Figure 1-2.[25]

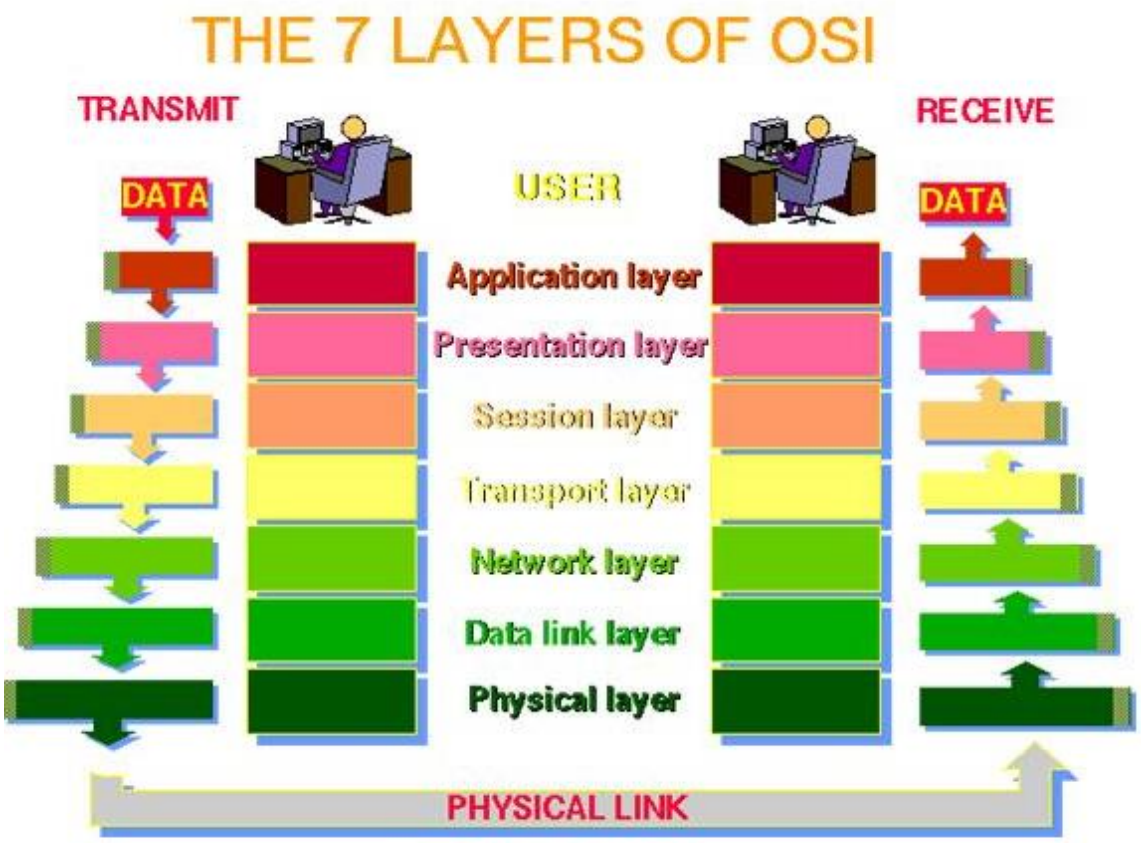


Figure 1-2. The Seven Transport Layers: Graphical Representation of the 7-Layer OSI Model [Ft. Note 27]

[25]This graphic is taken from The Abdus Salam International Centre for Theoretical Physics. (http://www.petri.co.il/osi_concepts.htm)

Appendix 2

Online Password Security Survey Questionnaire

Title: Password Security Survey

Objective: To establish the level of importance attached to Passwords and the awareness on the need for strong passwords.

Target Audience: Business and other Organisational Executives in Nigeria.

N.B.: Sir/Madam, Please note that you are neither required to write any of your passwords in the questionnaire below nor disclose your identity. This is not a means for procuring people's passwords for criminal intent. It is a means to facilitate an investigation which is part of an ongoing PhD research programme on the topic: Cryptography & Computer Communications Security; Social and Technological Aspects of Cyber Defence. Do please spare me some 5 minutes of your precious time to answer the eleven questions in the questionnaire and send to the returning email address at the end: Just select 'Forward' at the top of this email, insert 'X' in the 'Choice' column to reflect your choices, copy the returning email address at the end of the questionnaire on Table 2-1 and paste in the addressee space for sending emails (To: ……), and select 'Send'. The questionnaire is also attached to this mail, hence, you may choose to download the attachment, complete it, and then forward the completed attachment to the returning email address, depending on your convenience. With the Highest Regards for your Assistance.

Table 2-1**.** Questionnaire on Password Security Survey

S/N	**QUESTION**	**ALTERNATIVES**	**CHOICE** (Please insert 'X' against your chosen alternatives in this column or specify as requested)
1.	Which of the following describes you best?	a. Director or above b. Deputy Director c. Assistant Director d. Senior Enterprise Officer	a. b. c. d.
2.	Do you have a password for granting or denying access to your computer?	a. Yes b. No	a. b.
3.	If yes, what is the length of the password?	a. Less than 8 characters b. Eight characters c. More than 8 characters d. Others: please specify	a. b. c. d.
4.	What is the length of your email password?	a. Less than 8 characters b. Eight characters c. More than 8 characters d. Others: please, specify	a. b. c. d
5.	What is the nature of your passwords?	a. Meaningful/easily-remembered b. Meaningless/ easily-remembered c. Meaningless/hard-to-remember d. Others: please describe	a. b. c.

6.	What is the composition of your passwords?	a. Words or names b. Words or names and figures c. Lower or upper case Letters and figures d. Mixed case letters and figures e. Mixed case letters with figures and symbols (other characters on the keyboard)	a. b. c. d. e.
7.	How often do you change your passwords?	a. Daily b. Weekly c. Monthly d. Quarterly e. Annually f. Permanent (no change) g. Change only when compromised	a. b. c. d. e. f. g.
8.	What is the significance of passwords?	In very few words, state what a password means to you (definition)	
9.	How or where do you store your passwords?	a. In your memory b. In your computer memory c. Pasted on your computer or around the computer d. Elsewhere: please specify	a. b. c. d.
10.	Do you, or does your organisation or any superior executive in your organisation care about the security of passwords used by employees and take steps to ensure that they are strong and secure?	a. Yes b. No	a. b.
11.	How many people do you share your passwords with?	a. Nobody b. Everybody c. Others: please specify	a. b. c.

Returning Email Address: miadeka@student.bradford.ac.uk

Appendix 3

Structured Interviews: Sample Questions for GSM Mobile Services Survey

1. When was the GSM system introduced in Nigeria?

2. How many GSM service providers were there at inception, and how many are there now?

3. How has the GSM service contributed (positively/negatively) to the lives of Nigerians – commerce; education; governance; organisation; individual; and security?

4. How many customers (phone users) does your organisation have?

5. On the average, how many mobile phones does an individual have?

6. Is roaming of mobile services a common practice among Nigerians?

7. Which category of your customers roams their mobile services most frequently?

8. Which category of your customers roams their mobile services least frequently?

9. What is the incidence of roaming among your customers; is it season-discriminatory?

10. On the average, what percentage of your customers roam their mobile services – monthly; quarterly; and/or annually?

11. Would you say that your organisation encourages or discourages the roaming of mobile services?

12. What is the financial implication of roaming on the users?

13. What is the effect of roaming on the quality of communication (Quality of Service)?

14. What challenges do your organisation and/or customers face in connection with the roaming of services, and how are these challenges overcome?

15. As a service provider, can you identify the geographical location of your customers by merely receiving their calls: - if ‘yes’, how easy, accurate and fast is the process; if ‘no’, what can you do to facilitate this process?

16. How is the GSM mobile phone market in Nigeria; is it expanding or shrinking?

17. How do you differentiate between a local call and an international call?

18.* About how many times did you roam your GSM Phone Number (s) for phone calls while abroad in the following years? Please tick the appropriate column in the questionnaire in Table 3-1 below. Do please remember to indicate your age. You are also assured that your identity remains anonymous.

