Vol 21, No 2 (2014): Journal of Faculty of Engineering & Technology (JFET), Pages 135-146

A STUDY OF INTERNET THREATS, AVOIDANCE AND BIOMETRIC SECURITY TECHNIQUES - COMPARISON OF BIOMETRIC TECHNIQUES

M. Junaid Arshad[1,], Arjumand Iqbal[2], Amjad Farooq[1], M. Usman Ghani Khan[1], M. Afzal[1], Amna Wajid[1], Abdul Nasir[1]*

[1]Department of Computer Science and Engineering, UET, Lahore-Pakistan
[2]Department of Chemistry, UET, Lahore-Pakistan
[*]junaidarshad@uet.edu.pk, amna-wajid@hotmail.co.uk

Abstract

In today's IT world, most of the communication is done through networking. So, security of information is very crucial. A lot of techniques have been developed for security which involves passwords, encryption, digital signatures etc. But there are chances of vulnerabilities in these techniques and hackers can break the security algorithms of these techniques. So, in this era, researchers have moved towards biometric techniques of security. It involves identification of people based on their physical characteristics or psychological behaviors. A choice of biometric method to be used is made depending on the level of security required and the goals of the system. Biometric identification is very excellent and secure way of authenticating people. But it can also suffer from security threats, if proper design considerations are not taken into account. This work presents details of biometric techniques and a detailed comparison of most famous biometric techniques.

Keywords: Security Attributes; Security Attacks; Biometrics

1. Introduction

Computer network is formed by connecting a millions of computers worldwide. The exchange of information among these geographically distributed computers is done by using special internet protocols. The most widely used protocol is Transmission control protocol/Internet protocol (TCP/IP). The rapid development in the field of networks has not only reduced communication cost but also opened new opportunities for people belonging to every field of life. Nowadays, Internet is used in every walk of life. Today, almost every type information exchange and business is done through internet, which involves information storage, information sharing and communication with employees and clients. Beside all its advantages, internet also has the dark side of it. It has many risks associated with the information which is being stored on a network or which is being communicated. So, the security of the network is major goal now [1].

Internet is distributed system with no central control by any individual or organization. The major security risks on internet are due to e-commerce. There are three

[1] Corresponding Author E-mail: junaidarshad@uet.edu.pk
Phone no.: 0092-42-99029260;

major security goals which are integrity, confidentiality and availability [5]. Today internet frauds, theft of confidential information, information modification, induction of viruses and worms and gaining access of finance of someone else are common ways of compromising security of Internet. Due to these risks it is very difficult to fulfill security goals. A lot of techniques have been developed for security which involves passwords, encryption of data, digital signatures etc. Among all these techniques, password based security is said to be very weak and encryption based security is said to be very strong. But, despite of highly efficient and safe encryption techniques, there are chances of failure of these techniques. With today's advanced technologies, hackers can find a way to break the strong securities as well and can introduce vulnerabilities into the system.

To overcome the deficiencies of simple security techniques, the use of biometric based security techniques was started in the systems required to fulfill security goals strictly. It involves identification of people based on their physical characteristics or psychological behaviors. Physical biometrics comprise of fingerprints, hand or palm geometry, retina, iris or facial characteristics. Behavioral characters include signature, voice, keystroke pattern, and gait. Biometric technique of security is encouraged because it cannot be stolen by anyone else or forgotten by the person owing it. Along with all its advantage, biometric security can also suffer from security threat, if its security is not properly handled [2], [3], [4].

In this paper, we aim to study internet security threats and their solutions in detail. We also aim to study the different biometric techniques and advantages and disadvantages of biometric techniques. We aim to present a comparison of biometric techniques based on different factors.

The paper is organized as follows: Section II presents a literature survey which includes evolution of the Internet, common internet attacks and their solutions and biometric security techniques. In Section III we present a comparison of biometric techniques. Section IV consists of concluded remarks and future directions.

