The Strategic Implications of the Current Internet Design for Cyber Security

by

Charles M. Iheagwara
Ph.D., Computer Science
School of Computing, The University of Glamorgan, Wales, UK

Submitted to the System Design and Management Program
In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Engineering and Management

At the

Massachusetts Institute of Technology

February 2011
[June 2011]

Signature of Author _____
Charles Iheagwara
Submitted to the System Design and Management Program
February 2011

Certified by _____
James M. Utterback
Thesis Supervisor
David J. McGrath jr (1959) Professor of Management and Innovation and
Professor of Engineering Systems

Accepted by _____
Patrick Hale
Program Director
System Design and Management Program

Dedicated to my late niece Jane Nkechi Njoku who dreamt of a graduate engineering education at one of the world's best institutions such as MIT but whose life on earth was cut short at age 24 following graduation from college with a distinction in computer science/electrical engineering.

This page has been left intentionally blank

Acknowledgements

This submission is the result of the analytical research work with my supervisor, Dr. Jim Utterback and a few others.

I would like to express my gratitude and thanks Dr. Jim Utterback. As my supervisor, he received me with open arms for this research and provided me with continuous guidance and support throughout the entire duration of the work. I learnt from him many things in the field of Technology Strategy. He opened my thought process to the best ways to conduct effective research and taught me the best methods to conduct analytical work involving interpretation of data from different sources. I'd like to thank him for giving liberally of his time, for the entire duration of this work.

My thanks also go to Pat Hale, SDM Program Director. He provided invaluable support and feedback throughout the period of my study at the SDM.

And, I thank the entire faculty members of the Sloan School of Management and School of Engineering who expanded my knowledge in the different courses I took with them; and Professors Andrew Blyth of the University of Glamorgan, Geoff Jones and Amy Cuddy of Harvard Business School for their contributions to my education.

An essential contribution to every work is given by discussions and joint works. It is impossible to list all the researchers from whom I received valuable contributions and support throughout the period of my studies at MIT. Many thanks to David Clark, the Internet Architect Statesman for his insights on the best way forward and to my class mates Dr. Ruktai Ace Prurapark and Jang Hoon Yoo who contributed to some of the work on Stakeholder Analysis.

I want to also thank Chris Bates, Dave Schulz, Melissa Parrillo and the entire SDM staff for their support. I am indebted to Bill Foley for giving his time (whether by phone, or by e-mail), as we went through sorting out the administrative details of this program.

Of course, the works presented in this submission is strongly based on what preceded the last fourteen months. For all kinds of support, courtesy, love, patience and encouragement, I thank my wife Susan, my daughter Chinenye, my son Chinasa, my mother Lady Bernadette Iheagwara, and the other members of my extended family for standing with me throughout the period of this program.

And I am grateful to God the almighty father, for his grace, blessings and protection.

Finally, I would like to thank in a very big way someone who is not here anymore and who would have been happy to know about me and the progress of my study at MIT. Sir Livinus Iheagwara was a great father who taught me the value of hard work and the rewards of patience. He taught me to love and serve the Lord Jesus Christ and to love my fellow men and women. To a great father and my late niece, I dedicate this work.

TABLE OF CONTENTS

Abstract

The Strategic Implications of the Current Internet Design for Cyber Security

by

Charles M. Iheagwara

Submitted to the System Design and Management Program in Partial Fulfillment of the Requirements for the degree of
Master of Science in Engineering and Management

In the last two decades, the Internet system has evolved from a collection point of a few networks to a worldwide interconnection of millions of networks and users who connect to transact virtually all kinds of business. The evolved network system is also known as Cyberspace.

The use of Cyberspace is now greatly expanded to all fields of human endeavor by far exceeding the original design projection. And even though, the Internet architecture and design has been robust enough to accommodate the extended domains of uses and applications, it has also become a medium used to launch all sorts of Cyber attacks that results into several undesirable consequences to users.

This thesis analyzes the current Internet system architecture and design and how their flaws are exploited to launch Cyber attacks; evaluates reports from Internet traffic monitoring activities and research reports from several organizations; provides a mapping of Cyber attacks to Internet architecture and design flaw origin; conducts Internet system stakeholder analysis; derives strategic implications of the impact of Internet system weaknesses on Cyber security; and makes recommendations on the broader issues of developing effective strategies to implement Cyber security in enterprise systems that have increasingly become complex.

From a global architectural design perspective, the study conducted demonstrates that although the Internet is a robust design, the lack of any means of authentication on the system is primarily responsible for the host of Cyber security issues and thus has become the bane of the system.

Following the analysis, extrapolation of facts and by inferences we conclude that the myriad of Cyber security problems will remain and continue on the current exponential growth path until the Internet and in particular the TCP/IP stack is given the ability to authenticate and that only through a collaborative effort by all stakeholders of the Internet system can the other major Cyber security issues be resolved especially as it relates to envisioning and fashioning new Cyber security centric technologies.

Thesis Supervisor: James M. Utterback.
Title: David J. McGrath jr (1959) Professor of Management and Innovation and Professor of Engineering Systems

List of Figures

List of Tables

This page has been left intentionally blank

Chapter 1: Introduction

1.1 Motivation

In the last two decades, the Internet system has evolved from a collection point of a few networks to a worldwide interconnection of millions of networks and users who connect to transact virtually all kinds of business. Today, this evolved network system is also known as Cyberspace.

The use of Cyberspace is now greatly expanded to many areas by far exceeding the intent of use(s) of the original design and has increasingly been extended to all fields of human endeavor. Although, the Internet architecture and design has been robust enough to accommodate the extended uses and applications, it has also become a medium used to launch all sorts of Cyber attacks that results into several undesirable consequences to users.

What is interesting is that the scope and scale of the attacks continue to increase day by day even as new counter measures are adopted, new attack types emerge making this a wide open theater with many actors like Cyber criminals on the one hand wrecking havoc on the system and Information Technology (IT) security professionals, researchers, and others on the other hand cleaning up and addressing the issues created by Cyber criminals.

Hence, the motivation for this study is to look at the different dynamics at play and discern some facts from where we analyze which of the Internet design elements and factors gives rise to or contributes to Cyber attacks and then derive strategic implications arising from them.

1.2 Objective

The objective of this study is to analyze the current Internet system design with respect to the flaws inherent in the architecture and how these give rise to Cyber attacks.

Additional objectives are to conduct a stakeholder analysis to establish implied mandates for Cyber security responsibilities; and to discern strategic implications arising from unfulfilled stakeholder design goals and intents of the Internet system.

1.3 Approach to Research

We will follow the following logical approach for this study:

1. First, we will review and describe the Internet evolution, architecture and design; and Cyber space from different literature sources
2. Second, we will analyze the flaws inherent in the current architecture that serves as the conduit for Cyber attackss
3. Next, we will design a grid that maps each known Cyber attack to the Internet architecture
4. Following this, we will conduct a stakeholder analysis to discern expressed mandates in the design and roles and responsibilities associated with maintaining security on the Internet system
5. Then, we will derive the strategic implications of the design flaws – both intentional and unintentional – for Cyber security
6. Finally, we will conclude and make recommendations on how to improve the Internet design for Cyber security

Exhibit I is a graphical representation of the approach.

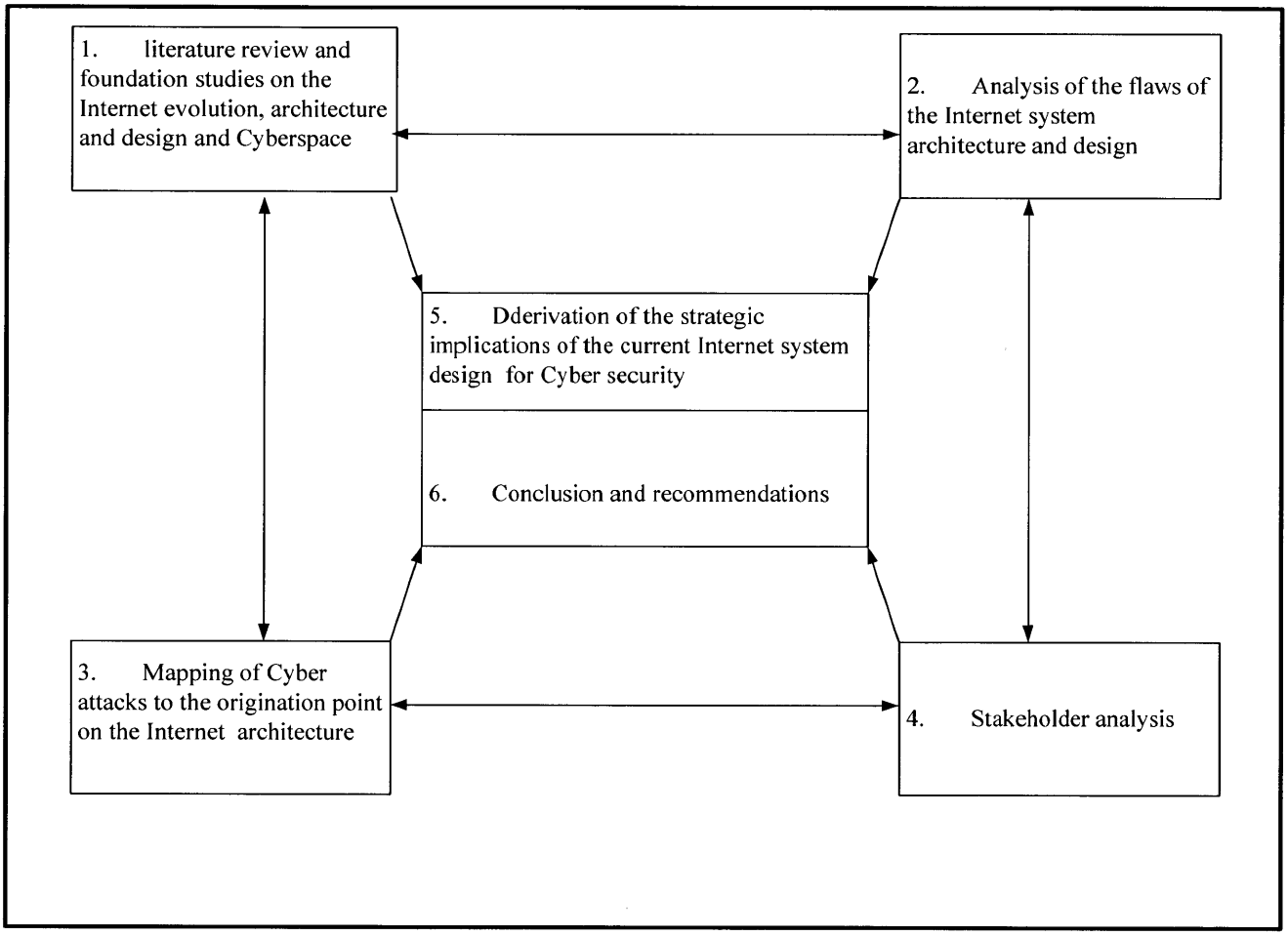

Exhibit 1: Thesis Research Approach

1.4 Summary of Work

The Internet design manifests a robust architecture that is elastic enough to integrate new processes, applications and technologies. This is at the very essence of the layering and stratification of the design which segregates stack functions at each layer and aims to simplify, satisfy the various demands and drive efficiency of the process. Stallings (2006) has provided a vivid description of the layering structure of the TCP/IP Internet model. For example, on the IP layer Stalling asserts: "this layered modularity gave rise to the "hourglass" metaphor for the Internet architecture the creation of a multi-layer suite of protocols, with a generic packet (datagram) delivery mechanism as a separate layer at the hourglass' waist. This abstract bit-level network service at the hourglass' waist is provided by IP and ensures the critical separation between an ever more versatile physical network infrastructure below the waist and an ever-increasing user demand for higher-level services and applications above the waist."

The resulting Internet design is one that has lived up to expectation of its robust and durable architecture, but, which nevertheless, lacks the mechanism to authenticate and provide a security platform. It is the lack of this together with the flaws of the TCP/IP protocol stack and other communication protocols that accounts for most of the Cyber attacks recorded today.

In this thesis, we analyze the current Internet design, Cyberspace and security, the flaws in the current architecture and stakeholder analysis of the Internet system.

Then, we review and analyze several research and monitoring reports, interpret the statistical data reported on Cyber attacks and develop a scheme that maps each attack type to specific Internet architecture layer.

Finally, we drive implications arising therefore for Cyber security.

The following summarizes the work completed and presented in this Thesis.

Chapter 2

Chapter 2 provides background information related to the Internet, and its use as a medium to conduct online transactions. To understand the nature of the medium, we conducted a literature review of Cyberspace. The results of our review shows that Cyber space is not sufficiently secure as several security breaches have occurred over it, and that it has also become a breeding ground for Cyber criminals.

In response to this, organizations now implement security measures on their information systems under the umbrella of Cyber security practice groups organized as new business units.

Further, in this Chapter we have studied the progressive evolution of Cyber security practices over the years and note that Cyber security as it is practiced today represents different standards and norms, each of which is interpreted and implemented to the extent permissible by organizational resources and constraints and that although not yet sufficient to combat current and future security issues, significant progress has been made at least by establishing the frameworks to implement security in Cyberspace. The "Bolts" and "Nuts' that have evolved over the years are discussed in their shapes and forms under the" Current State of Practice" in Section 2.5.

Chapter 3

Chapter 3 presents a description of the architecture and design of the TCP/IP protocol suite that serves as the primary transport and communication mechanism in Cyberspace. The five-layer TCP/IP protocol suite consists (from the bottom up) of the physical, link, internetwork, transport, and application layers.

In addition, we analyzed the flaws inherent in the Internet architecture and design flaws and note that the TCP/IP vulnerabilities are exploited by the threat agents given Table 2 to launch the Cyber attacks present in Appendix I.

Also, the Domain Name System is discussed in the context of its architecture and weaknesses that also serves as a conduit for Cyber attacks.

We note in conclusion:

1. ***Robustness:*** The Internet design manifests a robust architecture that is elastic enough to integrate new processes, applications and technologies.
2. ***Efficiency:*** The layered architecture is intended to provide efficiency through roles assignment.
3. ***Platform Independence and IP Layer:*** The Internet Protocol (IP) is the internetworking protocol for TCP/IP, and its main task is to adequately implement all the mechanisms necessary to knit together divergent networking technologies and administrative domains into a single virtual network (an "internet") so as to enable data communication between sending and receiving hosts, irrespective of where in the network they are.
4. ***TCP Layer:*** The layer above IP is the transport (TC) layer, where the most commonly used Transmission Control Protocol (TCP) deals, among other issues, with end-to-end congestion control and assures that arbitrarily large streams of data are reliably delivered and arrive at their destination in the order sent.
5. ***Application Layer:*** Also, the top layer in the TCP/IP protocol suite is the application layer, which contains a range of protocols that directly serve the user; e.g., telnet (for remote login), ftp (the File Transfer Protocol for transferring files, smtp (Simple Mail Transfer Protocol for e-mail), http (the HyperText Transfer Protocol for the World Wide Web).

Chapter 4

One of the key objectives of this Chapter is to match several well-known Cyber attack types to the Internet layer that serves as the conduit for such attacks and then quantify each attack type as a percentage of the overall Cyber attack types.

To accomplish this, we reviewed and analyzed several Internet traffic monitoring reports and statistical research studies on Cyber attacks, and deduced several facts to aid our interpretation of the domain knowledge.

Following the review and analysis and by inferences from research results and the data presented in the previous Chapters, we developed a grid that maps each Cyber attack type to specific Internet architecture layers and discerned several well-known trends in the constantly evolving Cyber attacks.

Finally, we conclude that quantification is difficult to realize because of insufficient and scanty data from which such quantification could be derived; and the lack of any known predictive (or adaptive) model that can help us to accomplish this.

Chapter 5

The Internet is an engineering system with different sub-systems that fuses together as a single whole. Over the years since its original design, it has become increasingly complex with the addition of millions of networks with different architectural make-ups and requirements. In effect, the Internet has become a massive infrastructure powered by different applications, technologies and linked networks.

Given the above, in Chapter 5, we have conducted a stakeholder-beneficiary analysis of the Internet system to among others discern stakeholder intent and goals evident in the original design and the security requirements mandated for the system.

Based on our analysis, we note that there is an expressed mandate in the original intent and goal for the architecture of the process to include security – even though the design element leaves this out. We delineated the different value related processes and instruments used to execute processes. Interestingly, the value related instruments such as routers, switches and other routing devices have become part of the internet massive infrastructure outlay and without adequate security have also become a bane of the process.

Finally, we conclude that stakeholders have the primary responsibility of assuring security on the system in a collaborative fashion.

Chapter 6

Based on the facts and inferences from our analysis, we discern several implications for Cyber security arising from the current Internet architecture vulnerabilities.

Primary among them are the implications for a potential Cyber warfare on nations and transnational infrastructures; constantly emerging threat and attack types that extends the security domain and perimeter of the enterprise, the emergence of a new underground economy where Cyber war lords rule over Cyberspace and aided with low entry barriers and technology can at will wreck havoc on any intended target.

These and the other implications we predict are gradually building up to what may potentially become a useful arsenal for rogue nations for Cyber warfare.

Finally, we conclude that the primary constraint here is the lack of any authentication mechanism on the Internet system around which an effective preventive defense can be built and mounted.

Chapter 7

Chapter 7 concludes our work with recommendations on areas of possible improvement of Cyber security. We conclude that although a robust design, the current Internet design has several flaws which have made using it to transact business risk – even with ad-hoc fixes - and portends enormous implications for Cyber security; and in particular, the original Internet protocols are not robust communications technology, are unsecured and can not to be used for business without coupling with extra security measures such as ad-hoc security fixes which are often very expensive and ever constantly changing and being re-defined in response to the constantly emerging new threats and Cyber attack types.

1.5 Organization of Document

This submission overview is organized as follows: Chaper1 outlines the motivation and objective of this study. Chapter 2 introduces the reader to background information, Cyber space, the threats, the "Bolt" and "Nuts" and the current state of the practice is statement and approach to research. Chapter 3 describes the Internet architecture and security flaws. Chapter 4 presents an analysis of Internet vulnerabilities and Cyber attacks. Chapter 5 presents a stakeholder analysis of the Internet system. Chapter 6 describes the strategic implications of the current Internet design for Cyber security. Finally, Chapter 7 presents the conclusions and summarizes our recommendations.

Chapter 2: Cyber Security

The exponential growth of the Internet has brought about a wave of security breaches on connected networks and online transactions by Cyber criminals who continue to defeat any scheme devised to protect Cyberspace. The breaches manifest in different shades and forms, and have giving rise to an underground economy run by Cyber criminals and powered by Bot-net Servers and other technologies. This sophisticated underground community is growing faster than imagined and have been able to defeat any known defense put in place. To stem the tide, virtually all online users including connected governments, commercial entities are increasingly implementing security measures to protect their online transactions.

In this Chapter, we will provide background information on Internet evolution and statistics, define Cyber security, describe Cyberspace security issues and threats, the "Bolts" and "Nuts" of Cyber Security and the current state of Cyber security practice.

2.1 Background

The Internet connects millions of users and businesses today and has become a vital resource that is changing the way many businesses and individuals communicate and do business. But, several issues plague the process as the Internet suffers from significant and widespread security problems. For example, many organizations and businesses have been attacked or probed by intruders, with resultant losses to revenue generation, productivity and reputation. Coupled with this are myriads of other problems attendant with Internet usage like temporary or prolonged disconnection from the Internet that are resolved with significant investment of resources to correct the problems with system and network configurations.

The emergence of Business to Business transactions over Web Sites have increased the significance of the Internet and often such Websites are unaware or ignorant of these problem and face the risk of being attacked by network intruders. Even sites that do observe good security practices face problems with new vulnerabilities in networking software and the persistence of some intruders.

The fundamental problem here is that the Internet was not designed to be very secure. Communication is accomplished using protocol suites that are known as the Transport Control Protocol and Internet Protocol (TCP/IP). By itself, the protocol suites are plagued with design and architectural flaws.

Some of the known inherent problems with the current Internet system are:

- The TCP/IP protocol stack has several security issues including the lack of ability to authenticate thereby serving as a conduit for multiple Cyber attacks.
- Vulnerable TCP/IP services -- a number of the TCP/IP services are not designed to be secure and can be compromised by knowledgeable intruders; services used for testing are particularly vulnerable.

- Lack of policy -- many sites are configured unintentionally for wide-open Internet access without regard for the potential for abuse from the Internet; many sites permit more TCP/IP services than they require for their operations and do not attempt to limit access to information about their computers that could prove valuable to intruders, and
- Complexity of configuration -- host security access controls are often complex to configure and monitor; controls that are accidentally mis-configured can result in unauthorized access.

A more extended description of the Internet system and their weaknesses is given in Section 2 of this Thesis.

Some of the security issues that result from the Internet system flaws are discussed in the next Sections.

2.2 Cyberspace and Security Issues

The medium created by the Internet is called Cyberspace and is essentially the global network of interdependent information technology infrastructures, telecommunications networks and computer processing systems, which by its very design is free and open to the public.

Computers at Risk[1], a 1991 report by the Computer Science & Telecommunications Board of the National Research Council begins:

> *"We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps more alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."*

It has been twenty years when these words were written, the first personal computers, web browsers and networks were still on the drawing board and the Internet was a place for high-tech aficionados. Since then, we have walked some distance and have come considerably far. Today, our dependence on inter-networked computing systems means that virtually every walk of life—whether personal or commercial, public or private, civilian or military—is intermediated by computer systems. But virtually none of these systems are trustworthy; all are subject to attack; in fact, many are actively under attack today.

In the last couple of years, several changes brought in IT have changed the nature of Cyberspace and for that matter have very much made the computing world risky:

---

[1] Computers at Risk: "Safe Computing in the Information Age," National Academies Press, Washington DC, 1991, http://books.nap.edu/catalog.php?record_id=1581. Last checked June 12, 2010.

- Novel embedded computing has become part of modern day computing
- Several large network as backbone for connectivity has sprung up and spread on Cyberspace
- There are now multiple service providers providing links
- Multiple Technologies to support network infrastructure CDMA, VSAT, DSL
- Multiple Applications

The convergence has created complexity of today's network (Figure 1). And, interconnected networks have grown to several millions.

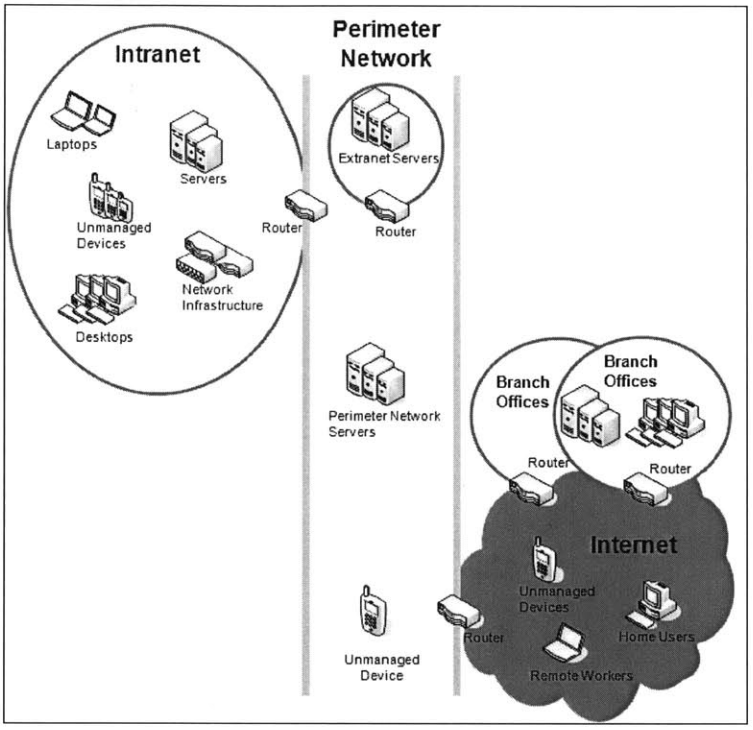

Figure 1: The Complexity of Today's Network from Gulshan R. (2009)

Not only is there an exponential increase in the number of interconnected networks, businesses and users but also a growing concern Gulshan R. (2009):

(i) That computing and the Internet has turned against us

(ii) With the exponential growth in security incidents with noticeable high profile cases:

a. Pentagon, US in 2007
b. Estonia in April 2007
c. Computer System of German Chancellery and three Ministries
d. Highly classified computer network in New Zealand & Australia"

(iii)With complex and target oriented software

(iv) With common computing technologies and systems

(v) With constant probing and mapping of network systems

Documented statistical evidence Gulshan R. (2009)[2] points to an increasing trend in the nature of incidents with a greater proportion of incidents attributed to Phishing that is prevalent in eCommerce.

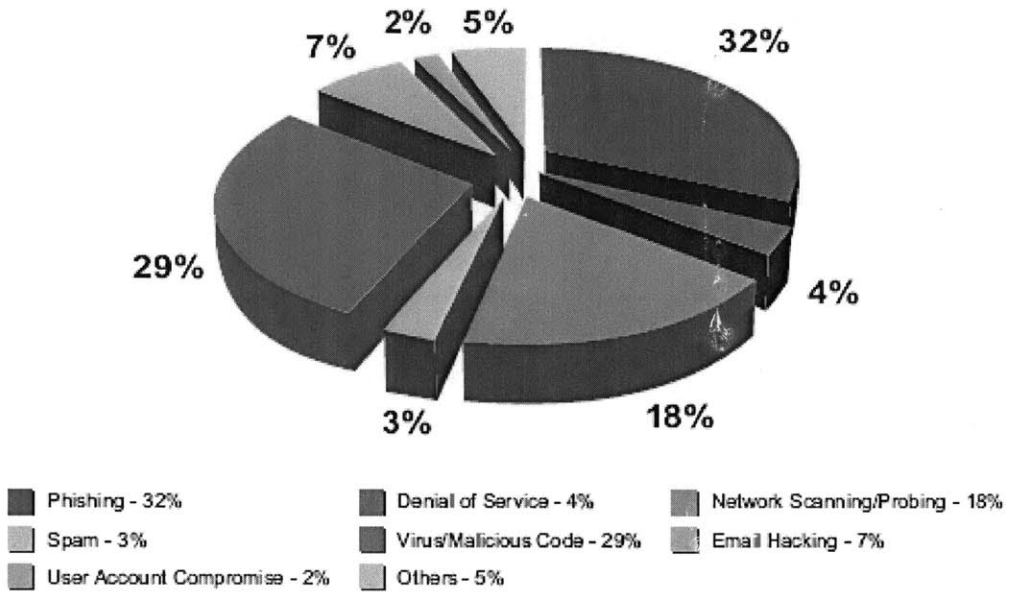

Figure 2: Security Incidents reported during 2008 from Gulshan R. (2009).

The statistics points to a very disturbing trend that does not bode well for a world that has come increasingly depend on Web sites for transacting virtually every type of business.

