VOL. 8, NO. 12, DECEMBER 2013 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

ENHANCED NETWORK SECURITY SYSTEM USING FIREWALLS

Nur Amalina[1], Raed Alsaqour[1], Mueen Uddin[2, 3], Ola Alsaqour[4] and Mohammed Al-Hubaishi[5,6]
[1]School of Computer Science, Faculty of Information Science and Technology, University Kebangsaan Malaysia, Bangi, Selangor, Malaysia
[2]Kulliah of Information and Communication Technology, International Islamic University Malaysia, Malaysia
[3]Asia Pacific University of Technology and Innovation, Kuala Lumpur, Malaysia
[4]Department of Computer Engineering, Faculty of Engineering and Technology, the University of Jordan, Amman, Jordan
[5]Faculty of Computer Science and Information System, Thamar University, Thamar, Republic of Yemen
[6]LAB, FCT-DEEI, Universidade Algarve Portugal, Faro, Portugal
E-Mail: raed.ftsm@gmail.com

ABSTRACT

The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. This paper discusses the security of computing systems and shows how to protect computer-related assets and resources. The paper highlights different security threats and concerns across computer networks and shows how firewalls detect these threats. At the end, different firewalls like Packet Filtering, Application Gateways and Personal Firewall are summarized and compared according to different network scenarios. The paper also proposes a new framework for the vulnerability, threat management and safeguard of network environments.

Keywords: security system, firewalls, threats, packet filtering, application gateways.

INTRODUCTION

In the last few years, the Internet has experienced an explosive growth. Along with the widespread evolution of new emerging services, the quantity and impact of attacks have been continuously increasing [1]. Defense system and network monitoring has become an essential component of the computer security to predict and prevent attacks. With the thriving technology and the great increase in the usage of computer networks, the risk of having these network to be under attacks have been increased. We interact with network every day and perform banking transaction, surfing Internet, buy online goods and pay it using online transaction. Life without networks would be considerably less convenient and many activities would be impossible.

Threats to computer security are computer crimes, including viruses, electronic break-ins, and natural and other hazard. Security measures consist of encryption, restricting access, anticipating disasters and making backup copies. Keeping information private depends on keeping computer systems safe from criminals, natural hazard and other threats. Computer crime is an illegal action which the perpetrator uses special knowledge of computer technology. Number of techniques have been created and designed to help in detecting and/or preventing such attacks [2].

NETWORK CONCEPTS

A network is a group of systems that are connected either using wired or wireless technology to allow sharing of resources, such as files, printers, or sharing of services, such as an Internet connection [3, 4]. The nodes in network can be computers, printers; connecting devices or any other components used for sending and receiving the data generated by other devices on the network (see Figure-1). The links connecting the devices are called communication channels in wireless networks.

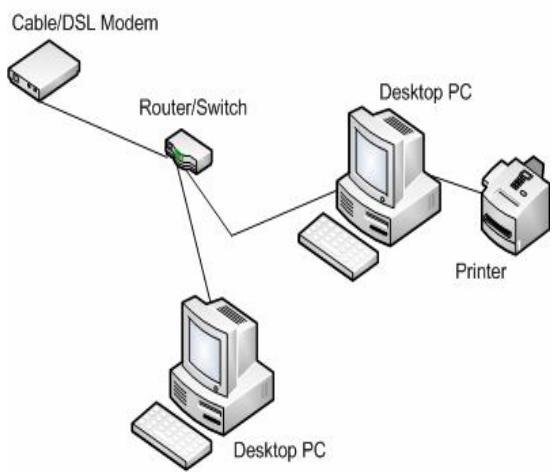

Figure-1. Basic network concept.

As networks become more common, several security issues and challenges are becoming more apparent. Some standard technologies currently used on the Internet are not secure. Awareness is the key if we want to further secure networks from infiltration. From the normal user's perspective, a network is sometimes designed in such a way that it looks like two end points with a single connection in the middle. Although this perspective view is functionally correct but sometimes it ignores the complex design, such as implementation and management of the network concept.

Categories of networks

The categories of networks are LAN, MAN and WAN. These networks are categories by their scope and geographical coverage area. The networks are continuously experiencing staggering and scaling growth as users demands increase. More people use the Internet to get connected to others and find and share information and other resources. Different types of networks are differentiated based on their size (in terms of the number of machines), their data transfer speed and their reach. Local Area Network (LANs) is a smaller network compared with Wide Area Network (WANs), which is simply a combination of multiple LAN networks. Metropolitan Area Network (MANs) is a network scattered in metropolitan cities and covers relatively smaller geographical area compare to a WAN network. Generally, they are localized to a single city or region. The network types are shown in Figure-2.

