Bachelor's Thesis (UAS)

Degree Program In Information Technology

Specialization: Internet Technology

2012

SULAIMON ADENIJI ADEBAYO

NETWORK SECURITY

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme In Internet Techonology

2012| 42

Instructor: Patric Granholm

Sulaimon Adeniji

Abstract

The rapid increase in computer, mobile applications and wireless networks has globally changed the features of network security. A series of Internet attack and fraudulent acts on companies and individual network have shown us that open computer networks have no immunity from intrusions.

The traditional way of protecting computer networks, such as firewalls and software encryption are insufficient and ineffective. The wireless ad-hoc network is susceptible to physical attack or harm due to its feature of open medium dynamic changing topology, monitoring and management point not being centralized, clear line not well defended and cooperative algorithms.

Since the techniques developed on fixed wired networks to detect intruders have been rendered inapplicable in this new environment, the need for ways and methods to develop new architecture and mechanisms to protect mobile computing applications and wireless networks is important.

This thesis looks into vulnerabilities and mitigations of wireless networks. Many problems small companies are facing due to intruders and attackers are also discussed. Basically, the vulnerabilities and mitigation this thesis examines will be very useful in the underdeveloped and developing nations.

FOREWORD

This project talks about network security, as we all know that for any company to move forward and progress in her operations, the first thing the company has to take into consideration is a very strong and good security, especially companies that deal with networking. Network security is a very large topic of networking; I decided to write this small part of it because of the importance of it to companies. I purposely chose this topic because of what I experienced in the place I did my placement (Benin), I noticed how porous their network is and I decided to write something on how such network porosity could be handle and find a lasting solution to it.

I give all praise to ALMIGHTY ALLAH who guides me through all my daily life endeavour and for the completion of this thesis, I give thanks to my parents who always helped me in prayers all times and for giving me advice on how to do things in the right way. My gratitude goes to my friends that always stood by me in times of needs, too. And finally, I really appreciate and give thanks to all my lecturers that impact knowledge in me; I pray God rewards them all abundantly.

2012, Turku.

Sulaimon Adeniji.

CONTENTS

APPENDIX

ACRONYMS, ABBREVIATIONS AND SYMBOLS

VLANs	Virtual Local Area Network
ACL	Acess Control List
AAA	authentication, authorization and accounting
(TACACS+)	Terminal Access Controller Access-Control System Plus
DMZ	Demilitarized Zone
IPSec	Internet Protocol Security
VPN	Virtual private networks
IOS	Internetwork Operating System
LAN	Local Area Network
CAM	Content-Addressable Memory
MAC	Media access control
STP	Spanning Tree Protocol
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
TCP	transmission control protocol
UDP	User datagram protocol
TFTP	Trivial File Transfer Protocol
IETF	Internet Engineering Task Force
NIS+	Network Information Service plus
IDS	intrusion detection system

1.0 **BACKGROUND TO THE WORK**

As the computers and networked systems increases in the world of today, the need for increase and strong computer and network security also becomes increasinly necessary and important. The increase in the computer network system has exposed many networks to various kinds of internet threats and with this exposure, one can see that the need for increased network security is vital and important in every organization. The security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. There is no laid-down procedure for designing a secure network. Network security has to be designed to fit the needs of one organization network and not anyone else's. For instance, a small-sized law company would allow access to case information for authorized users on the outside of the network, and at the same time ensure that full access to the internet is always available to staff on the inside of the network, in other cases to access a case file from the office or on the road. Good network security protects a network in a manner that is consistent with its purpose and precautions must be taken when chosing a network provider for an organization especially one like a law firm.

1.1 PROBLEM DEFINITION

Network security is sometimes more than what people always thought it to be, malware, virus, Trojan, hackers. Network security could be caused by unintentional human error and it could be compromised by human nature as well.

A common network security problem (Employees) most organizations are facing sometimes has to do with the company's employees and their various errors they make. According to Dr. Michael E. Whitman, CISM, CISSP, and the author of the textbook "*Principals of Information Security*, "Humans make mistakes; sometimes that is due to inexperience or improper training, and sometimes it is because an incorrect assumption was reached. But regardless of the reason—and the

lack of malicious intent—something as simple as a keyboarding error has the potential to cause a worldwide Internet outage". (Whitman and Mattord 2012)

The problem of piracy is another common network problem. Piracy is a situation where intellectual properties are compromised although there are technical mechanisms that aid in enforcing copyright laws to tackle this problem.

However it is not only human errors that can cause problem to network security, problems can also be caused by natural forces like fire breakouts, earthquakes, floods lightning etc.

The ways network administrators think about securing networks has been changed by an increasingly dynamic and technically challenging risk environment.

New business models rely on open networks with multiple access points to conduct business in real time, driving down costs and improving response to revenue generating opportunity by leveraging on the ability to quickly exchange critical information, share business files or folders and improve their competitive position.

1.2 PROJECT JUSTIFICATION

With increasing reliance on computer systems worldwide for data processing and information storage, the need for legitimate security of information and data cannot be overemphasized. Un-authorized access, revelation or destruction of data can violate individual privacy and even threaten the existence of an organization. Since information is regarded as the live wire of an organization, it is, therefore, necessary to secure computer systems and the stored information.

