ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (467-475), Month: July - September 2014, Available at: www.researchpublish.com

INTERNET SECURITY AND PRIVACY

[1]Raghav Arora, [2]Rana Rahul Sathyaprakash, [3]Saurabh Rauthan, [4]Shrey Jakhetia

Student, Department of Computer Science & Engineering, Dronacharya College of Engineering, India

Abstract: **With increase in usage of the Internet, there has been an exponential increase in the use of online social media on the Internet. Websites like Facebook, YouTube, Orkut, Twitter and Flickr have changed the way Internet is being used. There is a dire need to investigate study and characterize privacy and security of online social media from various perspectives (computational, cultural, and psychological). Real world scalable systems need to be built to detect and defend security and privacy issues on online social media. The main goals of the talk are to highlight and discuss latest issues, trends, and cutting-edge research approaches in security and privacy in online social media. Some of the prominent problems on which our group is working on are spam and phishing detection, credibility assessment, privacy leakage and fake profiles identification on online social media.**
The internet structure itself allowed many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

I. INTRODUCTION

The world is becoming more interconnected with the advent of the Internet and new networking technology. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet.

There are currently two fundamentally different networks, data networks and synchronous network comprised of switches. The internet is considered a data network. Since the current data network consists of computer-based routers, special programs, such as "Trojan horses," planted in the routers, can obtain information. The synchronous network that consists of switches does not buffer data and therefore are not threatened by attackers. That is why security is emphasized in data networks, such as the internet, and other networks that link to the internet.

The vast topic of network security is analysed by researching the following:

1. History of security in networks
2. Internet architecture and vulnerable security aspects of the Internet
3. Types of internet attacks and security methods
4. Security for networks with internet access
5. Current development in network security hardware and software

Based on this research, the future of network security is forecasted. New trends that are emerging will also be considered to understand where network security is heading.

II. NETWORK SECURITY

System and network technology is a key technology for a wide variety of applications. Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interface (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design.

When considering network security, it must be emphasized that the whole network is secure. Network security does not only concern the security in the computers at each end of the communication chain. When transmitting data the communication channel should not be vulnerable to attack. A possible hacker could target the communication channel, obtain the data, decrypt it and re-insert a false message. Securing the network is just as important as securing the computers and encrypting the message.

When developing a secure network, the following need to be considered [1]:

1. Access – authorized users are provided the means to communicate to and from a particular network
2. Confidentiality – Information in the network remains private
3. Authentication – Ensure the users of the network are who they say they are
4. Integrity – Ensure the message has not been modified in transit
5. Non-repudiation – Ensure the user does not refute that he used the network

An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack [1]. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavour.

To lessen the vulnerability of the computer to the network there are many products available. These tools are encryption, authentication mechanisms, intrusion-detection, security management and firewalls. Businesses throughout the world are using a combination of some of these tools. "Intranets" are both connected to the internet and reasonably protected from it. The internet architecture itself leads to vulnerabilities in the network. Understanding the security issues of the internet greatly assists in developing new security technologies and approaches for networks with internet access and internet security itself.

The types of attacks through the internet need to also be studied to be able to detect and guard against them. Intrusion detection systems are established based on the types of attacks most commonly used. Network intrusions consist of packets that are introduced to cause problems for the following reasons:

- To consume resources uselessly
- To interfere with any system resource's intended function
- To gain system knowledge that can be exploited in later attacks

The last reason for a network intrusion is most commonly guarded against and considered by most as the only intrusion motive. The other reasons mentioned need to be thwarted as well.

Typical security currently exists on the computers connected to the network. Security protocols sometimes usually appear as part of a single layer of the OSI network reference model. Current work is being performed in using a layered approach

to secure network design. The layers of the security model correspond to the OSI model layers. This security approach leads to an effective and efficient design that circumvents some of the common security problems.

III. HISTORY OF NETWORK SECURITY

Recent interest in security was fuelled by the crime committed by Kevin Mitnick. Kevin Mitnick committed the largest computer-related crime in U.S. history [3]. The losses were eighty million dollars in U.S. intellectual property and source code from a variety of companies [3]. Since then, information security came into the spotlight.