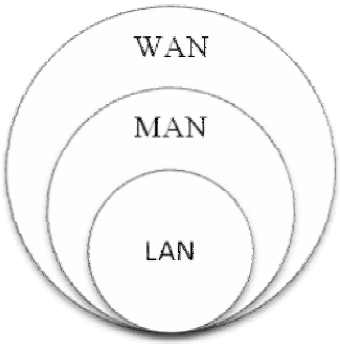

Figure-2. Types of network.

Local area network (LAN)

As shown in Figure-3, a LAN is a group of computers belonging to the same organization, in which all computers and other devices are linked within a small geographic area and using the same technology such as Ethernet and WiFi. LAN links several small components such as computers, word processors, printers and file storage devices. These components form a network within an office or building. The data transfer speed can reach from 10 Mbps to 1 Gbps depending on the devices and cabling system installed. The number of nodes can vary from 100 to 1000's nodes. Ethernet LAN is the most common type of LAN network available. The smallest home LAN network can have exactly two computers and a large LAN can contain thousands of computers. LANs can be divided into logical groups called subnets. An Internet Protocol (IP) "Class A" LAN can theoretically accommodate more than 16 million devices organized into subnets.

LAN networks are classified as Peer-to-peer networks [5] and Server-based networks [6]. A peer-to-peer network operates with no dedicated servers on the network. In this type of network, each host functions as a client and server. The computer systems are connected to each other via the Internet using IP such as Virtual Private Network connection [7]. The user's files can be shared directly between systems on the network without the need of a central server and they can determine what information or files they are willing to share with the other hosts on the network. However, Server-based networks have at least one host, which is dedicated to function as server. Client computers do not share any information with each other computers. All data is stored on the central server. Most corporate networks are based on this methodology. Within a Server-based network type, servers can play several roles.

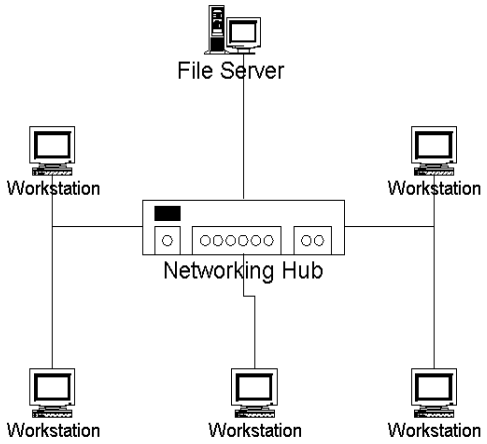

Figure-3. Local area network.

Metropolitan area network (MAN)

MANs are design to extend over an entire city. MANs are larger than a LANs networks but smaller than WAN. MAN networks adopt technologies from both LANs and WANs to serve its purpose as shown in Figure-4. MANs are typically owned by a large company or a government. Some legacy technologies used for MANs are ATM [8]. At the physical level, MAN links between LANs have been built on fiber optical cables or using wireless technologies called WiMAX [9]. MAN can also be a single network such as cable television network, or it may be a means of connecting a number of LANs into a larger network so that resources may be shared.

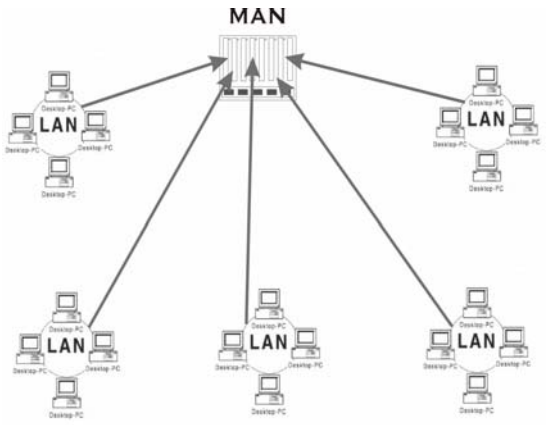

Figure-4. Metropolitan area network.

Wide area network (WAN)

WAN network covers long distances, and their communication facilities are provided by separate organizations. WANs differ from LAN in terms of size of network or distance and control or ownership. As shown in Figure-5, WANs are simply combinations of LANs, MANs and additional communications links between the LANs. WAN may belongs to a company with many offices, it may be even in different cities or countries, or it may be a cluster of independent organizations within a few miles of each other that share the network.