1.3 AIMS AND OBJECTIVES

Since the evolution of attack is endless, this thesis gives an overview of the best practices in mitigating 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. The various types of threat computer network is facing are discussed in Chapter two, while the different mitigating techniques are discussed in Chapter three. Finally, Chapter four of the thesis discusses the general procedure to implement the best security practices.

Security in any context is a broad concept that seems to have no perfection. There are various ways of mitigating the known attacks such as:

- Developing a Security policy.
- Training of Staff on proper Internet usage.
- Installation of security software, such as MacAfee, Norton, ESSET, etc.
- Creation of VLANs (Virtual LAN) and lots More.

1.4 ORGANISATION OF WORK

This thesis starts out with an overview of how insecurity came into the picture on networking and it also brings to the attention security challenges network administrator are facing as a result of the needed growth by the organization.

It progresses on to include the study of the problem at hand as well as how the known problems can be tackled. It delves further in to describe the various channels through which organization's network can be compromised through the OSI layer model and outlining the known attacks.

Also covered are the various ways of mitigating the known attacks and introducing the server that ensures that no intruder get into the network remotely.

Afterwards is a section that contains the best practices in securing a computer network physically through video surveillance and IP, locks and electronic code entrance.

System usage can be controlled with secured password or passphrase, security software, host-based intrusion detection and prevention. Remote access can be controlled with AAA (TACACS+), DMZ, IPSec-VPN, and IOS Firewall.

Lastly is a section that seeks to encourage network authorities to make use of the practices in this thesis and also makes further recommendation on how to improve on the practices in this paper.

1.5 DEFINITION OF TERMS

There are common and uncommon network terms that would be used often on this thesis. Below are some terms and their definitions.

1) Computer Network: collection of computers that work together in other to allow sharing of resources and information

2) Vulnerability: is a weakness that compromises either the security or the functionality of a system.

Examples:

I. Poor passwords.

II. Improper input handling.

III. Insecure communication.

3) Exploits: is the mechanism used to leverage vulnerability.

Examples include:

I. Password Guessing.

II. Shell Scripts.

III. Executable Codes.

4) Authentication: the process of confirming the true identity of a given user

5) Authorization: this is a process of permitting a user to access a certain resources or perform certain activities.

6) Firewalls: is a set of related programs that protects the resources of a private network.

7) Antivirus: is software that detects most viruses and many Trojans.

8) Backdoor: this a compromised tool installed in other to allow attacker to compromise system around any security mechanisms that are in place

9) Countermeasures: Reactive methods used to prevent an exploit from successfully occurring once a threat has been detected.

10) Demilitarized Zone (DMZ): is a network area (a sub network) configured like a firmware to secure local area network (LAN)

2.0 INTRODUCTION

Quick information accessibility on the Internet has become increasingly important for growing businesses. As companies begin to spread various business functions to the public network, precautions are highly needed to make sure that their network not been tampered with or does not fall to wrong hands. If a network is accessed by a hacker or dissatisfied employee, it could create havoc for organization proprietary data, affect company productivity negatively, and retard the ability to compete with other businesses. Unauthorized network access can also harm a company’s relationship with customers and business partners who may question the company's ability to protect their confidential information. Furthermore, any part of a network can be susceptible to attacks or unauthorized activity as earlier discussed. Company competitors or even internal employees can violate all routers switches and hosts.

In order to determine the appropriate ways of protecting a company's property against attackers, the Information Technology Manager of such company should understand the attacks that can be instigated and the havoc they can cause to business infrastructures.

2.1 LITERATURE REVIEW

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.

2.2 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. (Orbit-Computer Solutions 2012)

2.3 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), 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.

2.4 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-the-middle) 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.

2.4.1 PHYSICAL LAYER

The physical layer is responsible for transferring data over network communication media. It could also be refer to as most changeable and vulnerable layer. When dealing with this type of layer, unserious incidents like unplugging the computer power cord or removing a network cable could sometimes cause a great and untraceable havoc on a particular network, and it could cause great damage to the computer. (Reed 2003)

There are plenty of vulnerabilities that the physical layer is facing, few of which include: loss of environmental control, damage of hardware and data, disconnection of physical data links, power loss, input logging like keystroke and other physical theft of data and hardware, and undetectable interception of data. These vulnerabilities could cause great damage to network security through physical layers if prevention is not done at the right time. Nevertheless, there are always solutions available for any threat of damage caused to a network.

As mentioned above, there are always solutions for every problem. Perimeters and enclosures lock, electronic lock mechanisms for logging and detailed authorization, data storage cryptography, PIN and password secured locks, electromagnetic shielding, biometric authentication systems, and video and audio surveillance can all be used to prevent or secure any threat that is coming to attack a network or that has attacked a network via the physical layer.

2.4.2 DATA LINK LAYER

This is the layer where transmission of data packets has been prepared by the physical layer. Communication of the data link is somehow weak in terms of security. The key component at layer 2 communications is the switch, which is also used for communication at layer 3. Data link is susceptible to many layer 3 attacks. The prime example of the layer 2 element is 'wardriving' the method of going around searching for wireless LAN (802.11) Network with default security settings. VLAN in layer 2 switches are also vulnerable to attacks. (Reed 2003)

All the OSI layers face different threat that affect them at their various stages. Highlighted below are the problems faced by layer two of the OSI model and the solution to the problems.

