INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

# SYSTEM PROTECTION USING NETWORK SECURITY

**SUNNY W. THAKARE [1], SATISH J. ALASPURKAR[2]**

1. Department of C.S.E, M.E(G.H. Raisoni. C. E & M.Amravati).
2. Department of C.S.E, M.E(G. H. Raisoni. C. E & M. Amravati).

**Accepted Date:**

27/02/2013

**Publish Date:**

01/04/2013

**Keywords**

Secret, protection,

Firewall,

Threat,

RAS,

SSH,

SSL protocol

**Corresponding Author**

**Mr. Sunny W. Thakare**

## Abstract

Security incidents are rising at an alarming rate every year. As the complexity of the threats increases, so do the security measures required to protect networks. Data center Operators, network administrators, and other data center professionals need to comprehend the basics of security in order to safely deploy and manage networks today. With the rapid growth of interest in the Internet, network security has become a major concern to companies throughout the world. The tools needed to penetrate the security of corporate networks. Because of this increased focus on network security, network administrators often spend more effort protecting their networks than on actual network setup and administration. Tools that probe for system vulnerabilities such as the Security Administrator Tool for Analyzing Networks (SATAN) and some of the newly available scanning and intrusion detection packages and appliances are defined. Security is gaining much significance consequently. Cryptography, authentication and access control mechanisms play a very important role in secured communication as they form the major disciplines of network security. This paper covers the secure networking systems, including Firewalls, network topology and secure protocols. Best practices are also given that introduce the reader to some of the more critical aspects of securing a network.

## INTRODUCTION

Securing the modern business network and IT infrastructure demands an end-to-end approach and a firm grasp of vulnerabilities and associated protective measures. While such knowledge cannot thwart all attempts at network incursion or system attack, it can empower network engineers to eliminate certain general problems, greatly reduce potential damages, and quickly detect breaches. With the ever-increasing number and complexity of attacks, vigilant approaches to security in both large and small enterprises are a must. This paper presents security as well as some best practices regarding the network, computer hosts and infrastructure network elements. Figure1illustrates the steep rise in security incidents occurring each year, as reported to the CERT® Coordination Center (a center of Internet security expertise).

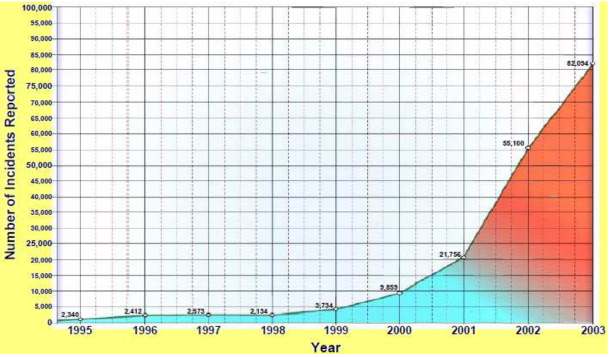


Figure 1 – Security incidents by year – CERT.ORG

## MATERIAL AND METHOD

### The people problem

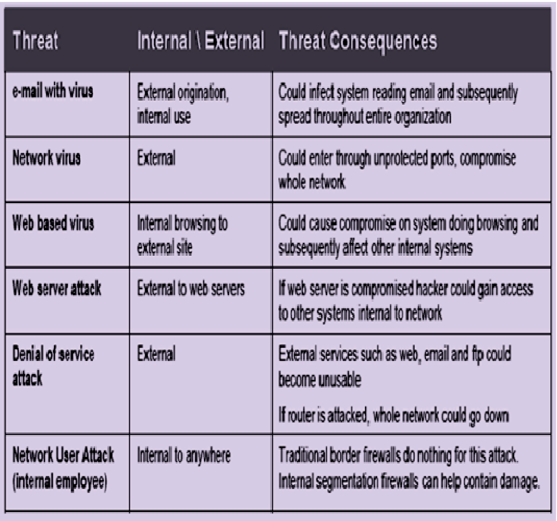
People are truly the weakest link in any security schema. Most people are not careful about keeping secrets such as passwords and access codes for secure systems. All security systems rely on a set of measures to control access, verify identity and protect sensitive information. These measures usually involve one or more “secrets”. Another example, many people have tendency to leave factory default passwords in certain network devices. Imagine a server bank with rock solid security protocols on each web and mail server crashed by a simple power cycle on an unprotected UPS!

