Review on Network Security Aspects (Introduction to Vulnerabilities, Threats, and Attacks)

Jincy T J
Government guest lecturer,
Department of BCA,
Mercy College
Palakkad, Kerala, 678706

***Abstract*--Attacks on your network can happen anytime and come from anywhere. Nobody wants to leak their company data or important information. There are so many attacks and hacking processes in/out your company with the goal of stealing your intellectual information. So here is the need of network security. Security is crucial to networks and all of the applications. We want to secure our hardware as well as software equally. The software must be periodically updated and managed to protect you from emerging threats. The range of study involves a brief history dating back to internet's beginnings and the current development in network security.**

I. INTRODUCTION

Network can be classified in to two Peer-to-peer network and client server network based on the network administration. The network security is provided by a network administrator or system administrator. The administrator implements the security policy. The network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access.

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. A network security system typically relies on layers of protection and consists of multiple components including networking monitoring and security software in addition to hardware and appliances. All components work together to increase the overall security of the computer network.

II. WHAT IS A NETWORK?

A network has been defined as any set of interlinking lines resembling a net, a network of roads an interconnected system, a network of alliances. This definition suits our purpose well: a computer network is simply a system of interconnected computers. Computer network can be used for numerous services, both for companies and individuals. For companies network of personal computers using shared server often provide access to corporate information. Typically they follow the client server model. For individuals, network offers access to a variety of information and entertainment resources.

A. The ISO/OSI Reference Model

The International Standards Organization (ISO) Open Systems Interconnect (OSI) Reference Model defines seven layers of communications types, and the interfaces among them. Each layer depends on the services provided by the layer below it, all the way down to the physical network hardware, such as the computer's network interface card, and the wires that connect the cards together. The given below figure shows the ISO/OSI 7 layers.

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL

B. Differentiating Data Security and Network Security

Data security is the aspect of security that allows a client's data to be transformed into unintelligible data for transmission. Strong cryptography in the past can be easily broken today. Cryptographic methods have to continue to advance due to the advancement of the hackers as well. When transferring cipher text over a network, it is helpful to have a secure network. A secure network will also prevent someone from inserting unauthorized messages into the network. Therefore, hard ciphers are needed as well as attack hard networks.

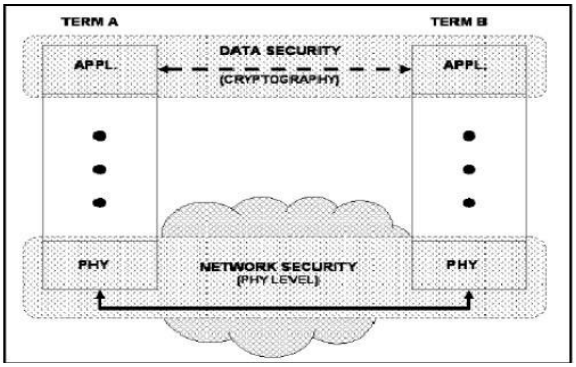

Figure: Based on the OSI model, data security and network security have a different security function

The relationship of network security and data security to the OSI model is shown in Figure. It can be seen that the cryptography occurs at the application layer; therefore the application writers are aware of its existence. Layers above the physical layers are also used to accomplish the network security required. Authentication is performed on a layer above the physical layer.

C. *Internet Protocol*

Features	IPV4	IPV6
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

D. *Internet and security aspects*

Internet is the collection of network. We can collect information, share data from anywhere. Fear of security breaches on the Internet is causing organizations to use protected private networks or intranets. The Internet Engineering Task Force (IETF) has introduced security mechanisms at various layers of the Internet Protocol Suite. The security architecture of the internet protocol, known as IP Security, is a standardization of internet security.

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 reinsert 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. Access to the network
2. Confidentiality
3. Authentication
4. Integrity
5. Non repudiation

E. *Introduction to Vulnerabilities, Threats, and Attacks*

There are four main computer security attributes. They were mentioned before in a slightly different form, but are restated for convenience and emphasis. These security attributes are confidentiality, integrity, privacy, and availability.

Computer security attributes	Attack methods	Technology for Internet security
Confidentiality	Eavesdropping Hacking phishing Dos and IP spoofing	IDS, firewall Cryptographic systems IP Sec and SSSL
Integrity	Viruses worms Trojans Eavesdropping Dos and IP spoofing	IDS, firewall Anti Malware software IP Sec and SSSL
privacy	Email bombing spamming hacking Dos and cookies	IDS, firewall Anti Malware software IP Sec and SSSL
availability	Email bombing spamming hacking Dos and cookies and system boot record infectors	IDS, firewall Anti Malware software

III. INTRODUCTION TO VULNERABILITIES, THREATS, AND ATTACKS

Common attack methods and the security technology will be briefly discussed. When discussing network security, the three common terms used are as follows:

- *Vulnerability*
- *Threats*
- *Attack*

A. *Vulnerabilities*

A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.

Vulnerabilities in network security can be summed up as the "soft spots" that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network. Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

■ Technology weaknesses
■ Configuration weaknesses
■ Security policy weaknesses

B. Threats

The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.

There are four primary classes of threats to network security,

Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company

Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.

External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents.

C. Attacks

The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops. Some kinds of attacks are

- Eavesdropping
- Viruses
- IP Spoofing Attacks
- Denial of Service

D. 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. Some of them are

Cryptographic system, Firewal, Intrusion Detection Systems, AntiMalware Software and scanners, Secure Socket Layer

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.

IV. 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. 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 four primary threats to network security include unstructured threats, structured threats, external threats, and internal threats. To defend against threats, an understanding of the common methods of attack must be established, including reconnaissance, access, DoS, and malicious code. Responses to security issues range from ignoring the problem to excessive spending on security devices and solutions. Neither approach will succeed without a good, sound policy, and highly skilled security professionals. The network security field may have to evolve more rapidly to deal with the threats further in the future.

REFERENCES

1. "Securi ty Overview," www.redhat.com/docs/manuals/enterprise/RHEL4 Manual/security guide/chsgsov.html.
2. Molva, R., Institute Eurecom, "Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787804, April 199913
3. Sotillo, S., East Carolina University, "IPv6 security issues," August 2006, www.infosecwriters.com/text_resources/pdf/IPv6_ SSot illo.pdf.
4. Andress J., "IPv6: the next internet protocol," April 2005, www.usenix.com/publications/login/2005 04/pdfs/andress0504.pdf.
5. Warfield M., "Security Implications of IPv6," Internet Security Systems White Paper,documents.iss.net/whitepapers/IPv6.pdf
6. Adeyinka,O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.7782, 1315 May 2008
7. Marin,G.A., "Network security basics," Security& Privacy, IEEE , vol.3, no.6, pp. 6872,Nov.Dec. 2005
8. "Internet History Timeline," www3.baylor.edu/~Sharon_P_Johnson/etg/inthistor y.htm
9. Landwehr, C.E.;Goldschlag,D.M., "Security issues in networks with Internet access," Proceedings of the IEEE, vol.85, no.12, pp.20342051, Dec 1997