CAM (Content-Addressable Memory) table overflow, MAC (Media access control) spoofing, STP (Spanning Tree Protocol) Manipulation, ARP (Address Resolution Protocol) attack, and VLAN hopping are the problems faced by data link layers.

CAM can be controlled by configuring port security on switch in order to provide a MAC address specification on a particular switch port so that it can be learnt and memorized by the port to detect an invalid address on the port.

Like in CAM, port security commands can also be used to control MAC-spoofing attacks. The command can allow the switch to specify a protection action whenever violations of port-security occur.

A BPDU guard is used to control manipulation of STP. This guard is put in place for network administrators to predict actively a network topology.

ARP attacks can be mitigated by using Hold-down timers in the configuration interface menu. This can be achieved by setting an entry-stayed time in the ARP cache.

Control of VLAN hopping could be done by issuing VLAN IDs for trunk ports, and disabling of unused switch port and putting them in an unused VLAN.

2.4.3 NETWORK LAYER

The network layer is a medium used by packets to get to their final destination over multiple data. As said earlier in the previous chapter above, virtually all the layers have challenges of security. The lowest third layer of the OSI model is known to face challenges of information privacy problems and Denial of Service attacks. Internet protocol (IP) is the well-known protocol for the network layer. There are many security risks associated with the IP in the network layer. The part of the security risk affecting network layers are network layer packet sniffing, route spoofing, IP Address spoofing.

Route policy controls - This mitigation gives a network administrator total control over the routing behaviour of particular system. This control also improves network stability.

Authentication— Packet sniffing can be mitigated by various methods, and the using of strong one-time passwords is one mitigating method It could also be controlled by deploying switch infrastructure to counter the use of packet sniffers.

2.4.4 TRANSPORT LAYER

The transport layer makes use of mechanisms such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) to provide end-to-end communication services, which allow data to completely arrive at its destination. Poor handling of undefined conditions is one the problems this layer is facing. Overuse of a particular port for multiple functions could also be a vulnerability of transport layers as well as poor handling of undefined conditions, transport protocol implementation differences, transport-layer mechanisms overloading.

Firewall rules that can be used to limit access to specific transmission protocols and sub protocol information should be strict.

Other measures include preventing out-of-state packets, by inspecting the layer at firewall from entering the perimeter and preventing the attacker and takeover of communications by implementing stronger transmission and layer session identification mechanisms.

2.4.5 SESSION LAYER

The session layer keeps track of data communications and organizes them into a logical flow. This layer also establishes, manages, and terminates sessions between applications and manages the data exchange between presentation layer entities. Attackers can cause damage to company`s network through this medium by unlimited attempts to guess the password, and they can as well make use of cruder methods to exhaust possible password strings. Weakness of used authentication mechanisms, hijacking and spoofing of session identification, failed authentication attempts could lead to information leakages, and unlimited failed sessions can help attackers to accessing credentials.

The following precautions should be put in place so as to prevent the error from happening or to eradicate it if happed already. Passwords should be well encrypted and change on a regular basis, there should be a specific expiry data for a particular user account for regular monitoring, session identification information should be protected through cryptographic means, the use of timing machine is encouraged for limiting failed session attempts.

2.4.6 PRESENTATION LAYER

The presentation layer deals with service request responsibility from the application layer and service request issuing to the session layer. The presentation layer is known for three functions: encoding and decoding data, encrypting and decrypting data, compressing and decompressing data. Although presentation layer is one of the most secured layer among the OSI model, it has its own threats. The threats common to this layer are fake certificate attacks and man-in-the-middle attacks.

Care should be taken when handling unexpected input, because it can crash applications, privacy protection could be exploited by cryptography flaws and remote manipulation or information leakage could occur when using external supply input unintentionally.

The solution that should be put in place to counter the above mentioned vulnerabilities include input coming into the application function should be carefully specified and checked; separating user input and program control functions; cryptography solutions should be reviewed continuously to ensure current security versus emerging threats.

2.4.7 APPLICATION LAYER

The application layer is the closest to the end user and it allow users to interact with the application and the networks. This interface could be a prime target for unauthorized use and abuse over the network if the application is weak or unauthenticated. For instance, an intruder has no challenge in guessing file names in TFTP protocol, because username or even password is not required to access files in the TFTP protocol.

Standard security control is bypassed through the backdoors and application design. If security controls force approach is not adequate, it results in excessive access or insufficient access; when application security is too complex, it is sometimes difficult for users to understand; and program logic flaws could sometimes cause programs to crash or undesired behavior.

The use of application level access controls in order to define access to application resources, use of baseline in measuring application implementation; such as application codes reviews and standard testing. using of host-based firewall systems to regulate traffic, application activities and inquiries monitored by the use of IDS systems are all means to control the vulnerabilities of application layers (Reed 2003)

2.5 RECONNAISSANCE ATTACKS

Administrators could overlook this attack because of the form it takes to penetrate the network. It always makes this kind of noise that might let the administrator to think is just a network noise. A reconnaissance attack is always used by hackers to gather information about a particular targeted network, which they subsequently used to access the network or as DoS attacks. (cisco 2005)

1) PACKET SNIFFERS

As its name implies, a packet sniffer is a very good device used by the administrators for detecting any kind of fault in the network. As it is a good device for administrators for monitoring or analyzing a network, so is it a good device for attackers for capturing packets sent across networks.