2. Literature Review

The internet is a network of networks. It connects millions of computers and networks around the world enabling communication between different users around the globe. It uses different sets of rules called protocols for successful communication. The most popular protocol nowadays is TCP/IP protocol [1]. Founder of the World Wide Web, Tim Berners-Lee describes the Internet as follows: "It's a bit like a postcard with a simple address on it. If you put the right address on a packet, and gave it to any computer which is connected as part of the Net, each computer would figure out which cable to send it down next so that it would get to its destination. That's what the Internet does. It delivers packets—anywhere in the world, normally well under a second [2]".

2.1 History of Emergence of the Internet

Emergence of Networking dates back to 1960, when during World War II, the US government identified the problem of destruction of telephone system of a city in case of nuclear attack [13]. During 1960's, circuit switching was used for communication of either voice or data. The biggest problem with this setup was the communication barrier due to the line breakup from source to destination [10], [11]. So, US air force assigned

the task of forming a decentralized communication system to a team of researchers working at advance Research Projects Agency (ARPA). Its goal was to make a reliable communication system that can continue it's working even in case of destruction of some part of communication system [8].

In 1962, J.C.R. Licklider while working at Massachusetts Institute of Technology (MIT) and ARPA, presented a solution of the problem of circuit switched systems. He proposed "galactic network" with the idea of connecting all computers around the globe enabling information exchange between any of the computers [14]. After that idea of packet switching was presented in parallel by three different research groups at a conference held at Defense Advanced Research Projects Agency (DARPA). These researchers include Leonard Kleinrock from MIT (1961-1967), Paul Baran from RAND (1962-1965) and Donald Davies and Roger Scantlebury from NPL (1964-1967) [15]. In 1966, ARPA, together with several research institutes started a program named "Resource Sharing Computer Networks". The goal of this program was to make a decentralized computer network system [12]. In 1967, Roberts with this research group published the plan for connecting computers using concept of packet switching. In 1969, the actual Network connecting four computers was deployed. Later, the name given to this project was ARPANET [9], [13], [14].

As the time passed, the size of network started growing. So, the researchers realized the need of some new technology for transmission of data. So, Vinton Cerf proposed a new protocol named, Transmission Control Protocol (TCP) which was proposed to make Internet a global network. Later on TCP was combined with Internet Protocol (IP) [13].

The TCP\IP protocol presented by Cerf was used to send important information and files from one computing machine to another. In 1991, a programmer named Berners-Lee from Switzerland introduced the idea of World Wide Web (WWW). WWW in addition to providing the way of sharing files and data, also provided a sea of information which enabled users to search and retrieve information related to his query. In 1992, The First user friendly browser named Mosaic was developed by a researchers and students group at University of Illinois. Mosaic made searching on the web very easy, it provided visual aids like scrollbars and hyperlinks. It displayed pictures and text on the same page first time in the history. In the same year, it was decided to use the web for commercial and business purposes. This resulted in the set up of websites by different companies to facilitate user and to gain benefit [13].

2.2 Evolution and Need of Information Security

This information security concept was aroused when the human learned to write and to send written messages to others. In the first Century, Julius Caesar first time invented the concept of secret code. In 1840, secret code was used by Julius to encrypt the message transmitted using telegraph. Later on, the information security concept was moved from security of hand written messages to security of electronic messages [16].

With the evolution of computers, different security techniques were also evolved depending upon the type of computer. In the early 1970s, Cryptographic techniques were presented. In 1980s, use of personal computers was started and number of computer users increased drastically. The companies started working on automating their operations through the use of computer. Because of the use of computer for almost all the

information storage and information exchange, security emerged as critical and vital aspect [16].

The information security scope was broadened, when the first intruder break-in was reported. This was by a group of hackers known as "414 gang". They broke into the systems of USA Stanford campus. Also during the same time, US military computers were hacked by a programmer from West German to steal the documents. Computer viruses by the use of diskettes were also reported. The 'Elk Cloner' made by Rick Skrenta and 'The Brain' made by two Pakistani brothers were among the first ever created viruses. First worm was created by Robert Morris in 1988. By the end of 1990, more and more security threats like denial of service, execution of malicious code using mail and web pages, phishing, eavesdropping were invented. Attackers now diverted their focus from single computers to the distributed computers, servers and gateways. So, with the new ways of attacks emerging day by day, more robust ways of security were invented to stop intruders to harm information. Firewalls and antivirus software were a major progress in the field [16].

