Volume 2, No. 7, July 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

TECHNICAL NOTE

Available Online at www.jgrcs.info

NETWORK SECURITY: AN APPROACH TOWARDS SECURE COMPUTING

Rahul Pareek

Lecturer, MCA Dept.
Rajasthan College of Engineering for Women
dhruvpareek@gmail.com

Abstract - The security of computer networks plays a strategic role in modern computer systems. In order to enforce high protection levels against malicious attack, a number of software tools have been currently developed. Intrusion Detection System has recently become a heated research topic due to its capability of detecting and preventing the attacks from malicious network users. A pattern matching IDS for network security has been proposed in this paper. Many network security applications rely on pattern matching to extract the threat from network traffic. The increase in network speed and traffic may make existing algorithms to become a performance bottleneck. Therefore it is very necessary to develop faster and more efficient pattern matching algorithm in order to overcome the troubles on performance.

Index term: Enemies, Effect of enemies, Security.

INTRODUCTION

Network Security

Network and computer security is critical to the financial health of every organization. Over the past few years, Internet-enabled business, or e-business, has drastically improved efficiency and revenue growth. E-business applications such as e-commerce, supply-chain management, and remote access allow companies to streamline processes, lower operating costs, and increase customer satisfaction. Such applications require mission-critical networks that accommodate voice, video, and data traffic, and these networks must be scalable to support increasing numbers of users and the need for greater capacity and performance. However, as networks enable more and more applications and are available to more and more users, they become ever more vulnerable to a wider range of security threats. To combat those threats and ensure that e-business transactions are not compromised, security technology must play a major role in today's networks.

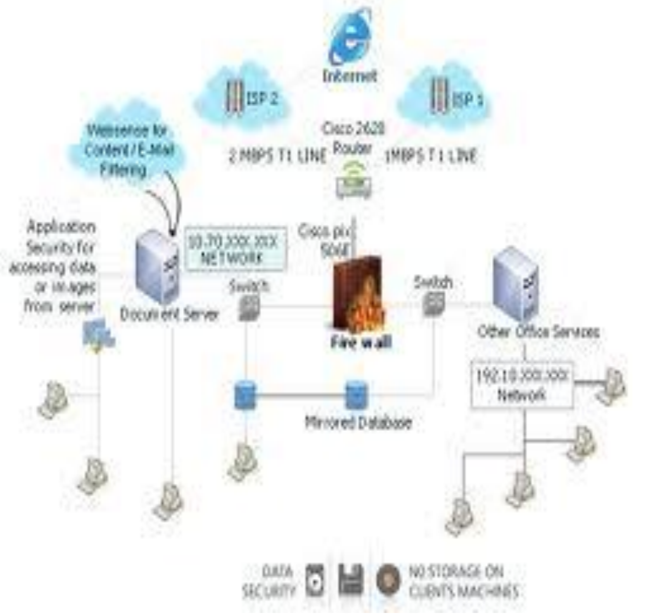

Figure: 1 Network Security

Necessity

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.

Objectives

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

Importance of Network Security

To protect company assets: One of the primary goals of computer and network security is the protection of company information that is housed on a company's computers and networks.

To gain a competitive advantage: Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition. Network security is particularly important in the arena of Internet financial services and e-commerce.

ENEMIES OF NETWORK SECURITY

Hackers:

This generic and often over-romanticized term applies to computer enthusiasts who take pleasure in gaining access to other people’s computers or networks.

Unaware Staff:

As employees focus on their specific job duties, they often overlook standard network security rules. Like simple password, use of Virus effecting CD/DVD etc.

Snoops:

Employees known as "snoops" partake in corporate espionage, gaining unauthorized access to confidential data in order to provide competitors with otherwise inaccessible information.

EFFECT OF ENEMIES

Viruses:

Viruses are the most widely known security threats, because they often garner extensive press coverage Viruses are computer programs that are written by devious programmers and are designed to replicate themselves and infect computers when triggered by a specific event.