2) PORT SCANS AND PING SWEEP

These applications run a series of tests against hosts and devices to identify vulnerable services that need to be attended to.

These attacks can attempt to:

I. Identify all services on the network.

II. Identify all hosts and devices on the network.

III. Identify the operating systems on the network.

IV. Identify vulnerabilities on the network.

3) INTERNET INFORMATION QUERY

“WHOIS” is the Internet weapon attackers use to view addresses by DNS queries so that they can present a targeted company live hosts. By querying the IP addresses, some information could be revealed, such as the range of addresses and domain associated to those addresses. All revealed information could prompt an attacker to carry out whatever attack they intend to do.

2.5.1 ACCESS ATTACK

Access attackers could be outsider hackers or inside users gaining entrance into a network in an unauthorized way to steal some vital and confidential information from the systems. They could also engage in destruction of resources so that some information that could lead to them could not be seen. There are different reasons for different attacks. Intruders use access attacks on networks or systems for the following reasons: to retrieve data, to gain access and escalate their access privileges. Access attacks can consist of the following:

1) PASSWORD ATTACKS

Hashes of passwords could be taken by L0phtCrack and the clear-text passwords could be generated from them; a brute-force password attack offers access to accounts that can be used to alter critical network services and files. A typical example for such attack that compromises the network integrity is when an attacker modifies the network’s routing tables. By doing so, the attacker ensures that all network packets are routed to the attacker before being transmitted to their final destination. In such cases, an intruder can monitor all network traffic. There are two methods for computing passwords with L0phtCrack:

I. Dictionary cracking: The password hashes for all words in a dictionary file are compared and computed against all of the password hashes for the users. This is an extremely fast method that finds very simple passwords.

II. Brute-force computation: In this method, particular character sets are used, such as A to Z plus 0 to 9 or A to Z, and compute the hash for every potential password made up of those characters. Brute-force compilation usually computes passwords if those passwords are made up of the character set someone has selected to test. The problem for the attacker is the time required for the completion of this type of attack.

2) TRUST EXPLOITATION

Trust exploitation is a situation where by an individual is taking advantage of a trustable and reliable relationship within a network. An example of such an attack is a perimeter network connected to a corporate network. Hacker leverages on the existing trust relationships. Several trust models that exist:

I. Windows

II. NIS+

III. Active directory

IV. NIS

V. Linux and UNIX

VI. Domains

3) PORT REDIRECTION

Port redirection attacks are a type of trust exploitation attack, which uses a host that is fragile in passing traffic that would otherwise be dropped via a firewall. A host on the outside can contact the host on the public services segment (mostly known as the demilitarized zone [DMZ]) (Host A), but not the host on the inside (Host B). The host on the public services segment can be reached by the host on both the inside and outside. If hackers successfully compromise the public services segment host, they will be able to install software to channel traffic from the outside host directly to the inside host. Even though neither communication fails to agree with the rules implemented in the firewall, the outside host has now achieved a good network connectivity to the inside host simply through the port redirection process on the public services host. A good example of an application that can render this kind of access is Netcat.

4) MAN-IN-THE MIDDLE ATTACK

A man-in-the-middle attack necessitates that the hacker possess access to network packets that come via a network. A man-in-the-middle attack could be implemented using network packet sniffers and routing and transport protocols.

Theft of information, hijacking of an ongoing session to gain access to internal network resources, traffic analysis to derive information about the network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions are possible tools uses by man-in-the-middle attacks to attack a network.

Someone working for an ISP can gain access to all network packets and perform all of the above operations.

2.5.2 DENIAL OF SEVICE ATTACKS

A denial of service (DoS) attack damages or corrupts a computer system or denies all forms of access to the networks, systems or services even within the hacker's community. Denial of Service (DoS) attacks is regarded as less important and considered a bad form because they require little effort to execute. Although DoS implementation is easy and can cause little potential significant damage the attacks deserve special attention from security administrators. DoS attacks can consist of the following:

I. IP Spoofing

IP spoofing; This is a technique used to acquire unauthorized access to computers. In this kind of technique, the intruder sends illegitimate messages to a computer with an IP address which shows that the message is coming from a reliable and trusted host. Engaging in IP spoofing, hackers firstly use a variety of techniques to look for an IP address of a trusted host, then they modify their packet headers to appear as though the packets are coming from that trusted host. Furthermore, attackers can also engage other unsuspecting hosts in order to generate traffic and make it appear like its coming from a trusted host, hence, flooding the network.