Gulshan R. (2009) notes that among the trends shaping the future of Cyberspace are:

- Ubiquitous computing, networking and mobility
- Embedded Computing
- Security
- Internet Protocol version six (IPv6)
- Voice over Internet Protocol (VoIP)

[2] Gulshan, R. (2009), "Cyber Security: Indian perspective," http://www.cyberseminar.cdit.org/pdf/09_02_09/gulshan.pdf. Last checked June 13, 2010.

Table 1: Number of Internet Web sites from Gulshan R. (2009).

The Growing number of Web Sites in the World	
Year	Number of Web sites
1993 (Web Invented and implemented)	**130**
1994	**2738**
1995	**23500**
2007	**550 Million**
2008	**850 Million**

And that, the nature of today's Cyberspace security issues is different from those of yester years; and more so have become very complex.

- Sophisticated attacks
  - Attackers are refining their methods and consolidating assets to create global networks that support coordinated criminal activity

- Rise of Cyber Spying and Targeted attacks
  - Mapping of network, probing for weakness/vulnerabilities

- Malware propagation through Website intrusion
  - Large scale Structured Query Language (SQL) Injection attacks like Asprox Botnet

- Malware propagation through Spam is on the rise
  - Storm worm, which is one of the most notorious malware programs seen during 2007-08, circulates through spam
- Phishing
  - Increase in cases of fast-flux phishing and rock-phish
  - Domain name phishing and Registrar impersonation
- Crimeware
  - Targeting personal information for financial frauds
- Information Stealing through social networking sites
- Rise in Attack toolkits
  - Toolkits like Mpack and Neospolit can launch exploits for browser and client-side vulnerabilities against users who visit a malicious or compromised sites

In addition, Cyber security issues are not localized to a particular nation but are indeed transglobal. To underscore this, the security lab of the giant security software provider

Websense, Inc. that produces daily aggregated statistics of security events and trends provided the 2008 overall Cyber attack percentages[3] in Figure 3 below.

Figure 3: Global Attack Trend in 2008 from Websense Report (2008).

The report shows wide spread attacks over several continents. Other statistics and trending analysis – discussed in Chapter 4 - on the scope, depth and nature of security attacks in Cyberspace show a similar spread and trend.

2.3 Cyber Security Defined

So then, what is Cyber security?

Cyber security exists in the context of Cyberspace and is the art and practice of implementing security in Cyberspace. Ordinarily expressed, Cyber security can be defined as the safeguarding or protection of all things Internet -- from the networks themselves to the information stored in computer databases and other applications. It forms part of the comprehensive set of coherent Internet-specific information security practices. It provides the basis to protect the Internet and its constituent protocols and is an integral part of overall security.

The concept of Cyber security grew out of necessity as the Internet became a medium to transact businesses and millions of users, business and organizational groups got connected and started sending more data and processes online. The trend has continued and it's even more crucial now with the emergence of Web 2.0 technologies, which fosters online collaboration and information sharing. Also, the need for a secure Internet is underscored by the rapid increase in Cyber attacks.

---

[3] Websense Report, (2008): "Global Attack Trend in 2008," http://securitylabs.websense.com/. Last checked July 6, 2010.

In enterprise internetworking, a typical Cyber security implementation will include proper security design and management for safe, secure, integrated operations; and is realized by setting organizational security goals, establishing security policies and putting in place risk management remediation processes to identify and implement needed proactive and corrective measures.

In the end, the objective of cyber security practices is to implement information technology (IT) security solutions that protect the confidentiality, integrity and availability of information and the safety and operational effectiveness of process control, as well as to prevent information from being used to compromise the physical security practices of companies. To be effective, these controls need to include not only technology, but also processes and people.

2.4 Cyber Security Threats

By functional classification, there are four broad categories of threats: the threat of disruption, the threat of exploitation, the threat of manipulation, and the threat of destruction.[4]

Threat of Disruption: These are threats related to the disruption of utilities, communication flow, economic transactions, public information campaigns, electric power grids, and present serious economic and political consequence for both the government and private sector entities.

Viruses and denial-of-service attacks are a few of the potent weapons used to accomplish this category of threat.

Threat of Exploitation: The threat here is exploitation of proprietary or classified information usually accomplished by Information theft, identity theft, online credit card fraud or theft of credit card numbers, and theft of national security levels of information (e.g., systematic probing of classified or unclassified but sensitive government systems).

Occurrences of this type of threat are very difficult to detect and often lead to systems being compromised; and as with the threat of disruption, the probability of occurrence is high.

The Threat of Manipulation: This category of threat is used to exert influence, retaliate or leverage some form of advantage or gains by perpetrators. The threat is used to accomplish political, economic, military, or inflammatory purpose. Several incidents of defaced Web sites (election campaigns, e-Business sites such as Microsoft, Google, etc. and of altered personal financial information on e-commerce sites) point to the clear potential for using the Internet as a powerful tool for manipulating information.

While several instances of manipulation serve the purpose of touting or making a statement, and can be remedied rapidly, the more dangerous instances can go undetected for a lengthy period of time including manipulation of financial data, military information, or functional infrastructure data (e.g., the timing of dam releases).

---

[4] Borchgrave, Cilluffo, Cardash, and Michèle, (2000), "Cyber Threats and Information Security Meeting the 21st Century Challenge," Center for Strategic and International Studies, December 2000.

The Threat of Destruction: Destruction to exert economic and security losses is the primary motive here. Essentially, information, material and critical infrastructure that have harmful economic and national security consequences are destroyed. Techniques employed include the disruption using such hacking techniques as logic bombs, virus implantations and Trojan Horses scheming.

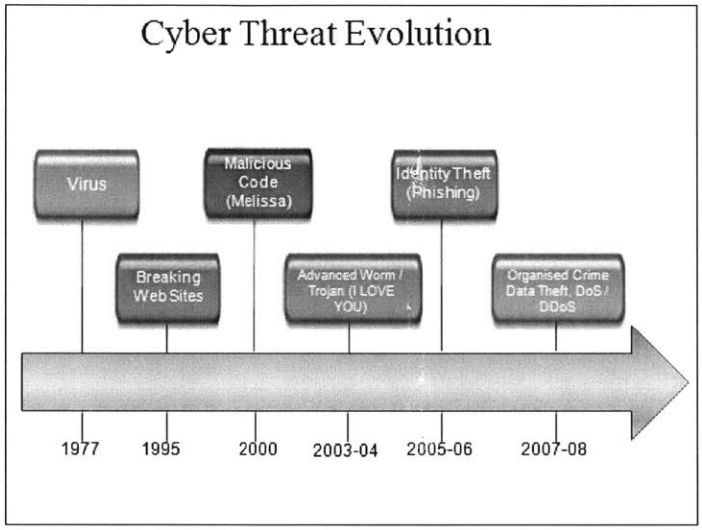

Figure 4: Cyber Threat Evolution from Gulshan R. (2009).

Gulshan R. (2009) opines that the threats highlighted above can be exploited when in-place security controls are weak resulting to different types of Cyber attacks defined in Table 14 (Appendix 2):

- Web defacement
- Spam
- Spoofing
- Proxy Scan
- Denial of Service
- Distributed Denial of Service
- Malicious Codes (Virus, Bots)
- Etc.

Specific threat agents have been given by the US General Accounting Office (GAO) in a recent report provided a description of different types of human threats that forms the larger part of the human Cyber crime community (see Table 2).

Table 2: Cyber Crime Human Threat Agents[5]

Threat	Description
Bot-network operators	Bot-network operators take over multiple systems in order to coordinate attacks and to distribute phishing schemes, spam, and malware attacks. The services of these networks are sometimes made available on underground markets (e.g., purchasing a denial-of-service attack or servers to relay spam or phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organized crime groups are using spam, phishing, and spyware/malware to commit identity theft and online fraud. International corporate spies and organized crime organizations also pose a threat to the United States through their ability to conduct industrial espionage and large-scale monetary theft and to hire or develop hacker talent.
Foreign intelligence services	Foreign intelligence services use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that could affect the daily lives of U.S. citizens across the country.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While gaining unauthorized access once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, while attack tools have become more sophisticated, they have also become easier to use. According to the Central Intelligence Agency, the large majority of hackers do not have the requisite expertise to threaten difficult targets such as critical U.S. networks. Nevertheless, the worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage.
Insiders	The disgruntled organization insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat includes contractors hired by the organization as well as employees who accidentally introduce malware into systems.
Phishers	Individuals, or small groups, execute phishing schemes in an attempt to steal identities or information for monetary gain. Phishers may also use spam and spyware/malware to accomplish their objectives.
Spammers	Individuals or organizations distribute unsolicited e-mail with hidden or false information in order to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations (i.e., denial of service).
Malware authors	Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa Macro Virus, the Explore.Zip worm, the CIH (Chernobyl) Virus, Nimda, Code Red, Slammer, and Blaster.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures in order to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. Terrorists may use phishing schemes or spyware/malware in order to generate funds or gather sensitive information.

[5] GAO Report Number: GAO-10-628, "Critical Infrastructure Protection," Report to the Congress of the US, July, 2010, http://www.scribd.com/doc/38237843/GAO-Cyber-Security. Last checked on September 14, 2010.

2.5 Critical Elements: The Bolts and Nuts of Cyber Security

Cyber security, an umbrella term that incorporates different IT strategies to protect networks comprises several components that address different aspects of network and system vulnerabilities that can be exploited to launch attacks. These typically revolve around the security frameworks and techniques that are used to implement protective measures.

Generally, there are ten (10) security domains that form the pipelines or *frameworks* designating a particular category of IT security knowledge that we hereby refer to as the "*Bolts*."

(i) Access Control Systems and Methodology
(ii) Telecommunications and Network Security
(iii)Business Continuity Planning and Disaster Recovery Planning
(iv)Security Management Practices
(v) Security Architecture and Models
(vi)Law, Investigation, and Ethics
(vii) Application and Systems Development
(viii) Cryptography
(ix)Computer Operations Security
(x) Physical Security

Each domain represents a distinctive area of Cyber security practice. Within each are several field practice areas or sub domains. For example, **Identity management,** a sub domain of access control systems is a process that incorporates validation methods for individuals accessing the network to verify they are who they say they are, and then monitors what they do on the network; **Risk management,** a sub domain of security management practices mandates identification of network vulnerabilities and threats and determines appropriate countermeasures based on the sensitivity of data; **Incident management,** a sub domain of law, investigation and ethics frameworks executes responses when security events threaten the network. There are several other management, operational and technical components that form the concentric circles within the Information Assurance principle of defense in-depth.

The method for applying the "Bolts" and deploying each *mechanism* that we hereby refer to as the "*Nut*" depends in part on an organization's missions and requirements.

Herbert B. (2008) [6] captures the essence of the Defense in-Depth principle (see Figure 4) which depicts the basic elements of program domains areas that are central to Cyber security best practices.

[6]Herbert, B. (2008), "Security/Cyber Security," International Telecommunication Union Presentation GSC-13 ITU-T Study Group 17 Presentation GSC13-XXXX-nn. July 1, 2008.

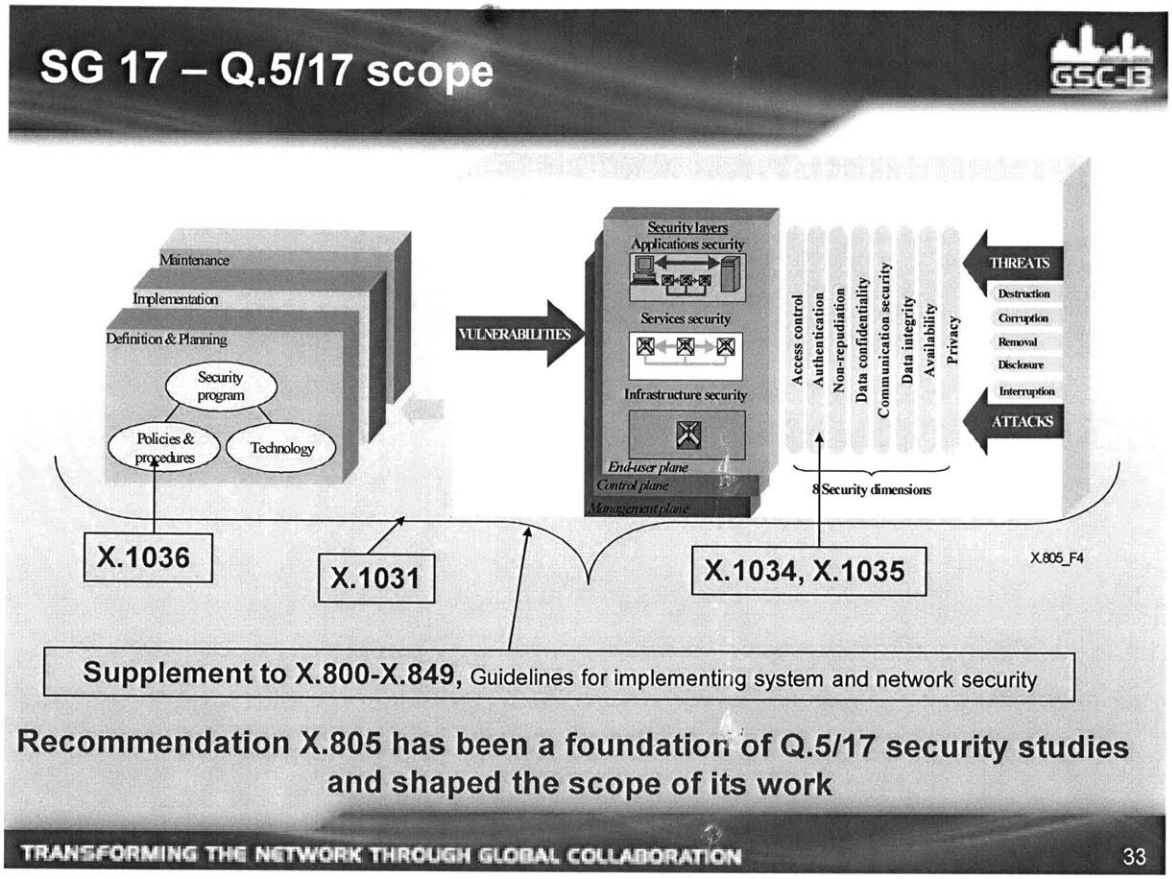

Figure 5: Guidelines for implementing system and network security from Herbert B. (2008).

In practical terms, Defense in Depth entails firmly enforced secure configurations (at installation time) for all applications, constantly verified patching and upgrading of both applications and system software, constant vulnerability scanning and rapid resolution of problems found, tightly configured firewalls and intrusion prevention systems, up-to-date anti-virus and anti-spyware at gateways as well as on desktops.

For example, on the aspect of access control, the Cyber security best practices pertaining to Defense in Depth typically would include **two-factor authentication**, which requires users to produce two credentials to access a system or application such as a fingerprint scan and a password or digital signatures, which verify the integrity and origin of a message. And, also include **encryption**, which translates data into a secret code so it is readable only by users who have the key to reassemble the message. These methods must be used in conjunction with customized information security policies and training. In essence, a holistic approach encapsulates the practice with different components being either "Bolts" or "Nuts."

Simply put, Defense in Depth is the layering of multiple defense techniques, mechanisms and devices to protect critical network assets, data, systems and users. These defenses are layered for two primary reasons: First, as one layer, device or mechanism ("Nut") fails, another will be there to mitigate, or at least track and notify the administrator, about the breach. Second, as detailed

above, attacks can come from a multitude of sources and can attack multiple methods of access. One defense mechanism will not address every potential path into the business. Therefore, the layered architecture provides somewhat of a solid defense.

Given in Figure 6 is a schematic of the layered structure for implementation of defensive mechanisms (Nuts – Access Control Servers, Firewalls, Routers with ACLs, VPN Servers, etc.) encapsulating a holistic approach in implementing security to protect data/information.

Defense in Depth emphasizes the triad that is prevention, detection and reaction/response and is a commonly used approach in IT security to address these principles. Thus, the underpinning and underlying assumption is that no single mechanism offers adequate protection. Defense in Depth utilizes multiple "layers" to protect an organization's critical assets. In other words, an attack that is not stopped by an outer layer will be stopped by an inner layer. And as such, any exploit will have to break through multiple defense layers for it to be successful.

Although, having a Defense in Depth architecture does not assure an organization that it won't be attacked, but it does make it as difficult as possible for the attacks that inevitably will occur to succeed. As attacks get more numerous and more complex, organizations need to develop more complex defense strategies.

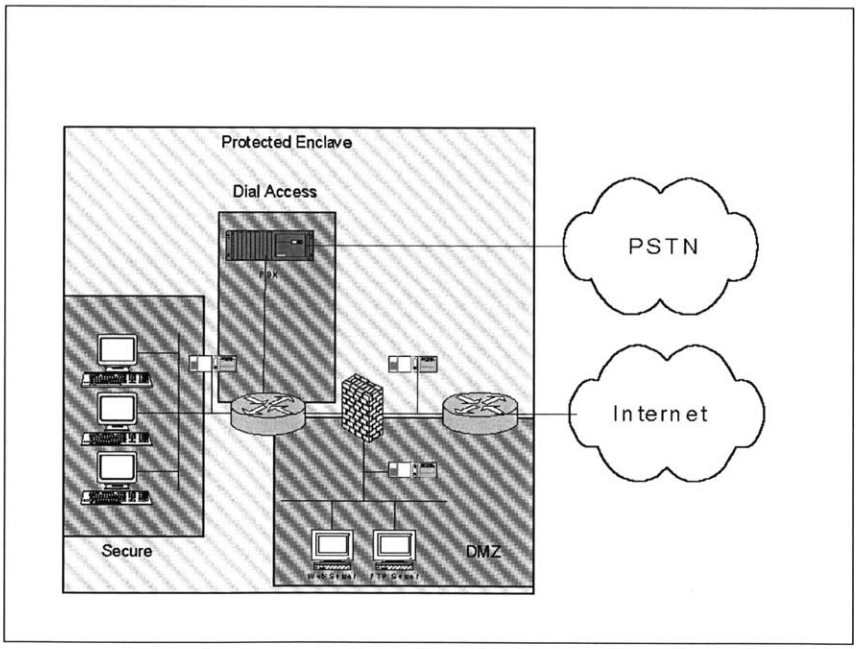

Figure 6: Sample Security Architecture Emphasizing the Defense-in-Depth Concept from Stallings W. (2000).

In Figure 6[7], a common router and firewall configuration known as the screened subnet is shown. In this case, the screened subnet has two packet-filtering routers and a firewall. This configuration creates an isolated subnetwork, which makes the internal network invisible to the Internet and the inside router advertises only the existence of the screened subnet to the internal

[7] Stallings, W. (2000) "Network Security Essentials," Applications and Standards,' P322-330 Prentice Hall, 2000.

network. Thus, two layers of defense between the outside and the DMZ and three layers between the outside and the internal secure network are created.

In essence, the concept of Defense-in-Depth in a way encapsulates the requirements that must be addressed when building a Cyber security architecture. It reflects the totality of enterprise assets that must be protected and brings into view the concentric and interdependent nature of security knowledge domain, processes, devices and the technologies that must be deployed to protect the enterprise from Cyber attacks. Invariably, Defense-in-Depth integrates the "Bolts" with the "Nuts" to implement Cyber security best practices.

Figure 7 serves to illustrate the "Bolts" and "Nuts" of Cyber security in an enterprise.

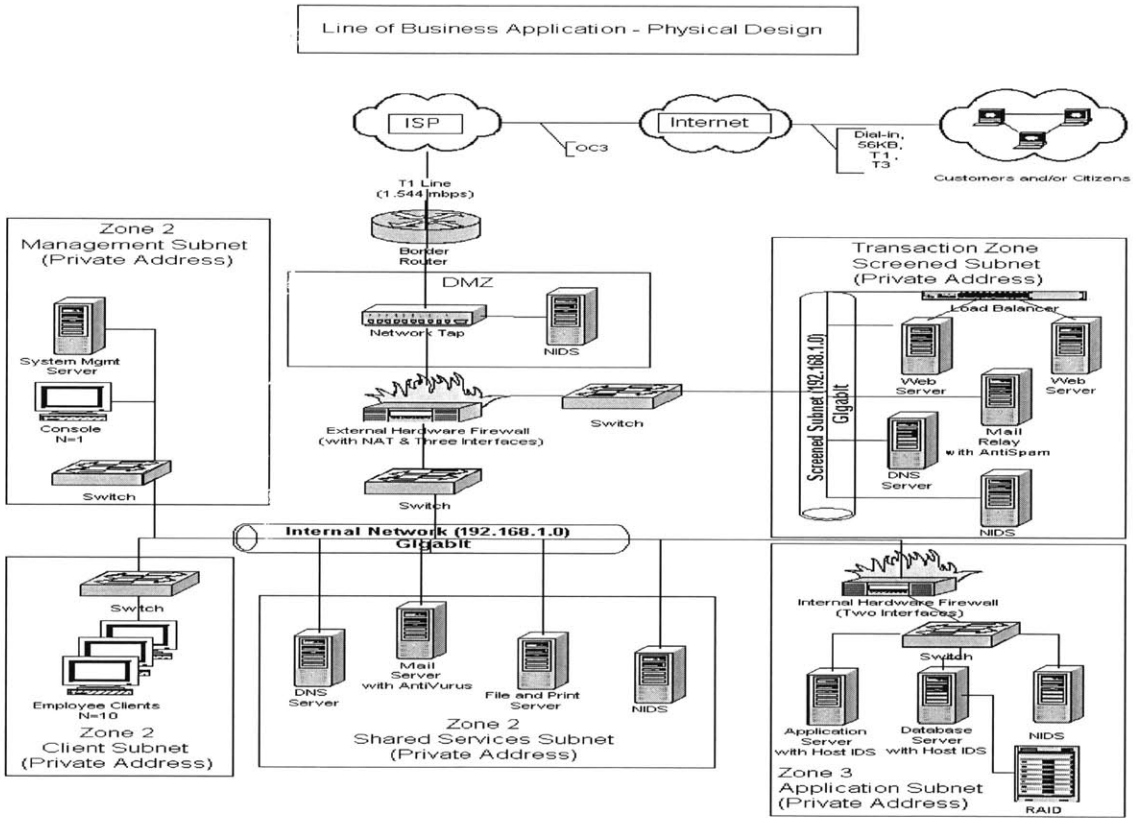

Figure 7: Enterprise Internet System Security Architecture from Stallings W. (2000).

In Figure 7, the "Nuts" are the basic technological devices and mechanisms such as firewalls, Intrusion Detection and Prevention Systems, Encryption technologies and other such technologies and devices which provide protection at the external, intermediate (DMZ) and internal protected network cycles.

Prominent in the list of devices used to implement Cyber defenses are:

- Routers with Access Control Lists
- Firewalls
- Intrusion Detection Systems

- Intrusion Prevention Systems
- Encryption Devices (Virtual Private Network)
- Authentication and Access Control Servers
- Cryptographic Mechanisms
- Digital Certificate Devices
- Etc.

2.6 The Current State of Cyber Security Practice in the Enterprise

The current state of Cyber security practice is generally considered matured and advanced from where it was five years ago. This has been made possible by advances in newly developed security technologies. For example, intrusion detection systems that were the industry norm for well over eight (8) years have been refined to include new features that when in operation makes it possible to detect intrusion essentially giving birth to a new device popularly known as intrusion prevention system.

By all accounts, the current state is a reflection of the industry "Best Practices" (BPs) which are constrained and by and large are a reflection of what can be implemented, and not by theoretical or hypothetical potential solutions. While BPs have attained a uniform industry standard with marketplace acceptance of such Standards as NIST, ISO, etc. there are still subtle differences and nuances in implementation from organization to organization.

In general, Hancock B. (2003)[8] asserts "BPs, as delivered, are best implemented under the following general driving principles:

1. **Defense-in-Depth (layered defense).** Singular, point-based security solutions can be breached or circumvented. Proper cyber security means that multiple layers of defense need to be implemented to safeguard assets. In this manner, if a particular layer is breached or circumvented, the next security layer will catch the breach and provide adequate security to protect the asset or will delay asset compromise until security teams can properly address the problem presented by the breach or bypass. An example might be to disable TELNET (virtual terminal) access through a router to a web site (this can be done through the implementation of Access Control Lists (ACLs) or packet port filters in an IP-based router). Additionally, proper security would include a firewall in front of the web site where TELNET would similarly be disabled and also have an operator notification alarm implemented in case of attempted access. If, later the network management team or security team were presented with a TELNET attempted access alarm from the firewall, they would quickly deduce that the router was somehow either breached or bypassed and an attacker attempted to go through the firewall which, as a layered defense mechanism, denied access to the assets. This allows for continual protection of the assets on the network and a rapid response to security events when they

[8] Hancock, B. (2003) "Summary Report and Proposals from Cyber Security Best Practices", Focus Group of Network Reliability and Interoperability Council, Homeland Defense, March 14, 2003 V1.3

occur. Furthermore, layered defenses can be implemented with existing infrastructure components and do not always require multiple, specialized security technology layers.

2. **Minimization of exposure.** A great many breaches happen because technologies that are not needed are left connected or remain otherwise accessible to external attackers. Minimization of exposure (capability minimization) is a widely known security concept where items that are not needed are disabled and technologies that are not required are removed. Another popular statement for this type of concept of least privilege, "deny all except what which is needed" from accessing network infrastructure. Exposure is minimized by "turning off" technologies, applications, etc., which is not needed to fulfill the company's mission or deliverables. For instance, sites with Internet connectivity would disable all access "ports" (applications) which are not used so that those "ports" could not be used by attackers to gain access to the infrastructure. Companies who fared well in the January 25, 2003, "Slammer" worm attack did so because they denied access to UDP ports 1433 and 1434 as part of their implementation best practices in network router, firewall and switch configurations. When the worm hit the infrastructure, it could not propagate through these ports because the principle of least privilege was in effect, effectively stopping the worm in its tracks. By disabling technology access where it is not needed, many access opportunities into the infrastructure are effectively disabled, in turn reducing opportunity for further attacks.

3. **Partitioning and isolation**. If complete access to all devices on a network is available to virtually any entity, the whole network can be disabled if the infrastructure is attacked in even simplistic ways. Traditional belief of only securing endpoints and the application has been proven by recent experiences not to work. Isolating critical components and partitioning the network infrastructure into smaller, protected areas, the opportunity to critically affect an entire network is dramatically reduced and network reliability is increased. This also helps isolate Cyber attacks in progress (by restricting Cyber attacks to known, bounded network locations that can be protected effectively while the Cyber attack on another section of the infrastructure is being dealt with.) An example might be to isolate network management out-of-band networks from general production or general access networks and further restrict access to the out-of-band network. In this manner, if one of the production networks is attacked, the out-of-band management network allows critical access to network technologies and the opportunity to assist in the management and eradication of the Cyber attack. Also, by establishing partitioning "zones" in the infrastructure, they can be disconnected from sections being attacked and continue to operate while an attack is in progress.

4. **Keep It Simple, Stupid (KISS).** This tried and true concept applies well to technologies where the complexity makes it vulnerable to attack(s). In cases where security is needed, application of less complexity is always preferred. As an example, blocking an application port on a router is a simple operation and much easier to do than installation of complex stateful filtering software on a server.