To properly oppose the challenges of new developments, innovative ideas and detailed analysis of security attributes, types of security attacks and security related issues is required [16].

2.3 Security Attributes

The objective of Information Security is to preserve integrity, confidentiality and availability of information being stored on a computer or being transferred through internet. The integrity, confidentiality and availability are known as security attributes [1]. Confidentiality is associated with the secrecy and privacy of information. Secrecy means protection of private data from unauthorized individuals. Integrity is associated with precision and correctness of data. Availability assures the uninterrupted access and availability of system resources to authorized users [1], [17].

2.4 Types of Security Attacks

Viruses: Viruses are a way of attack, through which a program is damaged. A virus attaches itself to an executable code of a program and when that program is opened by a human, the attached virus is automatically activated. After activation, it can do anything with that file. It can erase or modify the contents of the file. A virus also has the ability to replicate itself [1], [17], [19].

Worms: Worm is a program that is self-replicating. The design of worm is similar to virus. For the propagation to other programs, worms do not need infected program. They are propagated to other systems over the Internet. Two types of worms are network aware worms and email-worms [1], [17], [19].

Trojans: Trojan is a program which appears like useful and legitimate programs but in fact it has malicious intention. It embeds itself with code of some application and when it is run by a user, it starts damaging the system. It is also used to get unauthorized access to a system and its resources [1], [17], [19].

Spyware: Spyware is a software program which is used to collect information from a system and send that information to someone else without the permission of that systems authorized user. Some spyware are downloaded and installed on the system with the

installation of software by the user and user even does not know about the installation of spyware. Sometimes owner of an organization himself installs spyware software on all the systems in order to monitor activities of its employees [17], [20], [21].

Adware: Adware is a advertising software which is incorporated into a software. It causes pop-up of advertisements on the screen. It can also automatically redirect the browser to a marketing website [17].

Eavesdropping: Eavesdropping is a way of getting connected in a communication which is being taking place between an authorized sender and an authorized receiver. The intruder which gets connected in a communication can read or listen the messages exchanged between communicating entities. The two types of eavesdropping are passive and active eavesdropping [1].

Denial of Service: In a Denial of service (DoS) attack a server or host computer is flooded with false and fake requests. Due to these fake requests, host cannot fulfill the legal requests. In this attack, host is put into a wait state, as it waits for the completion of TCP handshake initiated by the attacker [1], [18].

Hacking: Hacking is attacking some system by finding a weakness of system and entering into the system. Hackers after gaining access of system can do anything with it. They can destroy information resources of target and can also steal that information [1], [18].

Phishing: Phishing is deceiving a user by showing it a masquerade webpage as legitimate webpage. The user after seeing the webpage cannot predict that whether it is a legitimate page or some illegal page designed by some attacker. User when enters his personal information on that page, the page is refreshed user is directed to original page and the data entered by user is sent to the attacker [1], [18].

IP Spoofing Attacks: In IP spoofing, an attacker modifies the host address of a packet such that when the packet reaches at its destination, it appears like a valid packet from a valid sender. After reaching at the destination, the reply from the destined receiver is sent to the forged address generated by the attacker and not to the original sender [1], [22].

Spamming: Spamming refers to sending unnecessary messages to a large number of recipients via email. The intention behind spam messages is to spread malware or to send some advertisement [1], [18].

Compromised Key Attack: For Secure transmission of data, it is encrypted at sender side and decrypted at receiver side. For encryption and decryption a secret code is used which is known as key. If an attacker gets success in determining the key then that key is known as compromised key. The attacker then uses that key to read the encrypted information [27].

2.5 Techniques for Avoidance from Security Attacks

Due to the use of internet in almost all types of business and due to the rapid growth of internet attacks, very strong and efficient security techniques are required [1]. Some security techniques are described in the next sub sections.

Firewall: A firewall is a filter which is used to filter traffic coming from outside to some private network and going from private network to outside network. The firewall

can be a hardware based, software based or blend of both hardware and software. Firewalls are of different types, two of which are packet based firewalls and proxy servers [1].