A network can be infected by a virus only if the virus enters the network through an outside source—most often through an infected floppy disk or a file downloaded from the Internet. When one computer on the network becomes infected, the other computers on the network are highly susceptible to contracting the virus.

Trojan horse Programs:

Trojan horse programs, or trojans, are delivery vehicles for destructive code. Trojans appear to be harmless or useful software programs, such as computer games, but they are actually enemies in disguise. Trojans can delete data, mail copies of themselves to e-mail address lists, and open up computers to additional attacks. Trojans can be contracted only by copying the trojan horse program to a system, via a disk, downloading from the Internet, or

opening an e-mail attachment. Neither trojans nor viruses can be spread through an e-mail message itself—they are spread only through e-mail attachments.

Vandals:

Web sites have come alive through the development of such software applications as ActiveX and Java Applets. These devices enable animation and other special effects to run, making Web sites more attractive and interactive. However, the ease with which these applications can be downloaded and run has provided a new vehicle for inflicting damage. A vandal is a software application or applet that causes destruction of varying degrees. A vandal can destroy just a single file or a major portion of a computer system.

Attacks:

Innumerable types of network attacks have been documented, and they are commonly classified in three general categories: Reconnaissance attacks, Access attacks and Denial of service (DoS) attacks. Reconnaissance attacks are essentially information gathering activities by which hackers collect data that is used to later compromise networks. Usually, software tools, such as sniffers and scanners, are used to map out network resources and exploit potential weaknesses in the targeted networks, hosts, and applications.

Access attacks are conducted to exploit vulnerabilities in such network areas as authentication services and File Transfer Protocol (FTP) functionality in order to gain entry to e-mail accounts, databases, and other confidential information.

DoS attacks prevent access to part or all of a computer system. They are usually achieved by sending large amounts of jumbled or otherwise unmanageable data to a machine that is connected to a corporate network or the Internet, blocking legitimate traffic from getting through. Even more malicious is a Distributed Denial of Service attack (DDoS) in which the attacker compromises multiple machines or hosts.

Data Interception:

Data transmitted via any type of network can be subject to interception by unauthorized parties. The perpetrators might eavesdrop on communications or even alter the data packets being transmitted. Perpetrators can use various methods to intercept the data IP spoofing.

Social Engineering:

Social engineering is the increasingly prevalent act of obtaining confidential network security information through non-technical means.

Spam:

Spam is the commonly used term for unsolicited electronic mail or the action of broadcasting unsolicited advertising messages via e-mail. Spam is usually harmless, but it can be a nuisance, taking up the recipient's time and storage space.

SECURITY TOOLS

After the potential sources of threats and the types of damage that can occur have been identified, putting the proper security policies and safeguards in place becomes much easier. Organizations have an extensive choice of technologies, ranging from anti-virus software packages to dedicated network security hardware, such as firewalls and intrusion detection systems, to provide protection for all areas of the network.

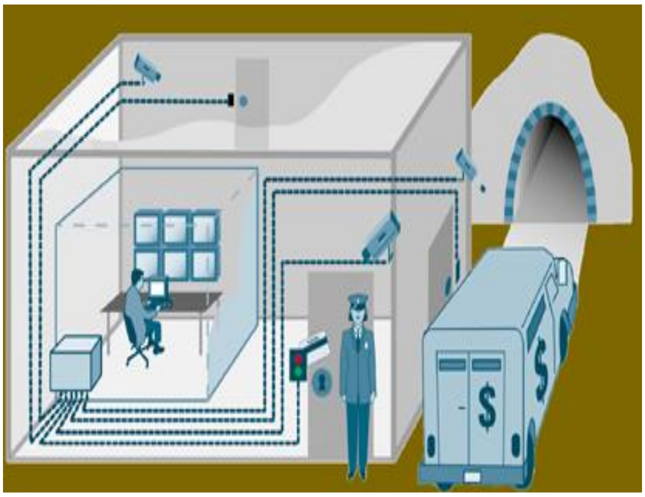

Figure: 2 Security

Anti-virus Packages:

Virus protection software is packaged with most computers and can counter most virus threats if the software is regularly updated and correctly maintained. The anti-virus industry relies on a vast network of users to provide early warnings of new viruses, so that antidotes can be developed and distributed quickly. With thousands of new viruses being generated every month, it is essential that the virus database is kept up to date. The virus database is the record held by the anti-virus package that helps it to identify known viruses when they attempt to strike. Reputable anti-virus software vendors will publish the latest antidotes on their Web sites, and the software can prompt users to periodically collect new data.

