International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.5., 2015
(Sept.-Oct.)

REVIEW ARTICLE

ISSN: 2321-7758

COMPUTER NETWORK ADMINISTRATION AND SECURITY

AJAY KUMAR[1], PREETI YADAV[2]

[1]Asst. Prof. in IGU Meerpur Rewari(Haryana)
[2]Asst. Prof. in Govt college Gurgoan(Haryana)

International Journal of Engineering Research-online (IJOER)

ISSN:2321-7758
www.ijoer.in

ABSTRACT

Network security has become most important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern Network security is main issue of this generation of computing because many types of attacks are increasing day by day. Establishing a network is not a big issue for network administrators but protecting the entire network is a big issue. There are various methods and tools are available today for destroying the existing network. In this paper we mainly emphasize on the network security also we present some major issues that can affect our network.

Keywords— Network Security, Threats, Cryptography, Ping.

I. INTRODUCTION

The security of network is a big issue for security administrators because network is growing day by day. Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues:

1. Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer.
2. Each and every client who is working on the internet wants security of information .Information is an asset that must be protected.
3. Network security is the process by which digital information assets are protected, the goals of security are to protect confidentiality, maintain integrity, and assure availability.

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. The vast topic of network security is analyzed 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. BASIC TYPES OF ATTACKS

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 ARPANet, which gains popularity as a conduit for the electronic exchange of data and information. During the 1970s, the Telnet protocol was developed. During the 1980s, the hackers and crimes relating to computers were beginning to emerge.

III. INTERNET ARCHITECTURE AND VULNERABLE SECURITY SPECTS

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

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.

IV. PV4 AND IPV6 ARCHITECTURES

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

1. 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.

2. Attacks through the Current Internet Protocol IPv4

There are four main computer security attributes. These security attributes are confidentiality, integrity, privacy, and availability. Confidentiality and integrity still hold to the same definition. Availability means the computer assets can be accessed by authorized people .Various attack methods relate to these four security attributes. Common attack methods and the security technology will be briefly discussed.

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

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.

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.

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.

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.

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.

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 un intelligible 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.

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

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.

VI. SECURITY ISSUES OF IP PROTOCOL IPV6

From a security point of view, IPv6 is a considerable advancement over the IPv4 internet protocol. Despite the IPv6's great security mechanisms, it still continues to be vulnerable to threats. Some areas of the IPv6 protocol still pose a potential security issue. The new internet protocol does not protect against servers, poorly designed applications, or poorly protected sites. The possible security problems emerge due to the following:

1. Header manipulation issues
2. Flooding issues
3. Mobility issues

Header manipulation issues arise due to the IPsec's embedded functionality. Extension headers deter some common sources of attacks because of header manipulation. The problem is that extension headers need to be processed by all stacks, and this can lead to a long chain of extension headers. The large number of extension headers can overwhelm a certain node and is a form of attack if it is deliberate. Spoofing continues to be a security threat on IPv6 protocol. A type of attack called port scanning occurs when a whole section of a network is scanned to find potential targets with open services. The address space of the IPv6 protocol is large but the protocol is still not invulnerable to this type of attack. Mobility is a new feature that is incorporated into the internet protocol IPv6. The feature requires special security measures. Network administrators need to be aware of these security needs when using IPv6's mobility feature.

VII. CURRENT DEVELOPMENTS IN NETWORK SECURITY

The network security field is continuing down the same route. 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. The research being performed assists in understanding current development and projecting the future developments of the field.

1. Hardware Developments

Hardware developments are not developing rapidly. Biometric systems and smart cards are the only new hardware technologies that are widely impacting security. 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. The main use of Biometric network security will be replacing 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 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'll 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. This PIN was assigned to the user by the administrator 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's 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, 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 still 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 analyzing 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 .Research in this area is currently being performed.

VIII. FUTURE TRENDS IN SECURITY

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.

IX. 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 network security field may have to evolve more rapidly to deal with the threats further in the future. Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc.

A. Security Threats. There are a number of security threats that can be the cause of a network security attack. Main security threats are denial of service, distributed denial of service, viruses, Trojan horses, spywares, malwares, unauthorized access to the network resources and data, accidental deletion of the files and the uncontrolled internet access.

B. Virus Attack. A computer virus is a small program or an executable code that when executed and replicated, perform different unwanted and harmful functions for a computer and a network. Viruses can destroy your hard disks and processors, consume memory at a very large scale and destroy the overall performance of a computer or network. A Trojan is a malicious code that performs harmful actions but it cannot be replicated.

C. Unauthorized Access. Access to the network resources and data should be allowed only to the authorized persons. Every shared folder and resources in your network should have been accessed only by the authorized persons and should also be scanned and monitored regularly.

D. Information Theft and cryptography attacks. Another threat to a network is to loss of the important information and this loss can be prevented, if you good encryption methods.

E. Unauthorized application installations .Another virus and security attack prevention method is to install only the authorized software applications to our network server and your all client computers. Nobody should be allowed to install any kind of program which can cause security threats such as songs or video programs, gaming software or other web based applications.

X. BASIC SECURITY TIPS

This basic Network Security useful security tips and methods to secure your network such as installing a update antivirus program, email scanning programs, network monitoring tools, internet access policy and other security prevention methods. Network security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security is a very important aspect of a computer network. Keeping the computer as well as network secure is the big responsibility of the network administrator and the security specialists. Regularly scan all the network devices, emails, open ports, server and client computers. It's the responsibility of the network administrators to check the missing security patches in all the network computers. They should also remove the unnecessary network shares, user's accounts, wireless access points and restrict the access to the network.

XI. 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/RHEL4 anual/security guide/chsgsov.html.

[4] Molva, R., Institut Eurecom,"Internet Security Architecture," in Computer Networks & ISDN Systems Journal, vol. 31, pp. 787-804, April 1999 13

[5] Sotillo, S., East Carolina University, "IPv6 security issues," August2006,www.infosecwriters.com/ text_resources/pdf/IPv6_ SSot illo.pdf.

[6] Andress J., "IPv6: the next internet protocol," April 2005, www.senix.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.2Jul2008<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

[20] Akin T.,"Hardening Cisco Routers,"O'Reilly & Associates, 2002.

[21] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323.

[22] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advnaced Communication Technology, 2004.

[23] "Internet History Timeline," www3. baylor.edu/~Sharon_P_ Johnson/etg/inthistory.htm.