Public networks are being relied upon to deliver financial and personal information. Due to the evolution of information that is made available through the internet, information security is also required to evolve. Due to Kevin Mitnick's offense, companies are emphasizing security for the intellectual property. Internet has been a driving force for data security improvement.

Internet protocols in the past were not developed to secure themselves. Within the TCP/IP communication stack, security protocols are not implemented. This leaves the internet open to attacks. Modern developments in the internet architecture have made communication more secure.

1. Security Timeline

Several key events contributed to the birth and evolution of computer and network security. The timeline can be started as far back as the 1930s. Polish cryptographers created an enigma machine in 1918 that converted plain messages to encrypted text. In 1930, Alan Turing, a brilliant mathematician broke the code for the Enigma. Securing communications was essential in World War II.

In the 1960s, a couple of Massachusetts Institute of Technology (MIT) students coins the term "hacker". The Department of Defence began the ARPANet, which gains popularity as a conduit for the electronic exchange of data and information [3]. This paves the way for the creation of the carrier network known today as the Internet. During the 1970s, the Telnet protocol was developed. This opened the door for public use of data networks that were originally restricted to government contractors and academic researchers [3].

During the 1980s, the hackers and crimes relating to computers were beginning to emerge. Authorities raid the 414 gang after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 was created because of Ian Murphy's crime of stealing information from military computers. A graduate student, Robert Morris, was convicted for unleashing the Morris Worm to over 6,000 vulnerable computers connected to the Internet. Based on concerns that the Morris Worm ordeal could be replicated, the Computer Emergency Response Team (CERT) was created to alert computer users of network security issues. In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide [3]. On any day, there are approximately 225 major incidences of a security breach [3]. These security breaches could also result in monetary losses of a large degree. Investment in proper security should be a priority for large organizations as well as common users.

IV. INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets [4]. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite [4]. These security mechanisms allow for the logical protection of data units that are transferred across the network. The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best-known deficiencies, they seem to be insufficient [5]. Figure 2 shows a visual representation of how IPsec is implemented to provide secure communications. IPsec is a point-to-point protocol, one side encrypts, the other decrypts and both sides share key or keys. IPsec can be used in two modes, namely transport mode and tunnel modes

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 3, pp: (1-4), Month: July - September 2014, Available at: www.researchpublish.com

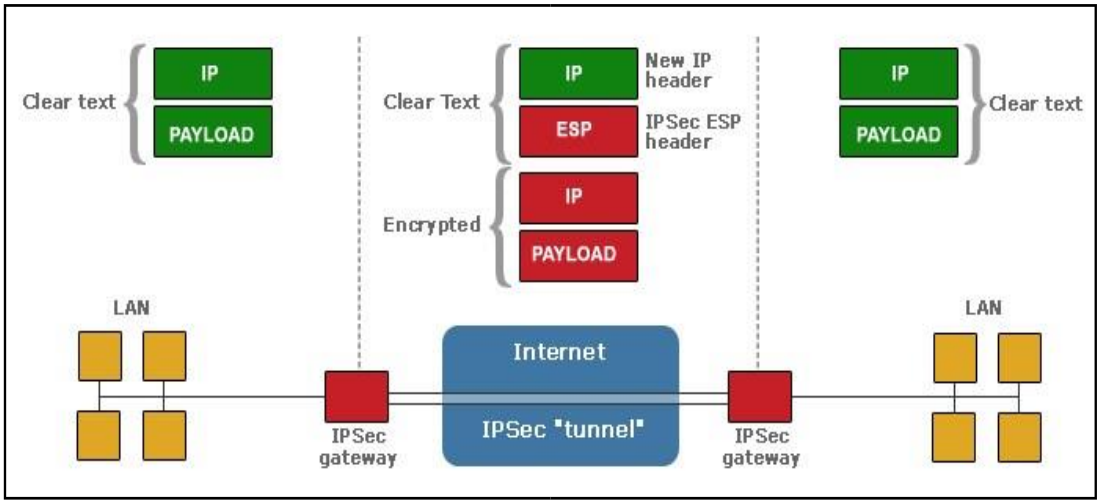

Figure 2: IPsec contains a gateway and a tunnel in order to secure communications. [17]

The current version and new version of the Internet Protocol are analysed to determine the security implications may be necessary. Although security may exist.

