Computer Network Security System

Ambarish Kumar Patel
School of Computer Science
Anjaneya University Raipur C.G.

ABSTRACT

Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The architecture of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The businesses create an "intranet" to remain connected to the internet but secured from possible threats. The entire field of network security is vast and in an evolutionary stage. The range of study encompasses a brief history dating back to internet's beginnings and the current development in network security. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed.

Keywords: Mitigation, Cryptography, Network, Security

1.0   Introduction

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.

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.

INTERNET ARCHITECTURE AND VULNERABLE SECURITY ASPECTS

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. These security mechanisms allow for the logical protection of data units that are transferred across the network. The security architecture of the internet protocol, known as IP Security, is a standardization of internet security. IP security, IPsec, covers the new generation of IP (IPv6) as well as the current version (IPv4). Although new techniques, such as IPsec, have been developed to overcome internet's best known deficiencies, they seem to be insufficient.

IPv4 and IPv6 Architectures

IPv4 was design in 1980 to replace the NCP protocol on the ARPANET. The IPv4 displayed many limitations after two decades. The IPv6 protocol was designed with IPv4's shortcomings in mind. IPv6 is not a superset of the IPv4 protocol; instead it is a new design. The internet protocol's design is so vast and cannot be covered fully. The main parts of the architecture relating to security are discussed in detail.

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

The IPv4 architecture has an address that is 32 bits wide. This limits the maximum number of computers that can be connected to the internet. The 32 bit address provides for a maximum of two billions computers to be connected to the internet. The problem of exceeding that number was not foreseen when the protocol was created. The small address space of the IPv4 facilitates malicious code distribution. Routing is a problem for this protocol because the routing tables are constantly increasing in size. The maximum theoretical size of the global routing tables was 2.1 million entries [6]. Methods have been adopted to reduce the number of entries in the routing table. This is helpful for a short period of time, but drastic change needs to be made to address this problem.

The TCP/IP based networking of IPv4 requires that the user supplies some data in order to configure a network. Some of the information required is the IP address, routing gateway address, subnet mask, and DNS server. The simplicity of configuring the network is not evident in the IPv4 protocol. The user can request appropriate network configuration from a central server. This eases configuration hassles for the user but not the network's administrators.

The lack of embedded security within the IPv4 protocol has led to the many attacks seen today.

Mechanisms to secure IPv4 do exist, but there are no requirements for their use. IPsec is a specific mechanism used to secure the protocol. IPsec secures the packet payloads by means of cryptography. IPsec provides the services of confidentiality, integrity, and authentication.

This form of protection does not account for the skilled hacker who may be able to break the encryption method and obtain the key. When internet was created, the quality of service (QoS) was standardized according to the information that was transferred across the network. The original transfer of information was mostly text based. As the internet expanded and technology evolved, other forms of communication began to be transmitted across the internet. The quality of service for streaming videos and music are much different than the standard text. The protocol does not have the functionality of dynamic QoS that changes based on the type of data being communicated.

AIM AND OBJECTIVES

Since the evolution of attack is endless, this thesis gives an overview of the best practices in reviewing the known attacks and recommendation on how to prevent reoccurrence attacks.

The objectives of this work are to reveal and define the concept of attack and threat to computer network, to highlight different mitigating techniques used to circumvent threats and attacks, to illustrate the procedure to implement the best security practices, and to extend the practices of an outsider trying to gain access into the network to the network engineer.

REVIEW OF PREVIOUS WORKS

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices. (Reed 2003). This
review addresses   how highly sophisticated intruders are penetrating internet networks despite high levels of security. But as the intruders increase, the network experts are deriving many techniques in preventing attackers from accessing company networks.

