SECURITY THREAT PERCEPTION TO A DIGITAL LIBRARY

by

Manoj Singh*
Vijai Kumar **
Gupta Rajiv ***

ABSTRACT

Internet technology has benefited the users of research & development library by providing effective & quick sharing of global information resources. Crime on the net has also increased with the growth of Internet. For smooth operation of net, the need-of-the-hour is to deploy a system that is ready for the worst and which, anticipates problems (internals & externals) before they occur. It should also be able to cope up when the net is down. This paper describes some major security threats with respect to Internet. It also discusses some security measures for managing and maintaining the local network.

Keywords: Digital Library, Firewall, Internet, Intranet and Security.

Library and Information Services Division, Bhabha Atomic Research Centre, Trombay, Mumbai -400085

0. Introduction

Internet has made tremendous impact not only on social activities but also in research & academic areas. The popularity of Internet is only due to its easy-to-use operations and availability of vast information irrespective of field and nature. Libraries are also becoming referencing hubs of information available on the Internet. Lots of authorized and unauthorized information stuff is available on the net. The easiness of net surfing & open architecture of net encourages intruders/crackers to play with the network security.

Mostly intruders/hackers try to penetrate the secured information stored on local area network on various devices such as file, application, web servers etc. Their main intention of stealing information or data is either for misuse or merely to show their IT/Network expertise to the web community or to attract media attention towards them. It has also been seen that some intruders/crackers are doing the mischief for fun and play. Data exchange without security on the web is as good as leaving your house door totally ajar. Hence, now a days it is very essential to keep your home well secured so that no one can walk through without any monitoring and detection.

1. Network Security

Network Security is the protection of data & information from malicious or accidental destruction and loss. Protecting data not only entails configuring the system but also to formulate adequate security policies and procedures. The network threats are mainly divided into two categories.

1.1 External Threats:

Many organisations are allowing users to establish a connection across the Internet to access resources using their home PC. There are problems inherent to this type of setup. The most pressing is the security risk allowing these remote users access internal assets. These security holes can lead to hackers attack from out side world, if not managed properly. External attackers deploy intelligent electronic listening devices to monitor network real traffic and probe all possible TCP and UDP ports for weakness. The main goal is to find a chink in the organisational defences that will help them infiltrate and give them some chance for pushing the attack code inside the network.

1.2 Internal Threats:

One of the first steps to maintain network security, integrity and confidentiality data is securing all physical components of a system. These measures ensure that unauthorized users cannot physically access the system. In a survey conducted by security watch organisations, the maximum threat arises from the organisation network management or staff connected directly or indirectly to security policies & procedures. Hence, it is very essential to configure the network security in a closed loop management only.

2. Internet Security Threats/Crimes:

The distinction among Intranets, Extranets and the Internet are now artificial with the availability of new security features. One can highlight the boundaries, secure the perimeters and bind staff & regional net with confidentiality agreements, without jeopardising the free movement of packets across the net. With these merging technologies, the network security is also on high alert for smooth flow of the data & information. Some of the security threats are:

2.1 Web Severs: It is observed that main risk and threats are concentrated on Web servers hosted inside or outside a public network. Many flavors of web services such as Internet Information Server 4/5 for Windows NT4/2000, Apache for Linux are widely used in the world. Among others National Center for supercomputing application's (NCSA) Apache is already the world's most popular web server. With careful management and sensible configuration, the world's most popular HHTP server can also be the world's most secure.

2.2 Mail Servers: Choking up mail server by continuous boosting bulk mails to mail server commonly seen as Internet mail threat. With this type of threat the mail server is always busy in receiving the mails, thereby, blocking all out going messages from it. This is not a serious crime and the hacker is not able to damage the data but slows down the traffic.

2.3 Spam: Spam refers to Electronic junk mail or junk newsgroup postings. Some people define Spam even more generally as any unsolicited e-mail. Real Spam is generally e-mail advertising for some product sent to a mailing list or newsgroup. In addition to wasting people's time with unwanted e-mail, spam also consumes a lot of network bandwidth.

2.4 Spoofing: In networking, spoof is used to describe a variety of ways in which hardware and software can be dogded. Mostly LAN protocols send out packets periodically to monitor the status of the network. LANs generally have enough bandwidth to easily absorb these network management packets. However, computers are connected to the LAN over wide-area network (WAN) connections, this added traffic could become a problem. Not only it can strain the bandwidth limits of the WAN connection, but it can also be expensive because many WAN connections incur fees only when they are transmitting data.