1. IPv4 Architecture

The protocol contains a couple aspects which caused problems with its use. These problems do not all relate to security. They are mentioned to gain a comprehensive understanding of the internet protocol and its shortcomings. The causes of problems with the protocol are:

1. Address Space
2. Routing
3. Configuration
4. Security
5. Quality of Service

The IPv4 architecture has an address that is 32 bits wide [6]. This limits the maximum number of computers that can be connected to the internet. The 32-bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution [5].

Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries [6]. Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period, but drastic change needs to be made to address this problem.

The TCP/IP-based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server [6]. This eases configuration hassles for the user but not the network's administrators.

The lack of embedded security within the IPv4 protocol has led to the many attacks seen today. Mechanisms to secure IPv4 do exist, but there are no requirements for their use [6]. IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication [6]. This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key.

When internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text-based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet. The quality of service for

streaming videos and music are much different from the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated [6].

2. Ipv6 Architecture

When IPv6 was being developed, emphasis was placed on aspects of the IPv4 protocol that needed to be improved. The development efforts were placed in the following areas:

1. Routing and addressing
2. Multi-protocol architecture
3. Security architecture
4. Traffic control

The IPv6 protocol's address space was extended by supporting 128-bit addresses. With 128 bit addresses, the protocol can support up to 3.4 10 ^38 machines. The address bits are used less efficiently in this protocol because it simplifies

addressing configuration. The IPv6 routing system is more efficient and enables smaller global routing tables. The host configuration is also simplified. Hosts can automatically configure themselves. This new design allows ease of configuration for the user as well as network administrator. The security architecture of the IPv6 protocol is of great interest. IPsec is embedded within the IPv6 protocol. IPsec functionality is the same for IPv4 and IPv6. The only difference is that IPv6 can utilize the security mechanism along the entire route [6].

The quality of service problem is handled with IPv6. The internet protocol allows for special handling of certain packets with a higher quality of service. From a high-level view, the major benefits of IPv6 are its scalability and increased security. IPv6 also offers other interesting features that are beyond the scope of this paper. It must be emphasized that after researching IPv6 and its security features, it is not necessarily more secure than IPv4. The approach to security is only slightly better, not a radical improvement.

V. COMMON INTERNET ATTACK METHODS

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack. Other forms of network intrusions also exist, such as land attacks, smurf attacks, and teardrop attacks. These attacks are not as well known as DoS attacks, but they are used in some form or another even if they are not mentioned by name.

1. Eavesdropping

Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. On the other hand, active eavesdropping is when the intruder listens and inserts something into the communication stream. This can lead to the messages being distorted. Sensitive information can be stolen this way [8].

2. Viruses

Viruses are self-replication programs that use files to infect and propagate [8]. Once a file is opened, the virus will activate within the system.

3. Worms

A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [8]. There are two main types of worms, mass-mailing worms and network aware worms. Mass mailing worms use email as a means to infect other computers. Network-aware worms are a major problem for the Internet. A network-aware worm selects a target and once the worm accesses the target host, it can infect it by means of a Trojan or otherwise.

4. Trojans

Trojans appear to be benign programs to the user, but will actually have some malicious purpose. Trojans usually carry some payload such as a virus [8].

5. Phishing

Phishing is an attempt to obtain confidential information from an individual, group, or organization [9]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information.

6. IP Spoofing Attacks

Spoofing means to have the address of the computer mirror the address of a trusted computer in order to gain access to other computers. The identity of the intruder is hidden by different means making detection and prevention difficult. With the current IP protocol technology, IP spoofed packets cannot be eliminated [8].

7. Denial of Service

Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors [9]. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

VI. TECHNOLOGY FOR INTERNET SECURITY

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the Internet. Different defence and detection mechanisms were developed to deal with these attacks.

1. Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

2. Firewall

A firewall is a typical border control mechanism or perimeter defence. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defence mechanism against intruders. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [8].

3. Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

4. Anti-Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so-called anti-Malware tools are used to detect them and cure an infected system.

5. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server by certificates. Clients present a certificate to the server to prove their identity.

VII. SECURITY IN DIFFERENT NETWORKS

The businesses today use combinations of firewalls, encryption, and authentication mechanisms to create “intranets” that are connected to the internet but protected from it at the same time. Intranet is a private computer network that uses internet protocols. Intranets differ from "Extranets" in that the former are generally restricted to employees of the organization while extranets can generally be accessed by customers, suppliers, or other approved parties.

There does not necessarily have to be any access from the organization's internal network to the Internet itself. When such access is provided, it is usually through a gateway with a firewall, along with user authentication, encryption of messages, and often makes use of virtual private networks (VPNs).

Although intranets can be set up quickly to share data in a controlled environment, that data is still at risk unless there is tight security. The disadvantage of a closed intranet is that vital data might not get into the hands of those who need it. Intranets have a place within agencies. However, for broader data sharing, it might be better to keep the networks open, with these safeguards:

1. Firewalls that detect and report intrusion attempts
2. Sophisticated virus checking at the firewall
3. Enforced rules for employee opening of email attachments
4. Encryption for all connections and data transfers
5. Authentication by synchronized, timed passwords or security certificates

It was mentioned that if the intranet wanted access to the internet, virtual private networks are often used. Intranets that exist across multiple locations generally run over separate leased lines or a newer approach of VPN can be utilized. VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee. Figure 3 is a graphical representation of an organization and VPN network.

VIII. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

1. Hardware Developments

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely influencing security. The most obvious use of biometrics for network security is for secure workstation logons for a workstation connected to a network. Each workstation requires some software support for biometric identification of the user as well as, depending on the biometric being used, some hardware device. The cost of hardware devices is one thing that may lead to the widespread use of voice biometric security identification, especially among companies and organizations on a low budget. Hardware device such as computer mice with built in thumbprint readers would be the next step up. These devices would be more expensive to implement on several computers, as each machine would require its own hardware device. A biometric mouse, with the software to support it, is available from around $120 in the U.S. The advantage of voice recognition software is that it can be centralized, thus reducing the cost of implementation per machine. At top of the range, a centralized voice biometric package can cost up to $50,000 but may be able to manage the secure login of up to 5000 machines.

The main use of Biometric network security will be to replace the current password system. Maintaining password security can be a major task for even a small organization. Passwords have to be changed every few months and people forget their password or lock themselves out of the system by incorrectly entering their password repeatedly. Very often people write their password down and keep it near their computer. This is of course completely undermines any effort at network security. Biometrics can replace this security identification method. The use of biometric identification stops this problem and while it may be expensive to set up at first, these devices save on administration and user assistance costs. Smart cards are usually a credit-card-sized digital electronic media. The card itself is designed to store encryption keys and other information used in authentication and other identification processes. The main idea behind smart cards is to provide undeniable proof of a user’s identity. Smartcards can be used for everything from logging in to the network to providing secure Web communications and secure e-mail transactions.

It may seem that smart cards are nothing more than a repository for storing passwords. Obviously, someone can easily steal a smart card from someone else. Fortunately, there are safety features built into smart cards to prevent someone from using a stolen card. Smart cards require anyone who is using them to enter a personal identification number (PIN) before they will be granted any level of access into the system. The PIN is similar to the PIN used by ATM machines.

When a user inserts the smart card into the card reader, the smart card prompts the user for a PIN. The administrator assigned this PIN to the user at the time the administrator issued the card to the user. Because the PIN is short and purely numeric, the user should have no trouble remembering it and therefore would be unlikely to write the PIN down.

But the interesting thing is what happens when the user inputs the PIN. The PIN is verified from inside the smart card. Because the PIN is never transmitted across the network, there is absolutely no danger of it being intercepted. The main benefit, though, is that the PIN is useless without the smart card, and the smart card is useless without the PIN.