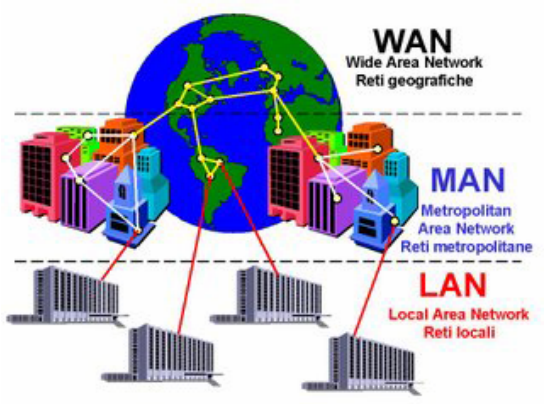

Figure-5. Wide area network.

Security issues in networks

Nowadays with the spreading of the Internet and online procedures requesting a secure channel, it has become an inevitable requirement to provide the network security. There are various threat sources including software bugs mostly as the operating systems and software used becomes more functional and larger in size. Intruders who do not have rights to access these data can steal valuable and private information belonging to network users. As network become more common, several security issues are becoming more apparent. Some antivirus and security network technology are not secure. A National Research Council report warned in 1991 that "emerging trend, point to growth in both level and the sophistication of threats. There is reason to believe that we are at a discontinuity: with respect to computer security, the past is not a significant predictor of the future". Events since 1991 have validated this belief [10].

Implications of security challenges are always discussed nowadays. Since networks are carrying and holding information of all types around the world, it is exceedingly attracting the targets to attack and take away important data and other resources. Networks bring more resources within the reach of more potential attackers. Like threats to computing systems, threats to networks can compromise confidentiality and integrity of devices and data stored.

There are different motivations why the attackers always attack and want to harm networks in a computing environment. A clever attacker investigates and plans before acting. Information is the attacker's greatest weapon. Insiders may collect the system information that they are authorized and provide to intruders. In order to obtain passwords or other secrets, outside intruders use social engineering and other tricks to attack networks and steal important information. Besides that, an easy way to gather network information is to use port scan, a program for a particular IP address, that reports which port respond to messages and which of several known vulnerabilities seem to be present. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate use in managing networks, but it also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Network security techniques

There are many security techniques currently available, this paper will discuss about firewalls and their types used to scan networks for security attacks.

Firewall

Firewalls were invented in early 1990s. They provide a fireproof barrier between parts of the buildings, making it harder for a fire in one part of the building to spread to other parts. Similarly, a network firewall is built around a network or subnetwork to protect it from the outside. Steven and William in [11] defines firewall as a collection of components placed between an inner network and an outer network to achieve the following goals; all traffic must pass through the firewall, only traffic that is authorized by the inner network's security policy is allowed to pass, the firewall cannot be penetrated [8]. Figure-6 illustrates a firewall usually located between the external world and the internal network.

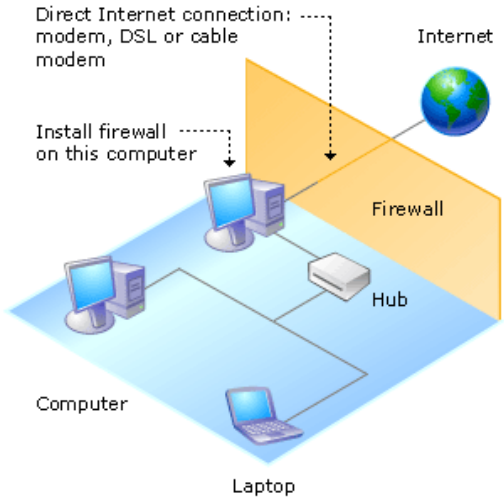

Figure-6. Firewall concept.

Firewalls are hardware or software systems placed in between two or more computer networks to stop

the committed attacks, by isolating these networks using the rules and policies determined for them. The firewall may protect a poorly secured network from external threats. Their use across the firewall can be prevented, while use inside the firewall is allowed. Firewall provides boundary service to the LAN network, making sure that all connection to and from the internal network passes through the firewall. A firewall can be figured to allow specific protocols to pass through the firewall if predefined criteria are met. Criteria also can be set to reject a packet if it does not pass inspection. The most powerful firewall mechanisms are packet filtering, application gateways and personal firewall [12-14]. Firewalls often provide authentication service.

Packet filtering

Network layer firewalls, also known as packet filtering, allows only certain packets to pass through the firewall. Each packet is compared to a set of rules configured for the interface. Rules can be set for both incoming and outgoing packets. The rules are based on information in the transport protocol header and the IP header. Table-1 shows some of the packet filter rules that can be established on a firewall.

Table-1. Packet filter rules.