Table 3-1**.** Questionnaire for GSM Call Roaming in Nigeria

YEARS	**NUMBER OF ROAMINGS PER YEAR**							Remarks
	0	1	2	3	4	5	Above 5	Digits 0-5 represent the no. of times you roamed your calls in each year
2006								
2007								
2008								
2009								
2010								
2011								
2012								
2013								
2014								
2015								

Your Age: ……

STRUCTURED INTERVIEWS: SAMPLE QUESTIONS FOR CYBERSECURITY SURVEY

1. When did computer literacy begin in the Nigerian society?
2. Compare the prevalence in the use of computers at inception with now.
3. When did Internet culture begin in Nigeria?
4. Would you say that Nigeria is now a member of the Global Village?
5. Briefly comment on the rate of Internet usage in Nigeria; comparing the situation at inception with the present experience.
6. How important is the Internet in the lives of Nigerians – Commerce; education; governance; organisation; individuals; and security?
7. Does your organisation or you face any challenges in the use of cyberspace?
8. What are the types of cybercrimes in Nigeria?
9. How common or frequent are cybercrimes in Nigeria; especially fraud and '419' (advance fee fraud)?
10. How do you and/or your organisation fare in combatting cybercrimes?
11. What is the incidence of DDoS (Distributed Denial of Service) attacks in Nigeria; cite examples, if any?
12. Have hackers played any significant roles in the Nigerian cyberspace; cite examples, if any?
13. What challenges do you or your organisation face in combatting cybercrimes – at personal, organisational and national levels?
14. What role does the government play in the Nigerian cyberspace?
15. How successful is your organisation or are you in the war against cybercrimes?
16. What do you suggest should be the way forward?

Appendix 4

CDRSAS-PT: Organisational Network Security Policy

Network Access and Authentication Policy	Created: 03/06/2015
Section of: Corporate Security Policies	Target Audience: Technical Staff
CONFIDENTIAL	Page 255 of 5

CDRSAS-PT is hereinafter referred to as "the company."

1.0 Overview

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduce the risk of a security incident by requiring consistent application of authentication and access standards across the network.[26]

2.0 Purpose

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

3.0 Scope

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network.

4.0 Policy

4.1 Account Setup

During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:

[26] InstantSecurityPolicy.com. *Custom Security Policies*. Available: http://www.instantsecuritypolicy.com/index-uk.html?gclid=CKrV1vr8zbYCFaTItAodsTAAvA. [Accessed: 3 Jun. 2015]

- ❖ Positive ID and coordination with Human Resources is required.

- ❖ Users will be granted least amount of network access required to perform his or her job function.

- ❖ Users will be granted access only if he or she accepts the Acceptable Use Policy.

- ❖ Access to the network will be granted in accordance with the Acceptable Use Policy.

4.2 Account Use

Network accounts must be implemented in a standard fashion and utilised consistently across the organisation. The following policies apply to account use:

- ❖ Accounts must be created using a standard format (i.e., firstname-lastname, or firstinitial-lastname, etc.)

- ❖ Accounts must be password protected (refer to the Password Policy for more detailed information).

- ❖ Accounts must be for individuals only. Account sharing and group accounts are not permitted.

- ❖ User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

- ❖ Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time; and disabled when the guest's work is completed.

- ❖ Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the ICT Manager or executive team, or as required by applicable regulations or third-party agreements.

4.3 Account Termination

When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, that employee's account can be disabled. Human Resources must create a process to notify the IT Manager in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.).

4.4 Authentication

User machines must be configured to request authentication against the domain at start up. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.

4.5 Use of Passwords

When accessing the network locally, two-factor authentication (such as smart cards, tokens, or biometrics) is required.

4.6 Remote Network Access

Remote access to the network can be provided for convenience to users but this comes at some risk to security. For that reason, the company encourages additional scrutiny of users remotely accessing the network. Due to the elevated risk, company policy dictates that when accessing the network remotely two-factor authentication (such as smart cards, tokens, or biometrics) must be used. This is in addition to a location-based authentication technique (using GPS). Multiple accesses and threshold accesses would be catered for as the need arises. Remote access must adhere to this Remote Access Policy.

4.7 Screensaver Passwords

Screensaver passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason, screensaver passwords are required to be activated after 5 to 15 minutes of inactivity, depending on the security classification of the computer; all company ICT facilities will be security-classified by the ICT Manager accordingly.

4.8 Minimum Configuration for Access

Any system connecting to the network can have a serious impact on the security of the entire network. Vulnerability, virus, or other malware may be inadvertently introduced in this process. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with product that provides network admission control.

4.9 Encryption

Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network such as the Internet.

4.10 Failed Logins

Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the ICT Manager; to avoid converting failed logins into inadvertent DoS attacks.

In order to protect against account guessing, when login failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password supplied were incorrect."

4.11 Non-Business Hours

Since the company's business does not require overnight network access, the company must restrict account login during off hours. In order to allow room for reasonable non-business-hour work, where necessary, `off hours' is defined as the hours between 10:00PM and 5:00AM local time on weekdays. On weekends, account access should be disabled 24 hours per day. However, this will be implemented at the discretion of the ICT Manager depending on the business need for weekend or off-hours access.

Exceptions to this policy will be granted on a case-by-case basis.

4.12 Applicability of other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the ICT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Glossary

Antivirus Software - An application used to protect a computer from viruses, typically through real time defences and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.

Authentication - A security method used to verify the identity of a user and authorise access to a system or network.

Biometrics - The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. It is used to protect data during transmission or while stored.

Password - A sequence of characters that is used to authenticate a user to a file, computer, or network. It is also known as a passphrase or passcode.

Smart Card - A plastic card containing a computer chip capable of storing information; typically used to prove the identity of the user. A card-reader is required to access the information.

Token - A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

Global Positioning System (GPS) – A technique used to determine the location of an object on earth using information acquired from a system of geostationary satellites in space.

7.0 Revision History

Revision 1.0, 03/06/2015

Appendix 5

Assess Yourself 7: Interpersonal Trust Scale[27]

Indicate the degree to which you agree or disagree with each statement by the following scale:

1 = strongly agree

2 = mildly agree

3 = agree and disagree equally

4 = mildly disagree

5 = strongly disagree

Once you have completed the 25 items, click 'CALCULATE'

	1	2	3	4	5
1. Hypocrisy is on the increase in our society.	--	--	--	--	--
2. One is better off being cautious when dealing with strangers until they have provided evidence that they are trustworthy.	--	--	--	--	--
3. This country has a dark future unless we can attract better people into politics.	--	--	--	--	--
4. Fear and social disgrace or punishment rather than conscience prevents most people from breaking the law.	--	--	--	--	--
5. An honor system in which teachers would not be present during exams would probably result in increased cheating.	--	--	--	--	--
6. Parents usually can be relied on to keep their promises.	--	--	--	--	--

[27] This scale can be obtained from Dr. J. B. Rotter, Department of Psychology, University of Connecticut, Storrs, Connecticut 06268. This scale was published in: Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. (1991). Measures of personality and social psychological attitudes. San Diego: Academic Press. Available: http://highered.mheducation.com/sites/dl/free/0072563974/87095/ch07.html. [Accessed: 15 Oct. 2016].

7. The United Nations will never be an effective force in keeping world peace.	--	--	--	--	--
8. The judiciary is a place where we can all get unbiased treatment.	--	--	--	--	--
9. Most people would be horrified if they knew how much of the news that the public hears and sees is distorted.	--	--	--	--	--
10. It is safe to believe that in spite of what people say most people are primarily interested in their own welfare.	--	--	--	--	--
11. Even though we have reports in newspapers, radio, TV, and the Internet, it is hard to get objective accounts of public events.	--	--	--	--	--
12. The future seems very promising.	--	--	--	--	--
13. If we really knew what was going on in international politics, the public would have reason to be more frightened than they now seem to be.	--	--	--	--	--
14. Most elected officials are really sincere in their campaign promises.	--	--	--	--	--
15. Many major national sports contests are fixed in one way or another.	--	--	--	--	--
16. Most experts can be relied upon to tell the truth about the limits of their knowledge.	--	--	--	--	--
17. Most parents can be relied upon to carry out Their threats of punishments.	--	--	--	--	--
18. Most people can be counted on to do what they say they will do.	--	--	--	--	--
19. In these competitive times one has to be alert or someone is likely to take advantage of you.	--	--	--	--	--
20. Most idealists are sincere and usually practice what they preach.	--	--	--	--	--
21. Most salesmen are honest in describing their products.	--	--	--	--	--
22. Most students in school would not cheat even if they were sure they could get away with it.	--	--	--	--	--
23. Most repairmen will not overcharge, even if					

they think you are ignorant of their specialty.	--	--	--	--	--
24. A large share of accident claims filed against insurance companies are phony.	--	--	--	--	--
25. Most people answer public opinion polls honestly.	--	--	--	--	--

CALCULATE

Appendix 6

Summary of the Detailed Functions of the CDRSAS Prototype

1. Introduction

The key technical background functionalities of the Cloud Data Repository Secure Access (CDRSA) prototype are as summarised hereunder; section by section. These relate to the roles of softwares and programming languages, such as HTML/CSS, Javascripts, PHP, Java/JSP and MySQL.

