3rd International Conference on Recent Innovations in Science Engineering and Management
Sri Venkateswara College of Engineering and Technology,Srikakulam,Andhra Pradesh (ICRISEM-16)
27 February 2016, www.conferenceworld.in ISBN: 978-81-932074-1-3

NETWORK SECURITY AND FUTURE

Nishi Parmar[1], Sakshi Mittal[2], Salomisara Thomas[3]

[1,2,3]*Dronacharya College of Engineering, Gurgaon (India)*

ABSTRACT

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become ``wired'', an increasing number of people need to understand the basics of security in a networked world. This document was written with the basic computer user and information systems manager in mind, explaining the concepts needed to read through the hype in the marketplace and understand risks and how to deal with them. So it is very important for all the users to get familiar with various aspects of network security. With the millions of Internet users able to pass information from the network, the security of business networks is a major concern. The very nature of the Internet makes it vulnerable to attack.

Keywords: Wired, System Manager, Vulnerable

I. INTRODUCTION

In the last decade, the number of computers in use has exploded. The growth of this industry has been driven by two separate forces which until recently have had different goals and end products. The first factor has been research interests and laboratories, these groups have always needed to share files, email and information across wide areas. The research labs developed several protocols and methods for this data transfer, most notably TCP/IP. Business interests are the second factor in network growth. For quite some time, business sharing data within an office or campus environment, this led to the development of various protocols suited specifically to this task.

This is a very rosy picture: businesses, governments and individuals communicating witheach other across the world. While reality is rapidly approaching this utopian picture, several relatively minor issues have changed status from low priority to extreme importance. Security is probably the most well-known of these problems.

When business and private communication obviously desire secure communications. Finally, Connecting a system to a network can open the system itself up to attacks. If a system is compromised the risk of data is high.

II. NEED FOR SECURITY

The object of security is to protect valuable or sensitive organizational information whilemaking it readily available. Attackers trying to harm a system or disrupt normal businessoperations exploit vulnerabilities by using various techniques, methods, and tools. Systemadministrators need to understand the various aspects of security to develop measures and policies to protect assets and limit their vulnerabilities. A common attitude among users is thatwhen no secret work is being performed, why bother implementing security. No firewall or proxy protection between the organizations private local area network (LAN) and the publicInternet makes

the company a target for cyber-crime. The way in which a system can beattacked are classified into four groups. These are Interruption, Interception, Modification and Fabrication.

III. TYPES OF NETWORK SECURITY

There are two basic types of network security-Transit security and Traffic regulation, which when combined can help guarantee that the right information is securely delivered to the right place. It should be apparent that there is also a need for ensuring that the host that receivethe information will properly processes it, this raises the entire spectre of host security: awide area which varies tremendously for each type of system. With the growth in business useof Internet, network security is rapidly becoming crucial to the development of the Internet.

IV. TRANSIT SECURITY

Currently, there are no systems in wide use that will keep data secure as ittransits a public network. Two important methods available to encrypt traffic between a fewcoordinated sites:

- Virtual Private Networks : This is the concept of creating a private network by usingTCP/IP to provide lower levels of a second TCP/IP stack.
- Packet Level Encryption: This is an approach to encrypt traffic at a higher layer in the TCP/IP stack. Both of these methods can have performance impacts on the hosts that implement the protocols, and on the networks, which connect those hosts. The relativelysimple act of encapsulating or converting a packet into a new form requires CPU time and uses additional network capacity. Encryption can be a very CPU-intensive process and encrypted packets may need to be padded to uniform length to guarantee the robustness of some algorithms. Further, both methods have impacts on other areas (security related and otherwise-such as address allocation, fault tolerance and load balancing)

V. TRAFFIC REGULATION

The most common form of network security on the Internet today is toclosely regulate which types of packets can move between networks. If a packet, which may dosomething malicious to a remote host never, gets there, the remote host will be unaffected. Traffic regulation provides this screen between hosts and remote sites. This typically happensat three basic areas of the network: routers, firewalls and hosts. Each provides similar services at different points in the networks. In fact the line between them is somewhat ill defined and arbitrary. In this article, I will use the following definitions:

- Router traffic regulation: Any traffic regulation that occurs on a router or terminalserver (hosts whose primary purpose is to forward the packets of other hosts) and is based on packet characteristics. This does not include application gateways but does include address translation.

Firewall traffic regulation: Traffic regulation or filtering that is performed viaapplication gateways or proxies.

- Host traffic regulation: Traffic regulation that is performed at the destination of a packet. Hosts are playing a smaller and smaller role in traffic regulation with the advent of filtering routers and firewalls.