II. DDoS EXAMPLE

DDoS(Distributed Denial of Service) attacks refer to the next generation of DoS attacks on the Internet. TCP SYN flooding and UDP, ICMP echo-request floods, and ICMP directed broadcasts (also refferred to as smurf attacks) are similar to DDos attacks, however, the attack has a new scope. Victims of DDoS attack experiences packet flooding from various sources perhaps spoofed IP source addresses that brings their network connectivity to a grinding malfunction. In the past, an attempt to flood a target host with packets is the typical DoS attack. The hacker uses a terminal to scan for systems to hack. After handler systems are accessed, the hacker installs software on these systems. This software attempts to scan for, compromise, and infect agent systems. When the agent systems are accessed, the intruder then loads remote control attack software to accomplish the DDoS attack. [Bidou 2000]

2.5.3 WORM, VIRUS AND TROJAN HORSE ATTACKS

Some threat are categorized according to minor or primary vulnerabilities for the end-user, which could be handled by a layman by just explaining what he/she has to do. These attacks could be solved by the use of antivirus software or by restoring the affected machine to factory settings.

I. VIRUS

Viruses are known as malicious software, which are attached to other programs and execute a particular undesirable or unwanted function on a user workstation. Typically, a virus propagates itself by infecting other programs on the same computer where it resides. Viruses can do serious damage, like erasing an entire storage media or erasing and manipulating files. These kinds of viruses cannot affect a new computer without human aid such as introducing a virus-infected file on a CD, or as an email attachment and mostly through file sharing.

II. WORMS

A worm is a self-replicating malware, which executes arbitrary code and also installs copies of itself on memory of infected computer; it can then infect other hosts from the infected computer. A worm is also a program that propagates itself like viruses do, but a worm can as well spread itself automatically across the network from one computer to the next unlike viruses that need human media to spread. They always take advantage of features of automatic file sending and receiving, found on many computers to propagate.

III. TROJAN HORSE

A Trojan horse does two things at a go: it can infect and convert the infected, and a Trojan can attack on three levels. It can attack as virus, as worm and as itself. A virus known as the Love Bug is a typical example of a Trojan horse because a love bug pretends to be a love letter when it actually carries a harmful program. Love Bug is definitely a virus because it infects all image files on the attacked disk, and turns them into new Trojans. Finally, Love Bug is worm as it propagates itself across the Internet by hiding in the Trojan horses, which is sent out using addresses in the attacked email address contact.

3.0 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.

3.1 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.

3.2 ENVIRONMENTAL THREAT MITIGATION

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.

3.3 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.

3.4 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.

3.5 PACKET SNIFFER ATTACK MITIGATION

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. An one-time 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 IPSecurity (IPsec), IPsecurity 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.

3.6 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.

3.7 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)

3.8 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.

3.9 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 IPSecurity tunnel. With this Encryption method, intruders or hackers can see only cipher text. (Mattsson 2006

3.10 DENIAL OF SERVICE ATTACKS AND MITIGATION

1) IP SPOOFING ATTACK MITIGATION

The threat of IP spoofing cannot be eliminated but can be reduced using the following measures:

I. Access control configuration: In order to reduce the effectiveness of IP spoofing, configuration of access control is required to deny any traffic from external network, which has a source address that should reside on the internal network.

II. Encryption: Encryption is another possible way to prevent IP spoofing, by encrypting all network traffic to avoid source and destinations hosts from being compromised. (Mattsson 2006)

III. Additional authentication: If additional authentication methods are used, they render IP spoofing attacks irrelevant. Cryptographic authentication is the best method of additional authentication. However, when cryptographic authentication is not possible, one time passwords(OTPS), which is a strong two-factor authentication, can be effective.

2) DoS(Denial Of Service) ATTACK MITIGATION

The threat of DoS(Denial Of Service) attacks can be reduced with the following techniques:

I. Anti-spoof features: Proper configuration of anti-spoof features on routers and firewalls can reduce risk of DoS attack. This configuration includes filtering to an RFC 2827 level. In this way, hackers' would not be able to mask their identities, and they will not attack.

II. Anti-DoS features: configured anti-DoS(denial Of Servuce) features on routers and firewall limit the effectiveness of an attack. Anti-DoS features often involve limiting the amount of half-open TCP connections that a system allows at any given time.

III. Traffic rate limiting: Some ISPs provide the implementation of traffic rate limiting. In filtering, the amount of unnecessary traffic that crosses the network segments at a certain rate is limited.

3.11 MITIGATING WORM ATTACKS

These are some steps to mitigate worm attacks:

I. Inoculation: method of patching all systems and, possibly, scanning for vulnerable systems.

II. Quarantine: Tracking down each infected machine inside a network. Any infected machine should be disconnected, blocked or removed from the network.

Iii. Treatment: Cleaning and patching each infected system is safe worm attack mitigation. Complete system reinstallation may be required to clean up a worm totally.

3.12 APPLICATION LAYER ATTACK MITIGATION

Measures that can be taken to reduce risks include the following:

1) Reading operating system and network log files, or have them analyzed by log analysis applications.

2) Subscribing to mailing lists that publicize vulnerabilities.

3) Keeping the operating system and applications current with the latest patches.

4) Using IDS/IPS in scanning known attacks, monitoring and logging attacks, and sometimes, preventing attacks.

3.13 SECURING REMOTE ACCESS

Cisco networking (Cisco 2005), devices support Authentication Authorization and Accounting (AAA) access control using line passwords, a local security database, or remote security server databases. The local security database is configured on the router for a group of network users using the username xyz and the strong password command. A remote security database is a separate server running an AAA security protocol, providing AAA services for multiple network devices and large numbers of network users.