2. Server Side Display Functions

These are carried out by a **Java** file which carries out the following functions:

- Handles form posts: note that each Servlet has two methods; **doGet** (default) and **doPost** (process).
- When a form is submitted by POST, it employs **doPost** method.
- When a form is submitted as a page default, it employs **doGet** method.

3. Client Side Display Functions

These are carried out by **Javascripts** file, which employs JQuery library and other utilities to:

- Implement Client side functionalities, which include- sending keypad values to the text box; getting GPS coordinates and placing them in appropriate fields; etc.

4. Starting Up

- On start-up, the Server loads the WebContent, WBB-INF, Web.xml, Project/Site title; the first page to display is the **UnlockDataRegister.Java**.
- The UnlockDataRegister.Java is a Servlet which displays **login.jsp** using **doGet….** (Line 36)
- When the user fills in login details, the UnlockDataRegister.Java processes them using **doPost**. … (Line 43)
- **Failed Login:** Checks if Admin has set up a Share (time); if not, sends error message; displays a new login page with the error message.
- **Successful Login:**

  - All conditions met – time is set; time is within the share duration; all credentials match.
  - Takes the user details and encrypts the password (MD5); checks against the Database (Db) values.
  - In the session, sets User Logged In = True.
  - Again sets the attribute for the user; this facilitates the display of the User Info on the web page.

5. Configuring the Admin Page/Sharing the Secret Data

Please note that, firstly, the Admin page must be fully configured by setting up all relevant data before a successful login on the client side could be carried out. The admin page Form is contained in **admin.JSP** file, while the completed form is processed in the **Admin.Java** file. The processes involved, which lead to the creation of shares by the Admin on the local host only, include:

- Fill the form details and click submit.
- Admin.Java doPost the details while **Data.reset** file resets/clears all previous share data.
- Get Form Info/Parameters:
  - Put these into variable and add to the session which is stored in Data.Java (Lines 54-83 parse check).
  - Admin.Java (Line 76) stops processing, if any error is found.
  - Executes logic checks (Lines 84-106).
  - Line 108: all data is correct/valid; start adding the data to the session (**Session = Data.Java**; as referenced throughout the programme).
  - Get the keys from Shamir (**PHP**) via HTTP POST request.
  - Returns **x** keys; these are assigned to the users, either serially or in staggered form, as programmed by the Admin.

- Displays Admin page (Page 2) with the master details (most pieces of information relative to the share session as programmed by the Admin (Page 1).
- Now, the system will allow users to log in and is ready for secret data sharing/reconstruction; at this stage, the secret data has already been shared – each user can now obtain a one-time access to his assigned key.

6. Secret Data Sharing/Reconstruction

Note that the secret data has already been shared (Paragraph 5); data reconstruction can now take place or at a later time/date. These functions are implemented using the Form **datashare.jsp** and the processing file **SetKeyForm.Java** as follow:

- Get all the form details (user inputs).
- Check for any blank field; send error message, if any.
- Check if all keys are correct and set the key data to the appropriate user in the session.
- Does every key match what the assigned user entered?
- If there are no errors in the user entries (and everything else is correct), display the normal page stating confirmation for all users; as for the authorised user (s), show the page with the **View Data** button.
- **For Authorised User (s) Only –** Using the Form **ChosenUser.jsp** and the processing file **ViewData.Java** – once the View Data button is clicked**:**

  - Double-check to ensure that all of this user's details are correct. (Line 443)

- Check for minimum number of keys; i.e., quorum satisfaction. (Line 447)
- Check if each user has entered the correct key. (Line 455)
- Check if the GPS coordinates are within accepted range. (Line 463)
- Send the keys to Shamir for final checks

- Display the appropriate result on the Secret Data Page; either Successful (secret data unlocked) or unsuccessful.

7. Time Check

If time runs out (expires), clear all system data relative to this session

8. Functions of Server Side Processing Files

The functions of the Java Server are as highlighted in this paragraph. Its Source (Src) Folder contains various files whose functions are as noted herein.

8.1 Source (Src) Folder:

- **Admin File** – Sets the configuration for shares.
- **Data file** – Class used to store all the user data and share information. All information the system had is referenced and updated here.
- **DTOSecret File** – DTO of the results from SSSS.
- **DTOSmsResult File** – Saves information on all results from the SMS Client (Gate way: SMS Text Marketer); i.e., fail, texts left, text used, etc.
- **GetUserDetails File** – Used class in ajax call to regulate the user edit details form.
- **OnetimePassCode File** – Displays the secret key for the user only once.
- **Reset File –** Resets all system variables.
- **ViewData File** – Carries out all the checks before the Authorised User (s) can view the data.

8.2 Database Folder:

- **DB_SecureShare File** – Main DB Class.
- **MYSQLDB File** – DB Connection class.
- **UserDao File** – interface for user details DB access.

8.3 Authentication Folder:

- **Authentication File** – Checks to ensure that login details are correct.
- **AuthenticationRegister File** – Creates/Registers new users.
- **Register File** – Displays Registration Form.

8.4 SecureShare Folder:

- **SendSMS File** – Class used to send SMS to user.
- **SetKeyForm File** – Handles all the user input for share.
- **UnlockDataRegister** – Checks Authorised User details before showing the secret data (final checks).

8.5 Utility Folder:

- **Utils File** – Various utilities' help functions.
- **GPSTest File** – Tests limitation of GPS distance.
- **TestSMS File** – Tests the XML; the SMS that Client sends back.

9. Functions Client Side Processing Functions

9.1 Javascript Folder:

- **JQuery File –** a library.
- **Utils File** - . Implementation of Client side functionalities, which include- sending keypad values to the text box; getting GPS coordinates and placing them in appropriate fields; etc.

10. Java Server Pages (JSP)

This is a technology that helps software developers to create dynamically generated web pages based on HTML and XML or other document types. Released by Sun Microsystems in 1999,[28] JSP is similar to PHP, but it uses the Java programming language. The functions of the various files are as highlighted herein.

10.1 JSP Folder:

- **Admin File** – Sets the login for share.
- **ChosenUser File** – Page where the Authorised User sees the unlocked secret data.
- **Don'tShowData File** – Page that displays error message for Authorised User; e.g., unsuccessful keys, GPS, etc.
- **DataAccepted File** – Page that shows when an unauthorised user enters his keys and other input data correctly.
- **DataShare File** – Page where keys and other data are entered; unlocks edit details; sends Authentication Code SMS; sends one-time key; countdown timer.
- **Header File** – Displays title and time at the top of page.
- **MasterShareData File** – Admin page (Page 2) results (master).
- **Register File** – Form to register new users.
- **Registered File** –Confirmation that a user has been registered.
- **Reset.jsp File** – Resets all the data.
- **ResetUser File** – Page that displays after the secret data has been unlocked; it resets the data.
- **ShowData File** – Show the Secret Data (Page that contains the View Data button).

[28] http://en.wikipedia.org/wiki/JavaServer_Pages

11. JUnit Tests

These are tests carried out to find out if the various Java Units (smallest code elements) actually perform their functions according to the design specifications.

12. Database

The database contains a table which is created to handle user information; such as ID number, Username, Password, GPS Lon, GPS Lat and Phone number. Of these, only the password is encrypted. These data could be edited in three possible ways: From the Admin page, all the data can be edited, except the ID; From the database, all the data can be edited except the ID and password; From the Client side, all the data can be edited by a user after due authentication, except the ID and Phone number. Without regard to personal ID, a user could just input these data directly from the Client side via the registration process. However, if the position of the ID is to be pre-determined, then, the Admin must assist the user by entering his phone number in the database to enable him edit the rest of the user data for the particular ID location from the Client side.