5. **Information Technology Hygiene.** Many breaches of network infrastructures are due to lack of good, basic Information Technology (IT) security concepts and products. For instance, network managers place a great deal of sensitive and critical information on their access systems (typically a laptop or notebook computer) with no external network controls (firewall), no strong authentication (e.g. token cards), encryption of on-system sensitive data, etc. Other examples include critical servers not being backed up, unnecessary services being made available, falling behind on patch management, inadequate risk assessment and classification of data, open file servers, database servers and email systems that are easily compromised and contain extensive information about the company, its infrastructure and its customers. Enforcement of proper IT security has a profound effect on overall security of network infrastructures.

6. **Avoid security by obscurity.** A common and grossly inadequate belief is that lack of general visage of a component is a security feature (if you can't see it, you won't try to attack it). BPs stress actions to protect infrastructures, not inactions or obscurity as a defensive tool. For instance, network address translation (NAT) technology is often promoted by some vendors as a security method with the principle being that a single external IP address "hides" internal private IP addresses via a translation system. It has been proven, painfully, time and time again that NAT is a fine technology to extend addressing ranges of networks to include unregistered and private address ranges to interoperate with registered IP address ranges. At the same time, NAT is often breached or bypassed by attackers to reach internal systems on a network and breach same. Security via obscurity is a bad idea at all times and is not included, encouraged or recommended as a technique for securing infrastructure.

In the end, due to the nature of Cyber threats and attacks, BPs are never implemented the same way across organizations, are never intended for mandatory regulatory efforts, as not all are appropriate for all services or architectural implementations.

2.7 Summary

In this Chapter, we have reviewed and provided background information related to the Internet as a medium of conducting online transactions. Following this review, we conclude that this medium otherwise known as Cyberspace is not sufficiently secure as several security breaches occur over it leading to several unintended consequences including unauthorized disclosure of proprietary and personal data/information, shutting down of businesses, data theft, financial loss, etc.

Also, we note that an information security practice also known as Cyber security has evolved over the years to address security issues in Cyberspace, and as is practiced today represents different standards and norms each of which is interpreted and implemented to the extent permissible by organizational resources and constraints. We conclude that although still inadequate to stem the tide, significant progress has been made and is evident in the current state of Cyber security practice.

Chapter 3: The Internet Design Security Flaws

The Internet architecture represents several software, hardware/infrastructure and link sub-systems that all fuse together to make a single whole. The current design grew out of the DOD DARPA project that was initially intended for lightweight use for a few connected networks. But today, it has grown to a collection of several millions of networks and connected systems by far exceeding its growth projection. This growth taps into and has been fostered by the robustness of the Internet design which has made it possible for new applications, processes and technologies to be deployed. Incidentally, most of these technologies are developed without security in mind and have thus given rise to all sorts of Cyberspace security problems.

In this Chapter, we present an overview of the Internet architecture and design, with a particular emphasis on the TCP/IP protocol stack that serves as the transport and communication mechanism of the system. We provide a description and analysis the flaws and weaknesses inherent in the current Internet system architecture and then provide details of well-known threat agents that have exploited the weaknesses to launch Cyber attacks. The facts established in this Chapter provide the basis for the discussions in Chapter 4.

3.1: Overview of Internet Design

The origin and evolution of the Internet, its current architecture and design has been extensively covered in documented literature available online and elsewhere. The Internet design can be described from two perspectives:

1. Hardware
2. Autonomous Systems

When viewed in terms of hardware, the Internet consists of hosts or endpoints (also called end systems), routers or internal switching stations (also referred to as gateways), and links that connect the various hosts and/or routers and can differ widely in speed (from slow modem connection to high-speed backbone links) as well as in technology (e.g., wired, wireless, satellite communication).

When viewed from the perspective of autonomous systems (ASs), where an AS is a collection of routers and links under a single administrative domain, the network is an internetwork consisting of a number of separate subnetworks or Ass (Figure 8), interlinked to give users the illusion of a single, seamlessly connected network (network of networks, or "internet").

In other words, the infrastructure of the Internet consists of a federation of connected networks that are each independently managed ("**autonomous system**"). Each "autonomous system may consist of multiple IP networks, and have a number (**AS number**). The autonomous systems represent a hierarchy of network service providers (NSPs):

- **Tier-1**: nation or worldwide network (US: less than 20)
- **Tier-2:** regional networks (in US: less than 100)
- **Tier-3:** local Internet service provider (in US: several thousand)

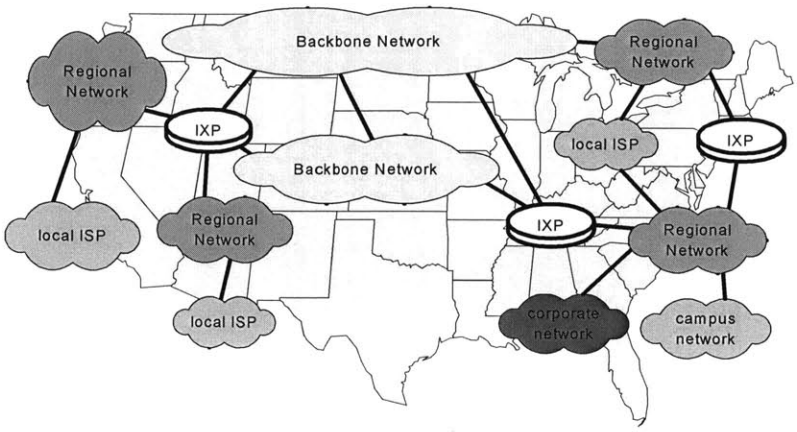

Figure 8: Internet Infrastructure.[9]

Historically, today's Internet system evolved from the architectural network design that was developed in the 1970s under the auspices of the Defense Advanced Research Project Agency (DARPA) of the US Department of Defense. Clark D. (1988)[10] of Massachusetts Institute of Technology has elaborated on the early reasoning behind the design philosophy that shaped the Internet protocol architecture (i.e., the "Internet architecture" as it became known).

In general, the Internet architecture is a reflection of how it is designed to work and includes both a technical design and a management structure.

The technical design is a complex meshing and interlocking set of hierarchical tree-like structures, like Internet Protocol addresses and domain names, mixed with networked structures like packet switching and routing protocols, all tied together with millions of lines of sophisticated software that continues to get better all the time.

The management structure consists of a generally democratic collection of loosely-coupled organizations and working groups with mostly non-overlapping responsibilities.

In essence, the Internet design is a combination of management and technical structures that must work well together to provide a reliable, powerful communication platform upon which the rest of the complex Internet system is built.

---

[9] The Internet lecture notes published at: www.cs.virginia.edu/~cs458/slides/**module04-internetV2.ppt**. Last checked September, 2010.

[10] D. D. Clark, (1988). "The design philosophy of the DARPA Internet protocols," Proceedings of the ACM SIGCOMM'88, in: ACM Computer Communication Reviews, Vol. 18, No. 4, pp. 106{114}, 1988.

So, what is the *Internet* architecture? Carpenter B. (1996) [11] in his paper titled: "*Architectural Principles of the Internet" notes:*

"Fortunately, nobody owns the Internet, there is no centralized control, and nobody can turn it off. Its evolution depends on rough consensus about technical proposals, and on running code. Engineering feed-back from real implementations is more important than any architectural principles."

Further, Carpenter notes that the lack of ownership of the Internet that has resulted into the collaborative architectural design by different stakeholders that now define the Internet.

The IAB (Internet Architecture Board) - the Internet Society is the overseer of the technical evolution of the Internet that supervises the Internet Engineering Task Force (IETF) that is tasked with overseeing the evolution of TCP/IP, and the Internet Research Task Force (IRTF) which works on network technology. The IAB defines the Internet Architecture as "a meta-network, a constantly changing collection of thousands of individual networks intercommunicating with a common protocol."

Going by the above definition, several graphicalization of the Internet architecture abound. A more vivid description and visualization has been given by Haynal, R. (2010).[12]

Haynal portrays the Internet architecture as an assembly that consists of several Sections:

- User PC - Multi-Media PCs equipped to send and receive all variety of audio and video
- User Communication Equipment - Connects the Users' PC(s) to the "Local Loop"
- Local Loop Carrier - Connects the User location to the ISP's Point of Presence
- ISP's POP - Connections from the user are accepted and authenticated here.
- User Services - Used by the User for access (DNS, EMAIL, etc).
- ISP Backbone - Interconnects the ISP's POPs, AND interconnects the ISP to Other ISP's and online content.
- Online Content - These are the host sites that the user interacts with.
- Origins Of Online Content - This is the original "real-world" sources for the online information.

Each of the Sections provided elaboration of the different components. For example, the User PC Section listed the architectural components as follows:

User PC - A Multi-Media PC equipped to send and receive all variety of audio and video.

1. Sound Board /Microphone/Speakers for telephony, MIDI, Creative Labs/SoundBlaster, Yahoo's List for Sound Cards.
2. Video/Graphics for 3D graphics, video, playback. Matrox, Diamond Multimedia, Yahoo's List for Video Cards.

---

[11] RFC 1958; B. Carpenter; Architectural Principles of the Internet; June, 1996.
[12] Haynal, R (2010), "Internet: The Big Picture: What are the major pieces of the Internet, and who are the major players in each segment." http://navigators.com/internet_architecture.html. Last checked in October, 2010.

3. Video camera - Connectix Yahoo's List for Video Conferencing, Yahoo's List for Manufacturers.
4. Voice recognition - Yahoo's List for Voice Recognition.

And, visualizes the user PC in Figure 9.

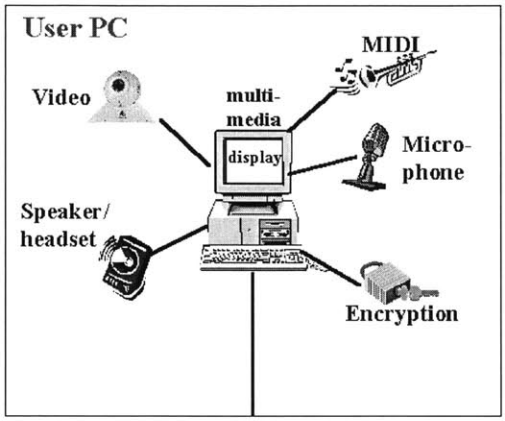

Figure 9: Sample Internet Sub-sectional Architecture from Haynal R. (2010).

Another description takes a cue from the coinage of the word Internet which is a short from of the compound word "inter-networking," and the architecture is based on the very specification of the standard TCP/IP protocol, designed to connect any two networks which may be very different in internal hardware, software, and technical design. Once two networks are interconnected, communication with TCP/IP is enabled end-to-end, so that any node on the Internet has the near magical ability to communicate with any other no matter where they are. It is this very structure that has made Internet architects assert that this openness of design has enabled the Internet architecture to grow to a global scale.

Topologically, the Internet technical architecture looks like a multi-dimensional river system, with small tributaries [Figure 10] feeding medium-sized streams feeding large rivers. For example, an individual's access to the Internet is often from home over a modem to a local Internet service provider who connects to a regional network connected to a national network. At the office, a desktop computer might be connected to a local area network with a company connection to a corporate Intranet connected to several national Internet service providers. In general, small local Internet service providers connect to medium-sized regional networks which connect to large national networks, which then connect to very large bandwidth networks on the Internet backbone. Most Internet service providers have several redundant network cross-connections (Figure 8) to other providers in order to ensure continuous availability.

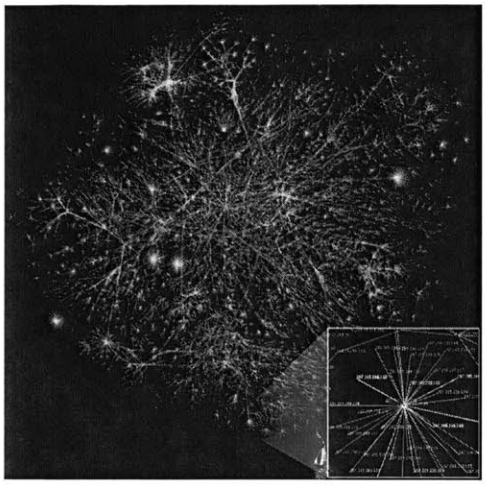

Figure 10: Tributary visualization of the various routes through a portion of the Internet.[13]

3.1.1: The Transport Control Protocol /Internet Protocol

The architecture of the TCP/IP protocol stack, the main stack of protocols used in the Internet is very-well described in several technical literatures. The five-layer TCP/IP protocol suite consists (from the bottom up) of the physical, link, internetwork, transport, and application layers.[14]

The physical layer concerns the physical aspects of data transmission on a particular link, such as characteristics of the transmission medium, the nature of the signal, and data rates. Above the physical layer is the link layer. Its mechanisms and protocols (e.g., signaling rules, frame formats, media-access control) control how packets are sent over the raw media of individual links.

Above it is the internetwork layer, responsible for getting a packet through an internet; that is, a series of networks with potentially very different bit-carrying infrastructures and possibly belonging to different administrative domains. The Internet Protocol (IP) is the internetworking protocol for TCP/IP, and its main task is to adequately implement all the mechanisms necessary to knit together divergent networking technologies and administrative domains into a single virtual network (an "Internet") so as to enable data communication between sending and receiving hosts, irrespective of where in the network they are.

The layer above IP is the transport layer, where the most commonly used Transmission Control Protocol (TCP) deals, among other issues, with end-to-end congestion control and assures that arbitrarily large streams of data are reliably delivered and arrive at their destination in the order sent.

---

[13] http://www.opte.org/maps/. Last checked on November 25, 2010.

[14] Stallings, W. (2006), Data and Computer Communications, Prentice Hall 2006, ISBN 0-13-243310-9

Finally, the top layer in the TCP/IP protocol suite is the application layer, which contains a range of protocols that directly serve the user; e.g., telnet (for remote login), ftp (the File Transfer Protocol for transferring files, smtp (Simple Mail Transfer Protocol for e-mail), http (the HyperText Transfer Protocol for the World Wide Web).

The essence of layering and stratification of functions of the stack is aimed at simplifying, satisfying the various demands and driving efficiency of the process. Willinger W. et. al (2002)[15] explains this as follows: "this layered modularity gave rise to the "hourglass" metaphor for the Internet architecture the creation of a multi-layer suite of protocols, with a generic packet (datagram) delivery mechanism as a separate layer at the hourglass' waist. This abstract bit-level network service at the hourglass' waist is provided by IP and ensures the critical separation between an ever more versatile physical network infrastructure below the waist and an ever-increasing user demand for higher-level services and applications above the waist."

Because several devices are used to realize the processed, all Internet infrastructure providers conform to agreed upon standards to ensure consistency of the IP. The standards consist of an agreed-upon set of features that has to be implemented according to an Internet-wide standard, and must be supported by all the routers in the network. This becomes the key to enabling communication (Figure 11) across the global Internet so that networking boundaries and infrastructures remain transparent to the users.

As a result of user and operational requirements, the roles assigned to each layer in the strata define their robust functionality of the designs to varying degrees. Willinger et al. (2002) asserts: " The layers below the waist (i.e., physical, and link) deal with the wide variety of existing transmission and link technologies and provide the protocols for running IP over whatever bit-carrying network infrastructure is in place ("IP over everything"). Aiming for a somewhat narrow waist reduces for, or even removes from the typical user the need to know about the details of and differences between these technologies (e.g., Ethernet local area networks (LAN), asynchronous transfer mode (ATM), and frame relay) and administrative domains. Above the waist is where enhancements to IP (e.g., TCP) are provided that simplify the process of writing applications through which users actually interact with the Internet ("everything over IP"). In this case, providing for a thin waist of the hourglass removes from the network providers the need to constantly change their infrastructures in response to a steady flow of innovations happening at the upper layers within the networking hierarchy (e.g., the emergence of "killer apps" such as e-mail, the Web, or Napster). The fact that this hourglass design predated some of the most popular communication technologies, services, and applications in use today and that within today's Internet, both new and old technologies and services can coexist and evolve attests to the vision of the early architects of the Internet when deciding in favor of the layering principle. "IP over everything and everything over IP" results not only in enormous robustness to changes below and above the hourglass' waist but also provides the flexibility needed for constant innovation and entrepreneurial spirit at the physical substrate of the network as well as at the application layer."

---

[15] Willinger, W and Doyle, J (2002), "Robustness and the Internet: Design and Evolution," AT&T Labs-Research, Florham Park, NJ, USA, March 1, 2002

Table 3: The TCP/IP Protocol Stack.[16]

Protocol Layer	Comments
Application Protocols Layer	Protocols specific to applications such as WWW, e-mail, FTP, etc.
Host to Host or Transport Layer	TCP directs packets to a specific application on a computer using a port number.
Internet Layer	IP directs packets to a specific computer using an IP address.
Network Access Layer	The network access layer is concerned with the exchange of data between a data transmission device (workstation, computer) and a transmission medium or network.
Physical Layer	Converts binary packet data to network signals and back. (E.g. Ethernet network card, modem for phone lines, etc.)

In Figure 11, two Internet hosts connected via two routers and the corresponding layers used at each hop.

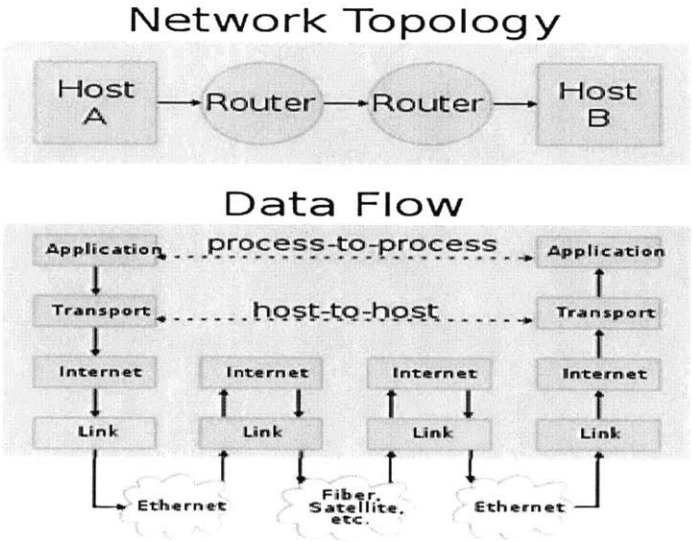

Figure 11: Communication Flow in another version (RFC 1122, Internet STD 3 (1989) four layer) of the TCP/IP Protocol Suite.[17]

---

[16] Tanenbaum, A. (2002), Computer Networks, Prentice Hall 2002, ISBN 0-13-066102-3

[17] Internet Engineering Task Force, RFC 1122. http://tools.ietf.org/html/rfc1122. Last Checked January 7, 2011.

3.2: The Design Flaws

In order to understand the security problems associated with TCP/IP, we summarize in the following Sections some of the known security flaws of the Internet communication protocols:

(i) TCP/IP protocol suite for the well-known vulnerabilities of both TCP/IP itself, and
(ii) Some protocols commonly used along with TCP/IP such as DNS, and
(iii)The Internet routing and messaging protocols such as the RIP.

3.2.1: The Communication Protocols (TCP/IP) Flaws

The TCP/IP protocols are the main transport and communication mechanisms used to transact business on the Internet. As the backbone of the internet, it is comprised of two protocols, TCP and IP. The design details are given for IP in [RFC 791], and for TCP in [RFC 793]. In their original design, they lack the most basic mechanisms for security, such as authentication or encryption. As usage of the Internet and TCP/IP protocols increase, their lack of in-built security becomes more and more problematic.

The evolution and growth of these protocols follows the evolution and growth of the Internet. Between 1980 and 1985, specifications were completed for the TCP and IP protocols. Then, the specifications were made for small network sizes which reflected the original intent of the role of the Internet i.e. interconnection of small research networks. But, over the past decades, the Internet has grown from a small network connecting a small community of researchers to its present state - a gigantic global network connecting people of all types. As such, it may be said that it evolved from a specialized project to a general-purpose tool.

At the same time, the growth of the Internet has created enormous security problems with wide ranging implications. One of the causes being that the TCP and IP protocols were designed when the Internet was small, and users generally trusted each other and as there were not the need for many features that are desirable or needed on an insecure network in today's big and extended interconnections.

A good description of the TCP/IP flaws, their manifestations and types are given in Appendix 1.[18]

[18] Chris Chambers, Justin Dolske, and Jayaraman Iyer: "TCP/IP Security," Department of Computer and Information Science, Ohio State University, Columbus, Ohio 43210 Available at: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html. Last checked January, 2011.

3.2.2. The Domain Name System Flaw

The Domain Name Service ("DNS") (Figure 12) is an indispensable protocol widely used on the Internet to map hostnames (i.e. "foo.bar.com") to IP addresses (i.e. 192.34.12.7), and also to execute the reverse mapping of IP addresses to hostnames. An attacker can use the latter property to fool name-based authentication[19].

For example, Bellovin S. (1989) asserts: "an administrator at alice.bar.com may decide to allow only local connections. This is often specified by name, such as "allow *.bar.com," rather than by IP address. Name-based authentication is easier to read, and allows easier administration if a domain contains multiple ranges of IP addresses. When a connection is established with alice.bar.com, alice uses DNS to convert the source IP address on the connection to a name, which is then checked using whatever form of name-based authentication the administrators have installed. If an attacker has access to their local DNS server, they can cause DNS queries on their IP address to reply with any hostname and domain! So, an attacker who knows that alice.bar.com trusts connections from within *.bar.com can alter his DNS server so that his IP address appeared to map to "trustme.bar.com"."

Also, other fundamental flaws such as cache poisoning exist in the DNS protocol with far reaching implications. In the cache poisoning attacks, data is introduced into a DNS name server's cache (djbdns, PowerDNS, MaraDNS, and Unbound) database that did not originate from authoritative DNS sources. Equally, for Internet-based applications that rely on the DNS Server(s) to locate their peers, a wide range of attacks such as web site impersonation, email interception, and authentication bypass are inherently possible. A more accurate description of these has been given elsewhere by Bellovin S. (1989) and others.

[19] Bellovin, S. (1989), "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Volume 19, Number 2, pp. 32-48, April 1989.

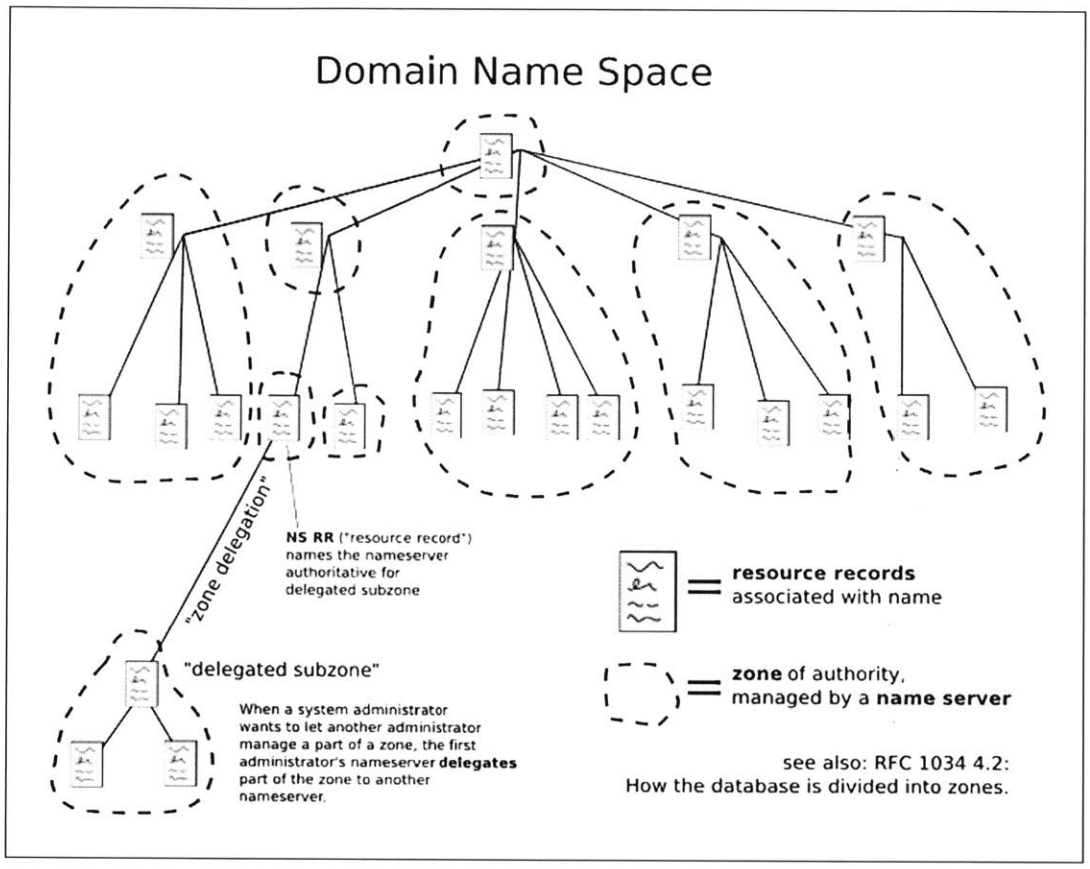

Figure 12: DNS Structure.[20]

The lack of unique identifiers

During the incubation period (1980's) of the Internet, an IP address is used to safely identify and locate a host. Addresses were both spatially unique (no one else had an identical address) and temporally unique (addresses didn't change). However, this is no longer the case [RFC2101]. Today, IP addresses may exhibit seemly strange behavior that makes identifying and locating hosts much harder. The widespread use of protocols such as PPP/SLIP [RFC1990] and DHCP [RFC1541] allow a specific host's address to change over time: per-connection in the case of PPP/SLIP, while DHCP allows hosts to "lease" IP addresses for arbitrary lengths of time. On even larger time scales, details in the current Internet routing structure (i.e., Classless InterDomain Routing, "CIDR" [RFC1519]) may require that if a domain changes service providers, they will have to change their assigned range of IP addresses. Firewalls, proxy socket servers, and other "Network Address Translators" further complicate the use of IP addresses as identifiers, because they may translate addresses as traffic moves between the internal and external networks. Different hosts may appear to be using identical IP addresses, or different IP addresses may be the same host.

[20] http://en.wikipedia.org/wiki/Domain_Name_System. Last checked January 31, 2011.

Thus, IP addresses can no longer be used to uniquely identify a host, even over short time periods. And on that account, any security schemes which rely upon IP addresses remaining temporally or spatially unique may have vulnerabilities.

3.2.3. Internet Routing and Messaging Protocol Flaws

Two major types of attacks are common in Internet Infrastructures: Routing Information Protocol ("RIP") and Internet Control Message Protocol ("ICMP"). Bellovin S. (1989) has described these as follows:

1. ***Routing (RIP)***

In a narrow context, Routing Information Protocol ("RIP") attacks are part of the extended security problem associated with the Internet infrastructure. Even though, it is not strictly a component of TCP/IP, the RIP is often an essential component in a TCP/IP network [RFC1058]. RIP is used to distribute routing information within networks, such as shortest-paths, and advertising routes out from the local network.