Router administrators and users who wish to access the corporate LAN through dial-in or Internet connections use AAA. The architecture enables systematic and scalable access security (Cisco network device (SND) v1.0) which is explained in details in the below architecture:

Authentication

Who are you?

I am a user student and my password validate it.

Authorization

What can you do? What can you access?

A user student can access host server XYZ using Telnet.

Accounting

What did you do? How long did you do it? How often did you do it?

User student accessed host server XYZ using Telnet for 15 minutes.

Remote Authentication Dial-In User Service (RADIUS): The Internet Engineering Task Force (IETF) developed RADIUS, which is essentially a security system that works to prevent the network against unauthorized access. Remote Authentication Dial-In User Service (RADIUS) is an open standard, which has been adopted by leading vendors, and it is now one of the most popular types of security servers.

It deploys a client/server architecture, where the principal clients are routers and the typical servers are Window or Unix device running RADIUS software.

The authentication process has three stages:

1) Username and password are prompted.

2) Usernames and encrypted passwords are sent to the RADIUS server across the network

3) The RADIUS server would reply with one of the following below;

Response	Meaning
Accept	The user has been successfully authenticated.
Reject	The username and password are not valid.
Challenge	The RADIUS server requests additional information.

Change Password	The user should select a new password.

Terminal Access Controller Access Control System (TACACS+): TACACS+ in the switch manages authentication of logon attempts through either the Console port or Telnet. is also a security server. It is similar in many ways to RADIUS, except that TACACS+ does not do entirely what RADIUS does and more. TACACS+ is developed by Cisco Systems so it is specifically designed to interact with Cisco's AAA services. If a company is using TACACS+, it has the entire menu of AAA features available —also handles each security aspect differently: (Hill 2001)

In addition to login and password functions, Authentication also includes messaging support, explicit control over user capabilities is enabled by authorizations and accounting delivers full information about user activities.

Kerberos: is an encryption and authentication service that is designed for using secrete-key cryptography to provide string authentication for server applications. Cisco routers also use it to prevent data being sniffed off on the network. Kerberos originated at the Massachusetts Institute of Technology (MIT), was designed to protect network services and provides some hefty security using the Data Encryption Standard (DES) cryptographic algorithm.

User authentication on Kerberos is similar to RADIUS or TACACS+; but after a user has been authenticated with Kerberos, they are granted something called an admission ticket.

This admission ticket gives the user access to other resources on the network without their having to resubmit their password across the network. These tickets are non-transferable and non-refundable and have a limited life span—they are valid for only one ride. Whenever a user's ticket expires, a renewed ticket is issued to the user to access resources again. Similarly, Cisco routers support Kerberos for Telnet, rsh, rcp, and rlogin. Kerberized sessions permit encrypted communication between the end station and the router. (MIT Kerberos Team 2012)

4.0 BEST PRACTICES IN SECURING A COMPUTER NETWORK

4.1 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.

4.1.1 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:

1) 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.

2) 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.

3) IP Connectivity: Separate physical cabling for CCTV functions is required for existing monitoring systems. Video surviellance 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.

4) 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 a single place.

5) 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.

6) 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)

4.1.2 LOCKS

A keyed lock is one of the most common means of restricting access. However, precautions need to be taken about the types of keys used. The options will vary depending on the type of building office is located in. Some keys have warnings on them to make it prohibit duplication, while others are of an uncommon shape, a copy can not be made even without a warning, If a set of duplicated keys are used in some certain for offices or server rooms, it may worth considering periodic changes of the locks and keys. This will effectively "expire" any unauthorized duplications.

4.1.3 ELECTRONIC CODE ENTRANCES

Many forms of electronic code locks exist in buildings today, some more advanced systems can be expensive and sophisticated. These systems require users to input code to gain access via a doorway. The apparent vulnerability with these systems is that if the code does not change, the entire facility may finally know the code, and when that occurs, there might as well be no entrance at all. In other to prevent this from happening, different codes should be provided to different employees. In this way, if an employee leaves the company, access code of such employee could be deactivated.

4.2 SYSTEM USAGE CONTROL

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

1) Default usernames and passwords should be changed immediately.

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

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

4) System should not be left on or un-lockd while not on sight.

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

4.2.1 SECURED PASSWORD

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

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

2) Accounts should be disabled after a certain number of unsuccessful logins. This practice prevents continuous password attempts.

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

4) 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.

4.2.2 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.

4.2.3 HOST INTRUSION DETECTION

Host-based intrusion typically implemented as Inline technology, called a host-based intrusion prevention system (HIPS), it stops the attack, prevents damage, and blocks the multiplication of worms and viruses. Active detection should be set to stop affected services automatically so that corrective action could be taken immediately. Companies can also require network administrators to notice when some external process tries modifying a system file in such a way that may include an underground program. Furthermore, remote access is a way an intruder can get into the network from a distance area where he cannot be noticed.

4.3 SECURE REMOTE ADMINISTRATIVE ACCESS USING SSH

Secure shell (SSH) has replaced Telnet as the best application for providing remote router administration with connections that support session integrity and strong privacy. SSH uses port TCP 22; it offers a similar functionality to an outbound Telnet connection, except that the connection is encrypted. With encryption and authentication, SSH allows for secure communications over an insecure network.