Cryptography: Cryptography means to encrypt or to change ordering of message which is to be sent. To encrypt the message, cryptographic algorithms with complex mathematical calculations are used. An encryption key is used to shuffle the original message's contents known as plain text. The shuffled message is called as cipher text [1].

Anti-Malware Software: Worms, viruses, Trojans are collectively known as malware. Anti malware software are used to detect and recover from such attacks. Most frequently used anti malware software is antivirus software [1].

Intrusion Detection: Intrusion Detection Systems (IDS) are extended form of firewall. IDS use to monitor the traffic coming into the system by using different techniques like port scanning, packet monitoring and packet signature and pattern [1], [24].

Internet Protocol (IP) Security: The purpose of IP Security is to provide security of communication at the IP layer of network architecture by using different protocols which were originally defined by Request for Comments (RFC). This security is provided by authenticating and encrypting all the communication at the IP layer. IP Security uses two types of protocols. These are Authentication Header (AH) and Encapsulating Security Payload (ESP). IP security protocols have no concern with the application layer [1], [23].

Secure Socket Layer (SSL): The SSL is a protocol used to establish a secure connection between a server and a web browser intended to communicate using encryption. SSL protects the data from attacks like session hijacking, eavesdropping. Today the websites using https make them secure by using SSL while sites using http are not secured and can be attacked easily [1].

2.6 Problems with Security Techniques

Olalekan Adeyinka [1] has shown the possible attack methods violating internet security attributes and the techniques which can be used to detect and recover from such attacks. With the advances in technology, new ways of exploiting security are being determined. Nothing is perfect, so there is downside of security techniques. The hackers and attackers can get benefit from this downside of such techniques and can attack systems even if system is made secure by different ways. The downside of each type of security technique is summarized in Table 1.

Table 1: Downside of Internet Security Techniques

Internet Security Technique	**Downside**
Firewall	– Deceived by IP-Spoofing [24] – No surety of data Integrity outside the Network where firewall was Deployed [25]
Anti Malware Software	– Need to be updated at all times [26] – New viruses are hard to detect if not present in antivirus software database [26]

Intrusion Detection Systems	– Requires much processing power [24] – Expensive [24] – Sometimes tag genuine traffic as attacks which results in unnecessary security alarms [24]
Internet Protocol Security	– Sometimes off-site legal access is blocked by VPN firewall [28] – Compromised pre shared key used for encryption [29]
Secure Socket Layer	– Requires TCP traffic, does not work with UDP [30] – Cannot work for VoIP applications, which requires UDP [30] – Requires heavy resources to encrypt and decrypt
Cryptography	– Requires complex calculations – Requires a lot of time and resources – Difficult management of keys

2.7 Shift to Biometric Technology

Due to the security risks associated with each security mechanism, biometric technology for authentication is used for highly critical systems. Biometric recognition is the process of authenticating an individual based on ones physical or behavioral characteristics. Common physical biometric characteristics consist of fingerprints, retina, iris, face recognition. Behavioral characteristics consist of voice, signature, gait, keystroke pattern recognition [3]. Today, most widely used biometric are fingerprints and voice recognition, which are used in companies. Banks can also use these techniques for securing their data. A lot of biometric methods to be used in banks have been proposed. In the next sub section an overview of each biometric technique is presented.

Fingerprint: Fingerprint recognition devices capture the image of finger and identify ridges and bifurcation and calculate minutiae. It then stores this minutiae information as a template and matches particular fingerprint with this template for recognition process [3], [31].

Face Recognition: In face recognition, facial features are used to authenticate a person. In it, an image of person is captured and after extraction of features it is stored in database as a template, which is used later to authenticate a user [3], [31].

Retina based Recognition: In retina based recognition, an analysis of blood vessels of eyes is done. To scan the retina pattern, a user is asked to focus on a certain point and the image is taken by using a light source along with optical coupler. If user does not focus on given point, then user can not be properly recognized [3].

Iris Based Recognition: In iris based recognition, the colored tissue around the pupil of eye is analyzed. Unlike retina based scanning, in iris scanning user need not to be focused on a certain point in order to be verified [3].