2.5 IP Spoofing: IP spoofing involves trickery that makes a message appear as if it came from an authorized IP address. Spoofing is also used as a network management technique to reduce traffic. This is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

2.6 Script Kidding: A Script kiddie normally performed by hackers who are not technologically sophisticated. The hacker randomly explores for a specific weakness over the Internet in order to gain root access to a system. A script kiddie is not looking to target specific information or a specific site but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability.

2.7 Sniffing: A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information of a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. On TCP/IP networks like Internet, where they sniff packets, they are often called packet sniffers.

2.8 Port Scanning: The act of systematically scanning a computer's ports is referred as port scanning. Since a port is a place where information goes into and out of a computer, port scanning identifies doors open to a computer. Port scanning has legitimate usage in managing networks, but port scanning also can be malicious in nature if someone is looking for a weak access point to break into computer. Port scanning is not a crime. There is no way to stop someone from port scanning your computer while you are on the Internet because accessing an Internet server opens a port, which opens a door to your computer. There are, however, software products that can stop a port scanner from doing any damage to the system.

2.9 Smurf: A type of network security breach in which a network connected to the Internet is swamped with replies to ICMP echo (PING) requests. A smurf attacker sends PING requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support up to 255 hosts, so a single PING request can be multiplied 255 times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the PING request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these PING messages per second can fill the victim's T-1 (or even T-3) line with ping replies, bring the entire Internet service to a chaos. Smurfing falls under the general category of Denial of Service attacks -- security attacks that don't try to steal information, but instead attempt to disable a computer or network.

2.10 DoS attack: Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

3. Security Precaution & Controls

?? Network security control is broadly divided into three major types. *Preventive*-- By implementing restrictive permissions on directories and files of servers. *Detective*– By Logging activities, generating reports and alerts by the system. *Corrective*-- By installing service packs, correction tools etc. based on reports generated by detective devices.

?? Installation of Web servers, its configuration features, super user passwords, path, directories, permissions, active services etc. should be confined to limited trusted staff only.

?? Discussion, chatting or talk related to network security features should never be raised in public, which in turn reduce the risk of leaking of defensive steps from internal staff.

?? Proxy Server is widely used tool for separating out Intranet & Internet. It is a server that sits between a client application such as a Web browser, and a real server. It intercepts all requests to the real server to see if it can fulfill the requests itself. If not, it forwards the request to the real server.

?? A firewall is considered a first line of defense in protecting private information. Firewall is a system designed to prevent unauthorized access to or from a private network like Internet. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques like Packet filtering, Application Gateway, Circuit-level gateway and proxy. In practice, many firewalls use two or more of these techniques in concert.

?? Internet threat for spoofing can be reduced by configuring the routers and other network devices from the remote node. Rather than sending the packets to the remote nodes and waiting for a reply from spoof, the devices generate their own-spoofed replies.

?? Implementation of Intrusion detective systems is also very helpful to tackle the attacks. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

?? Packet filtering also referred to, as static packet filtering is another tool for controlling Internet threats. This controls access to a network by analyzing the incoming and outgoing packets and letting them pass or stop depending upon the IP addresses of the source and destination. Packet filtering is one of the techniques for implementing security firewalls.

?? Honeypot is another detective and preventive tool for Internet hackers. An Internet-attached server that acts as a decoy, luring the potential hackers in order to study their activities and monitor how they are able to break into a system. Honeypots are designed to mimic systems that an intruder would like to break into but limit the intruder from having access to the entire network. If a honeypot is successful, the intruders will have no idea that they are being tricked and monitored. By luring a hacker into a system, a honeypot serves several purposes such as the administrator can watch the hacker activities and exploit the vulnerabilities of the system, thereby learning where the system has weaknesses that need to be redesigned. It would be possible to catch and stop the hacker while trying to obtain root access of the system. This facilitates the administrator to re-design the system in more secure way

?? With regards to all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like viruses, hackers are constantly dreaming up new DoS attacks.

?? The problem of IP spoofing can be configured in newer routers and firewall arrangements.