4.3.1 SECURE WITH IOS FIREWALL

With the IOS Firewall Authentication Proxy appropriately configured, users are impelled to authenticate before access is granted through the IOS Firewall. When a user attempts to initiate communications through the IOS Firewall, they are queried for a username and password, which are then sent to an external authentication, authorization, and accounting (AAA) server operating either TACACS+ or RADIUS. The server replies to the firewall's request with a user profile, which defines specific rights and limitations for same individual users access which is then adopted by the firewall for the entire period of the communication.

4.3.2 SECURE ROUTERS USING AAA (TACACS+) SERVICES

AAA is used by router administrators and users who wish to access the corporate LAN through dial-in or Internet connections. It provideS a higher degree of scalability than the line-level and privileged-EXEC authentication. In the Cisco environment, network and administrative access security whether it involves campus, dialup, or Internet access, is based on a modular architecture that has three functional components: authentication, authorization, and accounting: External AAA systems, like the Cisco Secure ACS Solution Engine or Cisco Secure ACS for Windows, communicate with Cisco routers and NASs using the Terminal Access Controller Access Control System Plus (TACACS+) [10]. TACACS+ can be configured in a different system interfaces, e.g., Cisco (IOS, CatOS), Juniper (ScreenOS, JUNOS), Huawei, HP, OneAccess, Linux-based systems (via PAM), but the configuration use In this thesis is Cisco (IOS) -based systems. The full configuration can be seen in Appendix 1.

4.3.3 SET UP A DMZ (DEMILITARIZED ZONE)

A DMZ is a small network that sits between the internal (corporate) network and the Internet. The DMZ prevents outside users from getting direct access to company computers. In a typical setup, the DMZ would receive requests from corporate users to access Web sites and other information on the external network. The DMZ initiates requests for the information and forwards the packets back to the requesting machine. Companies often place Web servers on their DMZ so that external users can access their Web site but not the private data ghosted on the corporate network. There are two types of DMZs; A three-homed perimeter network. In this type of DMZ setup, the firewall possesses three connections: one for internal network, a second for the Internet and the third for the demilitarized zone (DMZ). The second type of demilitarized zone (DMZ) is known as back-to-back perimeter network, and it makes use of two firewalls. One firewall has a connection to the Internet as well as the DMZ, while the second has connections to company's internal network and the demilitarized zone (DMZ). With this method, the demilitarized zone (DMZ) sits between the internal and external networks. In both setups, configuration is made to restrict traffic firewall in and out of each network.

4.3.4 SECURITY WITH IPSec VPNs

To provide a secure connection over a public network, Cisco utilizes IPsecs VPNs to provide secure connections.

Cisco employs IPSecurity (IPsec) Virtual Private Networks (VPNs) to offer a secure connection across a public network—connection, which can be planned, based on business needs of a company. Remote-access solutions can be used for telecommuters, site-to-site solutions for remote offices that require access to the corporate network, and extranet solutions, which provide customers and partners with the limited information they need. (B. N. I 2004-2009)

5.0 SUMMARY AND CONCLUSION

5.1 SUMMARY

To flourish 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.

5.2 CONLUSION

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 one-time 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.

Below is a list of additional configurations that should be in place and they complement the concepts described in this thesis.

1) All network devices should have an ACL(Acess Control List) that only allows network management workstations access to the device

2) The TACACS+ server should be behind a firewall that only allows

TACACS+ traffic (TCP port 49) in from all network devices.

3) User accounts synchronization could be done easily using the following script:

```
#!/bin/sh while true; do

for f in /etc/passwd /etc/shadow; do

for h in second_auth_server_name ; do rsync -azSHe ssh $f $h:$f

done done sleep 60 done
```

4) Administrators should use the port security feature and hard coded MAC addresses on switches and routers to help prevent against man-In-the-middle attacks that exploit ARP spoofing tactics.

Finally, network administrators should always find out the newest forms of threat and attack, test their network security design if vulnerable to the new threats and attacks and then review the security design or policy for further amendment.

REFERENCES

Bidou, R. 2000. *Denial of service attacks.* Retrieved: May 10 2012. Available at: http: //www.docstoc.com/docs/85149779/Denial-of-Service-Attacks

Cisco Security. 2005. *Securing Cisco Network Devices.* (v 1.0 ed.) Available at: http://www.scribd.com/doc/985242/Securing-Cisco-Network-Devices-SND-v1-0

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

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] .*

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?abstract_id=934271

MIT Kerberos Team Security Contact. *The Network Authentication Protocol. Retrieved: January 27, 2012. Available at: http://web.mit.edu/kerberos/contact.html*

Orbit-Computer Solutions. 2012. *Threats to physical and network infrastructure.* Retrieved: May 5 2012. Available at: , http://www.orbit-computer-solutions.com/Threats-to-Physical-and-Network-Infrastructure.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/whitepapers/networkdevs/implementing-secure-access-cisco-devices-tacacs-plus-ssh_1041

Pete, L. June 2003. The Emergence of the Physical Threat No. 2-3 P.O. Box 152, Malvern, PA 19355: Spire Security, LLC. Available at: http://***netbotz.com/library/Physical_Threat_Security.pd***