Voice Recognition: Voice recognition involves authenticating a person based on his voice. During authentication, samples of voice are stored in database and matched with the real time voice sample in order to authenticate a person. Voice authentication can suffer from background noise and also from voice change due to environmental changes [3].

Signature Verification: Signature based confirmation is based on user's style of writing. It is done based on features such as speed of writing, pressure on pen while writing and shape of signatures [3].

2.8 Advantages of Biometrics

Biometric authentication only verifies people. A person always has its identification with him. It cannot have danger of being stolen like a card or forgotten like a password. It is very hard to deceive a biometrics based system. So, it requires less administrative entities as compared to password or card based systems [2].

2.9 Drawbacks of Biometric Systems

The first and foremost drawback of a biometric system is that, 100 percent accuracy is not possible with it. It cannot be applicable to all people. For example, it is impractical to use voice recognition for a person who can't speak. Similarly it is not possible to use authentication by fingerprint for the people who does not have hand. Similarly behavioral changes with time also affect the biometrics. For example, fingerprint authentication will not work when finger is injured. Facial characteristics of a person change with age. Biometric authentication is still in development phase. So, it is costly to install these systems. If biometric will be use so frequently, then it would not be possible to keep the biometric samples of a user secure [2].

3. Proposed Work

In [3], Simon Liu and Mark Silverman have presented a comparison of various biometric techniques. In [31], Parvinder S. Sandhu et al. have also presented comparison of biometrics based on different parameters. The purpose of this research is to further extend the work and to present a comparison of biometric techniques based on the factors which are not considered by [3] and [31]. In this research, the factors which are considered for comparison are chosen keeping in mind to aid user to select a particular biometric. These parameters are cost of a biometric device, possible threats to the biometric, avoidance techniques from a threat, precision of a biometric method, limitations for authentication of a legitimate user. The details of this comparison are presented in next sub section and are summarized in Table 2.

3.1 Comparison of Biometric Methods

Hardware Cost: Hardware for iris and retina based recognition is most expensive than hardware of other techniques. As, it requires high quality cameras. Fingerprint and signature recognition hardware cost is also high. As, it requires to buy devices needed for these. Hardware for face recognition is not very expensive. It requires camera and now a days, a camera is already embedded in laptops, mobiles etc. Voice recognition requires a microphone, which is available today in all devices used for communication. So, for it to implement, an organization don't need to install its hardware on device of every user.

User Training: For use of fingerprint, face and voice recognition devices, a little bit training of users is required. While use of signature based techniques don't require any training, as everyone knows, how to do signatures. For use of iris and retina based devices, a proper training is required.

Factors Causing Authentication Failure: Fingerprint recognition device fail to authenticate a person, if the finger is injured or it has dust on it. It also fails if some color is applied on finger. Face recognition fails due to low lighting. It also gets affected with the aging of user, as aging results in corrugation of face. Retina based recognition fails, if person is wearing glasses. It also fails, if the person requiring authentication does not focus on a certain point. Iris based recognition fails due to the reflection in eye. Voice based recognition fails due to the background noise and due to the weather effects on the voice of person. Signature based technique fails, if signature of person changes from the specimen signature. This technique also takes into account the writing speed of person. So, it also fails, if person does signature below or above normal speed.

Security Threats: Most often, there are two types of security threats to biometric techniques. One is deceiving reader device if proper security is not applied and second is alteration of database templates of users. Fingerprint reader can be deceived by a finger made with some substance. Face recognition device can be deceived by using a picture of authenticated user. It is very difficult to deceive retina based device but it can be deceived by using synthetic images of retina of a human which are based on digital code of human retina sample. But the ratio of deceive of retina based device is very low. Iris based device can also be tricked with synthetic images which is described in [32]. Voice based devices can easily be tricked by using recorded voice of the authenticated person. Signature based authentication can also be easily tricked by replicating the signatures of authorized person.

Anti Measures for Security Maintenance: The threat associated with deceiving the device can be tackled by putting a aliveness check during the authentication process. Aliveness check can be put on fingerprint, face, iris, retina based devices, but it cannot be used for voice. It is also not applicable to signature based authentication, as it would always involve a live entity. The threat of alteration and stealing of database samples of an entity can be tackled by storing the encrypted sample in the database.