Rule #	Interface	Protocol	IP source	Source port	IP destination	Destination port
1	Internal	TCP	172.16.2.*	*	*	80
2	Internal	TCP	172.16.2.*	*	*	23
3	Internal	TCP	172.16.2.*	*	192.168.3.5	25
4	Internal	TCP	172.16.2.*	*	192.168.3.5	110
5	Internal	UDP	172.16.2.*	*	*	69
6	External	TCP	*	*	172.16.2.100	80

An asterisk (*) is a wildcard character that allows any valid entry for an IP address or port address to replace it.

This set of rules denies all packets except specified protocols and ports that are explicitly allowed through the firewall. The rules 1 allows any hosts in 172.16.2.* network to browse Internet resources with a Web browser on port 80. The rules 2 allows any hosts in 172.16.2.* network to connect to Telnet servers on an external network. The rules 3 allows any hosts in 172.16.2.* network to send mail through SMTP to the SMTP server at IP address 192.168.3.5. The rules 4 allows any hosts in 172.16.2.* network to receive POP3 mail from the POP3 server at IP address 192.168.3.5. The rules 5 allows any hosts in 172.16.2.* network to use TFTP to connect to any TFTP servers on the external network. The rules 6 allow all external hosts to connect to the internal Web server at IP address 172.16.2.100.

Application gateways

Compared to packet filtering, an application gateway uses higher-layer protocol information and implements additional security services, as well as more complex and customized policies. It is typically implemented on one or more host computers and involves custom software developed for the organization [6]. An application gateway provides proxy services that control access to the real services, such as Telnet and FTP. An outside user cannot use a service that has no proxy. Many organizations use mail gateways. A gateway can perform user identification and authentication for remote users. It can allow carefully limited traffic between two sub networks.

Personal firewall

A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Personal Firewall works in the application layer of firewall. Personal firewall runs on a workstation to block unwanted traffic, usually from the network. It can complement the work of a conventional firewall by screening the kind of data a single host will accept, or it can compensate for the lack of a regular firewall as cable or modem connection.

It is difficult to separate entirely advances in firewall technology from the commercial products that implement them. There is a large market for commercial firewall products, which has driven many crucial recent developments. At the same time, without direct inspection of the source code, it can be quite difficult. Commercial implementations of personal firewall include Norton Firewall from Symantec, Kaspersky Internet Security, Lavasoft Personal Firewall and MCAfee Personal Firewall.

Comparison between firewalls

Table-2 shows the comparison of different types of firewalls, and summarizes them according to their types and advantages and implementation.

Table-2. Comparison of firewalls.

Packet filtering	Application gateways	Personal firewall
Simplest	More complex	Similar to Packet Filtering
Sees only addresses and service protocol type	Sees full data portion of packet	Can see full data portion of packet
Auditing difficult	Can audit activity	Can audit activity
Screens based on connection rules	Screen based on behavior proxies	Typically, screens based on information in a single packet
Complex addressing rules can make configuration tricky	Simple proxies can substitute for complex addressing rules	Usually starts in "deny all inbound" mode, to which user adds trusted addresses as they appear

Framework of vulnerabilities threats and safeguard

The concepts of the vulnerability, threat and safeguard make up a useful technique for generating new ideas to build a framework of network security. Vulnerability [15] is a weakness or gap in a network system that could allow security to be violated. Vulnerabilities may result from weak passwords, software bugs, a computer virus or a script code injection, no antivirus and a SQL injection. A threat is a circumstance or event that could cause harm by violating security. A threat often exploits vulnerability. A safeguard [16] is any technique or procedure or any other measure that reduces vulnerability. A safeguard makes threats weaker or less risky. Safeguards are also called counter measures and their management is called controls.

This framework of the vulnerability, threat and safeguard are useful to security analyzing, and evaluating for deciding, which safeguards mechanisms to apply and use. Therefore, there is a relationship between framework elements as shown in Figure-7 below, which we represent vulnerability as V, threat as T and safeguard as S. Meanwhile, the proposed framework presents itself as the box which inside the box are computing system (V) with its procedures and controls (S). In contrast, outside the box is the threats (T), including the authorized users. In addition, a circle represents active events in the framework. This scenario describe how does framework behaves to save our system as we consider that safeguard S1 guards against the threat T1 which attempt to attack vulnerability V1 and also S2 guards against T2 which attempt to attackV2. Finally, S3 and S4 represented by the curved boundary, guards against any others threats that exploiting any of the vulnerabilities of the proposed framework.