Network security policy should stipulate that all computers on the network are kept up to date and, ideally, are all protected by the same anti-virus package—if only to keep maintenance and update costs to a minimum. It is also essential to update the software itself on a regular basis. Virus authors often make getting past the anti-virus packages their first priority.

Security Policies:

When setting up a network, whether it is a local area network (LAN), virtual LAN (VLAN), or wide area network (WAN), it is important to initially set the fundamental security policies. Security policies are rules that are electronically programmed and stored within security equipment to control such areas as access privileges.

The policies that are implemented should control who has access to which areas of the network and how unauthorized users are going to be prevented from entering restricted areas.

The individual or group of people who police and maintain the network and its security must have access to every area of the network.

Once your policies are set, identity methods and technologies must be employed to help positively authenticate and verify users and their access privileges.

Making sure that certain areas of the network are "password protected"—only accessible by those with particular passwords—is the simplest and most common way to ensure that only those who have permission can enter a particular part of the network.

The golden rules, or policies, for passwords are:

- Change passwords regularly
- Make passwords as meaningless as possible
- Never divulge passwords to anyone until leaving the Company.

Digital certificates or public key certificates are the electronic equivalents of driver's licenses or passports, and are issued by designated Certificate Authorities (CAs). Digital certificates are most often used for identification when establishing secure tunnels through the Internet, such as in virtual private networking (VPN).

Figure: 3 Card & Password Access

***Firewalls**:*

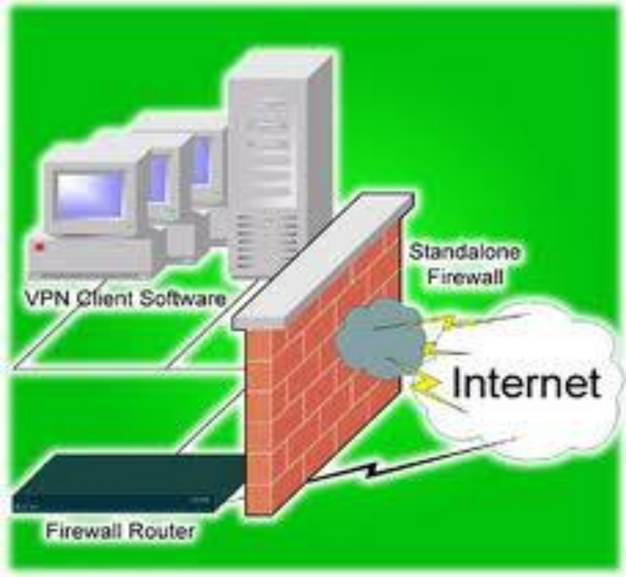

Figure: 4 Firewall

A firewall is a hardware or software solution implemented within the network infrastructure to enforce an organization's security policies by restricting access to specific network resources. In the physical security analogy, a firewall is the equivalent to a door lock on a perimeter door or on a door to a room inside of the building—it permits only authorized users, such as those with a key or access card, to enter. Firewall technology is even available in versions suitable for home use. The firewall creates a protective layer between the network and the outside world. In effect, the firewall replicates the network at the point of entry so that it can receive and transmit authorized data without significant delay. However, it has built-in filters that can disallow unauthorized or potentially dangerous material from entering the real system. It also logs an attempted intrusion and reports it to the network administrators.

Encryption: Encryption technology ensures that messages cannot be intercepted or read by anyone other than the authorized recipient. Encryption is usually deployed to protect data that is transported over a public network and uses advanced mathematical algorithms to "scramble" messages and their attachments.