CATEGORIES OF SECURITY THREATS

Security threat can be categorized into four parts and these categories are the ways or forms through which threats can be carried out on a network.

i.   UNSTRUCTURED THREATS

Unstructured security threat is the kind of threat created by an inexperienced person trying to gain access to a network. They commonly use common hacking tools, like shell scripts, and password crackers. A good security solution should easily thwart this kind of attack. In other words, these kinds of hackers could not be underestimated because they can cause serious damage to network.

ii.   STRUCTURED THREATS

Unlike unstructured threats, structured threat hackers are well experienced and highly sophisticated. They use sophisticated hacking tools to penetrate networks and they can break into government or business computers to extract information. On certain occasions, structured threats are carried out by organized criminal gangs or industry competitors.

iii.   EXTERNAL THREATS

Some unauthorized people outside the company who do not have access to the company's computer system or network could cause external threat. They usually break into company's network via the Internet or server. Both experienced and inexperienced hackers could pose external threats.

iv. INTERNAL THREATS

This kind of threat could be by a disgruntled employee who has authorized access to the company's network. Like external threats, the damage that could be caused by such a hacker depends on the expertise of the hacker.

PHYSICAL INSTALLATION ATTACK

Physical installation attacks, as the name implies originate from some basic threats that we can see with own eye but might not be prevented.

Firstly, hardware threat is a common example of a physical installation attack; this could be due to the old age of a particular system, and as a result of that, it start acting erratically and damage some data before it totally dies. Environmental threat, as discussed previously, can be caused by natural phenomena, such as extreme weather temperatures, earthquakes, and storms. Furthermore, electrical threat can cause extensive damage to a network. This kind of threat is common in countries where the power supply is always interrupted unexpectedly. Examples of this type of threat are: blackout (unexpected interruption of power supply), brownout (insufficient supply of power voltage) and noise (unconditioned power). Maintenance threat could also cause problem to network. Examples of maintenance threats are poor cabling, poor cable labelling, electrostatic discharge, and lack of critical spare parts.

DEVICE COMMUNICATION ATTACK

Technically competent hackers have been able to fashion a structured attack targeted at communication protocols. The OSI model has seven layers that are used for communication between networking devices, which are with vulnerabilities that can be controlled. Basically, higher layers cannot be secured while the lower layers are also not being secured, yet in recent years there has been limited attention to insecurities at the physical layer or data link layer despite changes in network operational practice that include

developments like nation-wide layer two networks and national and regional optical networks.
Currently known threats at lower levels of the OSI stack include ARP spoofing, MITM (man-in-themiddle) attacks at layer two, and physical layer attacks such as passive optical taps or the interception of wireless network signals by attackers. While these attacks are well known, little research is currently focused on addressing those concerns.

MITIGATIONS OF NETWORK THREATS AND ATTACKS

Due to the unfortunate case of numerous threats and attacks that have befallen the networking industry, it becomes imperative to find ways of mitigating each of the attacks. Chapter two above described the various types of threat facing network security, Chapter three and four discuss the solutions for the threats mentioned in the previous chapters.

HARDWARE THREAT MITIGATION

As a result of fault from physical installation, planning of physical security to limit damage or theft of equipment during the process of installing hardware is very important. Few of the many ways that this action could be monitored or controlled is by making sure that no unauthorized access from the doors, ceiling, raised floor, windows, ducts or vents, monitoring and control closet entry with electronic logs, use of security cameras, and if possible, electronic access control should be used and security systems should log all entry attempts and controlled by security personnel.

Physical security is discussed in detail in Chapter four of this thesis.

ENVIRONMENTAL THREATMITIGATION

The first stage of every attack has been from lack of environmental control, which brings about limiting damage by creating a proper operating environment through: Temperature control, humidity control and positive airflow.

ELECTRICAL THREAT MITIGATION

Loss of power can also be an opportunity for intruders to break into a controlled network, which could be prevented or controlled in many ways few of which are mentioned here; Electrical threat could be limited by ensuring uninterrupted power supply for network devices, by following a preventative maintenance plan designed for the purpose, and by performing remote alarming and monitoring.

MAINTENANCE-RELATED THREAT MITIGATION

Maintenance has always been a vital operation, for any organization that uses hardware. Maintenance related threats can be limited by:

• Using neat cable runs
• Labeling critical cables and components
• Using (electrostatic discharge) ESD procedures
• Stocking critical spares
• Controlling access to console ports

Console should neither be left connected nor logged into any console port, and ensure logging off administrative interfaces before leaving. A locked room should not be relied upon as the major protection for devices. No room is totally secured, and if intruders get in a secured room, there is nothing stopping them from making a connection to the console port of a router or a switch.