### Security BasicsKnowing the network

Each of these elements should have a relative value assigned to the organization. Examples are as servers, workstations, storage systems, routers, switches, hubs, network and Telco links, and any other network elements such as printers, UPS systems and HVAC systems are attached.[3]

Understanding different threats

The next step is to identify the “threats” as shown in Table 1. Threats can come from both internal and external sources. They may be human based, automated. One example is a power outage to a burglar alarm.[1]



| Threat | Internal \ External | Threat Consequences |
|---|---|---|
| e-mail with virus | External origination, internal use | Could infect system reading email and subsequently spread throughout entire organization |
| Network virus | External | Could enter through unprotected ports, compromise whole network |
| Web based virus | Internal browsing to external site | Could cause compromise on system doing browsing and subsequently affect other internal systems |
| Web server attack | External to web servers | If web server is compromised hacker could gain access to other systems internal to network |
| Denial of service attack | External | External services such as web, email and ftp could become unusable<br>If router is attacked, whole network could go down |
| Network User Attack (internal employee) | Internal to anywhere | Traditional border firewalls do nothing for this attack. Internal segmentation firewalls can help contain damage. |

Table 1 – Summary of various threats with Consequences

Physical security, protection on the inside

Most experts would agree that all security starts with physical security. Controlling physical access to machines and network is more critical than any other aspect of security. Access to an internal site creates a major exposure of the site. Secure files, passwords, certificates and all other data can be obtained if physical access is possible.

Partitioning and protecting network boundaries with firewalls

Almost every large-scale company getting full time on internet connectivity. Partitioning the boundary between the outside Internet and the internal intranet is a critical. Sometimes the inside is referred to as the “trusted” side and the external Internet as the “un-trusted” side. A firewall is a mechanism which is used to control network traffic. They run on embedded systems such as an internet appliance or server platform. The firewall process allowed traversing from one side to the other. The range is being simple to very complex. Fig.2 explains as:

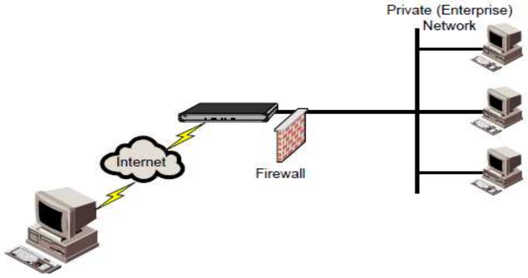


Figure 2 – Simple firewall to network

Aspects of security, firewall will depend upon factors such as traffic levels, services protection and the complexity. Firewalls can protection using denial of service (DOS) attacks. It is the ability to block network traffic to certain destinations. This includes both IP addresses and particular network service ports. External access that is web server can restrict all traffic to port 80 from the un-trusted side. Traffic from the trusted side is not restricted. Firewall often used by people with home or small business cable or DSL routers. & restrict ALL external access and allow only inside services. Only a connection request to the web server is allowed to complete and pass data, all others are blocked.[3] Fig.3 explains as:

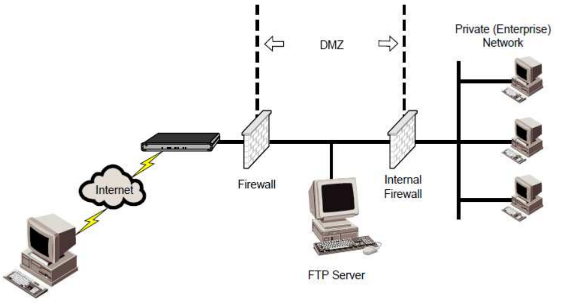


Figure 3 – Dual firewalls with DMZ

Use for basic port blocking approach by traffic behaviors, detect spoof attacks, denial of service attacks And other are “public” services such as web, ftp and e-mail while maintaining tight security of the intranet. The uses of DMZ (demilitarized zone), a euphemism from the cold war applied to the network & provided more protection.[2]

Workstation firewalls

There are several more dimensions to protecting networks. Varieties of worm, virus programs, and hijack computers can harm systems. Many of these Workstation firewall products can block all port accesses into hosts. Additionally firewall rules on the INTERNAL side that block suspicious connections out of the organization & can help prevent worms.

## RESULT AND DISCUSSION

### Basic Network Host Security

Port lockdown and minimizing running services

Many network devices and computer hosts startup network services by default, & service represent an opportunity for attackers, worms and Trojans. Doing port lockdown by turning off services reduces this exposure. Network firewalls, desktops and servers can run basic firewall software to block access to unnecessary IP ports on the host for internal protection. Desktop firewall software packages do a great job of protecting hosts, for example, Windows XP Service Pack 2.