Similar to the TCP/IP, it has no built in authentication, and the information provided in a RIP packet is often used without verifying it. Attacks on RIP Bellovin S. (1989) are different from those of other common attacks because RIP attacks change where data goes to, not where it came from. For example, an attacker could forge a RIP packet, claiming his host "X" has the fastest path out of the network. All packets sent out from that network would then be routed through X, where they could be modified or examined. An attacker could also use RIP to effectively impersonate any host, by causing all traffic sent to that host to be sent to the attacker's machine instead.

2. ***ICMP***

The Internet Control Message Protocol ("ICMP") is one of the most indispensable messaging protocols used by the IP layer to send one-way informational messages to a host. Its utility value lies in one of the most common (and well-known) diagnostics uses of ICMP is the "ping" utility. This utility sends an ICMP "Echo Request" to a host, and waits for that host to send back an ICMP "Echo Reply" message. Other messages in ICMP are of similar complexity; that is, they are all quite simple. It's not surprising that there is no authentication in ICMP, which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets.

The devastating "Denial of Service" attacks primarily use either the ICMP "Time exceeded" or "Destination unreachable" messages. The "Time exceeded" message indicates that the Time-To-Live field in the IP header has expired; this can normally be caused by routing loops or trying to reach a host that is extremely distant. "Destination unreachable" messages can have several meanings (based on a sub-field in the ICMP message), but all basically indicate that packets cannot successfully be sent to the desired host. Both of these ICMP messages can cause a host to immediately drop a connection (this is the desired result if the ICMP message is legitimate). An

attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating hosts. Their connection will then be broken.

Also, ICMP messages can also be used to intercept packets. For example, the ICMP "Redirect" message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network (and is thus attempting to send the packet via the gateway to). Similar to the RIP, an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host. The only distinction between the RIP and ICMP is that the ICMP messages only apply to existing connections, and the attacker (the host receiving redirected packets) must be on a local network.

3.2.4. The Lack of Authentication Mechanism: *Fundamental Design Security Architecture Flaw*

Good Architecting is one of the principles of architecture and is an embodiment of an ideal system. Arguably, it is also the most important principle that guides system design. Several other principles such as the principle of **Scalability espouses** that a good architecture must be scalable enough to accommodate both design and business needs; and **Flexibility espouses** that System architecture must be flexible enough to be redesigned and improved all play significant role when the Internet architecture is viewed or analyzed from a holistic perspective. The Internet architecture embodies all of these.

However, several loopholes have been found in the architecture relating to the frequent break-ins to distort or alter communication and wreck havocs on connected users and systems. At the root of this is the lack of an authentication mechanism that could forestall such break-ins.

On this, one of the Internet's "elder statesmen," MIT's David D. Clark[21] argues that the Internet has become a vast patchwork of firewalls, antispam programs, and software add-ons, with no overall security plan.

As an after-thought, the statement by Clark is a reflection of today's Internet architecture that lacks the basic security authentication platform.

As a consequence, Clark notes: "The Net's basic flaws cost firms billions, impede innovation, and threaten national security. It's time for a clean-slate approach."

The underpinning here is that there are far reaching implications drivable for the current Internet architecture and that the Internet's shortcomings have resulted in plunging security and a decreased ability to accommodate new technologies. "We are at an inflection point, a revolution point," Clark now argues (from Talbot, 2005). And he delivers a strikingly pessimistic assessment of where the Internet will end up without dramatic intervention. "We might just be at the point where the utility of the Internet stalls -- and perhaps turns downward."

---

21 Talbot, D. (2005), "The Internet Is Broken," December 19, 2005. http://www.technologyreview.com

The basic issue here is the Internet architecture lacked the mechanism to enforce security to adaptable new technologies that are integrated into it. For example, the TCP/IP; DNS and all other Internet communications protocols, sub-systems or applications have any mechanism to authentication even with the proliferation of Internet applications over the years (wireless devices, peer-to-peer file-sharing, telephony) companies and network engineers came up with ingenious and expedient patches, plugs, and workarounds.

As a consequence, there is an astronomical growth in the number of security incidents relating to Cyber attacks (viruses, spam, phishing, etc,) and there is no permanent effective defense leaving engineers with the arduous tasks of endlessly implementing ad-hoc solutions for protection with firewalls and antispam software as add-ons and security patches.

3.2.5. Summary

In this Chapter, we have described the weaknesses inherent in the architecture and design of the TCP/IP protocol suite; and have analyzed documented evidence on the vulnerabilities which are exploited by the threat agents given Table 2 to launch Cyber attacks.

The Domain Name System is discussed in the context of its architecture and weaknesses that also serves as another conduit pipe for certain types of Cyber attacks.

We also establish the following:

1. ***Robustness:*** The Internet design manifests a robust architecture that is elastic enough to integrate new processes, applications and technologies.
2. ***Efficiency:*** The layered architecture is intended to provide efficiency through roles assignment.
3. ***Platform Independence and IP Layer:*** The Internet Protocol (IP) is the internetworking protocol for TCP/IP, and its main task is to adequately implement all the mechanisms necessary to knit together divergent networking technologies and administrative domains into a single virtual network (an "internet") so as to enable data communication between sending and receiving hosts, irrespective of where in the network they are.
4. ***TCP Layer:*** The layer above IP is the transport (TC) layer, where the most commonly used Transmission Control Protocol (TCP) deals, among other issues, with end-to-end congestion control and assures that arbitrarily large streams of data are reliably delivered and arrive at their destination in the order sent.
5. ***Application Layer:*** Also, the top layer in the TCP/IP protocol suite is the application layer, which contains a range of protocols that directly serve the user; e.g., telnet (for remote login), ftp (the File Transfer Protocol for transferring files, smtp (Simple Mail Transfer Protocol for e-mail), http (the HyperText Transfer Protocol for the World Wide Web).

Chapter 4: Analysis of Internet Vulnerabilities and Cyber Attacks

The increasing use of Cyberspace to engage in all sorts of human endeavor including eBusiness, online education, etc. provides abundant opportunities for both the good and bad guys to engage in any desired activities. Sometimes, the activities are essentially Cyber attacks by the bad guys on vulnerable systems using all available means and technologies to exploit the weaknesses discussed in Chapter 3.

With each passing year, these attacks have progressively increased in number, scope and nature giving rise to new lines of Cyber security businesses and practices including reconnaissance and monitoring set up by several Internet security organizations to monitor internet traffic across the globe and provide daily or periodic listing of top vulnerabilities and attacks.

In this Chapter, we will analyze Internet traffic monitoring reports from several organizations and published statistical studies on Cyber attacks; and then develop a grid that maps each attack type to specific internet layer.

4.1 Internet Vulnerabilities

The number, types and nature of Internet vulnerabilities are not and cannot be completely known or predicted due to the nature of several complex elements at play such as complex network environments, poorly understood Cyber space architecture, etc. The lack of the ability to predict vulnerabilities is precisely the reason there are "Zero-day" attacks. Zero-day attacks are previously unknown attacks with no immediate defense.

Different Internet security monitoring organizations provide daily or periodic listing of top vulnerabilities. The list change frequently as new vulnerabilities are discovered all the time from almost all major software and hardware vendors providing the software, hardware or links that powers the Internet.

One of the best sources featuring a comprehensive listing of Internet vulnerabilities is Mitre corporation's "Common Vulnerabilities and Exposures" listing available at http://cve.mitre.org. The organization maintains lists pulled from different sources and has always been the most authoritative source of virtually any known and documented vulnerabilities. Other organizations within the commercial Cyber security practice space also maintain the listing.

4.2 Statistical Data

In the past, many organizations have been reluctant to report attacks. But recently, statistical data are beginning to emerge, that allows for the quantitative analysis of cyber incident data. By inception, it could be said that organized incident data reporting and compilation began with Computer Emergency Response Team/Coordination Center (CERT/CC) in Pittsburgh, which was created in 1988. Ever since then, CERT/CC has been the largest collector of cyber incidents. For example, a total of 319,992 incidents were reported to CERT/CC during 1988–2003 (CERT/CC, 2004 - http://www.cert.org/stats/).

Also, several other security organizations have also started collecting and analyzing Cyber attack data and have established monitoring units within their practices to track computer incidents and provide both quantitative and qualitative analysis to be used for Cyber defense research and planning. Among the leading organizations that provide daily, quarterly, yearly and other periodic reports are:

1. Computer Security Institute and the FBI – (joint effort)
2. The US Department of Homeland Security (National Vulnerability Database)
3. Symantec Intelligence Quarterly
4. Security Lab (by Positive Technologies)
5. IBM Internet Security Systems
6. Websense
7. SANS Institute
8. The Rand Corporation,
9. Arbor Networks
10. McAfee, Inc.
11. Etc.

All of these organizations have organized Cyber threat and attacks monitoring around somewhat of "Security Operation Centers" that deploy thousands of sensors to monitor all Internet traffic. The tools used are generally referred to as Monitoring Devices and are essentially intrusion detection systems (IDSs) (Figure 13)[22].

By definition, an IDS is a security technology that attempts to identify and isolate ``intrusions" against computer systems, i.e. the IDS monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization. Given the above, the main task of the IDS is to defend the computer system by detecting and possibly repelling attacks to it.

[22] Iheagwara, C. (2004), "The Effectiveness of Intrusion Detection Systems, Ph.D. Thesis, University of Glamorgan, Wales, Great Britain, 2004.

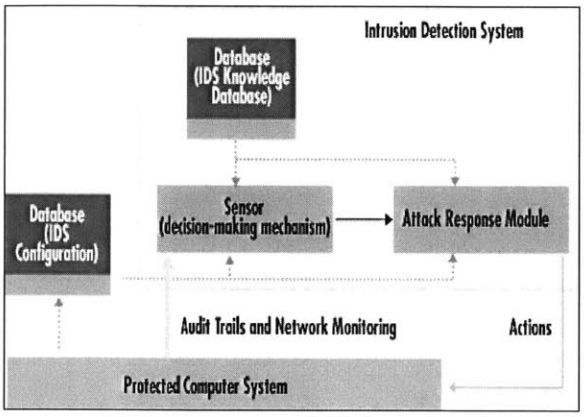

Figure 13: A sample IDS from Iheagwara C. (2004).

At the component level (Fig.13) the IDS always has its core element - a sensor (an analysis engine) - that is responsible for detecting intrusions. This sensor contains decision-making mechanisms regarding intrusions. Sensors receive raw data from three major information sources: own IDS knowledge base, syslog and audit trails. The syslog may include, for example, configuration of file system, user authorizations etc. This information creates the basis for a further decision-making process.

The component/mechanism responsible for data/information collection is integrated with the sensor (Fig. 14) — an event generator. The method of collection is determined by the event generator (which is usually the operating system, network or application) policy that defines the filtering mode of event notification information and produces a policy-consistent set of events that may be a log (or audit) of system events, or network packets. Storage of the policy set can either be in the protected system or outside.

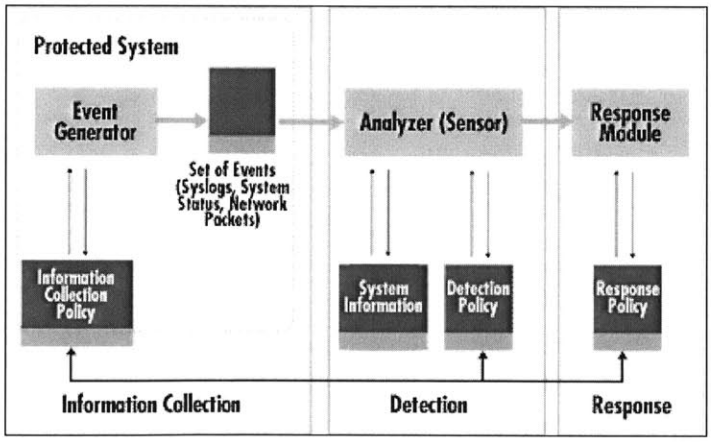

Figure 14: IDS components from Iheagwara C. (2004).

IDPs operate on similar principles and there are variations in technologies based on vendor offerings. Integral to their design are different components performing different roles. For

detection, a detection policy database (an information repository) is used for analysis by the analyzer. A typical content includes the following:

- Attack signatures
- Normal behavior profiles, and
- Necessary parameters for example, thresholds.

Additionally, the database holds IDP configuration parameters, including modes of communication with the response module. Also, the sensor also has its own database containing the dynamic history of potential complex intrusions.

The private Sector organizations mentioned above deploy their monitoring devices in several Internet backbone locations around the world each using different proprietary technologies that functions on the principles of the IDP.

For example, the Websense® Security Labs™ uses the Websense ThreatSeeker® Network located on different Internet locations to discover, classify, and monitor global Internet threats and trends. Featuring the world's first Internet HoneyGrid™, the system uses hundreds of technologies including honeyclients, honeypots, reputation systems, machine learning, and advanced grid computing systems to parse through more than 1 billion pieces of content daily, searching for security threats.

The ThreatSeeker Network scans more than 40 million websites for malicious code and nearly 10 million emails for unwanted content and malicious code every hour. Using more than 50 million real-time data collecting systems, it monitors and classifies Web, email, and data content. Together with the Websense Advanced Classification Engine (ACE) - an advanced composite content classification engine embedded in Websense solutions — the ThreatSeeker Network provides Websense with unparalleled visibility into the state of content on the Internet and in email.

Equally, Symantec Corporation has also established some of the most comprehensive sources of Internet threat data in the world with the Symantec™ Global Intelligence Network with more than 240,000 sensors located in over 200 countries and territories monitoring attack activity through a combination of Symantec products and services such as Symantec DeepSight™ Threat Management System, Symantec™ Managed Security Services, Norton™ consumer products, and third-party data sources.

The Symantec systems gathers malicious code intelligence (including Spam and phishing data) from more than 133 million client, server, and gateway systems that have deployed its antivirus products. Also, the Symantec distributed honeypot network collects data from around the globe, capturing previously unseen threats and attacks and providing valuable insight into attack methods.

The other private sector organizations have similar setups that collect billions of data, analyze them and produce daily, quarterly, yearly and other periodic reports.

At the US government level, the Department of Homeland Security has established a national monitoring system called the "Einstein Project" that tracks and analysis Internet traffic from several locations around the country (and possibly around the world). In principle, the technology and mode of operation is similar to those of commercially developed IDPs.

Statistical data collected and analyzed by the different organizations clearly demonstrate a rising trend in Cyber attacks with increasing sophiscatedness. In terms of reporting, each organization presents the results of its monitoring activities in different forms of published editions: research report, periodical, etc. For example, Symantec Corporation publishes quarterly and half-year reports.

The following are the highlights of some statistical report we have selected to analyze.

1. A taxonomy and comparison of computer security incidents from the commercial and government sectors [23] (Kjaerland (2005, 2006)

A recent study published in the **Computers & Security** Journal [23] analyzed 2755 Cyber attack incidents and provided the frequency analysis of some Cyber attack threat vectors. The software package LIFA (Liverpool interactive facet analysis) together with the statistical program SPSS was used to analyze the data. LIFA is a program that is used in criminal profiling while the SPSS is used for the conduction of the descriptive statistics.

In the study, Kjaerland was notable for adding a *quantitative* component to the classification of network attacks. In particular, her work sought not only to classify the attacks, but also to determine which factors were most likely to co-occur in an attack. Her analysis was based on a sample of 2,755 reported incidents to CERT/CC, from the years 2000-2002. She classified the incidents based on four categories:

- source sectors (com, gov, edu, intl, user, unknown)
- method of operation (misuse of resources, user/root compromise, social engineering, virus, web compromise, trojan, worm, denial of service)
- impact (disrupt, distort, destruct, disclosure, unknown)
- target services (com, gov)

After categorizing each of the reported incidents along these dimensions, she performed a smallest space analysis (SSA) to determine which of these factors were most likely to happen together. Her results showed, among other things, that "individual user" and "web compromise" were likely to occur together; conversely, "educational source" and "trojan" were not likely to co-occur. Although this analysis did not determine the causality of these incidents, this sort of correlative study is very useful in understanding the characteristics of the threat space.

The data input for the analysis consists of 1397 of the 2755 incidents in the excel binary data file where every incident is either present or absent on each variable given in Table 4. Every incident has a presence of one variable within each facet also given in the Table and the variables within each facet exclusively and exhaustively account for the aspects of reported cyber incidents.

---

[23] Kjaerland, M. (2006): "A taxonomy and comparison of computer security incidents from the commercial and government sectors," Computers & Security, Volume 25, Issue 7, October 2006, Pages 522-538.

Table 4: Frequencies and percentages of the variables in the Smallest Space Analysis from Kjaerland M. (2006).

Facets	Variables	Identification name SSA	Identification number SSA	Frequencies	%	*Sum %*
Impact	Disrupt	Disrupt	9	570	40.8	*98.3*
	Distort	Distort	10	531	38.0	
	Destruct	Destruct	11	60	4.3	
	Disclosure	Disclosure	12	199	14.2	
	Unknown	UnImpact	13	14	1.0	
Method of operation (MO)	Misuse of Resources	Misuse	1	73	5.2	*97.1*
	User Compromise	UserComp	2	85	6.1	
	Root Compromise	Root	3	433	31	
	Social Engineering	SocEng	4	7	0.5	
	Virus	Virus	5	299	21.4	
	Web Compromise	WecComp	6	143	10.2	
	Trojan	Trojan	7	10	0.7	
	Worm	Worm	8	41	2.9	
	Recon	Reconn	14	156	11.2	
	Denial of Service	**DoS**	**15**	**110**	**7.9**	
Source sectors	Com	Scom	18	121	8.7	*96.2*
	Gov	Sgov	19	21	1.5	
	Edu	Sedu	20	13	0.9	
	intl	Sintel	21	192	13.7	
	User	Suser	22	108	7.7	
	Unknown	Sunknown	23	890	63.7	
Target sectors	Com	Com	16	838	60.0	*100*
	Gov	Gov	17	559	40.0	

The 2-dimensional solution of the geographical solution is represented beneath (see Fig. 15) for the SSA plot and Table 4 for the descriptions of the variables). For clarity it should be mentioned that each point is a variable describing aspects of cyber intrusions. The numbers refer to the variables as listed in Table 4, although a brief title for the variable has also been placed on the plot to ease interpretation. The squares on the plot indicate either 'Com' or 'Gov' 'Target Sectors'. The circles indicate 'Impact', the diamonds indicate 'Source Sectors', and the triangles indicate 'Method of Operation'. The points 'Suser' (Individual User) and 'Web-Comp' (Web Compromise) are placed close together on the plot, indicating that they often co-occur in cyber incident offences. The points 'Sedu' (Educational Source) and 'Trojan' are on the contrary placed far from each other, indicating that they do not often co-occur in the cyber incidents analyzed.

With regards to the 'Target Sectors' that are being compared to each other, 'Com' is represented in 838 (60%) of the incidents, and 'Gov' in 559 (40%) of the incidents. Further, with regards to the 'Impact' of the cyber intrusions towards 'Com' and 'Gov', the most common effect was

'Disrupt' which is occurring in 570 of 1397 incidents (40.8%). 'Distort' is occurring in 531 of 1397 incidents (38.0%). 'Disrupt' is the least invasive nature of attack, and 'Distort' is more severe. 'Disrupt' means access change and that the organization is unable to access information systems.

The smallest space analysis (SSA) plot is shown with frequencies in Figure 15 is divided into three regions, with the outer region representing variables that have less than 5.2% occurrence:

- 'Trojan' (0.7%),
- 'SocEng' (Social Engineering) (0.5%),
- 'Worm' (2.9%),
- 'Sgov' (Government Source) (1.5%),
- 'UnImpact' (Unknown Impact) (1.0%), and
- 'Sedu' (Educational Source) (0.9%).

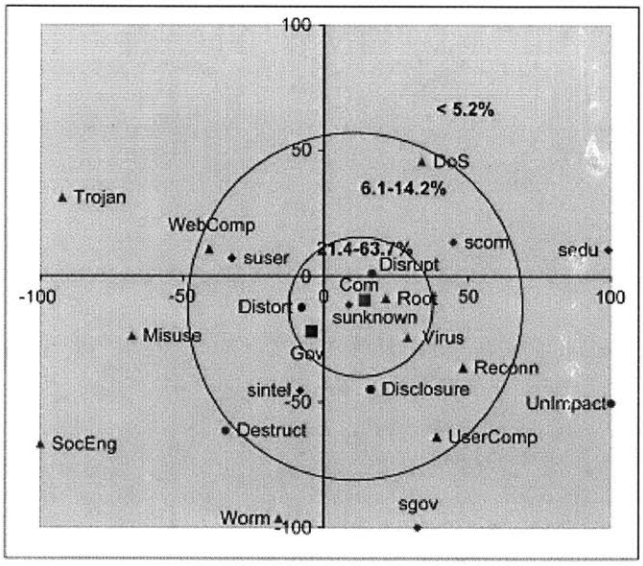

Figure 15: SSA showing the percentage ranges of the co-occurring variables from Kjaerland M. (2006).

The variables in the region of 6.1–14.2% (8–31%) are:

- 'WebComp' (Web Compromise) (10.2%),
- 'Suser' (User Source) (7.7%),
- 'sintel' (International Source) (13.7%),
- 'Disclosure' (14.2%),
- 'User Comp' (User Compromise) (6.1%),
- 'Reconn' (Recon) (11.2%),
- 'Scom' (Commercial Source) (8.7%), and
- 'DoS' (Denial of Service) (7.9%).

Finally, the variables within the inner circle of 21.4–63.7% (31–62%) are:

- 'Distort' (38.0%),
- 'Gov' (Government Target) (40.0%),
- 'Sunknown' (Unknown Source) (63.7%),
- 'Com' (Commercial Target) (60%),
- 'Virus' (21.4%),
- 'Root' (31%), and
- 'Disrupt' (40.8%).

The study further partitioned the variables in relation to what aspects of cyber intrusions are most commonly occurring in commercial versus government reported computer security incidents (see Figure 16).

The area defined as '**Commercial Sector'** contains the variables 'Sunknown' (Unknown Source), 'Com' (Commercial Target), 'Disrupt', 'Root', 'DoS' (Denial of Service), 'Scom' (Commercial Source), and 'Virus'.

The area defined as '**Governmental Sector'** contains the variables 'Web-Comp' (Web Compromise), 'Suser' (User Source), 'Distort', 'Gov' (Governmental Target), 'sintel' (International Source), 'Disclosure', 'UserComp' (User Compromise) and 'Reconn' (Recon).

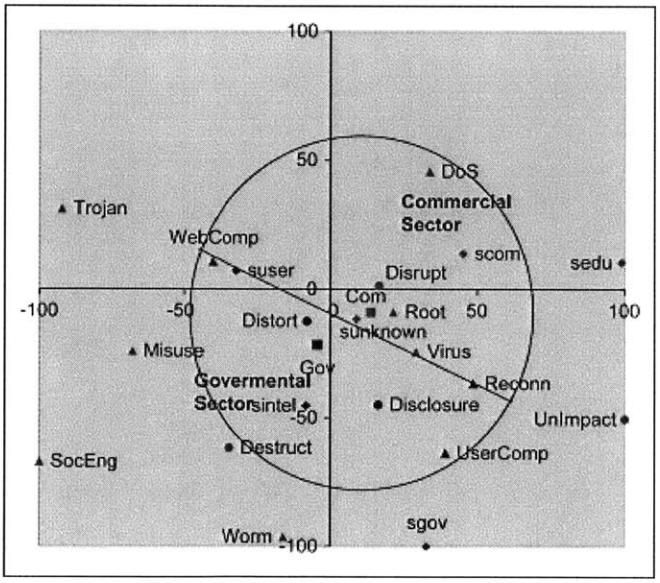

Figure 16: SSA showing partitioning between the targets Com and Gov in relation to impact, method of operation, and source sector from Kjaerland M (2006).

Also, the study presented (Table 4) the frequencies and percentages of the variables in the SSA and provides a pointer on which "Target Sector" the attacks are directed with 838 or 60% of the attacks or 60% directed towards the 'Com' Sector and 559 or 40% of the incidents directed towards the 'Gov' Sector. It also quantified the attack types. For example, the DoS accounts for

110 of the frequencies or 7.9% of the attacks. This is reflected in Figure 19 where the 'DoS' is generally not far inside the circle in the 2-dimensional-plot either, and the cross-tabulations show that 'DoS' is more common in attacks towards the 'Commercial Sector'.

2. Symantec Intelligence Quarterly, April - June 2010 [24]

The following highlights from the Symantec Intelligence Quarterly, April - June 2010 [24]and presents emerging statistical trends of attacks resulting from known Internet system vulnerabilities:

- The United States was the top country for malicious activity in this quarter, accounting for 21 percent of the total;
- The top Web-based attack for the quarter was related to malicious PDF activity, which accounted for 36 percent of the total;
- Credit card information was the most commonly advertised item for sale on underground economy servers known to Symantec in this quarter, accounting for 28 percent of all goods and services;
- Symantec created 457,641 new malicious code signatures during this quarter;
- The most common malicious code sample by potential infections during this quarter was the Sality.AE virus;
- Symantec observed 12.7 trillion spam messages during this quarter, accounting for approximately 89 percent of all email messages observed;
- The majority of brands used in phishing attacks this quarter were in the financial sector, which accounted for 73 percent of the total.

Malicious activities observed during the period are ranked by country/region of in Table5. The United States was the top ranked country for malicious activity, accounting for 21 percent of the total. Also, within specific category measurements, the United States ranked first in all categories except spam zombies.

India had the second highest amount of overall worldwide malicious activity this quarter, accounting for six percent. Within specific category measurements, India ranked first in spam zombies by a significantly large margin.

[24] http://www.symantec.com/content/en/us/enterprise/other_resources/b-symc_intelligence_quarterly_apr-jun_2010_21072009.en-us.pdf. Last checked February 19, 2011.

Table 5: Malicious activity by country/region [24].

Rank	Country/Region	Percentage	Malicious Code Rank	Spam Zombies Rank	Phishing Website Hosts Rank	Bots Rank	Attack Origin Rank
1	United States	21%	1	5	1	1	1
2	India	6%	2	1	20	20	9
3	Germany	6%	21	4	2	2	7
4	China	5%	3	35	8	6	2
5	Brazil	5%	5	2	10	5	5
6	Italy	4%	15	8	13	4	6
7	United Kingdom	4%	10	9	3	8	3
8	Taiwan	3%	22	13	14	3	10
9	Russia	3%	12	7	7	15	4
10	France	3%	19	18	6	11	8

Table 6 assesses the top distinct Web-based attacks that originate either from compromised legitimate sites or malicious sites that have been created to intentionally target Web users.

Table 6: Top Web-based attacks [24].

Rank	Attack	Percentage
1	PDF Suspicious File Download	36%
2	Microsoft® Internet Explorer® ADODB.Stream Object File Installation Weakness	33%
3	C6 Messenger ActiveX File Overwrite	7%
4	Microsoft Internet Explorer DHTML CreateControlRange Code Executable	5%
5	Adobe® SWF Remote Code Execution	5%
6	Embed Tag NPDSPlay DLL Buffer Overflow	3%
7	Microsoft Internet Explorer WPAD Spoofing	2%
8	Microsoft Internet Explorer Popup Window Address Bar Spoofing Weakness	1%
9	Microsoft Internet Explorer CreateTextRange Remote Code Execution	1%
10	Microsoft Internet Explorer Malformed IFRAME/EMBED Buffer Overflow	1%

The most common malicious code sample by potential infections during the period was the Sality.AE virus (Table 7). This virus infects executable files on compromised computers and removes security applications and services. Once the virus is installed, it also attempts to download and install additional threats onto infected computers.

