SECURITY MECHANISMS TO PROVIDE SECURITY AGAINST ATTACKS

SHYAMALA NAGAJYOTHI
Assistant Professor,
Department of CSE,
SCIENT INSTITUTE OF TECHNOLOGY,
Hyderabad, Telangana,[INDIA].

M.NAVEEN
Assistant Professor,
Department of CSE,
SCIENT INSTITUTE OF TECHNOLOGY,
Hyderabad, Telangana,[INDIA].

Abstract:

With the enormous development of computer technology, computer network continues to expand the scope of application with more and more users. Network security gradually attracts people's attention. Security is a fundamental component in the computing and networking technology. The first and foremost thing of every network designing, planning, building, and operating a network is the importance of a Network security has become more important to personal computer users, organizations, and the military. With the advent of the internet, security became a major concern. The internet structure itself allowed for many security threats to occur. Network security is becoming of great importance because of intellectual property that can be easily acquired through the internet. There are different kinds of attack that can be when sent across the network. By knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. There is a large amount of personal, commercial, military, and government information on networking infrastructures worldwide and all of these required different security mechanisms and strong security policies. This paper briefly introduces the concept of computer security, focuses on the threats of computer network security and discusses basic techniques. It proposes effective measures to improve the computer network security. We are trying to study most different kinds of attacks along with various different kinds of security mechanism that can be applied according to the need and architecture of the network.

Keywords : Network Security, attacks, hackers, Cloud-environment security, zero-trust model (ZTM), Trend Micro Internet Security.

I INTRODUCTION

Network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction or improper disclosure. Network Security management is different for all kinds of situations and is necessary as the growing use of internet. A home or small office may only require basic security while large businesses may require high maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming [1].New Threats Demand New Strategies as the network is the door to your organization for both legitimate users and would-be attackers. For years, IT professionals have

built barriers to prevent any unauthorized entry that could compromise the organization's network. And this network security is important for every network designing, planning, building, and operating that consist of strong security policies. The Network Security is constantly evolving, due to traffic growth, usage trends and the ever changing threat landscape [3]. For example, the widespread adoption of cloud computing, social networking and bring-your-own-device (BYOD) programs are introducing new challenges and threats to an already complex network. According to the UK Government, Information security is: "the practice of ensuring information is only read, heard, changed, broadcast and otherwise used by people who have the right to do so" (Source: UK Online for Business). Information systems need to be secure if they are to be reliable. Since many businesses are critically reliant on their information systems for key business processes (e.g. websites, production scheduling, transaction processing), security can be seen to be a very important area for management to get right. The vast topic of network security is analyzed by researching the following:

- History of security in networks
- Internet architecture and vulnerable security aspects of the Internet
- Types of internet attacks and security methods
- Security for networks with internet access
- Current development in network security hardware and software

When considering network security, it must be emphasized mainly that the whole network should be remain secure.Network security does not only concern the security in the computers at each end of the communication chain.When transmitting data the communication channel should not be vulnerable to attack, where the chances of threats are more penetrating. A possible hacker could target the communication channel, obtain the data, decrypt it and reinsert a false message. Hence, securing the network is just as important as securing the computers and encrypting the message which we want to be kept private.When developing a secure network, the following need to be considered [1]:

1. **Accessibility** – authorized users are provided the means to communicate to and from a particular network.
2. **Confidentiality** – Information in the network remains private, discloser should not be easily possible.
3. **Authentication** – Ensure the users of the network are, the user must be the person who they say they are.
4. **Integrity** – Ensure the message has not been modified in transit, the content must be same as they are sent.
5. **Non-repudiation** – Ensure the user does not refute that he used the network.

As an example, Figure 1 [2] shows a typical security implementation designed to protect and connect multiple parts of a corporate network. This is the most common design as according to the area of the network.