### Username and password management

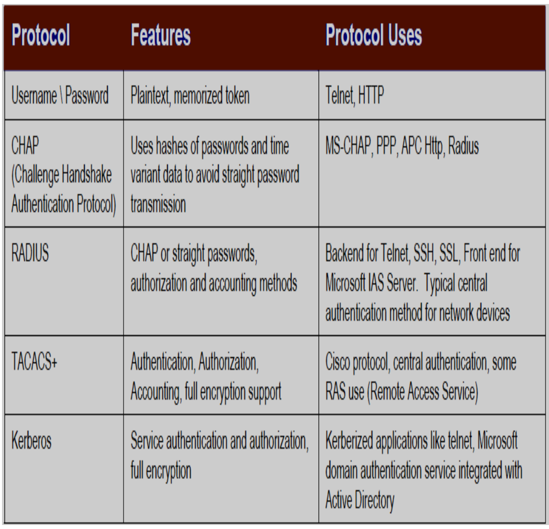
Poor username and password management is a typical problem in most enterprise networks. While sophisticated, centralized authentication systems can help reduce problems. Four basic rules can help tremendously that need to be followed for usernames and passwords include:1. do not use obvious passwords such as spouse's name, favorite sports team, etc. 2. Use longer passwords with mixed numbers or symbols. 3. Change passwords on a regular basis.4. NEVER leave default credentials in network equipment unless computers have built in policies

### Securing Access to Devices and Systems

Since data networks cannot always be protected from intrusion or data "sniffing", protocols have been created to increase the security of attached network devices. There are two separate issues as, authentication and encryption. And variety of schemes, protocols to secure systems and communication. The basics of authentication are discussed first and then encryption.

### User authentication for network devices

Authentication is necessary when one wants to control access to network elements, in particular network infrastructure devices. Authentication has two sub concerns, general access authentication and functional authorization. Consider the "User account". Authorization is concerned with individual user "rights". Restricting access to devices is most important aspects of securing a network. To protect servers, institute firewalls and secure access mechanisms is use, but leave with rudimentary security. All devices should have username password



| Protocol | Features | Protocol Uses |
|---|---|---|
| Username \ Password | Plaintext, memorized token | Telnet, HTTP |
| CHAP (Challenge Handshake Authentication Protocol) | Uses hashes of passwords and time variant data to avoid straight password transmission | MS-CHAP, PPP, APC Http, Radius |
| RADIUS | CHAP or straight passwords, authorization and accounting methods | Backend for Telnet, SSH, SSL, Front end for Microsoft IAS Server. Typical central authentication method for network devices |
| TACACS+ | Authentication, Authorization, Accounting, full encryption support | Cisco protocol, central authentication, some RAS use (Remote Access Service) |
| Kerberos | Service authentication and authorization, full encryption | Kerberized applications like telnet, Microsoft domain authentication service integrated with Active Directory |

authentication with non-trivial with perfect authorization[2]

Centralized authentication methods

Centralized authentication methods are even better.

Table.2 explain as: when either a) large numbers of users for devices are involved; or b) large numbers

Table 2–Summary of major authentication protocols

Of devices are in the network. Traditionally centralized authentication was used to solve problems found as (a) the remote network access, such as dial-up RAS. Potentially any user of the network could attempt to use any of the existing RAS access points. Placing all user information in all RAS units and then keeping that information up-to-date would exceed in large enterprise of users. Centralized authentication systems such as RADIUS and Kerberos solve this problem by using centralized user account information that the RAS units, or other types of equipment can access securely. If user information needs to be changed, such as a new password, Most RADIUS servers can communicate with RAS, protocol and then securely access account information stored in the directories.

Securing network data with encryption and authentication

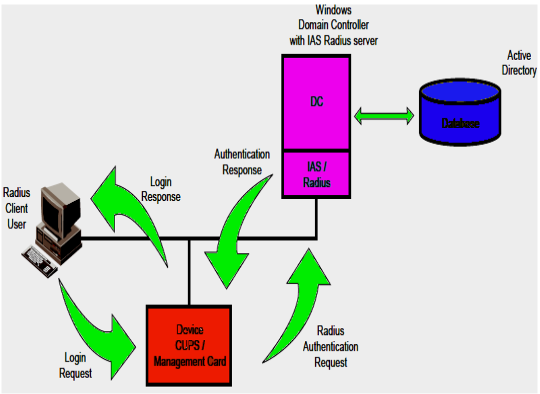
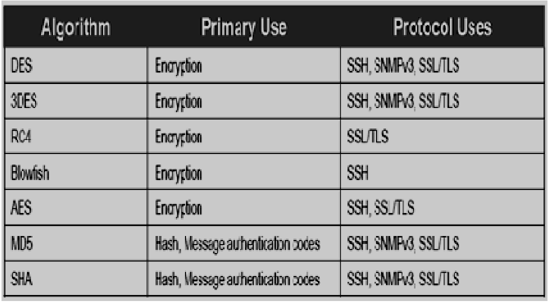