Table 7: Top malicious code samples [24].

Rank	Sample	Type	Infection Vector(s)	Impact
1	Sality.AE	Virus, worm	Executables	Removes security applications and services, downloads and installs additional threats
2	Mabezat.B	Worm, virus	SMTP, CIFS, removable drives	Encrypts and infects files
3	Downadup.B	Worm	Direct network connections, CIFS	Disables security applications and Windows Update, downloads and installs additional threats
4	Virut.CF	Virus	Executables	Infects files, downloads and installs additional threats
5	SillyFDC	Worm	Mapped, removable drives	Downloads and installs additional threats
6	Almanahe	Worm, virus	CIFS, mapped and removable drives	Infects executable files, ends security related processes and installs additional threats
7	Gammima.AG	Worm, virus	Removable drives	Steals online game account credentials
8	FakeAV	Trojan	N/A	Displays false security alerts and lowers security settings
9	Gampass	Trojan	N/A	Steals online game account credentials
10	Chir.B@mm	Virus, worm	SMTP	Infects executable and HTML files

In terms of the top phishing sectors, the majority of brands used in phishing attacks for the period were in the financial services sector (Table 8) accounting for 73 percent of the total reported phishing attacks. The financial sector is commonly the largest sector targeted in phishing attacks because the various associated services are the most likely to yield data that could be directly used for financial gain.

It is noteworthy that many phishing attacks that spoof financial services brands will prompt users to enter credit card information or banking credentials into fraudulent sites. If these tactics are successful, the phishers can then capture and sell such information in the underground economy.

Table 8: Top phishing sectors [24].

Rank	Sector	Percentage
1	Financial	73%
2	ISP	10%
3	Retail	5%
4	Insurance	3%
5	Internet community	2%
6	Government	2%
7	Telecom	2%
8	Computer hardware	2%
9	Online gaming	<1%
10	Computer consulting	<1%

3. Secunia's second-half year report for 2010 [25]

In Secunia's second-half year report for 2010 [25], there were six (6) most prevalent impact classes since 2005:

1. System access
2. Cross Site Scripting (XSS)
3. Exposure of sensitive information
4. Manipulation of data
5. DoS ,and
6. Security bypass

Of all, "System access" had the most impact with an average of 33% while Denial of Service attacks (DoS) declined from 14.5% to 13% in 2010.

4. Shadowserver Foundation [26]

A historical report by the Shadowserver Foundation[26] that gathers intelligence on internet-based attacks provides an extensive detail on the magnitude, scope and origins of Distributed Denial of Service (DDoS) attacks (Table 9) over approximately a two and half (2.5) year (2006 – 2008) span.

Table 9: Statistics of DDoS Attacks [26].

Date of Last Update	CC_Count	CC_ASN	CC_Country	DDoS_Count	Target_Count	Target_ ASN	Target_ Country
Total DDoS attack last updated December 4, 2008	1710	654	78	278965	59891	4483	151
2008 DDoS Attacks last updated December 4, 2008	562	300	62	193051	19835	1718	112
2007 DDoS Attacks	848	390	67	35566	15755	1633	107
2006 DDoS Attacks	414	215	40	50650	25953	3076	133

[25] http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf

[26] http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical

The legends used in the columns in Table 9 are explained as follows:

- CC_Count - How many unique Command and Controls conducted DDoS attacks
- CC_ASN - How many Unique ASN's did the Command and Control servers reside in that participated in DDoS attacks
- CC_Country - How many unique countries did the Command and Control servers reside in that participated in DDoS attacks
- DDoS_Count - How many DDoS attacks occurred during that period
- Target_Count - How many different targets were DDoS'ed
- Target_ASN - How many unique ASN's were affected by the DDoS's
- Target_Country - How many unique countries were affected by the DDoS's

The attacks and their paths are shown in the maps below in Figures 17 -20.

The pattern and trends of Cyber attacks are similar for those other organizations whose data and statistics are not presented here.

The classification and definitions of Cyber attack types is given in the General Accounting Office of the United States government report[27] in Appendix 2.

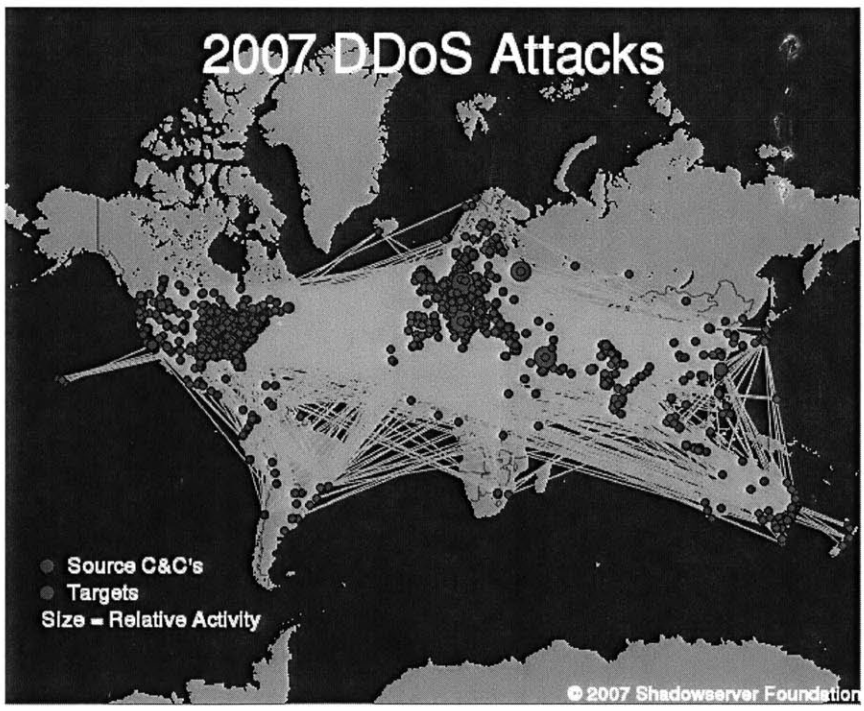

Figure 17: Map of the 2007 DDoS Worldwide Attacks [26].

[27] Source: GAO analysis of data from GAO and industry reports ((GAO-08-588) http://www.securingourecity.org/blog/diving-deeper/cyber-attack-types/

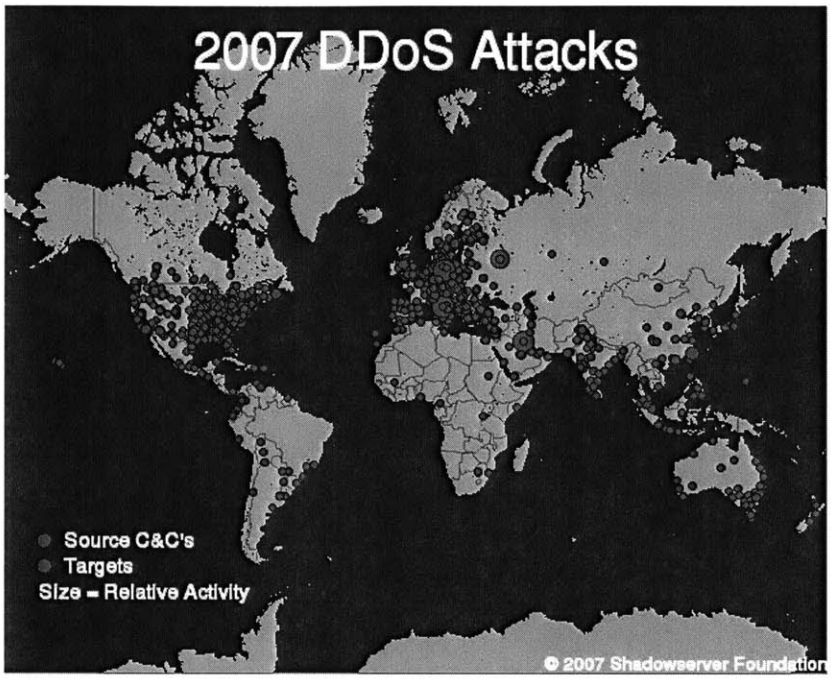

Figure 18: Map of the 2007 DDoS Attacks without Paths [26].

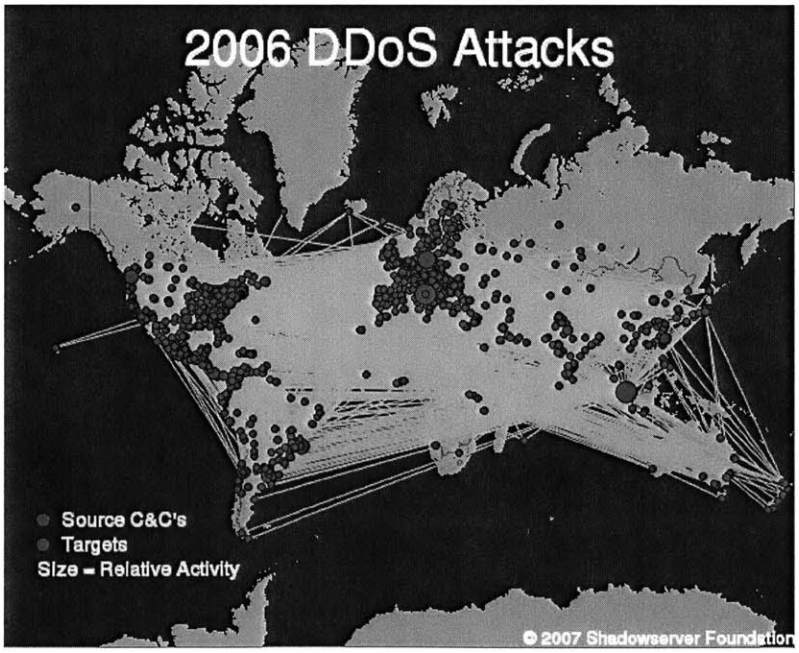

Figure 19: Map of the 2006 DDoS Worldwide Attacks [26].

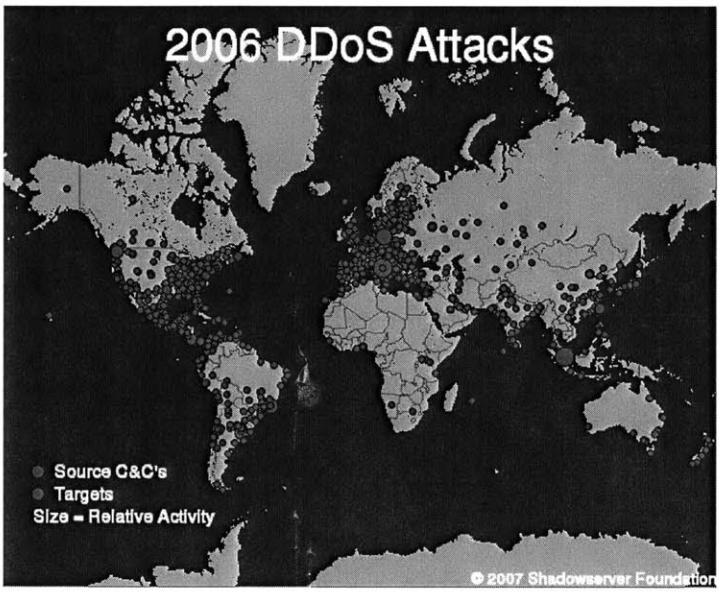

Figure 20: Map of 2006 DDoS Attacks without Paths [26].

4.3 Correlating Cyber Attack Statistical Data to Internet Vulnerabilities

Based on the statistical data presented in Section 4.2 and information from other literature sources, we map each Cyber attack type to the specific Internet layered architecture that serves as the conduit pipe for launching the attacks. The mapping provides a clearer picture and understanding on where additional Cyber security work should be concentrated on and forms part of the derived implications discussed in Chapter 5.

Figure 21 presents a mapping of Cyber attack types to specific Internet (TCP/IP reference model) layer. The attack types are populated on the header columns and the Internet layers populated on the header rows of the grid (with their functions and the TCP/IP weaknesses briefly explained).

The "Xs" represents a match i.e. an intersection point between the columns and rows where a particular Cyber attack type occur on the Internet layer.

Overall, the IP layer is the layer where most Cyber attacks take place followed by the Application layer. The least impervious to the attacks is the Physical/hardware layer.

Also, the lack of authentication mechanism on the Internet system is the greatest factor that makes the system vulnerable to all attack types. In the grid, this is represented as a "Non TCP/IP" layer.

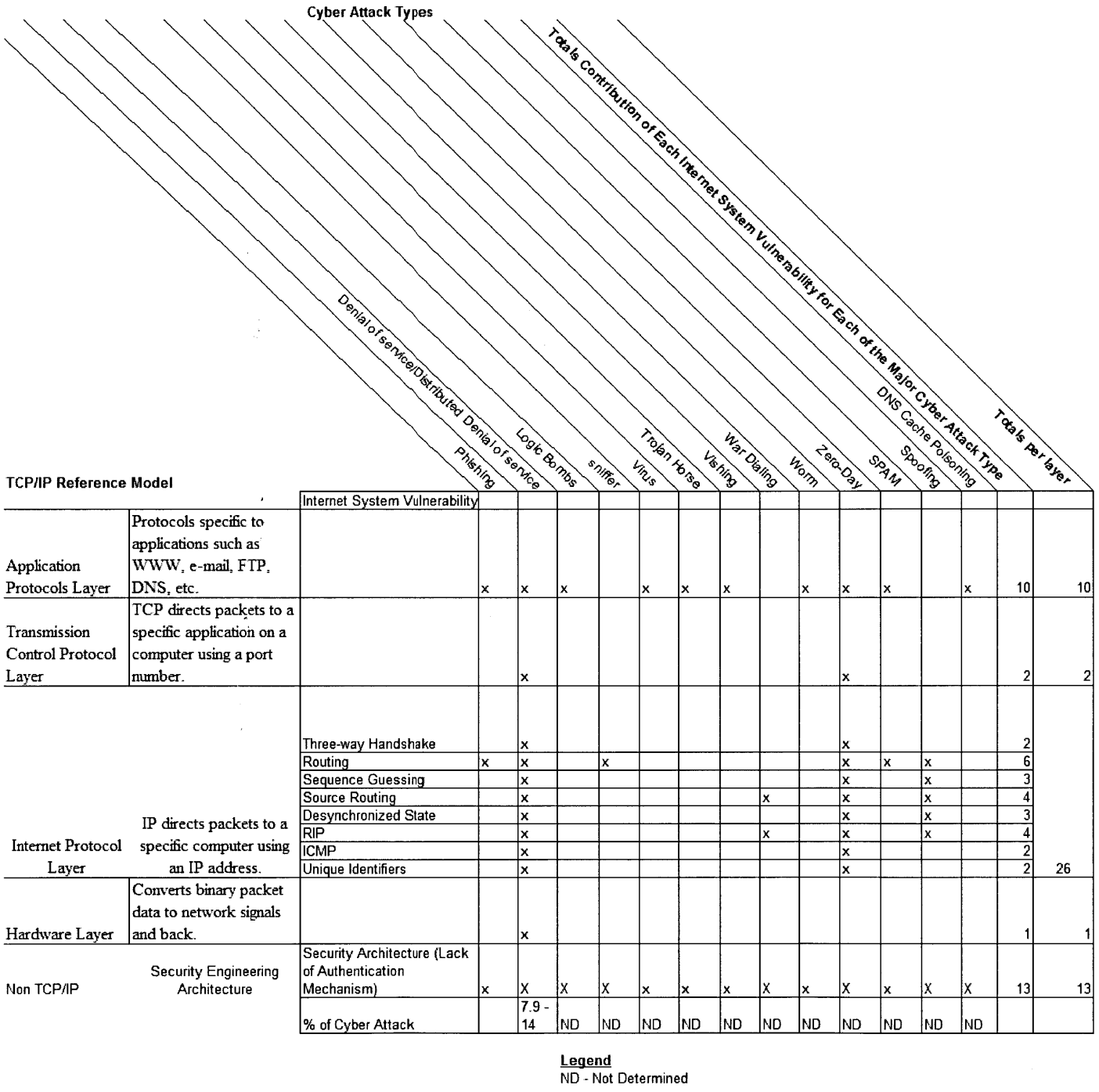

Figure 21: Mapping of Cyber Attacks to Their Sources of Origin on the Internet Layered Architecture from Iheagwara C. (2011).[28]

[28] Iheagwara, C. 2010, "Cyber Attacks –Internet Architecture Mapping," S.M. Thesis, MIT, 2010.

Based on the above mapping, the data and discussion presented in Section 4.2, we discern the following Cyber attack trends:

1. Most Cyber attacks originate from the vulnerabilities created in the IP layer of the TCP/IP protocol stack.

2. The lack of authentication mechanism can result to any type and number of Cyber attacks.

3. For the most part, all reports indicate that the level of total cyber attack activity has been steadily increasing. The reports also found that damage caused by recent blended threats, such as SPAM, phishing, and Opaserv, was considerably higher than that caused by old threats, such as Code Red. Mixed with the encouraging news at least for the noticeable decrease in old threats, the different sources also documented hundreds of new vulnerabilities in 2010, an increase of more than 21.5 percent over 2009. For all, it is widely believed that the possibility of future, high impact, blended threats continues to represent one of the greatest risks to the Internet community.

4. In terms of Cyber attacks resulting from Internet design flaws, DoS and DDoS are the most devastating and constitute between 7.9 (CSI/FBI report to 14% (Secunia report) of all Cyber attacks. Although, the DoS and DDoS attacks are smaller in number when compared with Phishing and SPAM attacks, their impact is more devastating as often the targets are companies who often are forced to shut down business activities for some time leading to significant economic loss. And, as Internet usage grows, DDoS and DoS based attacks grows.

5. The lethal Dos and DDoS are attackers exploit the weaknesses at the Internet Protocol layer and results in the most financial losses of all Cyber attacks.

6. Phishing, Spaming, Viruses and Worms are related to Application layer weaknesses that are introduced by software applications.

7. Power and Energy companies show the highest rate of both attack activity and severe event incidence. In addition, the Financial Services sector experienced an elevation in overall attack volume and severe event incidence.

8. Blended threats, continued to constitute the most frequently reported threat. Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. For example, eighty percent of all malicious code submissions were caused by only three blended threats: Klez, Opaserv, and Bugbear. Further, 78 percent of all cyber attack activity detected by Symantec was related to both old and recent blended threats.

4.4 Summary

In this Chapter, we reviewed and analyzed several Internet traffic monitoring reports and statistical research studies on Cyber attacks.

From the analysis, we deduced several facts which together with interpretations of the domain issues, inferences and the statistical data presented in the previous Chapters aided development of the grid presented as Figure 21 that maps each Cyber attack type to specific Internet architecture layers.

On the quantification of each Cyber attack type as a percentage of the overall Cyber attacks, we conclude that quantification is difficult to realize because of insufficient and scanty data from which such quantification could be derived; and the lack of any known predictive (or adaptive) model that can help us to accomplish this.

From our analysis, we discerned several well-known trends in the constantly evolving Cyberspace world. Primarily, most Cyber attacks occur at the TCP/IP layer with the physical (link) layer being the least affected. And most certainly, the lack of an authentication platform on system gives rise to all Cyber attack types.

Chapter 5: Stakeholder Analysis

In this Chapter, we conduct stakeholder and beneficiary analysis to better understand and conceptualize the Internet system design intent, goals and processes.

We create a statement of the goals (the system problem statement) at the highest level (i.e. without any decomposition to goals associated with the first level of decomposition of process or form); and comment on the "goals map to the system" and the "needs to goals framework."

We discuss the operand and value related solution neutral transformation, solution neutral function, function and form to delineate the security requirements explicit and implicit in the process. We interpret the needs of the beneficiary as goals to be satisfied by the stakeholder design and answer the "value questions" for a beneficiary and a stakeholder.

Based on critical characteristics of the system, we devise a conceptual typology of system. Further, we identify the key stakeholders and beneficiaries in the process and describe the roles played by them in addressing the problem of security.

5.1 Introduction

One of the important functions of a system architect is reducing ambiguity of the system being designed. Crawley E. (2010)[29] provides a contextual basis on how to proceed and realize this and asserts:

- The principal way to reduce *ambiguity* is to set clear goals for the system (also called requirements, specs, etc.)
- Ambiguity is reduced when we set goals that are:
    - Representative
    - Complete and consistent
    - Humanly understandable
    - Consistent with resources

While reducing ambiguity is a design goal, nonetheless, Crawley E. (2010) asserts "We will never succeed in *eliminating* ambiguity - there will be unresolved issues at any time, and the future will continue to introduce more ambiguity."

Relating this to the Internet system design, we will set out to analyze the architecture of the current Internet system to understand if there ambiguity in stakeholder design intent as it relates to the security mandates for the solution neutral statement and value related operand of system for safe (secure) connection and transmission.

[29] Crawley, E. (2010)"Identifying Value - Reducing Ambiguity in the System," Lecture Notes on System Architecture, October 8, 2010, MIT.

In accordance with the "**Framework - Needs to Goals Approach**" proposed by Crawley E. (2010), we will:

- Identify primary, and other beneficial stakeholders, and their needs
- Characterize their needs, prioritized by the benefit to the stakeholder and importance in supply
- Interpret the needs as goals, and mapping on to the project
- Prioritize the goals based on the integrated stakeholder needs, and create metrics
- Validate that the system meets the design intents to satisfy needs of the beneficiaries and the goals of stakeholders

5.2 Stakeholder Analysis as a Framework

As described in Chapter 2, the Internet system is an assembly of several components and subsystems from different entities that collaborate to fuel, enhance and sustain the system with a mutually assured responsibility for the security of the system. The degree to which each is responsible for the security of the system is a subject of this stakeholder analysis

Stakeholder analysis has become an established framework used to identify and examine the interactions between organizations and constituents in external environment. It was originally advocated by Freeman R. (1984)[30] as a tool for managers to proactively engage their external environment in the face of a rapidly changing global marketplace. Ever since then, it has been applied to different uses such as need-based analysis, justifications, impetus to launch a new project, etc. Although, in general, the term 'stakeholder' refers to individuals, groups or organizations that need to be taken into account by leaders and managers contemplating any action on an issue. While earlier researchers confined stakeholders to a firm based on their organizational membership, subsequent scholars have recognized the existence of stakeholders outside of firm boundaries. Mitchell et al (1997)[31] suggested a framework for stakeholder identification based on three criteria namely power, legitimacy and urgency. Stakeholder analysis has been widely applied in strategic management, corporate governance (Burgoyne et al. (1994)[32]; Donaldson et al. (1995)[33]) as well in information systems studies.

The activities and the five steps in establishing the framework for a stakeholder analysis is given in Figure 22.

---

[30] Freeman R. E. (1984), Strategic Management: A Stakeholder approach, Boston: Pitman.

[31] Mitchell, R, Agle, B & Wood, D (1997). Towards a theory of stakeholder identification: Defining the principle of who & what really counts, Academy of Management Review 22(4): 853-886.

[32] Burgoyne, John G., Stakeholder analysis, in Cassel. C. and G. Symon (ed.), Qualitative Methods in Organizational Research: a practical guide, Sage, New Delhi, pp. 187-207, 1994

[33] Donaldson T. and Preston L. E. (1995), The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications, Academy of Management Review, Vol. 20, No. 1, pp. 65-91.

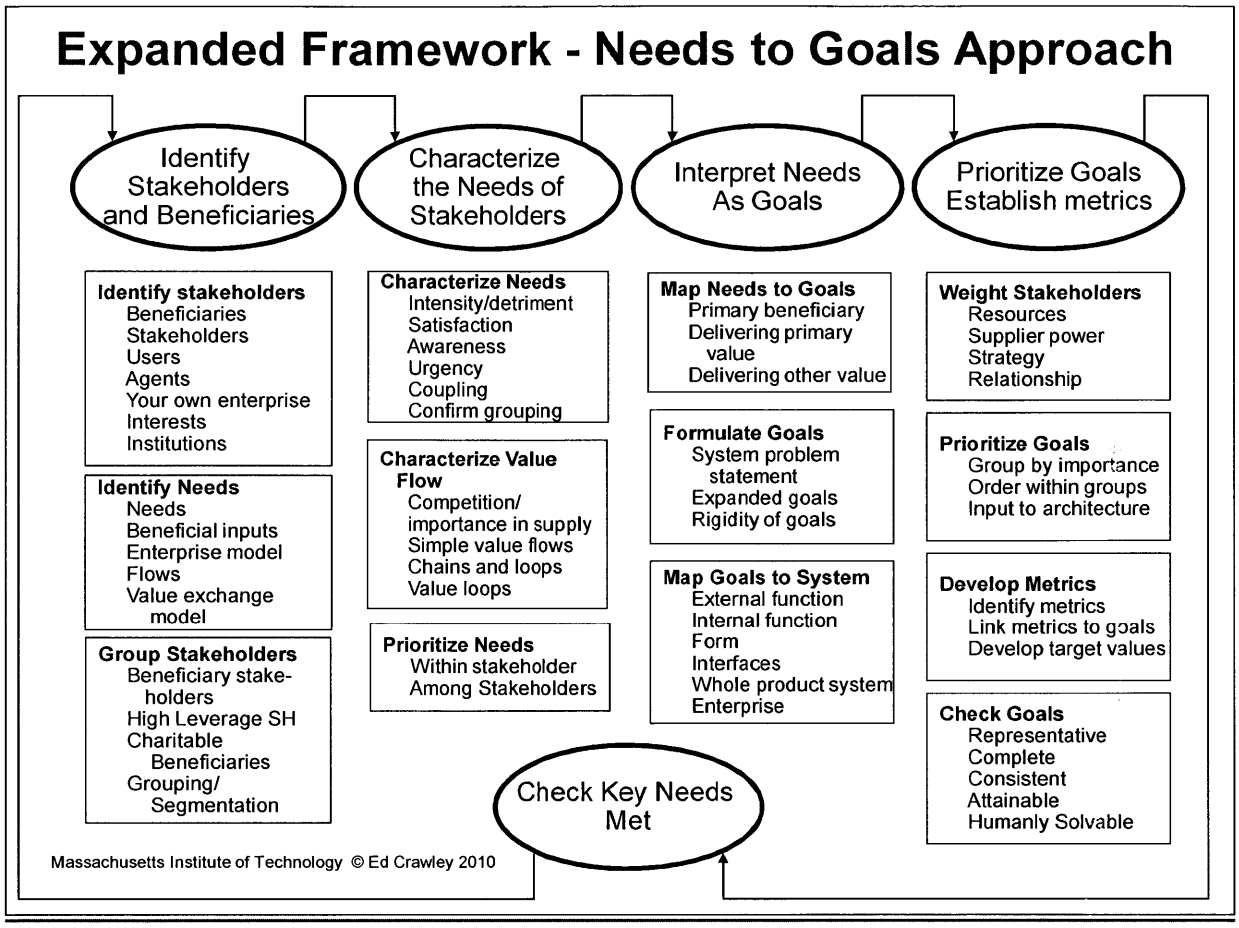

Figure 22: Expanded Framework for Stakeholder Analysis from Crawley E. (2010).