PACKET SNIFFER ATTACKMITIGATION

The following are the tools that can be used to control packet sniffer attacks;

Authentication: For defense against packet sniffers, the use of strong authentication should be the first mitigation option. Strong authentication is a technique of authenticating users that cannot be circumvented easily.One Time Passwords (OTPs) are a clear example of strong authentication. A onetime password is a security mechanism that makes use of a mobile device in generating password each time an application

requests for it.

Switched Infrastructure: This technique counters the use of packet sniffers in a network environment. For instance, if an organization deploys a layer-2 switched Ethernet, access by intruders can only be gained to the traffic flow of the connected port. Obviously a switched infrastructure does not totally eradicate the threat of packet sniffers, but their effectiveness is reduced considerably.

Anti-Sniffer Tools: Certainly, there would always be a solution for every threat, anti-sniffer is a software and hardware, designed for detection of the use of sniffers on a network, and can be implemented on networks.

Cryptography: A communication channel is cryptographically secure when the only data a packet sniffer detects is a cipher text (a random string of bits) and not the original message. Cisco deploys network-level cryptography based on IP Security (IPsec), IP security is a standard security method for networking devices in communicating privately through the use of Internet Protocol (IP). (CANS 2011)

Secure Sockets Layer (SSL) and Secure Shell Protocol (SSH) are also cryptographic protocols for network management.

Fundamental to security in distributed systems is the use of cryptographic techniques. The basic idea of applying these techniques is simple. Consider a sender *S* wanting to transmit message *m* to a receiver *R*. To protect the message against security threats, the sender first **encrypts** it into an unintelligible message *m′*, and subsequently sends *m′* to *R*. *R*, in turn, must **decrypt** the received message into its original form *m*.

PORT SCAN AND PING SWEEP ATTACK MITIGATION

The prevention of port scans and ping sweeps seems to be difficult without compromising network capabilities. However, the use of intrusion prevention systems at network and host levels is an advisable way of mitigating any damages. Ping sweeps can be stopped if ICMP (internet control message protocol) echo as well as echo- reply are turned off on edge routers.

Network-based intrusion prevention systems (IPSs) which compare incoming traffic to signatures in their database and host-based intrusion prevention systems (HIPS) can usually notify an administrator when a reconnaissance attack is under way.

Discovering stealth scans requires kernel level work.

ACCESS ATTACKS MITIGATION

The following are mitigation techniques for password attacks:
1)   Users should not be allowed to use the same passwords on multiple systems.
2)   Accounts should be disabled after detecting a certain amount of unsuccessful login attempts.
3)   The use of ordinary text passwords should not be allowed.
4)   Use of strong passwords (e.g., Use "mY8!Rthd8y@" rather than mybirthday)

TRUST EXPLOITATION ATTACK MITIGATION

Trust exploitation-based attacks can be mitigated by means of tight constraints on the level of trust within networks. The outside systems of a firewall should not be fully trusted by the inside Systems of the firewall, in other words trust should be limited to specific protocols where possible, and should also be validated by another parameters other than an IP address.

MAN-IN-THE-MIDDLE ATTACK MITIGATION

Cryptography (encryption) is the only effective mitigation technique for Man-in-the-middle attacks. Man-in-the- middle attack mitigation can be achieved by the encryption of traffic in an IP-Security tunnel. With this Encryption method, intruders or hackers can see only cipher text. (Mattsson 2006)

CHANNELS OF SECURING A COMPUTER NETWORK
PHYSICAL SECURITY

Information security professionals have long focused on virtual risks, but at some point all things virtual become physical. It is that crossing point—where physical infrastructure and systems provide an access

point to the virtual world -- that the link between physical threats and virtual threats are most apparent (Lindstrom 2003).

Many physical threats should be factored into a security program which includes; theft, human error, sabotage, and environmental disruption.

