ISSN: 2455 – 5428
International Journal of Current Research and Modern Education
Impact Factor 6.725, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

NETWORK SECURITY

R. Bhuvana Indumathi* & R. Bhuvaneswari**
Assistant Professor, Department of Home Science, Sri Sarada College for Women, Salem, Tamilnadu

Cite This Article: R. Bhuvana Indumathi & R. Bhuvaneswari, "Network Security", International Journal of Current Research and Modern Education, Special Issue, January, Page Number 50-52, 2017.

Introduction:

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for 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 for 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. 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, information can be obtained by special programs, such as "Trojan horses," planted in the routers. 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.

History of Network Security:

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. The 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. 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, the term "hacker" is coined by a couple of Massachusetts Institute of Technology (MIT) students. The Department of Defense began the ARPA Net, which gains popularity as a conduit for the electronic exchange of data and information. 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. In the 1990s, Internet became public and the security concerns increased tremendously. Approximately 950 million people use the internet today worldwide. On any day, there are approximately 225 major incidences of a security breach. 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.

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:

- ✓ Access – authorized users are provided the means to communicate to and from a particular network
- ✓ Confidentiality – Information in the network remains private

ISSN: 2455 – 5428
International Journal of Current Research and Modern Education
Impact Factor 6.725, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

- ✓ Authentication – Ensure the users of the network are who they say they are
- ✓ Integrity – Ensure the message has not been modified in transit
- ✓ 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. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed throughout this research endeavor. 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 which circumvents some of the common security problems.

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 aren't mentioned by name.

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.

Viruses:

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

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. 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.

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.

Phishing:

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

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.

Denial of Service:

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

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 defense and detection mechanisms were developed to deal with these attacks.

ISSN: 2455 – 5428
International Journal of Current Research and Modern Education
Impact Factor 6.725, Special Issue, January - 2017
International Conference on Smart Approaches in Computer Science Research Arena
On 5th January 2017 Organized By
Department of Computer Science, Sri Sarada College for Women (Autonomous), Salem, Tamilnadu

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.

Firewall:

A firewall is a typical border control mechanism or perimeter defense. 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 defense 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.

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.

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.

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 through the use of certificates. Clients present a certificate to the server to prove their identity.

Future Trends in Security:

What is going to drive the Internet security is the set of applications more than anything else. The future will possibly be that the security is similar to an immune system. The immune system fights off attacks and builds itself to fight tougher enemies. Similarly, the network security will be able to function as an immune system. The trend towards biometrics could have taken place a while ago, but it seems that it isn't being actively pursued. Many security developments that are taking place are within the same set of security technology that is being used today with some minor adjustments.

Conclusion:

Network security is an important field that is increasingly gaining attention as the internet expands. The security threats and internet protocol were analyzed to determine the necessary security technology. The security technology is mostly software based, but many common hardware devices are used. 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. International conference on, pp.1469- 1473, 19- 23 may 2008.
3. "Security overview," www.redhat.com/docs/manuals/enterprise/rhel - 4 - manual/security - guide /ch - sgs - ov.html.
4. molva, r., instituteurecom, "internet security architecture, " in computer networks & isdn systems journal, vol. 31, pp. 787- 8 04, 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.