Appendix 7

Cloud Data Repository Secure Access Service Prototype: Results for the JUnit Tests

Tests Conducted on: 24 May 2015

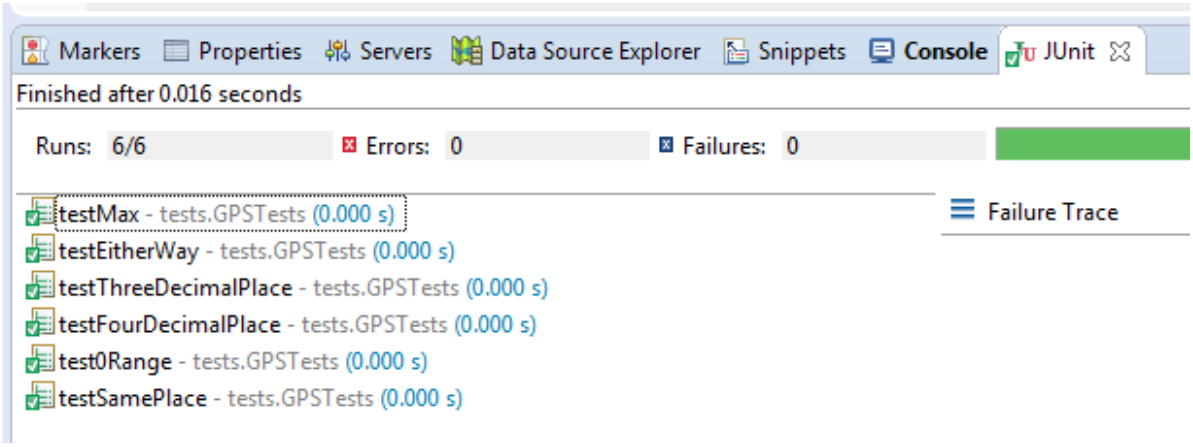


Figure 7-1. Result: JUnit.Test_GPSTests.java_PT

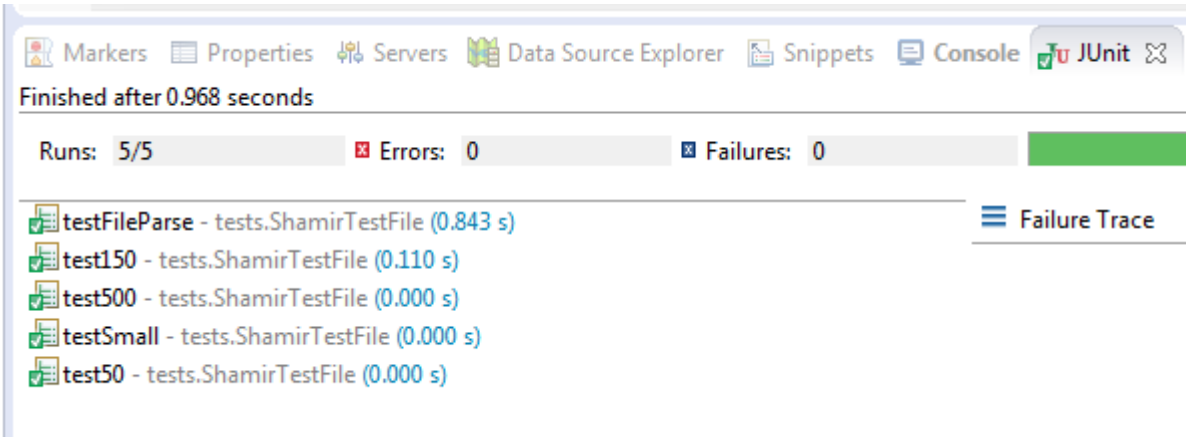


Figure 7-2. Result: JUnit.Test_ShamirTestUtils.java_PT

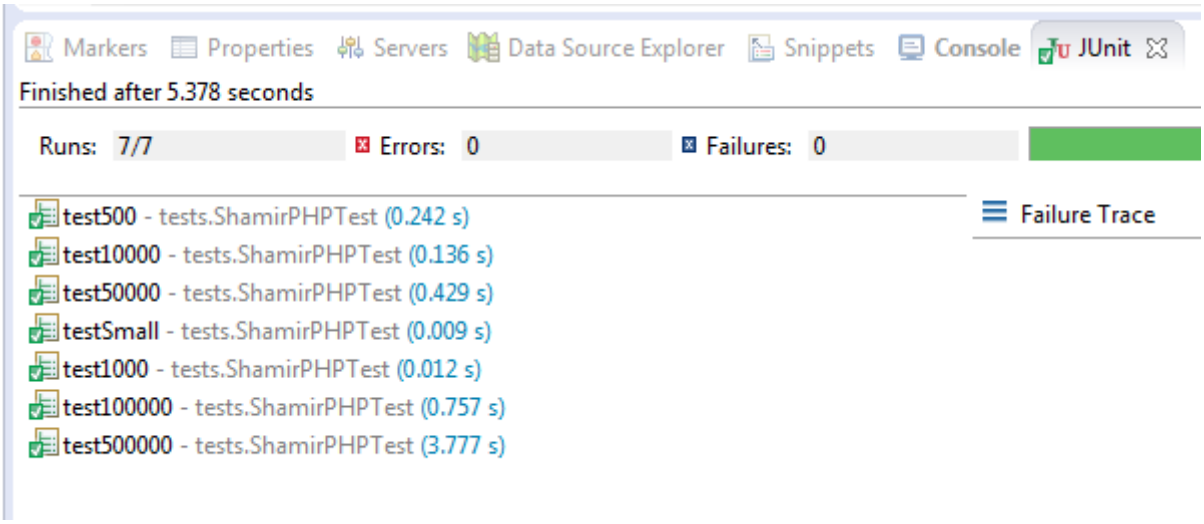


Figure 7-3**.** Result: JUnit.Test_ShamirPHPTest.java_PT

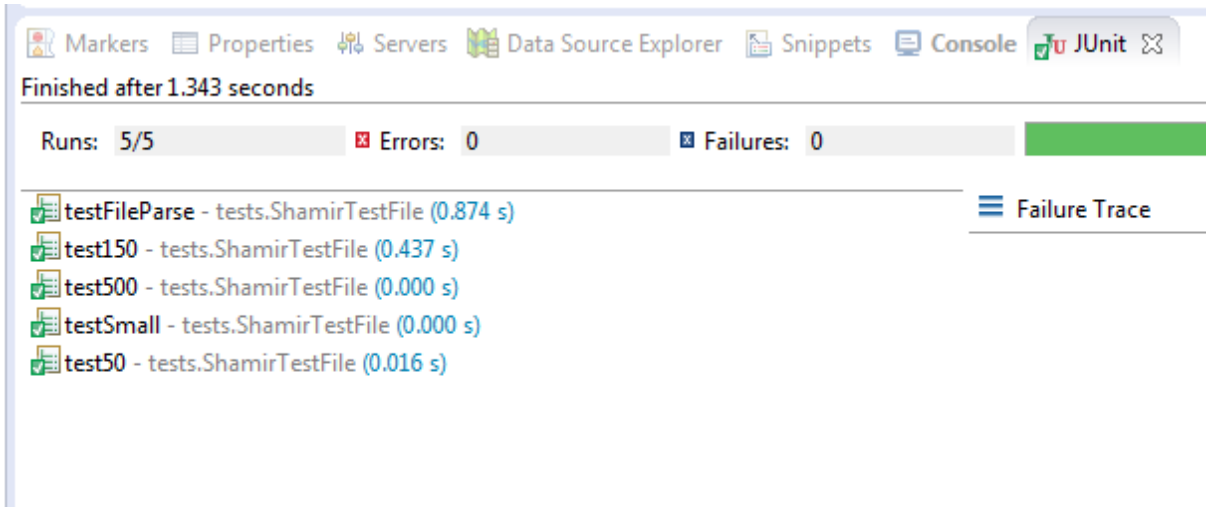


Figure 7-4. Result: JUnit.Test_ShamirTestFile.java_PT

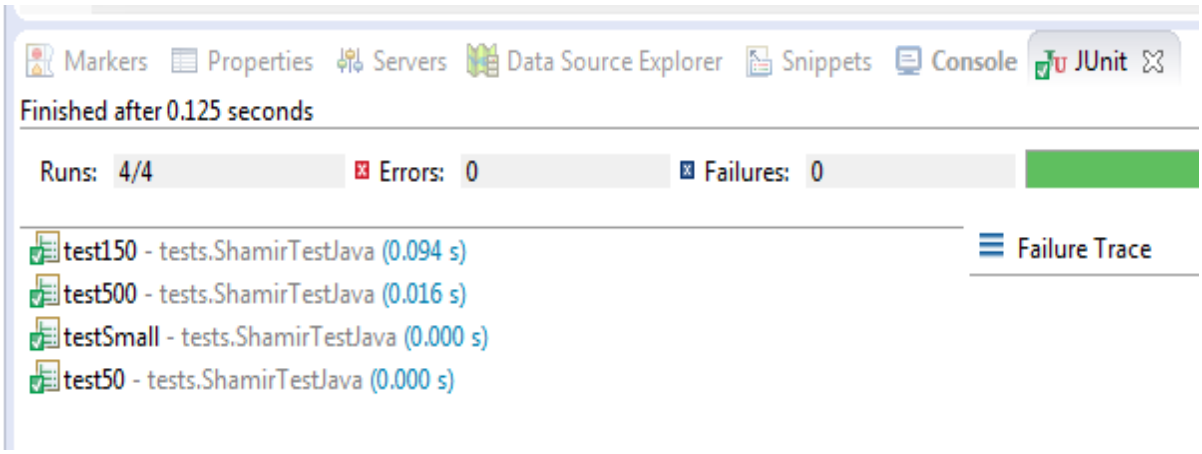


Figure 7-5. Result: JUnit.Test_ShamirTestFile.java_PT

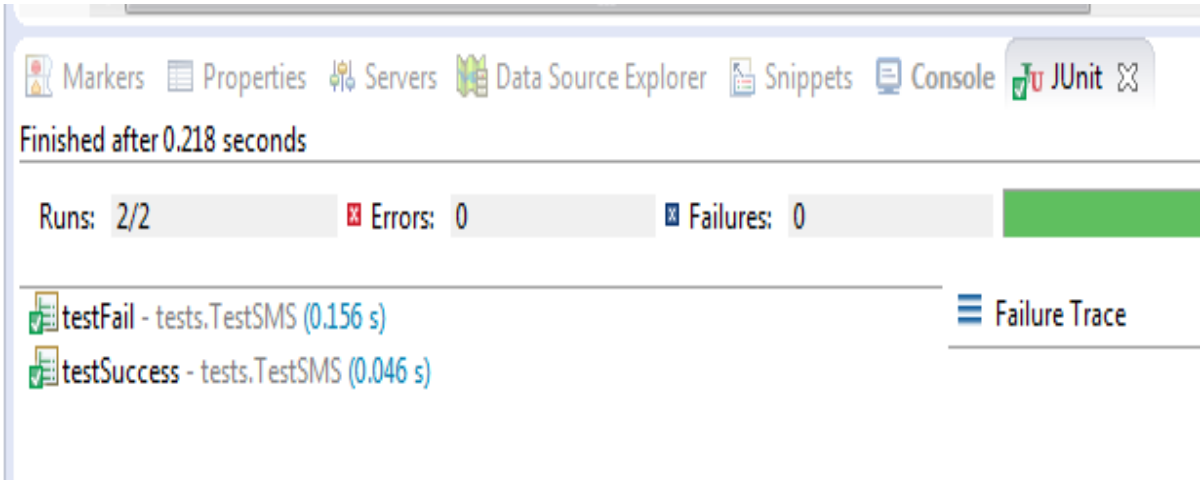


Figure 7-6. Result: JUnit.Test_TestSMS.java_PT

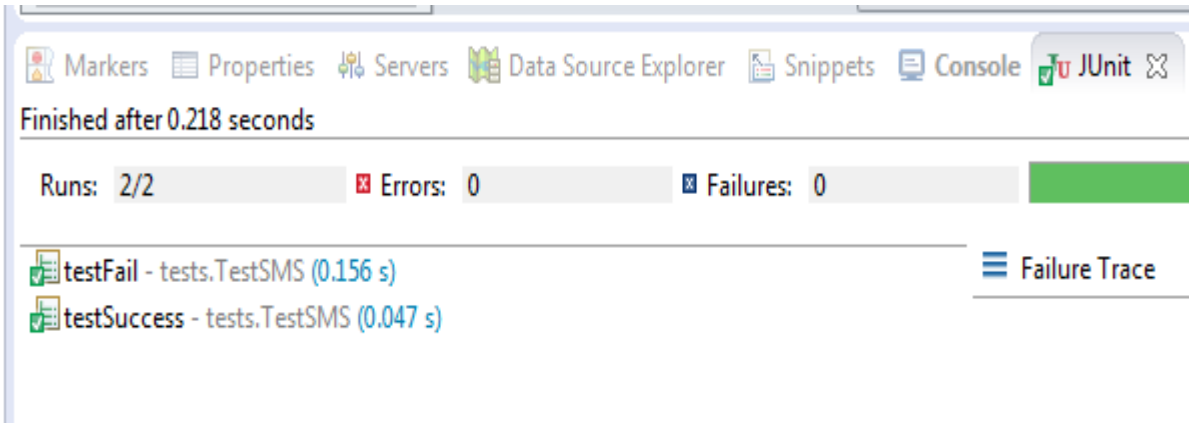


Figure 7-7. Result: JUnit.Test_test.docx_PT

Appendix 8

CDRSAS-DT: Projected Characteristics, Functions and Capabilities

1. Introduction

The Cloud Data Repository Secure Access Scheme (CDRSAS) – Deployment Type (DT) will be a global web-based secure data communication service. Its ubiquity is limited only by Internet connectivity; wherever there is Internet access, the CDRSAS will be there. It is essentially a Threshold Secret Sharing Scheme, with additional inherent capabilities for secure data transmissions and cloud data repository. This brief account seeks to highlight the projected characteristics, functions and capabilities of the CDRSAS-DT, when implemented by upgrading the CDRSAS-PT in future. The projected features which are not currently available in the Proto-type (PT) are asterisked (*) herein. The CDRSAS-DT will operate very similar to the CDRSAS-PT, except that, the former will have more enhanced security features with provisions for multiple simultaneous operations, while the later provides for only single operations in most cases. In addition, the Deployment Type will be adapted to handle a large volume of customers from a hosted website, although it could function from a computer-based server; the prototype is the exact opposite of this design. The highlights will cover the programming languages/software components to be used in building the system, its capabilities, security features and the basics of its operations from login to logout.

2. Programmimg Languages and Software Components

The CDRSAS-DT will be built using the following software components and programming languages, similar to the CDRSAS-PT:

a. PHP (PHP originally stood for '**P**ersonal **H**ome **P**age'; it now stands for **H**y**p**ertext **P**re-processor - a recursive backronym). It is used mainly for the Server side.

b. Javascript/JQuery {'JQuery' stands for Java Query (Library)}; used mainly for the Client side.