Type of Sensor: In the hardware of biometric device, a sensing device is used to sense the input. This sensor for face, iris and retina recognition is camera. For fingerprint recognition, it is some optical or capacitive surface. For voice recognition, it is microphone. For signature recognition, it is a digital pen to write and a digital surface to write on.

Physical Contact with Device: For fingerprint and signature based recognition, physical contact with the reader device is required. But for retina, iris, face and voice recognition physical contact with device is not required. These devices can be used from some distance away from devices.

Precision: The precision of biometric device is dependent upon number of factors. These are Human Behavior (the way of using device), device sensor and algorithm used for sample capturing, storing and recognition purposes. If very efficient algorithm is used and good sensors are used, then the accuracy of device is high. Similarly if user inputs a device properly, then the results are good. If during fingerprint recognition, a person does not put finger properly on the reader, then recognition is definitely affected. Similarly if an authenticated person does not speak properly during voice recognition, then he is not given access to system. Same happens with other techniques as well, if authorized person does not provide input properly.

Table 2: Comparison of Biometric Techniques

Parameters		**Fingerprint**	**Face**	**Retina**	**Iris**	**Voice**	**Signature**
Hardware Cost		High	Medium	Highest	Highest	Lowest	High
User Training		A little bit Required	A little bit Required	Required	Required	A little bit Required	Not Required
Factors causing Authentication Failure		Injury, Cut, Color applied on Finger, dust	Age, lighting	Glasses, Low Focus	Uncertainty due to reflection	Noise, Weather impact on user	Change in signature, Writing Speed
Security Threats	Deceiving reader device,	Yes	Yes	Yes but Difficult	Yes	Yes	Yes
	Alteration of database templates	Yes	Yes	Yes	Yes	Yes	Yes
Anti-measures for Security maintenance	Liveness Check	Yes	Yes	Yes	Yes	Not applicable	Not applicable
	Storage of Encrypted Samples	Yes	Yes	Yes	Yes	Yes	Yes
Type of Sensor		Optical, Capacitive	Camera	Camera	Camera	Micro-phone	Digital Pen, Digital Surface
Physical Contact with Device		Required	Not Required	Not Required	Not Required	Not Required	Required
Precision	Effect of Human Behavior	Yes	Yes	Yes	Yes	Yes	Yes
	Effect of Device Sensor	Yes	Yes	Yes	Yes	Yes	Yes
	Effect of Algorithm	Yes	Yes	Yes	Yes	Yes	Yes

4. Conclusion

Security of information is a critical issue in today's global world of Internet. With the advances in technology, new ways of stealing the sensitive information are being developed. So, as a counter act, security techniques are being made stronger in order to assure secrecy. A lot of research is being done to resolve this issue. Now, the research has moved to biometric technology and ways of flawless security through biometrics are being developed. Nowadays, Biometric Technology is only being used in the intranet of organizations requiring very high secrecy. But that day is not far, when it will be used for securing information exchange on the Internet.

References

[1]. Adeyinka, O. (2008). Internet attack methods and internet security technology. In Modeling & Simulation, In Proceedings of AICMS-08. IEEE Second Asia International Conference, pp. 77-82.

[2]. Fustier, A., & Burger, V. (2005). Internet Security and Privacy.

[3]. Liu, S., & Silverman, M. (2001). A practical guide to biometric security technology. IT Professional, 3(1), pp. 27-32.

[4]. Biometric Security Technology. (n.d.). Retrieved from PeterIndia.net: http://www.peterindia.net/BiometricsView.html#What is a Biometric.

[5]. Shoniregun, C. A. (2002). The future of internet security. Ubiquity, 2002 (October).