VI. FIREWALLS

6.1 Introduction to firewall

Firewalls make it possible to filter incoming and outgoing traffic that flows through your system.A firewall can use one or more sets of "rules" to inspect the network packets as they come in or go out of your network connections and either allows the traffic through or blocks it. The rules of a firewall can inspect one or more characteristics of the packets, including but not limited to the protocol type, the source or destination host address, and the source or destination port. Firewallscan greatly enhance the security of a host or a network. They can be used to do one or more of the following things:

- To protect and insulate the applications, services and machines of your internal network from unwanted traffic coming in from the public Internet.
- To limit or disable access from hosts of the internal network to servicesof the public Internet.
- To support network address translation (NAT), which allows your internal network touse private IP addresses and share a single connection to the public Internet (either with asingle IP address or by a shared pool of automatically assigned public addresses).

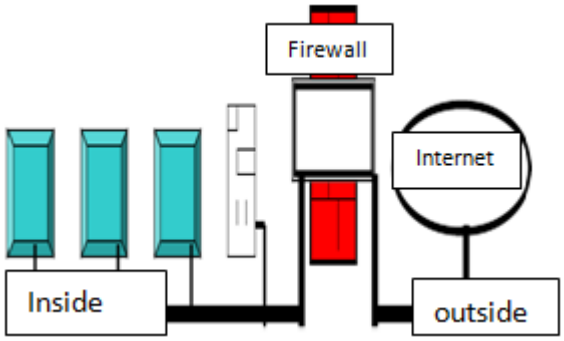

Figure 1-Diagrammatic representation of a Firewall

VII. TYPES OF FIREWALLS

There are three basic types of firewalls, and we'll consider each of them.

7.1 Application Gateways

The first firewalls were application gateways,and are sometimes known as proxy gateways. These are made up of bastionhosts that run special software to act as a proxy server. This software runs atthe Application Layer of our old friend the ISO/OSI Reference Model, hencethe name. Clients behind the firewall must be proxitized (that is, must know how to use the proxy, and be configured to do so) in order to use internet services. Traditionally, these have been the most secure, because they don'tallow anything to pass by default, but need to have the programs written andturned on in order to begin passing traffic.

7.2 Packet Filtering

Packet filtering is a technique whereby routers have ACLs (Access Control Lists) turned on.By default, a router will pass all traffic sent it, and will do so without any sort of restrictions.Employing ACLs is a method for enforcing your security policy with regard to what sorts of access you allow the outside world to have to your

internal network, and vice versa. There isless overhead in packet filtering than with an application gateway, because the feature of access control is performed at a lower ISO/OSI layer (typically, the transport or session layer).Due to the lower overhead and the fact that packet filtering is done with routers, which arespecialized computers optimized for tasks related to networking, a packet filtering gateway isoften much faster than its application layer cousins. Not that the possibility of something automatically makes it a good idea; openingthings up this way might very well compromise your level of security below what your policyallows.) There are problems with this method, though. Remember, TCP/IP has absolutely nomeans of guaranteeing that the source address is really what it claims to be. As a result, wehave to use layers of packet filters in order to localize the traffic. We can't get all the way downto the actual host, but with two layers of packet filters, we can differentiate between a packet that came from the Internet and one that came from our internal network. We can identifywhich network the packet came from with certainty, but we can't get more specific than that.

7.3 Hybrid Systems

In an attempt to marry the security of the application layer gateways with the flexibility andspeed of packet filtering, some vendors have created systems that use the principles of both. Insome of these systems, new connections must be authenticated and approved at the applicationlayer. Once this has been done, the remainder of the connection is passed down to the sessionlayer, where packet filters watch the connection to ensure that only packets that are part of anon-going (already authenticated and approved) conversation are being passed. Other possibilities include using both packet filtering and application layer proxies. The benefits hereinclude providing a measure of protection against your machines that provide services to theInternet (such as a public web server), as well as provide the security of an application layer gateway to the internal network. Additionally, using this method, an attacker, in order to get toservices on the internal network, will have to break through the access router, the bastion host,and the choke router.

7.4 Different Types of Threats to Network

- **E-mail bombs**

An email bomb is usually a personal attack. Someonesends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages

- **Macros**

To simplify complicated procedures, many applications allow youto create a script of commands that the application can run . This script isknown as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

- **Viruses**

Probably the most well-known threat is computer viruses. A virus isa small program that can copy itself to other computers .This way it canspread quickly from one system to the next.

Viruses range from harmlessmessages to erasing all of your data.

- **Spam**

Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites .Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.

7.5 Network security can be done by various methods

1. Virtual Private Network:

A virtual private network (VPN) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual userswith secure access to their organ ization's network. The goal of a VPN is to provide theorganization with the same capabilities, but at a much lower cost.

2. Firewalls:

A firewall provides a strong barrier between your private network and the Internet .You can set firewalls to restrict the number of open ports, what type of packets are pas sed through and which protocols are allowed through. You should already have agood firewall in place before you implement a VPN , but a firewall can also be usedto terminate the VPN sessions

VIII. 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.

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.

Website

www.iec.org/onlinehttp://ftp.research.att.com/dist/internetsecurity/