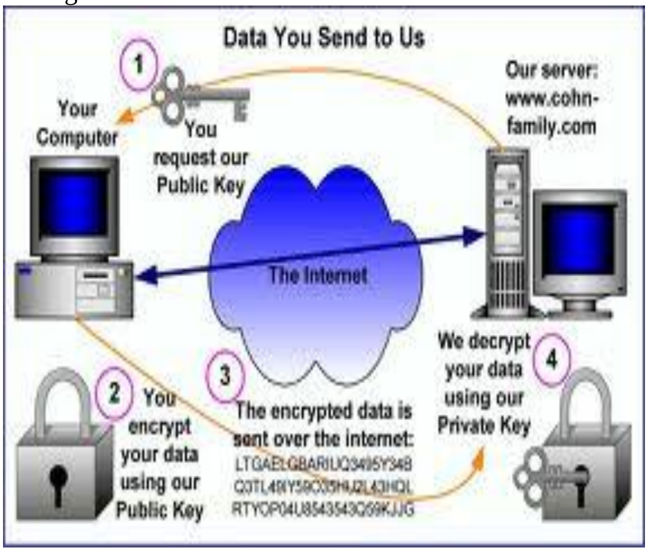
Data You Send to Us
1
You request our Public Key
Your Computer
Our server: www.cohn-family.com
The Internet
2
You encrypt your data using our Public Key
3
The encrypted data is sent over the internet:
LTGAELGBARIUQ3495Y34B
C0TL49IY59C05HUZL43HOL
RTYOP04U8543543Q59KJJG
4
We decrypt your data using our Private Key

Figure:5 Encryption

Intrusion Detection:

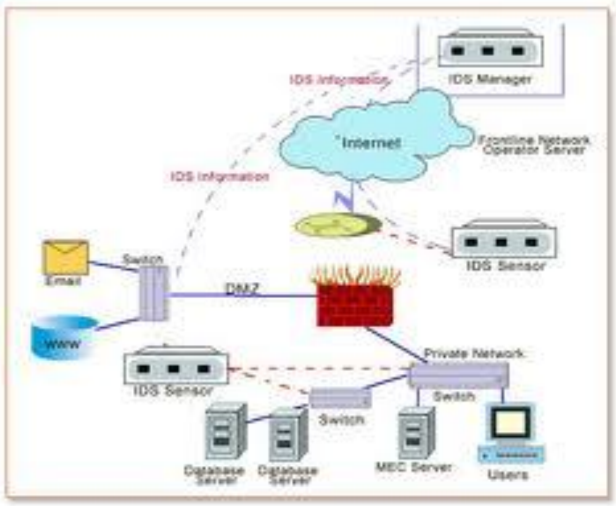

Figure: 6 Intrusion Detection

A network-based intrusion detection system (IDS) provides around-the-clock network surveillance. An IDS analyzes packet data streams within a network, searching for unauthorized activity, such as attacks by hackers, and enabling users to respond to security breaches before systems are compromised. When unauthorized activity is detected, the IDS can send alarms to a management console with details of the activity and can often order other systems, such as routers, to cut off the unauthorized sessions. In the physical analogy, an IDS is equivalent to a video camera and motion sensor; detecting unauthorized or suspicious activity and working with automated response systems, such as watch guards, to stop the activity.

CONCLUSION

As time goes on, more and more new technology will be developed to further improve the efficiency of business and communications. At the same time, breakthroughs in technology will provide even greater network security, therefore, greater piece of mind to operate in cutting edge business environments. Provided that enterprises stay on top of this emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks.

REFERENCES

[1] http://en.wikipedia.org/wiki/Network_security
[2] http://www.interhack.net/pubs/network-security/
[3] http://e-articles.info/e/s/s/Network-security/
[4] ijns.femto.com.tw/contents/ijns-v10-n1/ijns-v10-n1.html
[5] pnbiit.com/download/JulSep09.pdf