c. MySQL database {'My' **S**tructured **Q**uery **L**anguage; a Relational Database Management System (RDBMS} and Apache.

d. HTML (**H**yper**T**ext **M**arkup **L**anguage) - this is used as the backbone or structural framework for the programme.

e. CSS (**C**ascading **S**tyle **S**heets – a new feature being added to HTML) – used for styling to give the website a better outlook.

f. XAMPP Server (for a computer-based server), using Apache web server application; this runs together with MySQL database.

g. Eclipse IDE (for a computer-based server) – it is an Integrated programme Development Environment.

h. Random Integer Generator (In-built in PHP – used in place of Shamir's shared secret keys in the CDRSAS-PT system to improve security).

1. Projected Capabilities

The projected capabilities of the CDRSAS-DT could be summarised as follows – it will:

a. Register an *[29]Organisation, a *Sharer (Sender, Transmitter or Administrator) or a User (Sharee, Recipient or Participant) at any time; with requisite corporate/personal information. The projected organogram of the hierarchical family tree for the projected CDRSAS-DT is in Figure 8-1, attached herein.

b. Create a *group of Sharers (the CDRSAS-PT has only one Sharer, who also doubles as the Admin).

c. *Send a confirmation email to a designated email address for the Registrar (e.g., hamummadu2k7@yahoo.com) and the registered, on registration.

d. Create Shares within a time window; with start time and end time.

e. Transact in a session which is valid only within a time window; i.e., while registration could take place any time, the sharing/distribution/transmission, storing and unlocking of the shared/distributed/transmitted or stored secret item (text or document file) could only be accomplished within the time window (between the start time and end time; the limits of the time window is as configured by the Admin – it can be modified, as long as the window exists).

f. Display the received or unlocked message for view by the authorised User (s) only; this is to be viewed or downloaded once only.

g. Make Shares (message transmission sessions) to all or selected Users (collective or discriminatory sharing/communication).

h. Authorise all or selected Users only to view the sent/shared or stored message.

i. Start operation only after the Quorum has been configured; with one or more number of Users specified {Figure '1' is the default number of User (s) for the Quorum}. Depending on the configuration, the CDRSAS could serve as follow:

[29]*Capabilities which are not available in the Prototype (CDRSAS-PT); available only in the projected Deployment Type (CDRSAS-DT).