Video Surveillance and IP

Video surveillance and IP are modern technologies devices used in different part of the world toward protecting enterprises from the physical threat against their network as well as computing equipment. The attributes of this solution include:

•   **Secure:** The computer architecture of a video surveillance renders the security of transmission by encrypting communications for protection against captured data or inserted into the information stream. Additionally, tamper resistivity on sensors can be deployed with a protective casing. Finally, the ability to distribute and administer sensors offers redundancy to protect against focused attack on the sensor.

•   **Solid State:** Moving parts do not exist on the sensors. Moving parts are hereby susceptible to mechanical and physical damage, which requires site visits for repair. By developing the digital potentialities of the system, the system was able to eradicate the need for mechanical features whereby the likelihood of failure is reduced.

•   **IP Connectivity:** Separate physical cabling for CCTV functions is required for existing monitoring systems. Video surveillance uses the same technology it protects by incorporating it into the typical IP network which allows sensors to be positioned anywhere the network protects its components. In addition, it eradicates the necessity for duplicate cabling using various wire types.

•   **Multi-sensor collectors:** In keeping along with the "human senses" framework of threat monitoring, NetBotz provides the ability to gather data from multiple sensors in order to combine information into asingle place.

•   **Intelligent analysis software:** The more software grows intelligent, the more quickly individuals respond to threats. As technology produces the ability to aggregate data from various places, a level of analysis complexity is created which is best resolved through analytical software. Finally, this creates effective and efficient approach to the needs of identifying attacks and reacting to it.

•   **Simple Network Management Protocol (SNMP) Aggregator:** Some capabilities are associated with a physical threat monitoring system and works with the IP network with its ability to also collect SNMP (Simple Network Management Protocol) data and also passes the data along at appropriate times. (Pete, L. 2003)

USAGE OF SYSTEM CONTROL

Once an operating system is installed on a computer, some simple steps should be taken immediately after installation:

i.   Default usernames and passwords should be changed immediately.

ii.   Access to system resources should be restricted, so that only the authorized individuals can have access to the resources.

iii.   Any unnecessary application and services should be turned off and uninstalled, if possible.

iv.   System should not be left on or un-locked while not on sight.

v.   Users should subscribe and always check Subscribe and always check for patches and update to install from software and Hardware vendors.

SECURED PASSWORD

The practice of the following techniques can give a company rest of mind concerning passwords:

i.   Users should not be allowed to have the same password on multiple systems.

ii.   Accounts should be disabled after a certain number of unsuccessful logins. This practice prevents

continuous password attempts.

iii.   A plain-text passwords should be avoided. The use of either an OTP (One Time Password) or encrypted password is recommended.

iv.   The use of strong passwords or passphrase is highly recommended. Strong passwords should be at least eight characters long and uppercase letters, lowercase letters, symbols or special characters, and numbers should be used in passwords. Many systems provide strong password support and can also restrict a user to using of only strong passwords.

SECURITY SOFTWARE

To protect against known viruses, host antivirus software should be installed. Antivirus software detects most viruses and Trojan horse applications. It also prevents viruses from spreading in the network. Antivirus software does its protection in two ways:

1.   File scanning by comparing their contents with known viruses in a virus definition database or dictionary.

2.   Suspicious processes that run on a host and indicate infection are monitored. This monitoring may include port monitoring, data captures, and other methods.

SUMMARY

Flourishing in today's economy, service providers should provide open and easily accessible communications services, which will enable their end users to contact anyone in the world. The same open and freely scalable communication architecture offers limitless communications services to end users and also sets a very attractive target to hackers who would abuse that open communication access for their own financial benefits.

A security implementation of an organization, irrespective of its size, should consider all forms of access and intrusion on network hardware both physically and remotely, such as environmental monitoring, using video surveillance and IP, securing remote access using AAA (TACACS+) and deploying of firewalls and demilitarized zone (DMZ).

Because security is a long-term issue, service providers need a security strategy and staff that is well educated in that strategy. To that end, this thesis discussed the tools and practices that

are indispensable to network operators in securing their networks against denial of service (DoS) attacks and other common security threats. Finally, service providers can turn those necessary

security protections into profitable managed security services for their enterprise customers.