Using the expanded framework, we conduct the following Internet system stakeholder analysis.

5.3 Internet System Goals and Stakeholder Intent

Given that the primary goal of the Internet design is to establish Internet connection for a community of users who wishes to transact or communicate over the medium, there is an implied mandate for such transactions and communications to be accomplished inexpensively and safely in such manner that the integrity and timely delivery of the packets being transmitted is guaranteed. Figures 24 and 25 maps the problem statement and goals to the Internet system design and makes it obvious that meeting the design goal is integral to satisfying Internet security requirements.

In general, there are so many elements and factors that need to be considered when formulating system architectural goals and intents. Crawley E. (2010) discerns (in Figure 23) the following among the many elements to be considered when designing a system:

- **Business Case** - (reflecting customer needs, competitive environment, strategy, channels, etc.)
- **System Architecture (Benefit)** - (reflecting regulation, technology, competent supply chain, legacy elements, etc.)
- **Platforms** (bordering on System Architecture)
- **Product lines** (bordering on Business Case)

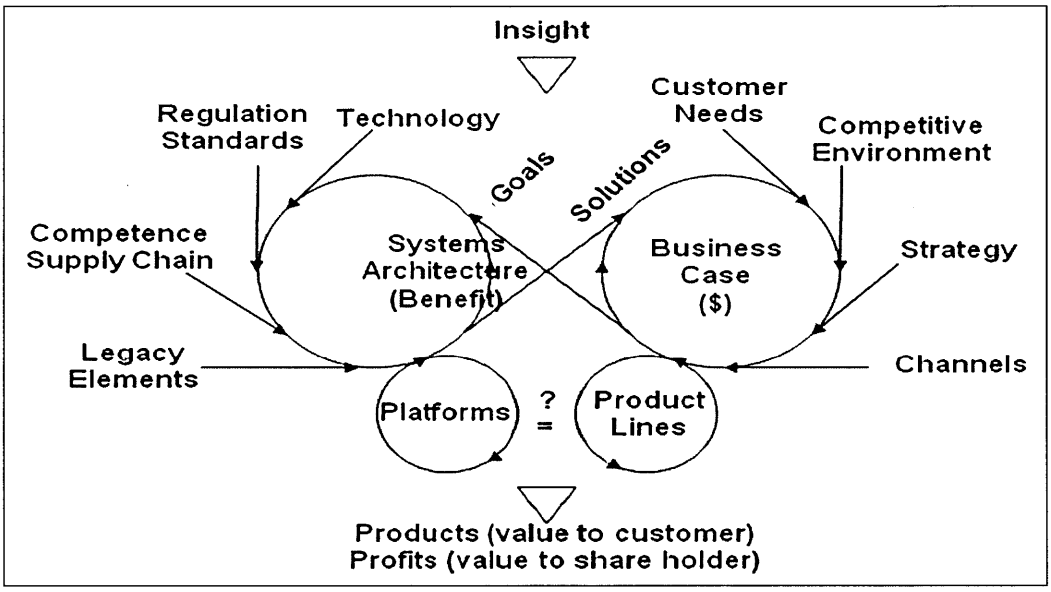

Figure 23: Driving a System Goal Factors from Crawley E. (2010).

For the Internet system, all of the above elements are integral to defining the goals of the system.

For example, the business case is the necessity to interconnect networks and users, the system architecture must be complaint with regulations using different technologies that are platform independent such that the different software applications and product lines can seamlessly fuse into the Internet system. This means that the Internet system is built on the concept that the system is platform independent to satisfy a variety of business cases and user needs and the different product lines that fuses into it.

A statement of goal by system problem statement [34]

We provide the following Internet system problem statement: *The goal of the Internet is to establish Internet connection in order to transmit messages or communicate inexpensively and safely from the Sender to the Recipient in such manner that guarantees the confidentiality, integrity and timely delivery of the packets being transmitted or the message being delivered.*

[34] Iheagwara, C, HoonYoo, J and Prurapark, R. A (2010): "Internet System Stakeholder Analysis" Systems Architecture (ESD.34) class project, MIT, Fall, 2010.

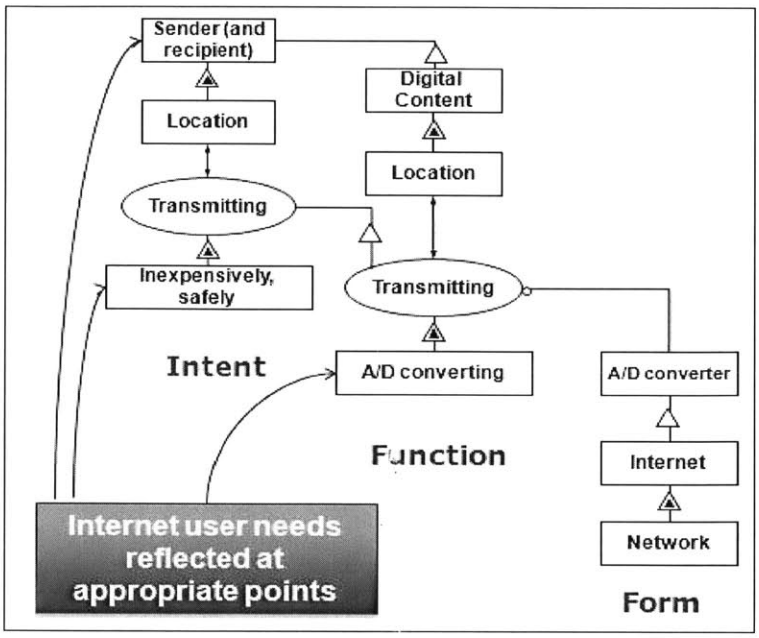

Figure 24: Internet System Problem Statement Mapping from Iheagwara C. et al. (2010).

Impliedly, the design goal of the Internet system is to design an inter-networking collaboration system that enables organizations, communities and users to connect so as to be able to communicate, exchange data/information and transact business.

This goal is clearly expressed in the solution neutral function, function, and form of the system given in Figure 25.

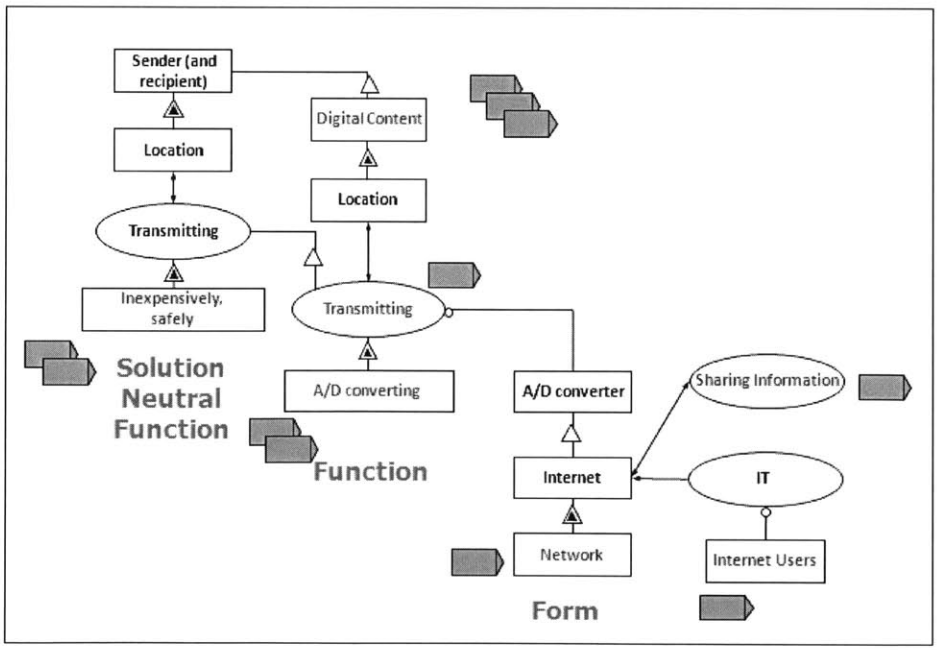

Figure 25: Mapping Goals to System from Iheagwara C. et al. (2010).

In a general sense, when faced with competing goals, some will assume greater importance and hence the need to prioritize the subsidiary goals into critical, important, etc. Followed by the development of appropriate metrics that would go with each of the subsidiary or expanded goals. And, prioritization entails drawing up descriptive goals.

For the Internet system, the descriptive goals can be characterized into three (3) categories:

- **Critically**
  - The Internet connectivity must be constantly available
  - Connections and transmissions must be secure
  - Must guarantee delivery of messages or communication
  - Must ensure the non repudiation of transmitted messages or communication
  - Must be platform independent
  - Must be interoperable with different networking technologies

- **Importantly**
  - Shall provide enough bandwidth to ensure Quality of Service (QoS) to guarantee user satisfaction
  - Must be flexible enough for re-architecting

- **Desirably**
  - Shall be affordable
  - Be adaptive to different usage technologies (in terms of applications and devices that can be coupled into it)

From here we derive one of the most important priorities which expresses that Internet "Connections and transmissions must be secure."

One of the post-design and in-operation goals is concrete proof that the design intent and goals are met. Often, metrics are used in the tests to verify and validate this.

On meeting the goals, Crawley E. (2010) expresses:

- If the goals are met - the product/system is a "success" (in principle)
- Only if the goals answer a real need (in context of competition, regulation, macroeconomic environment, etc.) will a product/system be a success *in reality*
- Goals are tradable surrogates for success
- Therefore, a representative goal is one that ensures that value will be delivered to meet need, within a competitive environment, regulation, etc. Metrics flow from goals and help "ensure" success

For the Internet system, a representative goal includes secure connection and transmission and meeting this goal is not only a measure of success for the system but also has implication for the stakeholder intents and the beneficiary needs.

Testing the goals entails validating that the goals are met, and if not that the needs of the stakeholders will be addressed.

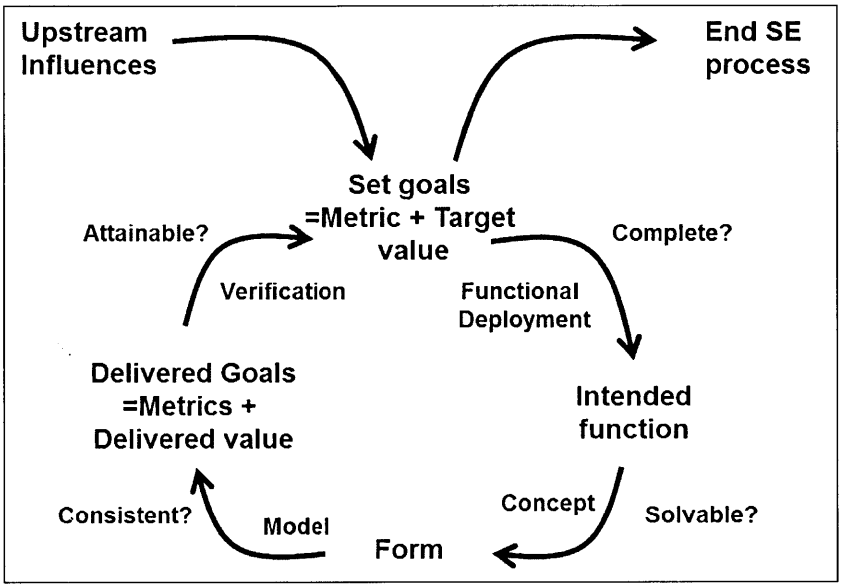

Figure 26: Framework to test a goal from Crawley E. (2010)

Going by the test model in Figure 26, Crawley E. (2010) notes:

- Completeness is usually clarified by the time functional description is made
- Consistency is usually clarified after concept, and models are created
- Attainability is usually clarified only after models simulate all goal metrics and their delivered value

For the Internet system, completeness, consistency and attainability have been tested by validation via different empirical metrics. The identification of a single goal set is not representative of true success since even today the Internet already has proven itself as one of the best ways for communication, attainable within resources & technology. It has not at the same time satisfied the goal of securing the system and compounds the fact that consistent and complete goals are vital to resolve ambiguity and creating the path for product success. And, the manifestation of hugely immense Cyber attacks is a clear indication of the failure of one of the design intent and goal.

We have established that the solution neutral function (Figure 25) of inexpensively and safely transmitting over the Internet is an implied mandate of intent to design a system that securely connects and transmits over the Internet. As this Internet stakeholder analysis reveals in Section 5.6, there are several key players with primarily responsibilities to implement security on the system. And, one way or the other, they stakes are affected by the Cyber security posture of the design and management of the Internet system.

In the end, the test of a good Internet system design lies in the question of "what responsibilities does stakeholders have when it comes to securing the value related processes over the Internet?"

5.4 Value Related Internal Processes and Operands

Figure 27 is an idealized graphical representation of the Internet system process and the key devices that form parts of the infrastructure. The value related instrument objects are the devices used to execute the value related internal processes where the **value related operand** is the Analog to Digital (A/D) converter, the **value related attribute** includes Speed, Safety (security), Size of the content, Latency and Throughput, the **solution neutral statement** (see Figure 25) **of the value related transformation** is the transmitting information, and **other important attributes of operand and transformation** include Speed of transmission, QoS (Quality of Service), and **Integrity of data packet**.

The Integrity of data packet is directly related to the security of the data being transmitted as any form of modification could mean violation of the confidentiality and actual data being transmitted.

The routers (value related instrument objects) and in some cases the switches operate at the Internet layer of the TCP/IP model **(**see Figure 27**).** The design and mode of operation of these devices have implications for Cyber security.

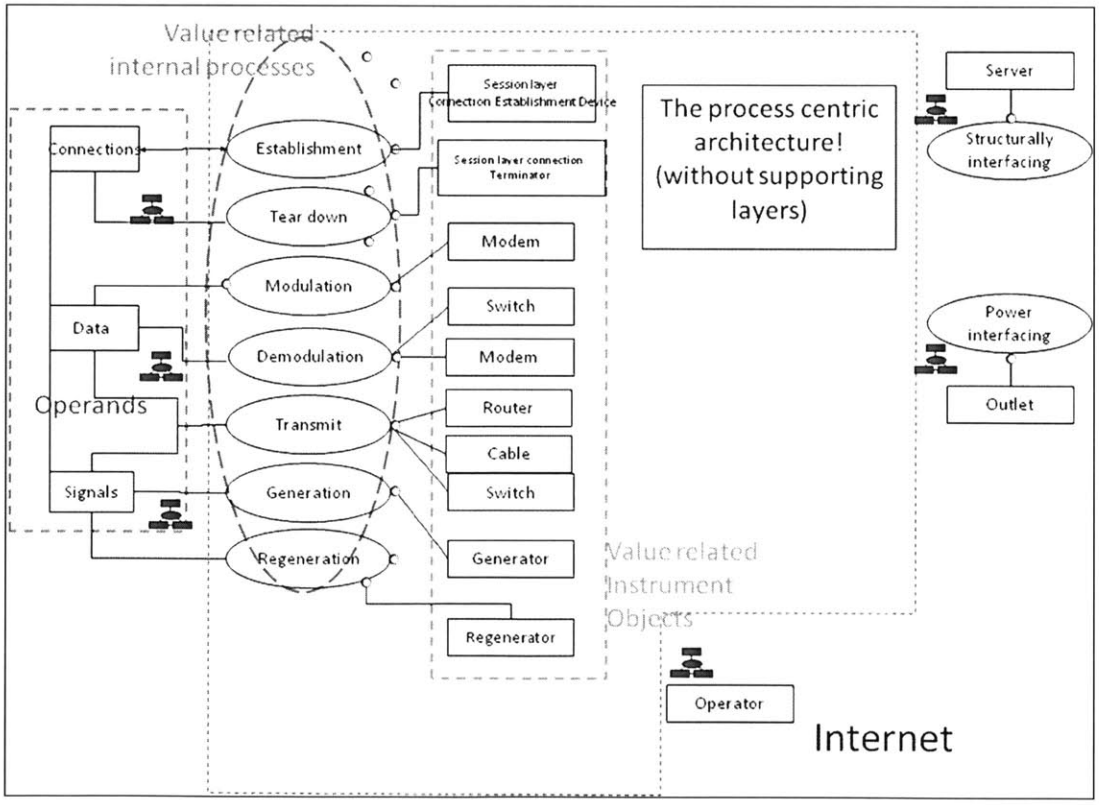

Figure 27: Map of Internet System Processes from Iheagwara C. et al. (2010).

Figure 27 illustrates that value related instrument objects (device) makers such as Cisco Systems that make the routers and others that builds the applications or provided the infrastructures that are part of the Internet system have responsibilities for securing the system.

In Section 5.5, we provide a description of four categories of Internet stakeholders.

5.4 Internet Infrastructure and Service Providers

Clearly, the process centric architecture (Figure 27) shows that there are different vested stakeholders. Going by system design, there are four primary groups of stakeholders. The several infrastructure devices identified for the process include routers, switches and modems that transform the data and move them from one location to another.

Given this, we categorize the infrastructure and service providers into four distinctive groups:

First, the category 'Internet System Architects and Designers' serves as the originator of the Internet and includes the IAB, IETF, and IRTF. Second, at the connection end are the Internet service providers (ISPs). Third, is a group of Internet infrastructure providers. This category includes:

(i) internetworking device providers like Cisco Systems who typically provide connection equipments (routers that operate at the Internetwork layer of the TCP/IP) that directly or indirectly control, manage and co-ordinate the transaction process for their customers, and

(ii) direct manufacturers of Internet hardware like backbone Servers and services. Fourth, the final group consists of Internet application and hardware developers that develop the applications that runs on the Internet and manufactures the hardware that hosts the applications.

Internet System Architects and Designers

The IAB (Internet Architecture Board) - the Internet Society is the overseer of the technical evolution of the Internet; and supervises the Internet Engineering Task Force (IETF), which is tasked with overseeing the evolution of TCP/IP, and the Internet Research Task Force (IRTF) which works on network technology, defines the Internet Architecture as "a meta-network, a constantly changing collection of thousands of individual networks intercommunicating with a common protocol."

Internet Service Providers (ISPs):
An important stakeholder in the Internet system process is the ISP, who provides the fundamental internet access services to both senders as well as recipients. Internet Service Providers have become a critical component of the commercial Internet providing customers Internet access, web hosting services, e-commerce technologies, and email access. According to the Electronic Commerce (EC Directive) Regulations 2002, ISPs are 'mere conduits' and as a result are not liable for the content of information they transmit through their networks. There is

a general argument that ISPs need to be the first line of defense in combating Cyber attacks. For example, the Internet Engineering Task Force's (IETF) Network Working Group has developed protocol standards (RFC 2871) and best practices (RFCs 2505 and 2635) for ISPs to follow in order to help reduce spam. These standards require ISPs to prevent their mail servers from being used by unauthorized third parties to relay e-mails and to provide sufficient information in e-mail headers to make it possible to verify the source of e-mail.

Internet Infrastructure Providers

This group is engaged in the business of providing connection equipment like routers and switches that work at the Internet layer of the TCP/IP protocol stack. Often called the Internet plumber, Cisco Systems is the dominant player here. They maintain customer contact databases and engage in commercial communication on behalf of other merchants and marketers. The growth of the Internet has been attributed to the several technologies and enabling infrastructures developed by this group.

Internet Application Developers and Hardware Providers

This group includes those who develop the software applications and hardware devices that are used directly by online customers and system integrators who provide software coupling and system integration services. Hewlett Packard, IBM, Microsoft Corporation, Oracle Corporation and a host of other companies belong to this group.

Figure 28 shows is a composite ecosystem of the Internet Infrastructure integrating different ISPs, Domain Systems, Applications, etc.

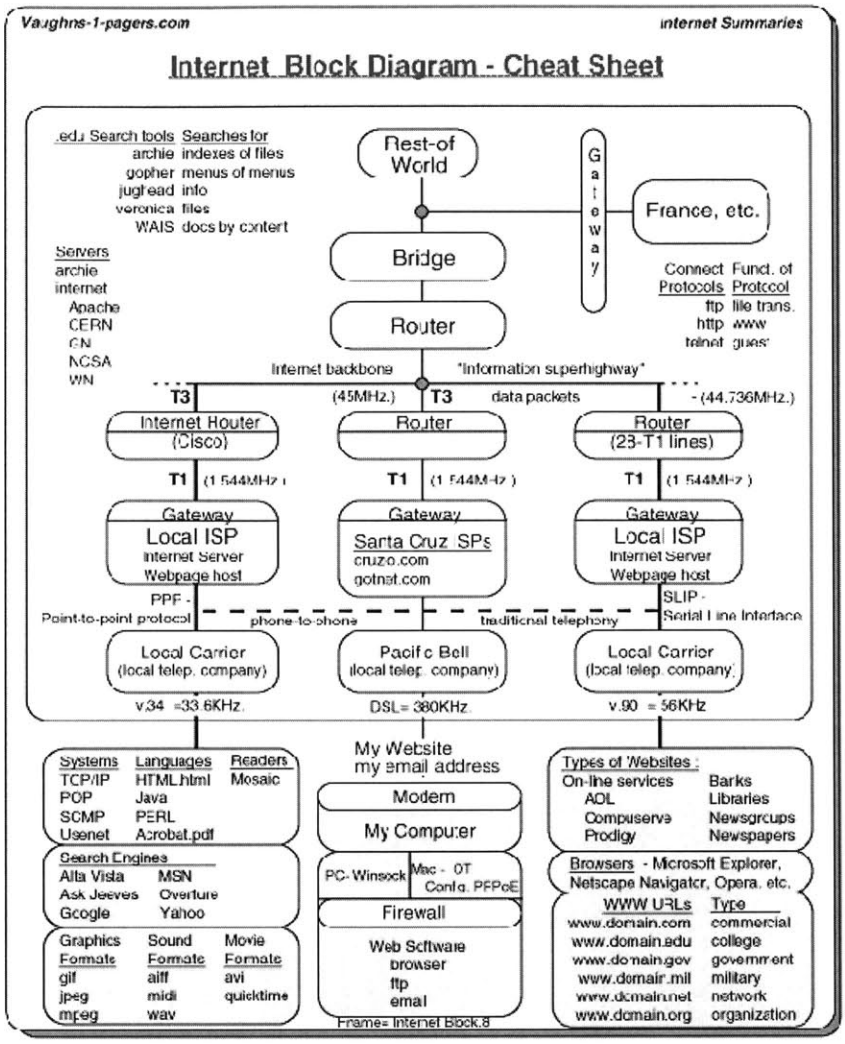

Figure 28: Typical Internet System Infrastructure.[35]

In the next Section we conduct a Stakeholder Beneficiary Analysis to discern the stakes and needs of the current Internet system.

[35] http://www.vaughns-1-pagers.com/internet/internet-diagram.gif

5.5 Internet Stakeholder Beneficiary Analysis

Needs is common to both the stakeholder and beneficiary in the Internet system. For the **Beneficiaries,** the Internet output is their needs, and the **Stakeholders** in return generate revenues and other needs from the beneficiaries. There is, therefore, mutual interdependence as both have an outcome or output which addresses each other's needs that must be considered.

In Tables 10 and 11 below we present the stakeholders analysis. Two major types of beneficiaries are illustrated in Table 10:

- **Direct beneficiary** - the primary beneficiary is anyone who sends or receives information or communicates using the Internet. The benefit that flows to them is the message/information/data that is transmitted including emails, downloads, etc. In other words the communication that flows through the system. Equally, the ability to have instant access to a wide variety of information/data on the Internet is an accruable benefit.

- **Indirect beneficiary** - the indirect benefits are those derived from the enabling utilities of the Internet such as **e-Commerce**. As a result of the Internet and its enabling infrastructures, many companies now conduct business on the Internet. Examples are eBay and Amazon. Also, almost all companies now have **Web sites** that describe their business. These would not have been possible without the Internet.

Table 10: Internet System Stakeholders and Beneficiaries [34].

Stakeholder (Those who have a stake in the Internet services; and have an outcome or output which addresses beneficiary's needs that are important.)	**Internet Output/Outcome**	**Direct Beneficiary** (Those who benefit directly from Internet Output)	Indirect Beneficiary (Those who benefit indirectly from Internet Output)
Internet Service Provider (ISP) - Qwest Communications	Internet connection	Connecting Entities i.e. corporations	Regulator (FCC); Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Verizon Communications	Telecommunications (i.e. Telephony service)	Subscribers, customers, etc.	Regulator (FCC); Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Web Hosting Provider – Ipage	Messaging i.e. email	Corporate users i.e. email Users: • Employees • Contractors • Business Partners	Regulator (FCC): eMessaging Software Vendors i.e. Microsoft (for Outlook; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Budget Conferencing, Skype	Teleconference/Telemeeting	Corporate users i.e. email Users: • Employees • Contractors • Business Partners	Regulator (FCC): Collaboration Software Vendors; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Facebook, LinkedIn, etc	Social Networking	All subscribing Internet Users including corporate employees	Regulator (FCC); Social Networking Software Vendors i.e. phpFox; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
eBay, Amazon, etc	Online Marketing	Consumers	Regulator (FCC); Auctioneers; Publishers
Media organizations, e.g. CNN	News& Information	General Public	Regulator (FCC); Cable Technology vendors
Media organizations, Walt Disney	Online Entertainment	Consumers	Regulator (FCC); Artists, Comic, Film Makers, etc.
Colleges	Educational Services (Distance Learning)	Students	US Dept of Ed; Teachers, Publishers, Book stores, etc.
Citibank, BOA, etc	Online banking & financial services	Clients/Customers	FDIC
Etc.	Etc.	Etc.	Etc.

Notes: Given the complexity of the Internet system, the growing needs, uses, technologies and others that have converged on it, Table 10 is only a partial listing of the stakeholders and beneficiaries as they are still and constantly evolving.

Table 11 presents stakeholder and beneficiaries needs.

Table 11: Internet System Stakeholder -Beneficiary Needs Analysis [34].