Reed D. November 21, 2003. *Network Model to Information Security.* Retrieved: . Available at: http://www.sans.org/reading_room/whitepapers/protocols/applying-osi-layer-network-model-information-security_1309

APPENDIX 1

TACACS+ Server configuration

“The TACACS+ server discussed in this paper was written by Devrim Seral and can be downloaded from www.gazi.edu.tr/tacacs”

```
# tar zxvf tac_plus_v9a

# cd tac_plus_v9a

# ./configure

# make tac_plus

# make install
```

After compiling and installation, copy default configuration to the /etc directory and open it on any text-editor. The following sections will explain each part of the configuration in details

```
############################################################

# Default Config

############################################################

# Key, very important

key = thisshouldbealongrandomstring

# Use /etc/passwd file to do authentication default authentication = file /etc/passwd

# Accounting records log file

accounting file = /var/log/tacacs/tac_acc.log
```

The first configuration line is the “key” directive, which specifies the shared secret that will be used between all of devices and the TACACS+ server. The TACACS+ needs to be the same on the devices and the server in order for TACACS+ to function efficiently. The next line shows the TACACS+ server the location for authentication; in this case it looks into the local UNIX /etc/passwd file. Finally, the TACACS+ server writes the accounting logs, which will be setup to log command execution and logon/logoffs to all devices

The next configuration is for users and groups:

```
##################################################################

# Group Definitions

##################################################################

group = netadmin { default service = permit service = exec {

priv-lvl = 15

}

}

group = users {

default service = deny service = exec {

priv-lvl = 1

}

}
```

To keep things simple, two groups will be used, a privileged group and a non-privilege group. The “netadmin” group in the configuration code will include all network administrators who need enable access to the devices, and is granted privilege level 15, this is the highest level of access on Cisco devices

Users configuration:

```
# Netadmin users

##################################################################

user = bjones {

member = netadmin

}
```

```
################################################################

# Unprivileged Users

################################################################

user = sjones { member = users cmd = show { deny ip

deny tacacs permit .*

}

cmd = quit {

permit .*

}

cmd = exit {

permit .*

}

cmd = logout {

permit .*

}

cmd = ssh {

permit 192\.168\.1\.[0-9]+

deny .*

}

}
```

In the first section of the code above we place the user “bjones” in the netadmins group, to grant privilege level 15 on all devices on the network. “bjones” also exists in the local Unix /etc/passwd file, and it’s the same case for all users whom company wish to grant access through TACACS+. The next section of code is unprivileged user “sjones”, in which level privilege granted. The group members on the TACACS+

server has a default deny statement, by so doing, no commands are allowed default. Users are allowed to run nearly every “show” command for debugging purposes, but not given the privilege to see any IP or TACACS+ information. And also SSH is allowed to machines on 192.168.1.0/24 subnet, with use of a regular expression in the Secure Shell (SSH) section. Finally, exit is allowed from the router, using any of the three commands that allow logoff. This section could be modified to fit company needs. Once the configuration file is adjusted to fit company needs, the TACACS+ command can follow: # /usr/local/sbin/tac_plus -C /etc/tac_plus.cfg -d 248

The “-C” options shows the daemon the location of the configuration file while the “-d 248” is the debugging level, which is set to 248, giving plenty of information in the logs (see the tacplus man page for more details). User account should be created on the system and added to the tacplus.cfg file. Thus, it is recommended to have minimum of two TACACS+ servers and use of "rsync" for user accounts synchronization and TACACS+ configuration.

IOS Configuration

The section below configuration can be added to all of the IOS (Internetwork Operating System) based network devices (primarily routers and switches). Proper orderliness should be ascertained when putting the commands; otherwise, someone could be easily locked out of the device.

Firstly, setup the TACACS+ servers:

tacacs-server host 192.168.1.5 tacacs-server host 192.168.1.6

tacacs-server key thisshouldbealongrandomstring

The device uses the first server on the list if available, and then uses the second, and so on. The key should be set to the same value as set on the TACACS+ server. The next line of configuration codes creates a local user; called “admin”, with privilege level of 15, and a good password: Username Admin privilege 15-password aGoOdpaSsworDstring

This is the username/password pair that is needed to be use if the TACACS+ server is unavailable. Local account IS needed in order to provide remote access via SSH only, and providing this local account will allow telnet access turned off to the device while still allowing access if the TACACS+ server is unavailable.

The AAA configuration code:

```
aaa new-model

aaa authentication login default group tacacs+ local enable

aaa authorization exec default group tacacs+ local none

aaa authorization commands 0 default group tacacs+ local none

aaa authorization commands 1 default group tacacs+ local none

aaa authorization commands 15 default group tacacs+ local none

aaa accounting exec default start-stop group tacacs+

aaa accounting commands 0 default start-stop group tacacs+

aaa accounting commands 1 default start-stop group tacacs+

aaa accounting commands 15 default start-stop group tacac+
```

The configuration above directs the device to handle all interactive user logins and what users will be able to do once logged in. The first line creates a new AAA schema, which allows user to enter all commands that follows. The second line which is the authentication tells the device that once a user logs in it will confirm the username and password against the TACACS+ server, then check through a local username and password database, and finally, it defaults to the enable password. The only period it defaults to the enable password is when local username is not setup. The exec and command authorization works the same way. [Paul, A. 2003]