CONCLUSION

Because security is a long-term issue, service providers need to develop a security strategy. A good place to start is to educate staff on best practices. When implementing a security plan, it is important to begin by implementing the most obvious protections first and by deploying equipment that is capable of the most advanced protections, deploying equipment capable of providing privileged-EXEC authentication and a higher level of scalability than line-level, such as AAA Services.

Other straightforward steps include: protection of servers and routers by using onetime passwords and allowing only authorized users to get to routers, by applying authorization systems based on TACACS+ or RADIUS. Administrators can also implement a mechanism to manage incoming traffic, which can include DoS attacks against the control processors of routers. In general, operators should turn off unused and unneeded services, even when this may entail turning off features on servers.

Finally, the increase in physical infrastructure as well as its growing implication to an organization has created the necessity to physically protect the systems themselves, not only from cyber-attacks, but also from the physical attacks that can be perpetrated against them. Implementing policy-based security also brings many advantages to the security arsenal, because it automates the implementation of the security philosophy and lessens the chance of user error in protecting the network. When implementing security policy, it is necessary to keep in mind that mechanisms such as DMZ, IPSec- VPNs, firewalls and intrusion detection and prevention techniques that are so critical to securing network infrastructure can

be turned into managed security services that could be sold to enterprise customers.

REFERENCES

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

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

Andress J., "IPv6: the next internet protocol," April 2005, www.usenix.com/publications/login/2005 04/pdfs/andress0504.pdf. Bidou, R. 2000. Denial of service attacks. Retrieved: May 10 2012. Available at: http://www.docstoc.com/docs/85149779/De nial-of-Service-Attacks Cisco Security. 2005. Securing Cisco Network Devices. (v 1.0 ed.) Available at: http://www.scribd.com/doc/985242/Securin g-Cisco- Network- Devices-SND-v1-0

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

Hill, J. 2001. An Analysis of the RADIUS Authentication Protocol. Retrieved: April 16 2012. Available at: http://www.untruth.org/~josh/security/radius/radius-auth.html

Kartalopoulos, S. V., "Differentiating Data Security and Network Security," Communications, 2008. ICC '08.IEEE International Conference on, pp.1469 1473, 19 23 May 2008

Landwehr, C.E.; Goldschlag, D.M., "Security issues in networks with Internet access," Proceedings of theIEEE, vol.85, no.12, pp.2034 2051, Dec 1997

Lin, D.; Tsudik, G.; Wang, X. Cryptology and Network Security, in Proceedings of 10th International Conference on Cryptology and Network Security: Sanya, China,2011, [p 3]

Marin, G.A., "Network security basics," Security & Privacy, IEEE , vol.3, no.6, pp. 68 72, Nov. Dec. 2005

Mattsson, U.T. October 03, 2006. Best Practice for Enterprise Database Encryption Solutions. Retrieved: May 5,

2012. Available at:http://papers.ssrn.com/sol3/papers.cfm?ab stract_id=934271

MIT Kerberos Team Security Contact. The Network Authentication Protocol. Retrieved: January 27, 2012.

Available   at: http://web.mit.edu/kerberos/contact.html

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

Orbit-Computer Solutions. 2012. Threats to physical and network infrastructure. Retrieved: May 5 2012. Available   at: ,   http://www.orbit-computersolutions.   com/Threats-to-Physical-and-NetworkInfrastructure.php

Paul, A. May 13 2003. Implementing secure access to Cisco devices using TACACS+ and SSH. Retrieved,February 28, 2012.

Available at: http://www.sans.org/reading_room/whitepap ers/networkdevs/implementingsecureaccess-cisco-devices-tacacs-plusssh_1041

Pete, L. June 2003. The Emergence of the Physical Threat No. 2-3 P.O. Box 152, Malvern, PA 19355: SpireSecurity, LLC.

Available at: http://netbotz.com/library/Physical_Threat_ Security.pdf

Reed D. November 21, 2003. Network Model to Information Security. Retrieved: Available at: http://www.sans.org/reading_room/whitepap   ers/protocols/applying-osilayer-networkmodel-information-security_1309

Sotillo, S., East Carolina University, "IPv6 security issues," August 2006,