Stakeholder →	Need	Need →	Direct Beneficiary Stakeholder	Need →	Indirect Beneficiary Stakeholder
Internet Service Provider (ISP) - Qwest Communications Verizon Communications	Customers Revenue (Stream) Providing Constant and high-quality Service	Internet Connection Uninterrupted service	Internet service subscribing or connecting entities i.e. Unatek, Inc.	Acceptable Internet usage Protection of society from Internet abuse and predatorial activities Customers Revenue	Regulator (FCC); Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Verizon Communications	Telecommunications Customers Revenue (Stream) Providing Constant and high-quality Service	Telephone services (tele, fax, cell, etc.) Affordable Plan High-Quality Service	Subscribers, customers, etc.	Acceptable Telecom usage Protection of society from Internet abuse and predatorial activities Customers Revenue	Regulator (FCC); Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Web Hosting Provider – Ipage .	Website hosting Customers Revenue (Stream) Providing Constant and high-quality Service	eMail services Low cost Constant Availability High-quality	Corporate users: Employees Contractors Business Partners	Acceptable Internet usage Protection of society from hosting abuse and predatorial activities Customers Revenue	Regulator (FCC): eMessaging Software Vendors i.e. Microsoft (for Outlook; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Budget Conferencing, Skype	Internet Video Streaming Teleconferecing	Video conferencing Teleconferencing	Corporate users Students Teachers	Acceptable Internet usage Protection of society	Regulator (FCC): Video/Telecon

	Customers Revenue (Stream) Providing Constant and high-quality Service Revenue (Stream)				from telecon abuse and predatorial activities Customers Revenue	Software Vendors i.e. Skype; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
Facebook, LinkedIn, etc	Customers Revenue (Stream) Providing Constant and high-quality Service		Social Networking Messaging Group discussions Group Forum Advertisements	All subscribing social networking Users such as individuals, corporate account users, social groups, etc.	Acceptable usage of social networking Protection of society from abuse and predatorial activities Customers Revenue	Regulator (FCC); Social Networking Software Vendors i.e. phpFox; Internetworking Vendors i.e. CISCO, NOKIA, AVAYA, etc.
eBay, Amazon, etc	Online Marketing Customers Auctioneers Retail Outlets Distribution Channels Merchandise Suppliers Revenue (Stream)		Goods, Merchandize and products of all sorts	Online Consumers	Acceptable e-Commerce usage Protection of society from abuse and predatorial activities Prevention of online e-Commerce scams Customers Revenue	Regulator (FCC); US Dept. of Commerce Auctioneers; Publishers
Media organizations, e.g. CNN	Network Television Viewers/consumers Advertisers Revenue (Stream) Clients Show promoters Entertainers Film makers		News Entertainment	Viewers/consumers	Acceptable mass media usage Protection of society from abuse and predatorial activities Customers Revenue	Regulator (FCC); Cable Technology vendors
Colleges	Long Distance Learning Revenue (Stream) Students		Education	Students	Acceptable Internet usage Protection of society from abuse and	US Dept of Ed; Teachers, Publishers, Book stores, etc.

						predatorial activities Colleges Students Customers Revenue	
Citibank, BOA, etc	Online Banking Revenue Customers			Clients/Customers		Prevention of online banking fraud Protection of society from Internet abuse and predatorial activities	FDIC
Etc.	Etc.		Etc.	Etc.		ETC	Etc.

Notes: Table 11 is only a partial listing of the still and constantly evolving needs of the Internet system stakeholders and beneficiaries.

5.6 Summary

In this Chapter, we have conducted a stakeholder-beneficiary analysis of the Internet system and have discerned stakeholder intent and goals evident in the original design and the security requirements mandated for the system.

Based on our analysis, we note that there is an expressed mandate for a process architecture that includes security and that the current design leaves this out. We delineated the different value related processes and instruments used to execute processes. Interestingly, the value related instruments such as routers, switches and other routing devices have become part of the internet massive infrastructure outlay and those that did not address security of the system have also become a bane of the process.

Finally, we conclude that stakeholders have the primary responsibility of assuring security on the system in a collaborative fashion.

Chapter 6: Strategic Implications of the Current Internet System Architecture Flaws on Cyber Security

In the preceding Chapters we explored Cyber security from several viewpoints and provided a description of Cyberspace, analyzed the Internet architecture and its inherent weaknesses that are exploited and serves as the conduit to launch Cyber attacks. We also discussed the different types of well-known Cyber attacks, how they are monitored and analyzed, attempted to quantify each type as a percentage of the overall Cyber attacks and then mapped specific attack types to the Internet architecture layer where they occur. Additionally, we conducted a stakeholder analysis of the Internet system from a design standpoint and established that it is a design intent that security be implemented on all connections and transmissions taking place over the Internet medium otherwise known as Cyberspace and that all stakeholders share a responsibility in ensuring that.

All of the above and the other issues explored and discussed in the preceding Chapters provide the impetus, background and the basis to derive the following strategic implications of the current Internet design for Cyber security.

6.1 Implications Number One: Unfulfilled Stakeholder Intent

In Figure 26, it is noted that one of the solution neutral functions of the Internet is to safely transmit transactions. As an engineering statement, this embodies an expressed stakeholder intent that requires the system to guarantee safe delivery of transactions which occur over it.

Secure or safe Internet transaction has been interpreted by different groups and people to mean different things. As was noted by David Clark (from Iheagwara C. 2010)[36], there are issues that revolve around defining security in the context of sender-recipient. Privacy, Safety, Integrity, Confidentiality, and even availability have been used by the different interest groups to denote and define Internet security to suit their purpose. Hence, there is no agreement on what constitute security and for that matter, the scope and extent that will be acceptable as adequate for Internet transaction.

What is obvious is that secure transmission of Internet transaction embodies an essential requirement of the design. The lack of which negates the stakeholder intent and gives rise to the multitude of Cyber security issues.

Satisfying the stakeholder intent requires addressing the issues as there is no "silver bullet" solution for the myriad of Cyber security issues unless stakeholders collaborate to address security to enhance trust and confidence of users in networks, applications and services. A wide range of questions bring the issues front and center and have far reaching implications if not addressed.

[36] Iheagwara, C. (2010), Interview with David Clark, MIT, December 14, 2010.

For example:

- With global cyberspace, what are the security priorities for the Internet stakeholders with the government / private sector partnership and users?
- Is there a need for top-down strategic direction to complement bottom-up, contribution-driven process?
- Can a balance be established between centralized and distributed efforts on security standards?
- Who assume responsibility for legal and regulatory aspects of Cyber security, spam, identity/privacy?
- Can stakeholders collaborate to address full cycle – vulnerabilities, threats and risk analysis; prevention; detection; response and mitigation; forensics; learning
- Can they agree uniform definitions of Cyber security terms and definitions?
- Can they work towards the full integration of and acceptance of marketplace Information Security Management System (ISMS) standards (ISO/IEC 27000-series and ITU-T X.1051) – the security equivalent to ISO 9000-series?
- Can an effective cooperation and collaboration across the many bodies doing Cyber security work?

Ultimately, the lack of or inadequate cooperation among various stakeholders to address the issues will result into inability to create the necessary security architecture and framework.

6.2 Implications Number Two: Ad-hoc Solutions and Expediencies have become the Order of the Day (with constant patchwork and fixes)

Willinger et al. (2002) implies the original design objectives of the Internet specified a set of first and second-level objectives - on to how to make the Internet design more effective. Quoting from [26], these requirements are (in decreasing order of importance):

- Robustness: Internet communication must continue despite loss of networks or gateways/routers.
- Heterogeneity (Services): The Internet must support multiple types of communications services.
- Heterogeneity (Networks): The Internet architecture must accommodate a variety of networks.
- Distributed Management: The Internet architecture must permit distributed management of its resources.
- Cost: The Internet architecture must be cost effective.
- Ease of Attachment: The Internet architecture must permit host attachment with a low level of effort.
- Accountability: The resources used in the Internet architecture must be accountable.

Further, Willinger et al. (2002) states "The intent of the two tier requirement specification was based on the need to architect a network of networks and make for flexibility for the complex systems that comprise the architecture. Thus, while the top-level requirement of internetworking was mainly responsible for defining the basic structure of the common architecture shared by the

different networks that composed the "network of networks" (or "Internet" as we now know it), this priority-ordered list of second-level requirements, first and foremost among them the robustness criterion, has to a large degree been responsible for shaping the architectural model and the design of the protocols (standards governing the exchange of data) that define today's Internet. This includes the Internet's well-known "hourglass" architecture and the enormously successful "fate-sharing" approach to its protocol design."[37]

Impliedly, the design principles did not mandate "security" as a requirement and contradicts the stakeholder's intent to transmit data or information securely. This may well account for the lack of basic "Authentication" security requirement that provides the system the ability to authenticate. In addition, lacking are several platforms including the platform for:

- Security architecture aspects of end users and networks in routing
- Extensible Authentication Protocol (based Authentication and Key Management) in a Data Communication Network
- Specifying protocols and procedures that support functions of the password Authentication security dimension (Password-Authenticated Key Exchange Protocol (PAK))
- Framework for creation, storage, distribution and enforcement of policies for network security.

These are just a few of the platforms which need to be addressed for effective security enforcement on Cyber space.

As discussed in Chapter 2, the Lack of Extensible Authentication Protocol based Authentication and Key Management in a Data Communication Network is a big problem. The current design did not address or specify a protocol, which would ensure mutual authentication of all parties in the act of establishing communication and exchanges; and therefore cannot contain or abate emerging threats as ad-hoc solutions have limitations and are no silver-bullet solutions.

All these complicates the task of securing Cyberspace and is compounded by the fact that over the years, the originally simple communications technology have increasingly become complex; more fragile and difficult to manage with each passing day just as Internet applications grew both in product and service mix with wireless devices, peer-to-peer file-sharing, telephony and others even as companies and network engineers resort – and sometimes in desperate fashions – to coming up with ingenious and expedient patches, plugs, and workarounds.

---

[37] Computer Science and Telecommunications Board (CSTB), National Research Council. The Internet's Coming of Age. National Academy Press, Washington, D.C., 2001.

In the face of this, many experts in the field are proposing rethinking the way the Internet works. For example, Clark argues (from Talbot, 2005) that "it's time to rethink the Internet's basic architecture, to potentially start over with a fresh design -- and equally important, with a plausible strategy for proving the design's viability, that we somehow failed to include," says Clark. "We need so that it stands a chance of implementation."It's not as if there is some killer technology at the protocol or network level to take all the technologies we already know and fit them together so that we get a different overall system. This is not about building a technology innovation that changes the world but about architecture -- pulling the pieces together in a different way to achieve high-level objectives."

6.3 Implications Number Three: Constantly Evolving New Threats and Threat Vectors

Talbot (2005) asserts "Cyber-Security threats are always evolving around Internet system weaknesses including software/hardware/link vulnerabilities; with hackers, spammers and other forms of online criminality adapting to the changing security environment of business networks exploiting the weaknesses. The effect is an exponential growth and overlapping deluge of cyber-attacks on governments and companies being targeted by criminals and nation-states seeking economic or military advantage becoming so large that those responsible for security are having trouble identifying which new threats should take priority in their threat management regimes."

All available data and statistics on Cyber security supports Talbot's assertion and points to the increasing magnitude and scope of the emerging new threats exploiting Internet weaknesses to launch new forms of Cyber attacks. Figures 29, 30 and 31 accurately illustrate the trend and it is doubtful that ad-hoc solutions are going to abate or slow the trend.

But, it is worthy to note that the exponential growth and overlapping deluge stems from the lack of any Internet security authentication mechanism; and the emergence of Bot- network (a collection of malicious software agents, or robots, that run autonomously and automatically) operations is the single most important driver for this exponential growth.

.

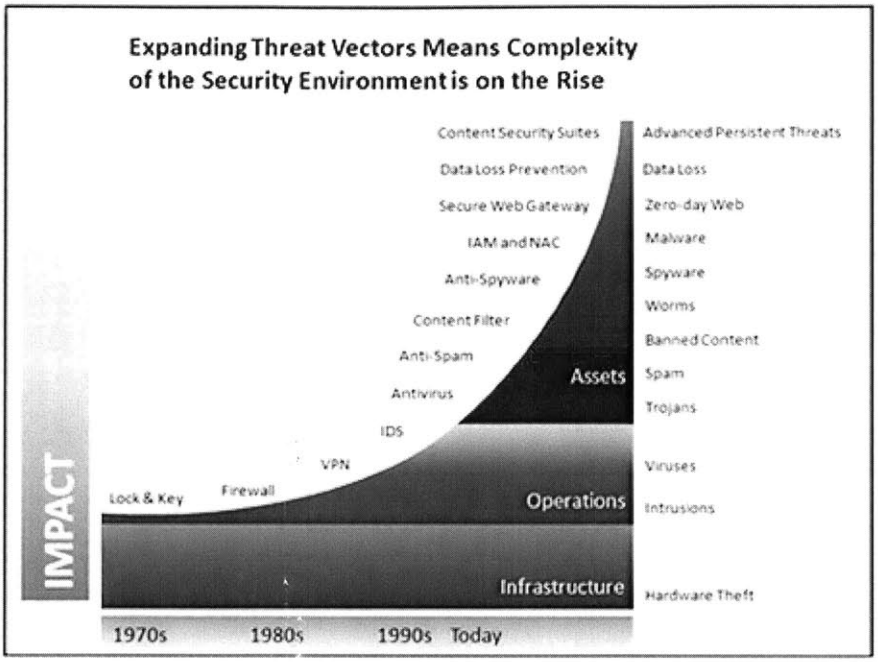

Figure 29: Nine Sources of Emerging Cyber security Threats.[38]

Lipson H. (2002)[39] provides an excellent summary of cyber attacks over time, as reproduced in Figure 30.

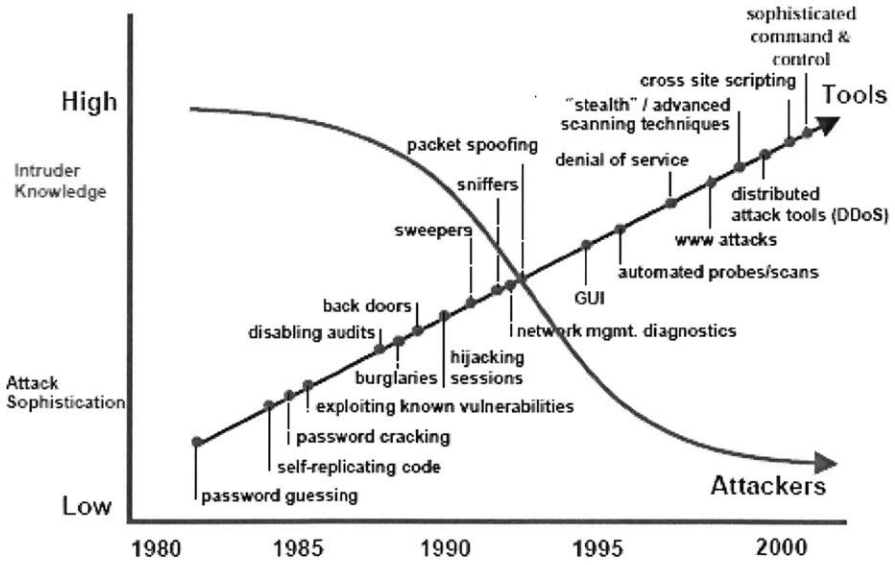

Figure 30: Sophistication of Cyber Attacks and Attackers over Time, from Lipson (2002).

---

[38] Cyber Crime Report. http://securingourecity.org/blog/#. Last checked August 2010.

[39] Lipson, H (2002), "Tracking and tracing cyber attacks: technical challenges and global policy issues." Technical Report CMU/SEI-2002-SR-009, Carnegie Mellon University, 2002. Accessed at http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02sr009.pdf.

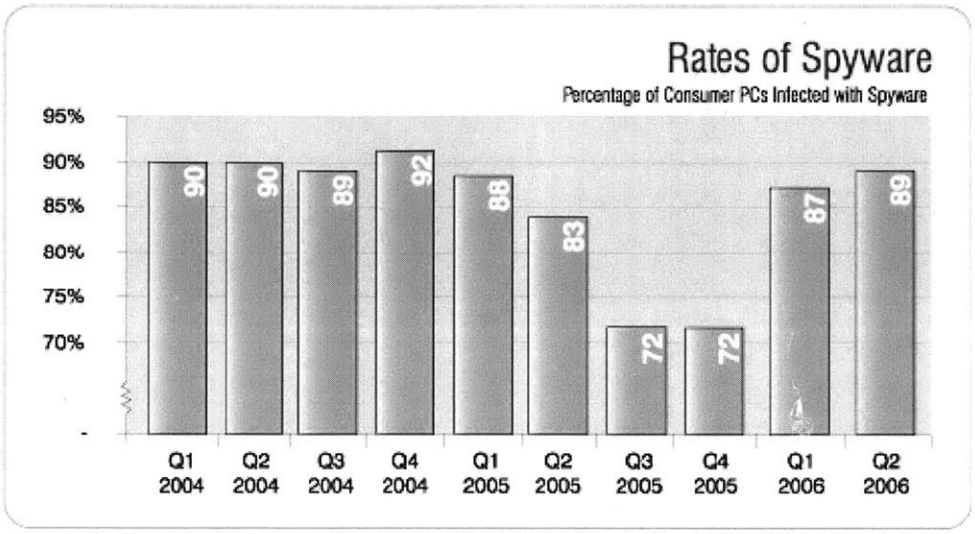

Figure 31: Spyware Infections from 2004 – mid 2006.[40]

In the end, the implication is that organizations and online users will increasingly continue to devise schemes and ad-hoc solutions to deal with the new threats until the issues identified are resolved and the Internet is given the ability to authenticate.

6.4 Implications Number Four: The Emergence of the Underground Economy

An entire underground economy has been built by Cyber criminals for the purpose of stealing, packaging, and reselling electronic information and data. This economy consists of online black market forums formed for the purpose of promoting and trading stolen information and services. The infrastructure that powers the economy is a fairly extended network of well-built Servers powered by Bot-net and other technologies and operated using remote Internet access to corporate systems, embedded malware in computers, applications and devices and with little visibility into the security protocols of suppliers and business units.

While the emergence of the underground economy may be considered another threat agent, its rapid growth is a pointer to the difficulties and inability of the current Cyber security practices to contain, slow down or eliminate the economy altogether.

Symantec Quarterly Intelligence Report (see Table 12) presents statistical data on the Underground Economy. According to the report, the most frequently advertised items for sale observed on underground economy servers, was credit card information, accounting for 28 percent of all goods. A host of very private and personal items such as bio-data or personal identity data are also available.

---

[40] State of Spyware Q2 2006. Webroot Software, Inc. (2006, June). http://www.webroot.com/resources/stateofspyware/excerpt.html. Last checked June 17, 2010.

Table 12: Goods and services available for sale on underground economy servers [24].

Rank	Item	Percentage	Range of Prices
1	Credit cards	28%	$1 - $30
2	Bank accounts	24%	$10 - $125
3	Email accounts	8%	$5 - $12
4	Email addresses	5%	$5 - $10 per MB
5	Credit card dumps	4%	No specified prices
6	R57 & C99 shells	3%	$2 - $5
7	Full identity	3%	$3 - $20
8	Mailers	3%	$1 - $5
9	Attack toolkits	3%	$5 - $20 or $120 per month
10	Cash-out services	2%	$200 - 100 or 50% - 70%

While the net effect might not necessarily be the lost of material possession, the divulging of very private and personal information to a public that has yet come to terms – but will with time - with the negative implications that in all certainty will expand in scope in time and present more difficulties.

The other attendant effect which will most definitely increase with time is the cost associated with enhancing and developing new security measures and the collateral cost incurred when networked and system assets are compromised through underground economy attacks.

6.5 Implications Number Five: Cyber Security has become a Business Process

The plethora of Cyber security problems discussed in the preceding Sections has made Cyber security a business process in the enterprise. And, the diversity of Cyber security problems, scope and magnitude of efforts required to cope with emerging threats are undoubtedly the driver of most new Cyberspace security initiatives and counter measures.

As a result, several practice areas have sprung up as lucrative businesses to service the expanding Cyber security industry. For example, Computer Forensics Investigations and Incident Response, Certification and Accreditation, FISMA compliance, Continuous Monitoring, Identity Management, etc are among the many areas of security practices organized as business units in the multi-billion dollar Cyber security industry.

Echoes of what this means are abundant and have come from both government leaders and corporate executives. Many in the industry now regard security as the "Third (3^{rd}) Estate of the Realm" for the IT industry. Or as Intel CEO Paul Otellini put it (from Talbot, 2005) - in the wake of the consolidation taking place with security vendors - "We have concluded that security has become the third pillar of computing." and he questions "Vendors are seeing a big shift in security, what about enterprises? The answer is that enterprises have also shifted gears and made significant progress in Cyber security practices since the question was posed – although at a colossal economic cost. Several federal security mandates such as HIPAA, GBLA, SOX,

FISMA and commercially developed standards have been implemented as part of the process by almost all institutions and commercial entities.

Consequently, Cyber security has now become an integral part of and can't be separated from business operations as security teams are organized into business lines around the new enterprise with new mandates, approaches their roles and dispositions. Echoing the words of Paul Otellini (from Talbot, 2005) "in the past, a CIO's role was laptop distribution. Today, CIOs build supply chains. In the past, CISOs distributed anti-virus and set up firewalls. Today, they must know where data resides, where it moves and how to protect it, which requires a serious, comprehensive data security practice. This means security teams need to become business process experts to keep the bad guys disarmed while keeping the good guys productive."

6.6 Implications Number Six: Limitations in Designing and Introducing Effective Cyber Security Solutions

Securing an enterprise network system is becoming increasingly complex due to several factors one of which is the changing network and system conditions. Traditionally, network infrastructures were developed and fostered in a collaborative non-hostile environment and were built upon assumed trusts which were conducive to sharing with minimum security - if any. But today, a huge stock of and multitude of software products have been developed with significant insecure coding across all platforms makes it impossible to develop uniform security systems. The UNIX (and its variation Linux), Windows and Mac systems applications are developed with different requirements and address different needs. Also, a host of software applications are developed for different needs, in different environments and platforms and operate at different layers of the TCP/IP protocol suite making hardware and software integrating security difficult especially with no security platform in the current Internet design to address Vulnerabilities.

Consequently, the plethora of networking, software, hardware and other Internet infrastructure development some of whose requirements run counter to security only signify the difficulties encountered to develop a common platform security solution. A case in point is intrusion detection and prevention devices that took more twenty (20) years to be perfected to their current state and still do not address all security issues they were designed to address.

While there is no short term answer, research and development coupled with proper funding and effort is needed to solve infrastructures security problems in the long-term. Going by the industry trend, this will be achieved as an evolutionary path over time, incorporating new security solutions and methods to achieve proper security base levels needed to protect the data flowing over the infrastructures. Also, Internet system stakeholders should consider a separate, future work item to investigate and explore the issues of creating a secure network infrastructure.

6.7 Implications Number Seven: Fusion of Information Technology with Telecommunication Imposes Extra Burden and Additional Requirements

The fusion of telecommunication with information technology is creating so many opportunities for the twenty-first century computing. And with it, have come several new products, technologies and processes both for the wired and wireless world. The latter being a post-Internet design technology. Increasingly, we have seen billions of wireless devices being deployed for telephony, corporate business use with Business Process Outsourced services, teleconferencing and instant messaging and for other purposes by billions of users worldwide. This has given rise to one area of concern, the inevitable introduction of Cyberspace security issues by the convergent communications technologies, networks and infrastructure that were not evident during the original Internet design.

Consequently, what we are dealing with is connection of different components, systems, sub-systems, processes and technologies with different degrees of security – and in some cases, none at all. The implication is that if a non-secure infrastructure is connected to a secure infrastructure, the result is a weakened secure infrastructure, not an increased secure infrastructure for the non-secure side.

Security is said to be as strong as its weakest link. A case in point is the converged networks (video, audio, data), where the interconnectivity of networks with security architectural deficiencies will allow those security-weak networks to affect the converged network (from Talbot, 2005). The effect is that the converged networks may have serious security problems from the inception, left over from previous security issues that were not dealt with or solved.

Equally, converged networks with improper security controls will allow improper access to a wider range of network resources than today's isolated networks. An example is classic analog voice networks that have unique protocols and connection methods which are typically expensive and difficult to connect to without specialized equipment, protocols and access. With Voice over IP (VoIP), however, the ability to use any TCP/IP network with enough speed means that voice traffic can converge with data traffic over a singular network. It also means that the previously isolated voice traffic is now on a more available network with its own set of security problems that can now effect, negatively, the voice traffic used by the vendor, supplier or customer. With this simple example of convergence, it can be seen that while the resulting network may save on transport costs for providers, the security implications become rather serious for the voice side of the deployment where they were previously not as serious a matter due to the difficulty in connectivity of voice methods in an analog connection methodology.

As a result, many new threats will emerge with new lethal and potent attack vectors.

6.8 Implications Number Eight: Limited and Easy Entry Barriers for Criminals

Talbot (2005) asserts that there is an unarguably very Low entry barrier for cyber-criminals. This results from several factors – both technical and non-technical. The barriers could be the legal and non legal restraints on those aspiring to become Cyber criminals.

First, there is the legal aspect. Many nation states lack the legal instruments to prosecute Cyber criminals. In fact, some support the cause of Cyber terrorists. Even for the nations that have implemented the legal framework, prosecution is hardly easy and often so many Cyber attacks with significant evidence are never prosecuted and if there was ever a prosecution fails in the courts that have often weighed on the privacy side more in favor of the perpetrators. Also, it is extremely difficult to collaborate amongst nation states because of nuances related to jurisdictions.

Second, the technical barrier is very weak as professional hackers, crackers and kiddies are skilled in the art of breaking into networks bypassing the security controls in place. There are many reasons for this including the fact that many in the field (developers, security professionals, etc.) can effectively become the bad guys for financial, revenge or other reasons. Also, the technologies from which the codes are written are easily available.

According to the Computer Security Institute/FBI report about two-thirds of all attacks are internally driven and the perpetrators are in most cases the developers, security professionals and others who have internal and intimate knowledge of the business process.

6.9 Implications Number Nine: Increased Risks of Cyber Attacks and Warfare on National and Transnational Infrastructures

The infrastructure systems of many nations are now linked to the global Internet network system. Power generation plants, mass transit systems and other important national and international infrastructures now sit on the Internet grid. These infrastructures have in effect become complex networks and associated with critical systems of national and transnational entities.

Both, there is the issue of securing them as they were never built with any planned security considerations sophisticated enough to effectively counter Bot-net onslaughts even with implementation of extremely complex security methods that does not go far enough and only produces base-level security protection for the connected networks, systems and applications.

And with the different stakeholders not able to mount a strong united front for various marketplace reasons, proper long-term security of connected components will not be achieved until there is substantial planning and investment for an architectural evolution of the national infrastructure with security platforms that are able to proactively contain emerging threats of all types.

Although, implementing Cyber security on some of the systems is an arduous task whose adequacy could fall far short of what is required to contend the threats from Cyber criminals, in many cases, proper infrastructure security will not be achieved with the existing network infrastructure due to original design precepts of all connected entities being trusted. As has been discussed and demonstrated in the preceding Sections of this Thesis many current Internet protocols, hardware, software and other associated components do not have any method of properly being secured against current threats (much less future ones) and provide a great number of inherent security vulnerabilities that cannot be solved with existing security solutions. This means that even after application of the Cyber security best practices (BPs), the infrastructures will remain at risk to Cyber attacks for which BPs cannot stop due to protocol architecture or other issues that cannot be solved by BPs.

The President's Information Technology Advisory Committee report[41] issued in early 2005, notes: "Today, the threat clearly is growing." "Most indicators and studies of the frequency, impact, scope, and cost of cyber security incidents -- among both organizations and individuals -- point to continuously increasing levels and varieties of attacks."