2. Software Developments

The software aspect of network security is very vast. It includes firewalls, antivirus, VPN, intrusion detection, and much more. The research development of all security software is not feasible to study at this point. The goal is to obtain a view of where the security software is heading based on emphasis being placed now.

The improvement of the standard security software remains the same. When new viruses emerge, the antivirus is updated to be able to guard against those threats. This process is the same for firewalls and intrusion detection systems. Many research papers that have been skimmed were based on analysing attack patterns in order to create smarter security software.

As the security hardware transitions to biometrics, the software also needs to be able to use the information appropriately. Current research is being performed on security software using neural networks. The objective of the research is to use neural networks for the facial recognition software.

Many small and complex devices can be connected to the internet. Most of the current security algorithms are computational intensive and require substantial processing power. This power, however, is not available in small devices like sensors. Therefore, there is a need for designing light-weight security algorithms. Research in this area is currently being performed.

IX. CONCLUSION

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analysed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. The current development in network security is not very impressive.

Originally, it was assumed that with the importance of the network security field, new approaches to security, both hardware and software, would be actively researched. It was a surprise to see most of the development-taking place in the same technologies being currently used. The embedded security of the new internet protocol IPv6 may provide many benefits to internet users. Although some security issues were observed, the IPv6 internet protocol seems to evade many of the current popular attacks. Combined use of IPv6 and security tools such as firewalls, intrusion detection, and authentication mechanisms will prove effective in guarding intellectual property for the near future. The network security field may have to evolve more rapidly to deal with the threats further in the future.

REFERENCES

[1] Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998.

[2] Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08. IEEE International Conference on, pp.1469-1473, 19-23 May 2008.

[3] “Security Overview,” www.redhat.com/docs/manuals/enterprise/RHEL-4Manual/security-guide/ch-sgs-ov.html.

[4] Molva, R., Institute Eurecom,“Internet Security Architecture,” in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999.

[5] Sotillo, S., East Carolina University, "IPv6 security issues," August 2006, www.infosecwriters.com/ text_resources/pdf/IPv6_SSot illo.pdf.

[6] Andress J., "IPv6: the next internet protocol," April 2005, www.usenix.com/publications/login/ 2005-04/pdfs/ andress0504.pdf.

[7] Warfield M., "Security Implications of IPv6," Internet Security Systems White Paper, documents.iss.net/ whitepapers/IPv6.pdf

[8] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.

[9] Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68-72, Nov.-Dec. 2005.

[10] "Internet History Timeline," www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.htm.

[11] Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no.12, pp.2034-2051, Dec 1997.

[12] "Intranet." Wikipedia, The Free Encyclopedia. 23 Jun 2008, 10:43 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Intranet&ol did=221174244>.

[13] "Virtual private network." Wikipedia, The Free Encyclopedia. 30 Jun 2008, 19:32 UTC. Wikimedia Foundation, Inc. 2 Jul 2008 <http://en.wikipedia.org/w/index.php?title=Virtual_private_network&oldid=222715612>.

[14] Tyson, J.,"How Virtual private networks work," http://www.howstuffworks.com/vpn.htm.

[15] Al-Salqan, Y.Y., "Future trends in Internet security," Distributed Computing Systems, 1997., Proceedings of the Sixth IEEE Computer Society Workshop on Future Trends of , vol., no., pp.216-217, 29-31 Oct 1997.

[16] Curtin, M. "Introduction to Network Security,"http://www.interhack.net/pubs/network-security.

[17] "Improving Security," http://www.cert.org/tech_tips, 2006.

[18] Serpanos, D.N.; Voyiatzis, A.G., "Secure network design: A layered approach," Autonomous Decentralized System, 2002. The 2nd International Workshop on, vol., no., pp. 95-100, 6-7 Nov. 2002.

[19] Ohta, T.; Chikaraishi, T., "Network security model," Networks, 1993. International Conference on Information Engineering '93. 'Communications and Networks for the Year 2000', Proceedings of IEEE Singapore International Conference on, vol.2, no., pp.507-511 vol.2, 6-11 Sep 1993.