4. Emerging Technology and Tools

With hackers/intruders building up new ways and tricks for finding weaknesses of the network, there are many technologies coming up to counter these. The question of-the-hour is to decide on technology, which a digital library should adopt. Digital managers/Network administrator should keep in mind five technology features e.g. Suitability to the task, Impact on the organisation, Maturity, Manageability and Scalability before choosing one or a combination. Some of the emerging technologies are:

4.1 Virtual Private Networks (VPN): A VPN is a wide area communications network operated by a common carrier providing backbone trunks shared among all as in public network like Internet. A VPN allows a private network like Intranet to be configured within a public network like Internet in a completely secure and cost-effective environment. VPN products are becoming a choice for opting secure communication over the Internet. VPN basically work on encryption technology i.e. data is first encoded at the exit point of network and decoded when it reaches the destination. No one can view the contents of the message in between, even if it is intercepted. The valid sender and receiver are known by some means of identification so that they are able to decrypt message. Currently four standards are being used and widely available using IP Security (IPsec), Simple Key Management for IP (SKIP), Internet Secure Association Key Management Protocol (ISAKMP) and Point-to-point Tunneling protocol (PPTP).

4.2 Public Key Infrastructure (PKI): It is a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity involved in an Internet transaction. The National Institute of Standards and Technology (NIST) is taking a leadership role in the development of a Federal Public Key Infrastructure that supports digital signatures and other public key-enabled security services. This technology has still to achieve the maturity level but has promise for a better digital exchange of information & data over the Internet.

4.3 Firewall: Firewall is an essential front door guard if local network area connects Internet. Although Firewall is certainly a requirement for network protection but it does not give guarantee. Firewall permits some packets in, this puts the network on risk.

Hence, implementation of firewall requires high expertise. One has to understand which packet absolutely has to be allowed in, and how to minimize the risk in doing so. Various Firewalls are now available with authentication, VPN capabilities, URL screening, virus scanning etc. Check Point and Cisco have integrated IDS achieving in turn further reduction in the risk.

4.4 Intrusion Detection System (IDS): An intrusion detection system (IDS) inspects all inbound/outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. Few IDS products are available in market, which can be, configured either for actively monitoring the operating system or network traffic or both for attacks and security. IDS are overwhelmingly gaining popularity among all other techniques. IDS can give the administrator the opportunity to react to the attack, or possibly even stop them. IDS products are still very expensive and expertise is required to install and monitor in real-time.

4.5 Vulnerability Assessment Tools (VAT): VAT are also known as security scanners, who take a protective approach to network security, aiming to provide efficient, thorough, automated identification security holes at both and network levels. It uses internal databases of known flaws to determine whether a system is vulnerable to specific type of attack. The major problems with VAT are its frequency of updates, which take longer time to integrate with next version of the product.

4.6 Kerberos: Kerberos is an emerging authentication protocol that lets clients and servers reliably verify each other's identity before establishing a network connection. It works on secret key cryptography known as symmetric key cryptography, which converts a plain text into cipher text message and then converted back to plain text using one secret key. Hence, a secret key is responsible to encrypt and decrypt the communication over the net. Recently, due to kerberos's protocol inclusion in Microsoft's Windows 2000 operating system, the authentication protocol now has the potential to reach many organisations and libraries setups.

4.7 Anti Virus Software: E-mail born macro-viruses spread like wildfire whenever one opens an infected email attachment. With increasing usage of viruses and their non-reproducing cousins, Trojan, warm etc, as means for hackers to bypass firewall protection, anti virus software demand increase as preventive measures for the net. The ability of an anti virus software should be judged by its capability to prevent damage from traditional & self-spreading viruses and recovering the damages over the net. The softwares offered by vendors support good detection and cleaning job with online update mechanism for fighting the latest strains of viruses. This technology is very cost effective and easily manageable.

5. Conclusion

Information and Data are the treasures of a digital library. Protecting the digital content while ensuring its uninterrupted flow at gigabit speed with low operating cost is the most crucial challenge to the network administrators/managers. Our observation shows that the most matured technology for prevention, detection and correction should be adopted to meet Internet threats. We also conclude that to keep maximum uptime of a net, security &

protection mission-critical data & information should be uppermost in minds of those who manage, maintain and use it.

References

- ?? www.networkcomputing.com
- ?? www.expresscomputeronline.com
- ?? Microsoft Technical Reference