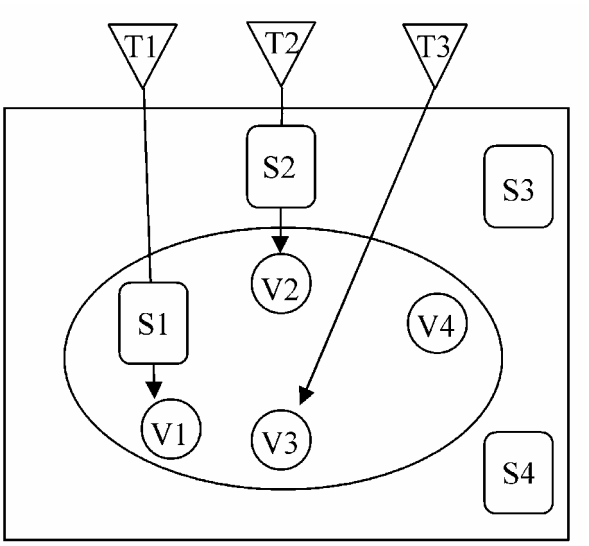

Figure-7. Framework of the vulnerability, threat and safeguard.

CONCLUSIONS

Networking technology and applications are advancing rapidly and network security is struggling to catch up. Networking is the source of many computer security threats and it magnifiers others. Secure computing depends on the secure network and vice versa. With networking technology increasingly under attack, it's no wonder that people are starting to take network security more seriously. In this article, we have shown some issues in network security as well as a general idea of a new framework of the vulnerability, threat and safeguard. In future work, we aim to implement this framework in the real network with different scenarios.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the support of this work by the Centre for Research and Instrumentation Management (CRIM), University Kebangsaan Malaysia UKM), Malaysia. Grant numbers: UKM-GGPM-ICT-035-2011 and UKM-GUP-2012-089.

REFERENCES

[1] M. Abdelhaq, R. Alsaqour, M. Al-Hubaishi, T. Alahdal and M. Uddin. 2014. The Impact of Resource Consumption Attack on Mobile Ad-hoc Network Routing. International Journal of Network Security. 16: 399-404.

[2] M. Uddin, A. A. Rehman, N. Uddin, J. Memon, R. Alsaqour and S. Kazi. 2013. Signature-based Multi-Layer Distributed Intrusion Detection System using Mobile Agents. International Journal of Network Security. 15: 79-87.

[3] C. Hunt. 2010. TCP/IP network administration: O'reilly.

[4] M. Uddin, R. Alsaqour and M. Abdelhaq. 2013. Intrusion Detection System to Detect DDoS Attack in Gnutella Hybrid P2P Network. Indian Journal of Science and Technology. 6: 71-83.

[5] G. Fox. 2001. Peer-to-peer networks. Computing in Science and Engineering. 3: 75-77.

[6] Z.-L. Zhang, Y. Wang, D. H. Du and D. Shu. 2000. Video staging: a proxy-server-based approach to end-to-end video delivery over wide-area networks. IEEE/ACM Transactions on Networking (TON). 8: 429-442.

[7] C. Mahalakshmi and M. Ramaswamy. 2012. Data transfer strategy for multiple destination nodes in virtual private networks. Journal of Engineering & Applied Sciences. 7: 1372-1378.

[8] J.-Y. Le Boudec. 1992. The asynchronous transfer mode: a tutorial. Computer Networks and ISDN systems. 24: 279-309.

[9] J. G. Andrews, A. Ghosh and R. Muhamed. 2007. Fundamentals of WiMAX: understanding broadband wireless networking: Pearson Education.

[10] R. C. Summers. 1997. Secure computing: threats and safeguards: McGraw-Hill, Inc.

[11] W. R. Cheswick, S. M. Bellovin and A. D. Rubin. 2003. Firewalls and Internet security: repelling the wily hacke. Addison-Wesley Longman Publishing Co., Inc.

[12] D. B. Chapman. 1992. Network (in) security through IP packet filtering. In: Proceedings of the 3rd UNIX Security Symposium.

[13] C.-X. Qi and Q.-D. Du. 2009. A Smart IVR system based on application gateways. In Hybrid Intelligent Systems. HIS'09. 9th International Conference on. pp. 110-115.

[14] A. Herzog and N. Shahmehri. 2007. Usability and security of personal firewalls. In New Approaches for Security, Privacy and Trust in Complex Environments, Ed: Springer. pp. 37-48.

[15] S. Jajodia, S. Noel and B. O'Berry. 2005. Topological analysis of network attack vulnerability. In Managing Cyber Threats, Ed: Springer. pp. 247-266.

[16] P. Qianwei. 2002. The crisis of and safeguard for network information environment [J]. Researches in Library Science. 5: 017.