[6]. A Brief Guide to the History of the Internet. (n.d.). Retrieved from investintech.com: http://www.investintech.com/content/historyinternet/

[7]. Siasoco, R. V. (2007). The History of the Internet. Retrieved from Fact Monster: http://www.factmonster.com/spot/99internet1.html

[8]. History of the Internet. (2013, September). Retrieved from Kioskea.net: http://en.kioskea.net/contents/238-history-of-the-internet

[9]. A Brief History of the Internet. (2008, May 24). Retrieved from Dynamic Web Solutions: http://www.dynamicwebs.com.au/tutorials/history.htm

[10]. Packet Switching History. (n.d.). Retrieved from http://www.livinginternet.com/i/iw_packet_inv.htm

[11]. ARPANET. (n.d.). Retrieved from WikiPedia: http://en.wikipedia.org/wiki/ARPANET

[12]. Strickland, J. (n.d.). How ARPANET Works. Retrieved from How Stuff Works:

[13]. http://computer.howstuffworks.com/arpanet.htm, The Invention of the Internet. (n.d.). Retrieved from History: http://www.history.com/topics/invention-of-the-internet

[14]. History of the Internet. (n.d.). Retrieved from New Media Institute: http://www.newmedia.org/history-of-the-internet.html

[15]. Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., ... & Wolff, S. (2009). A brief history of the Internet. ACM SIGCOMM Computer Communication Review, 39(5), 22-31.

[16]. Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. computers & security, 28(3), 189-198.

[17]. Stallings, W. (2007). Network Security Essentials: Applications and Standards, 4/e. Pearson Education India.

[18]. Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. Information systems, 36(3), 675-705.

[19]. Beal, V. (2013). The Difference Between a Computer Virus, Worm and Trojan Horse. Retrieved from WeboPedia: http://www.webopedia.com/DidYouKnow/Internet/2004/virus.asp

[20]. Spyware. (n.d.). Retrieved from WikiPedia: http://en.wikipedia.org/wiki/Spyware

[21]. Moshchuk, A., Bragin, T., Gribble, S. D., & Levy, H. M. (2006, February). A Crawler-based Study of Spyware in the Web. In NDSS.

[22]. Tanase, M. (2003). IP spoofing: an introduction. Security Focus, 11.

[23]. Bojkovic, Z. (2008, May). Some IP security issues. In Proceedings of the 10th WSEAS International Conference on Mathematical Methods and Computational Techniques in Electrical Engineering (pp. 138-144). World Scientific and Engineering Academy and Society (WSEAS).

[24]. Northrup, T. (n.d.) Firewalls. Retrieved from Security TechCenter:http://technet.microsoft.com/en-us/library/cc700820.aspx

[25]. Firewall Q&A. (2002). Retrieved from VicomSoft: http://www.vicomsoft.com/downloads/learning/firewall_qa.pdf

[26]. McDowell, R. (n.d.). What Are the Disadvantages of Antiviruses? Retrieved from eHow:http://www.ehow.com/list_7285310_disadvantages-antiviruses_.html
[27]. Security issues with IP. (2005). Retrieved from microsoft TechNet: http://technet.microsoft.com/en-us/library/cc783463(v=ws.10).aspx
[28]. Taylor, S., & Wexler, J. (2004). The pros and cons of IPSec. Retrieved from Network World: http://www.networkworld.com/newsletters/2004/1108wan2.html
[29]. Everard, J. (2003). Remote Access IPSec VPNs: Pros and Cons of 2 Common Clients. Retrieved from SANS Institute: http://www.sans.org/reading-room/whitepapers/vpns/remote-access-ipsec-vpns-pros-cons-2-common-clients-877?show=remote-access-ipsec-vpns-pros-cons-2-common-clients-877&cat=vpns
[30]. Taylor, S., & Wexler, J. (2004). The pros and cons of SL. Retrieved from Network World: http://www.networkworld.com/newsletters/2004/1115wan1.html
[31]. Sandhu, P. S., Kaur, I., Verma, A., Jindal, S., & Singh, S. (2009). Biometric methods and implementation of algorithms. International Journal of Electrical and Electronics Engineering, 3(8).
[32]. BOWE, R. (2012). Red Flag On Biometrics: Iris Scanners Can Be Tricked. Retrieved from Electronic Frontier
[33]. Foundation: https://www.eff.org/deeplinks/2012/07/red-flag-biometrics-iris-scanner-vulnerability-revealed.