Figure 4 – Windows Domain Controller

Figure 4 shows a Windows Domain controller operating as both an Active Directory server and a RADIUS server for network. Disclosing the Information that is exchanged between network elements and computers systems. Certainly not access a bank account theirs capture personal information that may be transmitted over a network. To avoid data disclosure over a network, encryption methods must be employed that make the transmitted data unreadable to capture the data as it traverses a network. Methods to “encrypt” data network devices such as UPS systems that are value of protecting data such as UPS voltages and power strip currents. The non-disclosure of authentication credentials such as usernames and passwords is critical in any system over non-secure networks. For example, even within organizations' private networks, protection of these credentials is a best practice. In some case, cryptographic methods must be employed. Encryption of data is accomplished by the combination of plaintext data with a secret key using a particular encryption algorithm. The output is ciphertext. Unless the secret key cannot convert the ciphertext back to plaintext. This basic methodology is at the core of any of the secure protocols. The building block of cryptographic systems is the "hash". Hash methods take some plaintext input as key then compute a large number called a hash. The encryption methods are reversible, that are used as special IDs in various protocol systems because they can provide a check mechanism on data similar to a CRC on a disk file to detect data alteration. The hashes are used as a data authentication method. Alter data across a network will alter the hash values thus causing detection.[4]Table.3 explains as:



| Algorithm | Primary Use | Protocol Uses |
|---|---|---|
| DES | Encryption | SSH, SNMPv3, SSL/TLS |
| 3DES | Encryption | SSH, SNMPv3, SSL/TLS |
| RC4 | Encryption | SSL/TLS |
| Blowfish | Encryption | SSH |
| AES | Encryption | SSH, SSL/TLS |
| MD5 | Hash, Message authentication codes | SSH, SNMPv3, SSL/TLS |
| SHA | Hash, Message authentication codes | SSH, SNMPv3, SSL/TLS |

Table 3 Summary of major cryptographic algorithms.

Secure Access Protocols

There are a variety of protocols such as SSH and SSL that employ various cryptographic mechanisms to provide security through authentication and encryption methods. The level of security provided is dependent upon many things such as the cryptographic methods used, the access to the transmitted data, algorithm key lengths, server and client implementations and most importantly, the human factor. The most ingenious crypto scheme is user's access credential, such as a password or certificate, is obtained by a third party.[2]

The SSH protocol

The Secure Shell (SSH) client-server protocol was developed in the mid-1990s in order to provide a secure mechanism to access computer consoles or shells remotely over unprotected or “non-secure” networks. The protocol provides “secure” methods by addressing user, server authentication and full encryption of all traffic exchanged between the client and server. The protocol has two versions, V1 and V2. Additionally, V2 is superior in its ability to protect against certain types of “attacks”. It has traditionally been less employed in secondary infrastructure equipment such as UPS and HVAC.[5]

## The SSL\TLS protocol

The Secure Socket Layer (SSL) and Transport Layer Security (TLS) protocol method of securing web traffic and other protocols such as SMTP (mail). TLS is the most recent version of SSL and SSL is interchangeably with the term TLS. SSL and SSH differ with respect to the client and server authentication mechanisms built into the protocols. TLS was also accepted as an IETF (Internet Engineering Task Force) standard. SSL is protects http web traffic, also https for “http secure”. Both Netscape and Internet Explorer support both SSL and TLS. The client can also be authenticated with certificates, though usernames and passwords. SSL is always used on web sites that wish to be secure for banking and other commercial purposes since clients usually access sites over the public Internet. SSL can also protect other non-http communication.

## Conclusions

With the increased number of threats to networks such as worms, viruses and clever hackers, security can no longer be viewed as an option, even within “private” networks. Securing all equipment, including physical infrastructure equipment such as UPS systems and HVAC systems, is critical to maintaining uptime and seamless access to services. Today, the amount of time spent repairing a network due to just a single worm or virus attack. Fortunately, there are many options in systems and software to increase the security of the network. Even basic practices with periodic software updates, locking down all devices using centralized authentication and secure access methods can go increase the overall protection of the network.

Acknowledgment

First and foremost, I would like to thank Dr. P.V.Ingole for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper. Second, I would like to thank Mr.S.J.Alaspurkar to read my thesis and to provide valuable advices to reproof the paper, as well as all the other professors who have taught me the master degree. Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this research paper would not be possible without all of them.

Reference

1. Canavan, John E. Fundamentals of network security. http://www.artechhouse.com 802.7 security by Bruce Potter.
2. S.M. Bellovin. Security Problems in the TCP/IP Protocol Suite. Vol. 19, No. 2, pp. 32-48, April 1989.
3. Internet security by Chris Prossie.
4. J.P. Holbrook, J.K. Reynolds. ``Site Security Handbook.'' RFC 1244.