(1) If the total number of User (s) is set to ‘1’, it facilitates the use of the CDRSAS-DT as a web-based storage facility (i.e., a secure cloud data repository) or a point-to-point (one-to-one) secure data transmission system, depending on the duration of the time window;

(2) If the total number of Users is anything from 5 and above, and the Quorum is set to some reasonable number of Users (e.g., 5 Users), with only one or a few (e.g., 2 or 3) Users designated as ‘Authorised Users’, it facilitates the use of the CDRSAS-DT as a Threshold Secret Sharing Scheme or a discriminatory data broadcaster;

(3) If the total number of Users in a session is any size but the number of Authorised Users is equal to the total number of Users, and the Quorum being set to any reasonable number, this facilitates the use of the CDRSAS-DT as a data broadcaster; and

(4) In all the configurations, depending on the time window, the CDRSAS-DT would serve as a web-based storage facility (i.e., a secure cloud data repository) and secure data transmitter.

j. Choose both secret texts and *files or *either of the two to send, share or store (in a cloud data repository); either on a wired/wireless network or website.

k. Select an appropriate security classification; including ULTRA SECRET.

l. *Assign a Share name; a name given to each transaction session in order to be able to distinguish one Share session from another.

m. *Configure a post-share options; either delete or save.

n. *Display the list of available pending Shares, if any.

o. *Display the list of Shares; with notifications as to whether there are Shares to be unlocked (for that day/date) or not.

p. *Go back to a Share that has been completed but waiting to be unlocked, within its time window, and edit its settings.

q. Allow a User to edit his personal data; *subject to confirmation by the Admin (Administrator).

2. Security Features

The security features of the CDRSAS-DT will include the following:

a. Use of Password that is encrypted with SHA-1 encryption (MD5 for the CDRSAS-PT).

b. GPS coordinates; the system employs the browser to acquire its geo-location tag, which is delivered to the User to be used for authentication.

c. SMS Authentication Code; using HTTP protocol – possible only when the Server is connected to the Internet.

d. Randomly generated key (using a random key generator); it is a one-time key which is destroyed after usage. The CDRSAS-PT originally used the Shamir's key that is derived from the encrypted output of the original message itself; this could be of security concern when homomorphic encryption becomes a reality.

e. Use of Username.

f. The FTP access to the Server (Website) is disabled; via Server configuration.

g. The secret text is encrypted (SHA-1).

5. Operations from Login to Logout

The operations that may take place within the system from Login to Logout could be summarised as follow:

a. On login, the system calls the database to check if the login details are correct.

b. If all the login details are correct, a User Profile is created and added to the session. This will display the correct web page with three options; namely, a web page for an *Organisation, a *Sharer and User.

c. **Logging in as an Organisation** – If one logs in as an Organisation, one can create Sharers.

d. **Logging in as a Sharer –** If one logs in as a Sharer, one can create Users and set up Shares among them (the Users). When a Share is made, it is set up in the database; this creates a randomly generated one-time authentication key and a one-time mobile SMS verification code. These are stored in the session.

e. **Logging in as a User –** If one logs in as a User, one would see the following:

(1) One's pending Shares, if any; if it is within the time window.

(2) Unlock Share instructions, if one has any pending Share (s); provided it is within the time window.

(3) One would not see anything, if one had no pending Share (s), or if the time window had expired.

f. **Creating or Setting Up a Share Session -** For a User to be able to participate in a Share or Transmission/Communication session, after the Admin has configured the system and declared the Share session open, it would require the following:

(1) The randomly generated one-time authentication key sent to the User (s) from the Admin (Server); either via the CDRSAS system or any other means of communication – e.g., email (for now, it is designed to be sent through the system);

(2) The randomly generated one-time mobile SMS verification code sent to the User (s) via HTTP POST Request;

(3) The GPS coordinates; popped up by the browser of the User (s) from its geo-location tag; and

(4) All of the data enumerated above must be entered by the User (s) within the time window and checked, for accuracy, by the system, in addition to other login details like the username and password. If all the details are correct, then, a successful Share is created, with a successful message displayed (Share Status: Successful). This flags the Share to be unlocked.

(5) The unlocking of the Share must be accomplished within the time window; if the time window expires, it will not be possible to unlock the Share. If any of the above data is incorrect, or it is not entered before the time window expires, an unsuccessful Share will result, with an error message displayed.

g. **Unlocking Shares (Receiving Transmitted Messages) –** In order for one to be able to unlock a Share, one must not only be a registered User in the system, but must have also taken part in creating or setting up the particular Share session. The process of unlocking a Share requires the following:

(1) The User enters own GPS coordinates, one-time key and SMS authentication code. The system checks to see if all other Users have completed their shares, and also entered their unlocking details. When all the data entries (i.e., password, username, key, GPS and SMS code) are correct and the Quorum is satisfied within the time window, the Share can then be unlocked;

(2) Only the Authorised User (s) can unlock the secret data or transmitted message/document file.

(3) When unlocked, the received data/file can be viewed/downloaded (either see an on-screen message or a link to download an attachment) by the Authorised User (s) only once.

(4) Thereafter, the post-Share option configuration (action; either to delete or save the Share session) is automatically activated.

(5) If any of the details is incorrect, or the Quorum is not met within the time window, the Share cannot be unlocked; an on-screen failure message will be displayed instead.

6. **Conclusion**

As briefly illustrated above, the CDRSAS-DT will be a secure web-based service, to be designed with the security industry in focus. It will be designed to handle secret data communications in large organisational or industrial settings with a global reach. However, it will be so versatile that it could also handle normal routine correspondences, and even serve as a secure cloud data repository, both for individual users and organisations. All these will be in addition to its unique function as a secure Threshold Secret Sharing Scheme. Although some level of computer literacy will be required of users, a basic introductory training would suffice to enable effective handling of the system by most users. When implemented, the system will be tested for sustainable high-volume traffic operations before presentation to the public. Public presentation is expected to create room for the accommodation of further modifications in its features.

Bradford, UK
July 2015

MIU ADEKA
Doctoral Research Student

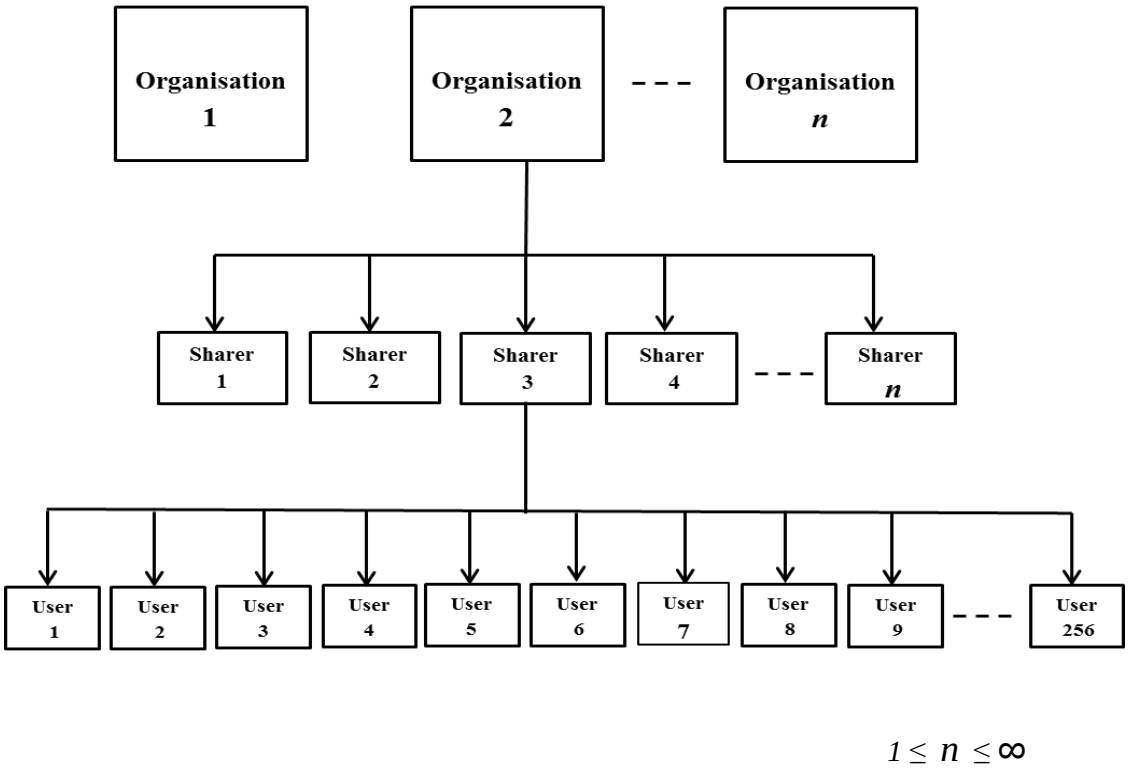


Figure 8-1. A Projected Organogram for the Cloud Data Repository Secure Access Scheme – Deployment Type (CDRSAS-DT)

List of Author's Contributions

1. **Review: The Context of Technology in Network Security Engineering** (Circulated at the London Cyber-security Summit in November 2011).