Many leading experts contend that Cyber terrorism is at infancy. In 2005, Richard Clarke, White House Cyber Terror Czar predicts the dawn of "the real act of cyber terror", the "digital Pearl Harbor" a phenomenon likened to a time bomb slowly building up to explode later. He gave a classic example of the nation's electrical grid that relies on continuous network-based communications between power plants and grid managers to maintain a balance between production and demand that a well-placed attack could trigger a costly blackout that would cripple part of the country.

The conclusion of the advisory council's report could not have been starker: "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects."

The Internet system functions as well as it does only because of "the forbearance of the virus authors themselves," says Jonathan Zittrain (from Talbot, 2005), who cofounded the Berkman Center for Internet and Society at Harvard Law School and holds the Chair in Internet Governance and Regulation at the University of Oxford. "With one or two additional lines of code...the viruses could wipe their hosts' hard drives clean or quietly insinuate false data into spreadsheets or documents. Take any of the top ten viruses and add a bit of poison to them and most of the world wakes up on a Tuesday morning unable to surf the Net -- or finding much less there if it can."

Also, Jonathan Zittrain asserts that the environment and elements that could trigger the "Digital Pearl Harbor" are building up and recent Cyber security events points to that direction. The statistical evidence presented in Section 4.2 demonstrates that national and transnational infrastructures are extremely prone to DoS and DDoS attacks amongst other.

---

[41] President's Information Technology Advisory Committee: "Cyber Security: A Crisis of Prioritization", Report to the President, February, 2005.

Consequently, due to lack of Internet security architecture and base security capabilities in the infrastructures or lack of appropriate technologies to solve security problems that exist in the infrastructures, national and transnational infrastructures are heavily prone to Cyber attacks.

6.10 Implications Number Ten: Existing Internet Infrastructure is an Impediment to New Technologies

The Internet's basic flaws cost firms billions, impede innovation, and threaten national security. "It's time for a clean-slate approach" says MIT's David D. Clark (from Talbot, 2005).

The existing Internet architecture might not fuse well with and therefore stand in the way of some new technologies for various reasons including the entirely different communication requirements of some newer technologies such as networks of intelligent sensors used in to collectively monitor and interpret data/information related to factory and weather conditions, video images, etc.

Equally, as embedded content computing increasingly become a commonplace, different Internet security architecture will be required to integrate them. It is also quite conceivable that future network and internetwork designs will be different from the current and earlier PCs to PCs, PCs to mainframe networks. All of which will create integration or interoperability problems.

6.11 Summary

Based on the facts and inferences from our discussions and analysis in the preceding Chapters, we have deduced several implications for Cyber security arising from the current Internet architecture vulnerabilities.

Primary among them are the implications for a potential Cyber warfare on nations and transnational infrastructures; constantly emerging threat and attack types that extends the security domain and perimeter of the enterprise, the emergence of a new underground economy where Cyber war lords rule over Cyberspace and aided with low entry barriers and with sophisticated Bot-net technologies are able to wreck havoc on any intended target.

These and the other implications are gradually building up to what may potentially become a useful arsenal for Cyber warfare for rogue nations.

Finally, we conclude that the primary constraint in achieving effective counter measures against current and emerging Cyber security threats is the lack of any authentication mechanism on the Internet system that could serve as the anchor around which an effective Cyber security practice can be built and mounted.

Chapter 7: Conclusions and Recommendations

7.1 Conclusions

In this thesis, we have reviewed the background information related to the Internet as a medium that connects millions of networks and users for the purpose of communicating and conducting transactions over it; analyzed the current Internet design and the flaws in the current Internet architecture; described Cyberspace and the security problems that plagues the system; and conducted a stakeholder analysis of the Internet system.

Additionally, we analyzed several research studies and Cyberspace monitoring reports and interpreted the statistical data documented on Cyber attacks and using this developed a grid that maps each Cyber attack type to specific Internet architecture layer.

Based on all the facts and information available, we derived several strategic implications of the current Internet design for Cyber security.

From the studies, we draw the following conclusions:

1. Based on the analysis, extrapolation of facts and by inferences we assert that the myriad of Cyber security problems will remain and continue on the current exponential growth path until the Internet and in particular the TCP/IP stack is given the ability to authenticate and that only through a collaborative effort by all stakeholders of the Internet system can the other major Cyber security issues be resolved especially as it relates to envisioning and fashioning new Cyber security technologies

2. Although a robust design, the current Internet system has several architectural flaws primary of which is lack of in-built authentication platform that has given rise to virtually all kinds of Cyber attack types described in Appendix 1 and mapped in Figure 21

3. The scope and nature of the Cyber attacks observed today will continue to grow exponentially unless the Internet is re-designed and coupled with an architecture that provides several platforms that addresses different areas of security including authentication

4. The /IP layer serves as a major conduit for several types of Cyber security attacks and has implications for stakeholder responsibilities that provide the Internetworking and routing devices that function at this layer

5. The Application layer is the source of newer Cyber attacks and constitutes a significant growth area for Cyber attacks due to the fact that most of the applications coupled to this layer were developed without security in mind

6. The emergence of Bot-net technologies has incubated a new type of underground economy that is a breeding ground for Cyber criminals and has an unmatched potential to inflict heavy catastrophic damage on the economy and of many organized business entities, nations and transnational organizations

7. There is a great potential for an increase in the scope and magnitude of massive and devastating Cyber warfare on critical national and transnational infrastructures unless the Internet system vulnerabilities are mitigated

Finally, we conclude that the robust Internet architecture presents abundant opportunities for users, firms, governments and others to engage in creative endeavors and such endeavors can only thrive with an effective Internet security that includes the ability to authenticate users on the Internet without which the full extent of the potentials will not be realized.

7.2 Recommendations

In recognition of the fact that Cyber security is a moving target that will require ***continual*** refinement, additions and improvement; and that there will continue to exist security conditions that will require development of technologies and techniques that are not currently practical or available to solve the security issues they create, we make the following the recommendations.

1. **Stakeholder Shared Responsibilities**
   Internet system stakeholders all share the responsibility to collaboratively provide and promote a secure Cyberspace environment based on a new architecture that mandates basic security enforcement mechanisms across the board.

2. **Collaboration on Infrastructure and Services**
   Security vendors and Internet infrastructure providers should collaboratively develop a plug and play platform with security layers and buffer to address the needs of new and emerging technologies and applications.

3. We fully subscribe to **David Clark's recommendations** on creating a new Internet Architecture that:

   a. Gives the medium basic security architecture -- the ability to authenticate.

   b. Makes the new architecture practical by devising protocols that allow Internet service providers to better route traffic and collaborate to offer advanced services without compromising their businesses.

c. Allows future computing devices of any size to connect to the Internet -- not just PCs but sensors and embedded processors.

d. Adds technology that makes the network easier to manage and more resilient. For example, a new design that allows all pieces of the network to detect and report emerging problems -- whether technical breakdowns, traffic jams, or replicating worms -- to network administrators."

4. Giving the TCP/IP Protocol the Ability to Authenticate

The TCP/IP protocol suite lacks authentication the ability to authenticate and is therefore not suitable for connection to ubiquitous, global and un-trusted networks. This weakness results into malicious attacks. While current practices exist to mitigate the vulnerabilities through network layer controls, ACL's and filters, these measures are complicated, hard to manage and can often not be fully implemented because of performance impacts, therefore some vulnerabilities still exist.

Consequently, longer-term industry work is needed to define new or extended protocols with authentication; improved secure network element technology; define business process and criteria for establishing trust relationships; and establish interoperable implementation plans for rolling-out changes, that by definition cannot be backward compatible.

5. Addressing the Technical Protocol Issues

The Internet Engineering Task Force organizations (IETF) as an open, multi-vendor forum that includes participants from both the public and private sectors should provide the forum for definition the protocols, and address technical protocol issues, practical operational, deployment, and infrastructure issues to ensure:

1) That the protocols can be deployed in a manner that doesn't introduce more vulnerability into the Internet and in a manner that is practical to support operationally.
2) Vendor products support new, standards-based protocols in operationally supportable configurations.
3) For updated protocols that require use of certificate-based authentication or similar mechanisms, that
   - there are industry agreements on what the requirements for the identity certificates are,
   - suitable entities are identified as the certification authority
   - scalable key distribution mechanisms exist.

Bibliography

Bellovin, S. (1989), "Security Problems in the TCP/IP Protocol Suite", ACM Computer Communications Review, Volume 19, Number 2, pp. 32-48, April 1989.

Borchgrave, Cilluffo, Cardash, and Michèle, (2000), "Cyber Threats and Information Security Meeting the 21st Century Challenge," Center for Strategic and International Studies, December 2000.

Burgoyne, John G., Stakeholder analysis, in Cassel. C. and G. Symon (ed.), Qualitative Methods In Organizational Research: a practical guide, Sage, New Delhi, pp. 187-207, 1994.

Chris Chambers, Justin Dolske, and Jayaraman Iyer: "TCP/IP Security," Department of Computer and Information Science, Ohio State University, Columbus, Ohio 43210 Available at: http://www.linuxsecurity.com/resource_files/documentation/tcpip-security.html. Last checked January, 2011.

Computer Science and Telecommunications Board (CSTB), National Research Council. The Internet's Coming of Age. National Academy Press, Washington, D.C., 2001.

Computers at Risk: "Safe Computing in the Information Age," National Academies Press, Washington DC, 1991, http://books.nap.edu/catalog.php?record_id=1581. Last checked June 12, 2010.

Crawley, E. (2010), "Identifying Value - Reducing Ambiguity in the System," Lecture Notes on System Architecture, October 8, 2010, MIT.

Cyber Crime Report. http://securingourecity.org/blog/#. Last checked August 2010.

Clark, D. D. (1988). "The design philosophy of the DARPA Internet protocols," Proceedings of the ACM SIGCOMM'88, in: ACM Computer Communication Reviews, Vol. 18, No. 4, pp. 106{114}, 1988.

Donaldson T. and Preston L. E. (1995), "The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications," Academy of Management Review, Vol. 20, No. 1, pp. 65-91.

Freeman R. E. (1984), Strategic Management: A Stakeholder approach, Boston: Pitman.

GAO Report Number: GAO-10-628, "Critical Infrastructure Protection," Report to the Congress of the US, July, 2010, http://www.scribd.com/doc/38237843/GAO-Cyber-Security. Last checked on September 14, 2010.

Gulshan, R. (2009), "Cyber Security: Indian perspective," http://www.cyberseminar.cdit.org/pdf/09_02_09/gulshan.pdf. Last checked June 13, 2010

Hancock, B. (2003) "Summary Report and Proposals from Cyber Security Best Practices", Focus Group of Network Reliability and Interoperability Council, Homeland Defense, March 14, 2003 V1.3.

Haynal, R (2010), "Internet: The Big Picture: What are the major pieces of the Internet, and who are the major players in each segment." http://navigators.com/internet_architecture.html. Last checked in October, 2010.

Herbert, B. (2008), "Security/Cyber Security," International Telecommunication Union GSC-13 ITU-T Study Group 17 Presentation GSC13-XXXX-nn, July 1, 2008.

http://en.wikipedia.org/wiki/Domain_Name_System. Last checked January 31, 2011.

http://secunia.com/gfx/pdf/Secunia_Half_Year_Report_2010.pdf.

http://www.opte.org/maps/. Last checked on November 25, 2010.

http://www.securingourecity.org/blog/diving-deeper/cyber-attack-types/. Last checked January 31, 2011.

http://www.shadowserver.org/wiki/pmwiki.php/Stats/DDoSHistorical. Last checked January 31, 2011.

http://www.symantec.com/content/en/us/enterprise/other_resources/b-symc_intelligence_quarterly_apr-jun_2010_21072009.en-us.pdf. Last checked February 19, 2011.

http://www.vaughns-1-pagers.com/internet/internet-diagram.gif. Last checked January 31, 2011.

Iheagwara, C, HoonYoo, J and Prurapark, R. A (2010): "Internet System Stakeholder Analysis" Systems Architecture (ESD.34) class project, MIT, Fall, 2010.

Iheagwara, C. (2004), "The Effectiveness of Intrusion Detection Systems, Ph.D. Thesis, University of Glamorgan, Wales, Great Britain, 2004.

Iheagwara, C. 2010, "Cyber Attacks –Internet Architecture Mapping," S.M. Thesis, MIT, 2010.

Iheagwara, C. (2010), Interview with David Clark, MIT, December 14, 2010.

Internet Engineering Task Force, RFC 1122. http://tools.ietf.org/html/rfc1122. Last Checked January 7, 2011.

Kjaerland, M. (2006): "A taxonomy and comparison of computer security incidents from the commercial and government sectors," Computers & Security, Volume 25, Issue 7, October 2006, Pages 522-538.

Lipson, H (2002), "Tracking and tracing cyber attacks: technical challenges and global policy issues." Technical Report CMU/SEI-2002-SR-009, Carnegie Mellon University, 2002.
Accessed at http://www.sei.cmu.edu/pub/documents/02.reports/pdf/02sr009.pdf.

Mitchell, R, Agle, B & Wood, D (1997). "Towards a theory of stakeholder identification: Defining the principle of who & what really counts", Academy of Management Review 22(4): 853-886.

President's Information Technology Advisory Committee: "Cyber Security: A Crisis of Prioritization", Report to the President, February, 2005.

RFC 1958; B. Carpenter; Architectural Principles of the Internet; June, 1996.

GAO analysis of data from GAO and industry reports ((GAO-08-588).

Stallings, W. (2000) "Network Security Essentials," Applications and Standards,' P322-330 Prentice Hall, 2000.

Stallings, W. (2006), Data and Computer Communications, Prentice Hall 2006, ISBN 0-13-243310-9 Willinger, W and Doyle, J (2002), "Robustness and the Internet: Design and Evolution," AT&T Labs-Research, Florham Park, NJ, USA, March 1, 2002.

State of Spyware Q2 2006. Webroot Software, Inc. (2006, June). http://www.webroot.com/resources/stateofspyware/excerpt.html. Last checked June 17, 2010.

Talbot, D. (2005), "The Internet Is Broken," December 19, 2005. http://www.technologyreview.com. Last checked February 15, 2011.

Tanenbaum, A. (2002), Computer Networks, Prentice Hall 2002, ISBN 0-13-066102-3

The Internet lecture notes published at: www.cs.virginia.edu/~cs458/slides/**module04-internetV2.ppt**. Last checked September, 2010.

Websense Report, (2008), "Global Attack Trend in 2008," http://securitylabs.websense.com/. Last checked July 6, 2010.

Appendix 1: Several well-known TCP/IP vulnerabilities and Cyber Attacks [18]

Table 13: TCP/IP Attacks.

The Three-way Handshake (TCP "SYN")	***Sequence Guessing and Source Routing***	***Desynchronized State (Man-in-the-middle-attack)***
SYN attacks result from a very serious flaw that leads to Denial of Service (DoS) attacks. The current architecture of the TCP/IP assures a delivery system that experience in an Internet environment, a high message latency and loss, resulting in messages that arrive late or in non sequential order. The TCP half of TCP/IP uses sequence numbers so that it can ensure data is given to the user in the correct order, regardless of when the data is actually received. These sequence numbers are initially established during the opening phase of a TCP connection, in the three-way handshake. SYN attacks (also known as SYN Flooding) take advantage of a flaw in how most hosts (sending and receiving computer) implement this three-way handshake. The three-way handshake in Transmission Control Protocol (also called the three message handshake) is the method used to establish and tear down network connections. This handshaking technique is referred to as the 3-way handshake or as "SYN-SYN-ACK" (or more accurately SYN, SYN-ACK, ACK). The TCP handshaking mechanism is designed so that two computers attempting to communicate can negotiate the parameters of the network connection before beginning communication. This process is also designed so that both ends can initiate and negotiate separate connections at the same time.	In computer networking, the term **IP address spoofing** or **IP spoofing** refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system." (Wikipedia) IP Spoofing is an attack where an attacker pretends to be sending data from an IP address other than its own [Morris85, Bellovin89]. The IP layer assumes that the source address on any IP packet it receives is the same IP address as the system that actually sent the packet -- it does no authentication. There are variants of IP spoofing:	Sometimes called "Man –in-the-middle-attack" this interesting variant on IP spoofing allows a host to insert itself in the middle of a connection between two hosts -- connection hijacking [Joncheray95]. This type of attack is sophisticated in that the attacker is able to bypass security mechanisms in place. For example, IP spoofing alone may not bypass additional security, such as authentication by the Unix password mechanism, Kerberos, or one-time password systems like SKEY [RFC1760]. But with this attack, an attacker can allow normal authentication to proceed between the two hosts, and then seize control of the connection. Connection hijacking exploits a "desynchronized state" in TCP communication. When the sequence number in a received packet is not the same as the expected sequence number, the connection is said to be "desynchronized." Depending on the actual value of the received sequence number, the TCP layer may either discard or buffer the packet. There is a choice, because TCP uses a sliding window protocol to allow efficient communication even in the presence of packet loss and high network latency. So, if the received packet is not the one expected, but is within the current window, the packet will be saved on the premise that it will be expected later (various TCP mechanisms ensure that

An illustration of this phenomenon is given in Figure 13. When Host B receives the SYN request from A, it must keep track of the partially opened connection in a "listen queue" for at least 75 seconds. This is to allow successful connections even with long network delays. The problem with doing this is that many implementations can only keep track of a very limited number of connections (most track only 5 connections by default, though some like SGI's IRIX track up to 1024 [Luckenbach96]). A malicious host can exploit the small size of the listen queue by sending multiple SYN requests to a host, but never replying to the SYN&ACK the other host sends back. By doing so, the other host's listen queue is quickly filled up, and it will stop accepting new connections, until a partially opened connection in the queue is completed or times out. This ability to effectively remove a host from the network for at least 75 seconds can be used solely as a denial-of-service attack, or it can be used as a tool to implement other attacks, like IP Spoofing.		the expected packet will eventually arrive). If the received packet is outside of the current window, it will be discarded. Thus, when two hosts are desynchronized enough, they will discard (ignore) packets from each other. An attacker can then inject forged packets with the correct sequence numbers (and potentially modify or add commands to the communication). Obviously, this requires the attacker to be located on the communication path between the two hosts so that he may eavesdrop, in order to replicate packets being sent. The key to this attack is creating the desynchronized state. Joncheray describes two possible ways to do this: one is during the three-way handshake, and the other is in the middle of an established connection.
	Sequence Guessing:	***Desynchronization during connection establishment:***
	The sequence number used in TCP connections is a 32 bit number, so it would seem that the odds of guessing the correct ISN are exceedingly low. However, if the ISN for a connection is assigned in a predictable way, it becomes relatively easy to guess. This flaw in TCP/IP implementations was recognized as far back as 1985, when Robert Morris described how to exploit predictable ISN's in BSD 4.2, a Unix derivative [Morris85]. In BSD 4.2, the ISN for a connection is assigned from a global counter. This counter is incremented by 128 each second, and by 64 after each new connection (i.e., whenever an ISN is assigned). By first establishing a real	In this form of desynchronization, the attacker resets a connection during the three-way handshake. After host B sends the SYN&ACK packet to host A, the attacker forges new packets from B (to A) in which the connection is first closed via the RST bit, and then a new three-way handshake is initiated with A -- identical to the original, "real" handshake but with different sequence numbers. Host B now ignores messages from A (because A is using the attacker's new sequence numbers), and Host A ignores messages from B (because A is expecting messages with the attacker's sequence numbers). The attacker then replicates new packets, with the correct sequence numbers, whenever A and B try to communicate. In doing so, the attacker may also

	connection to the victim, the attacker can determine the current state of the system's counter. The attacker then knows that the next ISN to be assigned by the victim is quite likely to be the predetermined ISN, plus 64. The attacker has an even higher chance of correctly guessing the ISN if he sends a number of spoofed IP frames, each with a different, but likely, ISN. However, when the host receiving spoofed packets completes its part of the three-way handshake, it will send a SYN&ACK to the spoofed host. This host will reject the SYN&ACK, because *it* never started a connection -- the host indicates this by sending a reset command (RST), and the attacker's connection will be aborted. To avoid this, the attacker can use the aforementioned SYN attack to swamp the host it is imitating. The SYN&ACK sent by the attacked host will then be ignored, along with any other packets sent while the host is flooded. The attacker then has free reign to finish with his attack. Of course, if the impersonated host happens to be off-line (or was somehow forced off-line), the attacker need not worry about what the victim is sending out. Incrementing the ISN counter more often, as other operating systems may do, does not appear to help. Even if the counter is incremented 250,000 times a second (as suggested by the TCP standard), an attacker may still be able to approximately predict the ISN. By repeatedly guessing, it	modify the messages or inject his own.

	is likely that the attacker will establish a connection with the correct ISN within a few hours	
	Source Routing:	***Desynchronization in the middle of a connection:***
	Another variant of IP spoofing makes use of a rarely used IP option, "Source Routing" **[Bellovin89].** Source routing allows the originating host to specify the path (route) that the receiver should use to reply to it. An attacker may take advantage of this by specifying a route that by-passes the real host, and instead directs replies to a path it can monitor (e.g., to itself or a local subnet). Although simple, this attack may not be as successful now, as routers are commonly configured to drop packets with source routing enabled.	The previous attack is limited to the initial connection. If a RST packet is sent in the middle of a connection, the connection is closed -- and the application/user is notified of this. To cause desynchronization in the middle of a connection, without closing the connection, only the sequence number counters should be altered. The Telnet protocol, in particular, provides an interesting mechanism to do this. Telnet allows special "NOP" commands to be sent. These commands do nothing, but the act of sending the bytes in the NOP command increments the expected sequence number counter on the receiver. By sending enough of these NOP commands, an attacker can cause the connection to become desynchronized. The attacker can then begin replicating new packets, with the correct sequence numbers, as before.

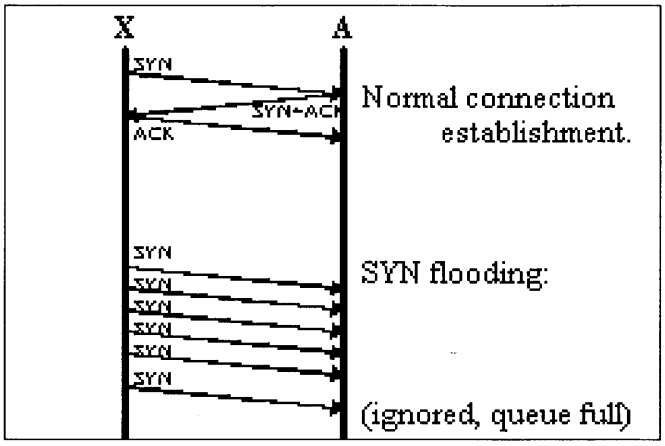

Figure 32: SYN Flooding [18].

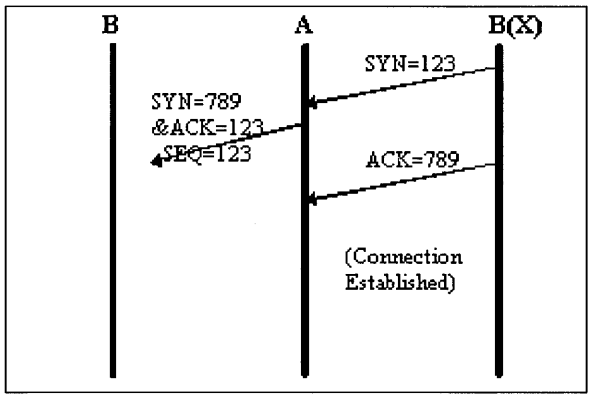

Figure 33: IP Spoofing via Sequence Guessing [18].

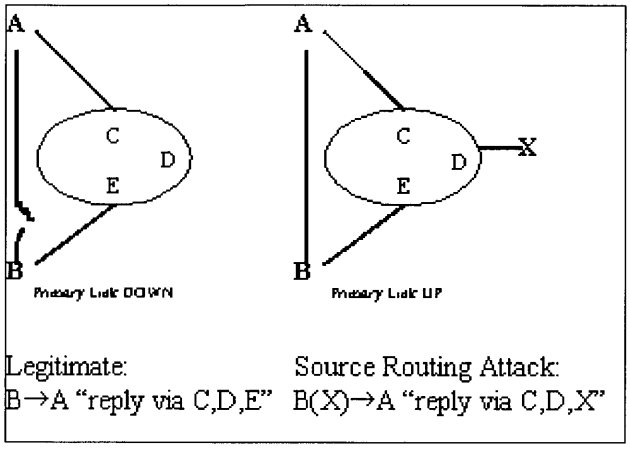

Figure 34: Source Routing [18].

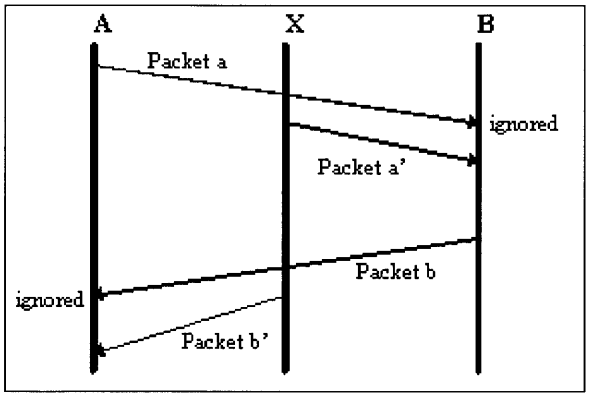

Figure 35: Connection Hijacking [18].

Appendix 2: Cyber attack Types.

Table 14: Types of Cyber Attacks [27].

Types of Cyber Attacks	Description
Denial of service	A method of attack from a single source that denies system access to legitimate users by overwhelming the target computer with messages and blocking legitimate traffic. It can prevent a system from being able to exchange data with other systems or use the Internet.
Distributed denial of service	A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers rather than from a single source. It often makes use of worms to spread to multiple computers that can then attack the target.
Exploit tools	Publicly available and sophisticated tools that intruders of various skill levels can use to determine vulnerabilities and gain entry into targeted systems.
Logic bombs	A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment.
Phishing	The creation and use of e-mails and Web sites—designed to look like those of well-known legitimate businesses, financial institutions, and government agencies—in order to deceive Internet users into disclosing their personal data, such as bank and financial account information and passwords. The phishers then use that information for criminal purposes, such as identity theft and fraud.
Sniffer	Synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.
Trojan horse	A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute.
Virus	A program that infects computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the infected file is loaded into memory, allowing the virus to infect other files. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Vishing	A method of phishing based on voice-over-Internet Protocol technology and open-source call center software that have made it inexpensive for scammers to set up phony call centers and criminals to send e-mail or text messages to potential victims, saying there has been a security problem and they need to call their bank to reactivate a credit or debit card, or send text messages to cell phones, instructing potential victims to contact fake online banks to renew their accounts.
War driving	A method of gaining entry into wireless computer networks using a laptop, antennas, and a wireless network adaptor that involves patrolling locations to gain unauthorized access.
Worm	An independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.
Zero-day exploit	A cyber threat taking advantage of security vulnerability on the same day that the vulnerability becomes known to the general public and for which there are no available fixes.