2. **Threat Analysis versus Risk Analysis in Intelligence and Security Assessment** (Published as Chapter 36 in 'Nigerian Defence and Security: Essays in Commemoration of Nigerian Defence Academy Golden Jubilee', September 2014).

3. **Resolving the Password Security Purgatory in the Contexts of Technology, Security and Human Factors** {Presented at: International Conference on Computer Applications Technology, 20-22 January 2013 (ICCAT 2013 Sousse, Tunisia); Published in ICCAT 2013 Conference Proceedings & IEEE Xplore}.

4. **Password Security Awareness in African Countries within the Context of Password Security Purgatory {**Published by Dline Journals: Journal of Information Security Research (http://www.dline.info/index.php/about-us; www.iccat2013.org**)}.**

5. **Extending the Security Perimeter through a Web of Trust: The Impact of GPS Technology on Location-Based Authentication Techniques** (Published in ITA 2013 Conference Proceedings).

6. **Nigeria: Cyberspace Security vis a vis Computerisation, Miniaturisation and Location-Based Authentication** (Published in WICON 2014 Conference Proceedings).

7. **Africa: cyber-security and its mutual impacts with computerisation, miniaturisation and location-based authentication** (Submitted for EAI Journal Publication 2015; under review).

8. **A Versatile and Ubiquitous Secret Sharing: A cloud data repository secure access** (Presented and Published in ITA 2015 Conference Proceedings, Wales, UK).

9. **Telecommunication Network Security** (Published by Nova Science Publishers, Inc., New York, as Chapter 1, in Horizons in Computer Science Research, Volume 10, 2015, with online Independent Chapter Open Access at: https://www.novapublishers.com/catalog/product_info.php?products_id=53065).

10. Theoretical and Conceptual Issues in Leadership and Complex Military Operations (Published by Nigerian Defence Academy Publishing, Kaduna (Nigeria), as Chapter 5, in Leadership and Complex Military Operations, 2016).

Author's Contributions

1. **Review: The Context of Technology in Network Security Engineering**

(Circulated at the London Cyber-security Summit in November 2011).

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed

School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstract. This paper reviews the context of technology in the overall network security system. This is done with a view to finding out its singular effectiveness in cyber defence. Security solutions have a technological component but security is fundamentally a people problem. This is because a security system is only as strong as its weakest link, while the weakest link of any security system is the human infrastructure. In this regard, the significance of social engineering as a tool for cyber defence has been underplayed, compared to technological tools like cryptography. Unless this trend is reversed, it is likely that the current state of insecurity in the cyberspace will get more compounded as network systems become more complex. Further studies are being conducted with a view to establishing a tripartite relationship among Cryptography, Social Engineering and the Effectiveness of Cyber Defence mechanism.

Keywords: Technology, Cryptography, Human Infrastructure/Social Engineering, Computer Communication, Cybersecurity/ Network Security.

2. **Threat Analysis versus Risk Analysis in Intelligence and Security Assessment** (Published as Chapter 36 in 'Nigerian Defence and Security: Essays in Commemoration of Nigerian Defence Academy Golden Jubilee', September 2014 - Book cover attached on Page 277).

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed

School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstract

A realisation of the relationships among the security terms threat, vulnerability and risk, led to a perception of inconsistency about the security assessment procedure in the defence and public security industry in Nigeria. This is a practice whereby threat analysis is usually over-emphasised to the detriment of vulnerability and risk analyses.

An original misconception surrounding the term analysis, as employed in the Intelligence Cycle, and its opposite counterpart, synthesis, was suspect. This paper was designed to sort out the technical relationship between analysis and synthesis, with a view to exploiting the implications optimally.

It was revealed that the two terms are opposite in meaning but need to be intricately inter-woven in their employment as evaluation techniques. Unfortunately, most intelligence and security "analysts" embark on analysis with little or no idea about synthesis, thus muddling up the two concepts to the advantage of analysis. This original misconception led to a culture of non-systematism and haphazardness in the intelligence assessment procedure. This culture was transmitted, in situ, from intelligence 'analysis' to security 'analysis.' Thus, the terms vulnerability and risk in security assessment suffer an almost identical fate with synthesis. It is the same reason that is most probably responsible for the divergence in the security assessment procedure between the public and private segments of the security industry.

The implications of this anomaly include the virtual disappearance of synthesist in the global professional vocabulary of intelligence and security organisations, except for India; with resultant inconsistencies in the definition of intelligence analysis, and a culture of lack of systematism and accountability in the security assessment procedure. It is proposed that the phrase intelligence analysis, as employed in intelligence processing, should be replaced with intelligence synthesis. Intelligence products should be made amenable to re-evaluation and accountability. In military and security operations, the object of security assessment should be risk analysis, as opposed to threat analysis. Newly suggested terminologies are analosynthesis, synthonalysis and equisynalysis. Similarly, thesis, as a synonym of dissertation, should be replaced with synthesis.

Key Words: Analysis, Thesis, Synthesis, Threat, Vulnerability, Risk, Intelligence.

3. **Resolving the Password Security Purgatory in the Contexts of Technology, Security and Human Factors** {Presented at: International Conference on Computer Applications Technology, 20-22 January 2013 (ICCAT 2013 Sousse, Tunisia); Published in ICCAT 2013 Conference Proceedings & IEEE Xplore}.

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed
School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstract - Passwords are the most popular and constitute the first line of defence in computer-based security systems; despite the existence of more attack-resistant authentication schemes. In order to enhance password security, it is imperative to strike a balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. It is noted that the human factor is the most critical element in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. This illustrates the significance of social engineering in security designs, and the fact that security is indeed a function of both technology and human factors; bearing in mind the fact that there can be no technical hacking in vacuum. This

paper examines the current divergence among security engineers as regards the rules governing best practices in the use of passwords: should they be written down or memorised; changed frequently or remain permanent? It also attempts to elucidate the facts surrounding some of the myths associated with computer security. This paper posits that destitution of requisite balance between the factors of technology and factors of humanity is responsible for the purgatory posture of password security related problems. It is thus recommended that, in the handling of password security issues, human factors should be given priority over technological factors. The paper proposes the use of the (k, n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of the password repository. This presupposes an inclination towards writing down the password: after all, Diamond, Platinum, Gold and Silver are not memorised; they are stored.

Keywords – technology; cryptography; computer security; social engineering; human hacking; socio-cryptanalysis; password; password repository; purgatory

4. **Password Security Awareness in African Countries within the Context of Password Security Purgatory {**published by Dline Journals: Journal of Information Security Research - Journal cover attached on Page 278 (http://www.dline.info/index.php/about-us; www.iccat2013.org**)}.**

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed
School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstract – In spite of the existence of more attack-resistant authentication schemes, passwords are the most popular means of access control. They also constitute the first line of defence in cyber-based security systems. Unfortunately, the twin problem of multiplicity of passwords combined with destructive human factors has resulted in numerous rules which have made password management cumbersome. The resultant evasive tendency on the part of users has created a divergence among security experts. Using a survey, this paper examines the level of password security awareness in Africa, vis a vis the current divergence among security engineers as regards the rules governing best practices in the use of passwords: should they be written down or memorised; changed frequently or remain permanent? It also proposes a possible way out in respect of the password security purgatory phenomenon. It is posited that, in order to enhance password security, there should be a delicate balance between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions; i.e., human factors should be given priority over technological factors. The password security survey further confirmed the fear that most Internet users are inclined to choosing passwords that are both meaningful and easily remember-able. Similarly, in Africa, and probably most developing countries, senior executives are less security conscious compared to their subordinates, as regards password related matters. The paper proposes the use of the (k, n)-Threshold Scheme, such as the Shamir's secret-sharing scheme, to enhance the security of the password repository. This presupposes an inclination towards writing down the password: they could be stored securely, along with other valuables, even where other modern technological facilities are not available.

Keywords: cryptography, computer security, social engineering, human hacking/socio-cryptanalysis, password repository, purgatory

5. **Extending the Security Perimeter through a Web of Trust: The Impact of GPS Technology on Location-Based Authentication Techniques** (Published in ITA 2013 Conference Proceedings).

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed
School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom

{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstracts

Security is a function of the trust that is associated with the active variables in a system. Thus, the human factor being the most critical element in security systems, the security perimeter could be defined in relation to the human trust level. Trust level could be measured via positive identification of the person/device on the other side of the interaction medium, using various authentication schemes; location-based being one of the latest. As for the location-based services, the identity of a customer remains hazy as long as his location is unknown; he virtually remains a ghost in the air, with implications on trust. This paper reviews the various location-based authentication techniques with a focus on the role that GPS could play in optimising this authentication approach. It advocates the urgent need to make all transmission devices GPS-compliant as a way forward, despite the privacy issues that might arise.

Keywords

Security perimeter, Web of trust, GPS, GPS-compliant, Authentication

6. Nigeria: Cyberspace Security vis a vis Computerisation, Miniaturisation and Location-Based Authentication (Published in WICON 2014 Conference Proceedings).

Authors

[1]Muhammad Adeka, [1]Mohammad Ngala, [2]E. Ibrahim, [1]Simon Shepherd, [3]Issa Elfergani, [3]Ash S Hussaini, [1]Fauzi Elmegri and [1]Raed Abd-Alhameed

[1]Mobile and Satellite Communications Centre, University of Bradford, UK
[2]College of Electronic Technology Bani Walid – Libya
[3]Instituto de Telecomunicacoes – Aveiro, Portugal
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Abstract. The degree of insecurity occasioned by fraudulent practices in Nigeria has been of great concern economically, especially as it relates to overseas transactions. This paper was designed to mitigate this problem for Nigeria and countries with similar dispositions. Based on a survey involving field trip to Nigeria, the paper examines the general security situation in Nigeria and its mutual impacts with computerisation, miniaturisation and Location-Based

Authentication (LBA). It was discovered that both computerisation and miniaturisation had some negative effects on cyber-security, as these were being exploited by fraudsters, especially using 'advance fee fraud;' popularly called 419. As a countermeasure, the research examined the possibility of using LBA and further digitisation of the GSM Mobile country codes down to City/Area codes along with GSM Mobile/Global Positioning System (GPS) authentications. Where necessary, these could be combined with the use of a web-based Secret Sharing Scheme for services with very high security demands. The anticipated challenges were also examined and considered to be of negligible impacts; especially roaming.

Keywords: Cyberspace, Computerisation, Miniaturisation, Authentication, Advance Fee Fraud (419), Digitisation and Tele-density.

7. Africa: cyber-security and its mutual impacts with computerisation, miniaturisation and location-based authentication (Submitted for EAI Journal Publication 2015; under review).

Authors

M.I. Adeka[1,30], M. Ngala[1], E. Ibrahim[2], S.J. Shepherd[1], I. Elfergani[3], A.S. Hussaini[3], F. Elmegri[1] and R.A. Abd-Alhameed[1]

[1]Mobile and Satellite Communications Centre, University of Bradford, UK
[2]College of Electronic Technology Bani Walid – Libya
[3]Instituto de Telecomunicacoes – Aveiro, Portugal

Abstract

The state of insecurity occasioned by fraudulent practices in Africa has been of concern economically, both at home and abroad. This paper was designed to mitigate this problem, using Nigeria as a case study. Based on a survey in West Africa, the paper examines the security situation in the continent and its mutual impacts with computerisation, miniaturisation and Location-Based Authentication (LBA). It was discovered that computerisation and miniaturisation had negative effects on cyber-security, as these were being exploited by fraudsters, using advance fee fraud; called 419. As a countermeasure, the research examined the possibility of using LBA and digitisation of the GSM Mobile country codes down to City/Area codes along with GSM/GPS authentications. These could also be combined with the use of a web-based Secret Sharing Scheme for services with very high security demands. The anticipated challenges were also examined and considered to be of negligible impacts; e.g., roaming.

Keywords: cyberspace, computerisation, miniaturisation, authentication, advance fee fraud (419), digitisation and tele-density.

8. A Versatile and Ubiquitous Secret Sharing: A cloud data repository secure access (Accepted for Presentation in September at ITA 2015, Wales, UK).

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed

[30] M.I. Adeka, miadeka@student.bradford.ac.uk

School of Electrical Engineering and Computer Science, Faculty of Engineering and Informatics
University of Bradford,
Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student., S.J.Shepherd@, R.A.A.Abd@}Bradford.ac.uk

Abstract - The Versatile and Ubiquitous Secret Sharing System, a cloud data repository secure access and a web based authentication scheme. It is designed to implement the sharing, distribution and reconstruction of sensitive secret data that could compromise the functioning of an organisation, if leaked to unauthorised persons. This is carried out in a secure web environment, globally. It is a threshold secret sharing scheme, designed to extend the human trust security perimeter. The system could be adapted to serve as a cloud data repository and secure data communication scheme. A secret sharing scheme is a method by which a dealer distributes shares of a secret data to trustees, such that only authorised subsets of the trustees can reconstruct the secret. This paper gives a brief summary of the layout and functions of a 15-page secure server-based website prototype; the main focus of a PhD research effort titled 'Cryptography and Computer Communications Security: Extending the Human Security Perimeter through a Web of Trust'. The prototype, which has been successfully tested, has globalised the distribution and reconstruction processes.

Keywords – authentication; secret sharing; cryptography; key management; interpolation; authorised user; human security perimeter; (k, n)-threshold; participants (trustees); dealer or distributor; combiner; cloud data repository

9. **Chapter 1 – Telecommunication Network Security** (Published by Nova Science Publishers, Inc., New York, as Chapter 1, in Horizons in Computer Science Research, Volume 10, with online Independent Chapter Open Access at: https://www.novapublishers.com/catalog/product_info.php?products_id=53065 – Book cover attached on Page 279).

Authors

Muhammad Adeka, Simon Shepherd, Raed Abd-Alhameed
School of Engineering, Design and Technology, University of Bradford, Bradford, West Yorkshire, BD7 1DP, United Kingdom
{M.I.Adeka@student.,S.J.Shepherd@,R.A.A.Abd@}Bradford.ac.uk

Chapter Summary
(Chapter 1 – Telecommunication Network Security)

Our global age is practically defined by the ubiquity of the Internet; the worldwide interconnection of cyber networks that facilitates accessibility to virtually all ICT and other elements of critical infrastructural facilities, with a click of a button. This is regardless of the user's location and state of equilibrium; whether static or mobile. However, such interconnectivity is not without security consequences.

A telecommunication system is indeed a communication system with the distinguishing key word, the Greek tele-, which means "at a distance," to imply that the source and sink of the system are at some distance apart. Its purpose is to transfer information from some source to a distant user; the key concepts being

information, transmission and distance. These would require a means, each, to send, convey and receive the information with safety and some degree of fidelity that is acceptable to both the source and the sink.

Chapter K begins with an effort to conceptualise the telecommunication network security environment, using relevant ITU-T[31*] recommendations and terminologies for secure telecommunications.

The chapter is primarily concerned with the **security** aspect of computer-mediated telecommunications. Telecommunications should not be seen as an isolated phenomenon; it is a critical resource for the functioning of cross-industrial businesses in connection with IT. Hence, just as information, data or a computer/local computer-based network must have appropriate level of security, so also a telecommunication network must have equivalent security measures; these may often be the same as or similar to those for other ICT resources, e.g., password management.

In view of the forgoing, the chapter provides a brief coverage of the subject matter by first assessing the context of security and the threat landscape. This is followed by an assessment of telecommunication network security requirements; identification of threats to the systems, the conceivable counter or mitigating measures and their implementation techniques. These bring into focus various cryptographic/crypt analytical concepts, vis a vis social engineering/socio-crypt analytical techniques and password management.

The chapter noted that the human factor is the most critical factor in the security system for at least three possible reasons; it is the weakest link, the only factor that exercises initiatives, as well as the factor that transcends all the other elements of the entire system. This underscores the significance of social engineering in every facet of security arrangement. It is also noted that password security could be enhanced, if a balance is struck between having enough rules to maintain good security and not having too many rules that would compel users to take evasive actions which would, in turn, compromise security. The chapter is of the view that network security is inversely proportional to its complexity. In addition to the traditional authentication techniques, the chapter gives a reasonable attention to location-based authentication. The chapter concludes that security solutions have a technological component, but security is fundamentally a people problem. This is because a security system is only as strong as its weakest link, while the weakest link of any security system is the human infrastructure.

A projection for the future of telecommunication network security postulates that, network security would continue to get worse unless there is a change in the prevailing practice of externality or vicarious liability in the computer/security industry; where consumers of security products, as opposed to producers, bear the cost of security ineffectiveness. It is suggested that all transmission devices be made GPS-compliant, with inherent capabilities for location-based mutual authentication. This could enhance the future of telecommunication security.

[31*] International Telecommunications Union - Telecommunication Standardisation Sector