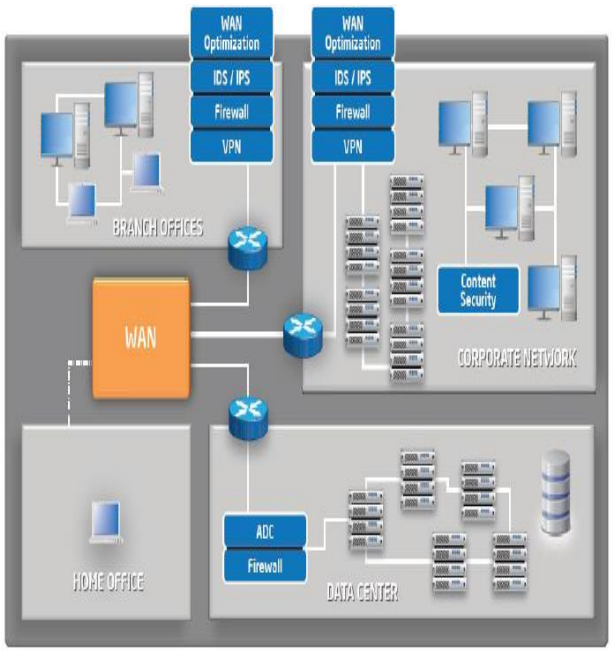

Fig 1: Security present in the different kinds of the Network.

With the progress of time, computer technology has been greatly developed and today's network communication system has spread to every corner of the world, involving political, economic, and military and all walks of social life. It plays an extremely important role. However, besides fun and convenience, computer also brings to us a lot of security risks due to its openness and connectivity. Users are now faced with a large number of security threats.Criminal cases are frequently visitors of domestic and international coverage. Reports on systematic security vulnerabilities are never rare. Table 1 shows the report on security vulnerabilities of information system by the U.S. security organization CERT / CC.

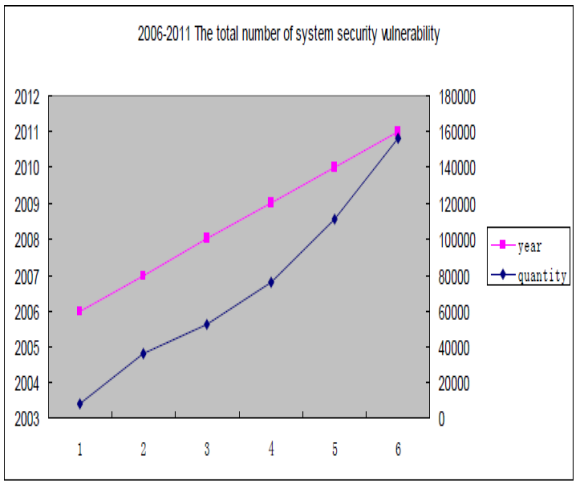

Table 1: Graph on system security vulnerability

II BASIC TECHNOLOGIES TO IMPROVE NETWORK SECURITY

2.1 Firewall technology

Firewall technology is an array of safety applications to exert mandatory access on external network by using predetermined safety facilities between network systems. Data transfer between two or more networks should follow certain safety measures to monitor the performance, determine whether the communication between the networks is allowed, and monitor the running of the network.

2.2 Data encryption technology

Data encryption technology categories can be divided in data storage, data transfer, data integrity, authentication and key management techniques. Data encryption is stored in the memory in order to prevent data loss and destruction. The transmission process in the information encrypted is commonly in the form of circuit encryption and port encryption. Data integrity identification technology is to protect information transfer, storage, access, identification and confidential treatment of

people and data. In this process, the system is characterized by the parameter value judgment on whether the input is in line with the set value. Data are subject to validation, and encryption enhanced the protection. Key management is a common encryption in many cases. Key management techniques include key generation, distribution, storage, and destruction, etc.

2.3 Intrusion detection technology

Intrusion detection technology is to ensure the safety of the design and the rational allocation. Intrusion detection technology can quickly find anomalies in the system and the authorized condition in the report. It can address and resolve system vulnerabilities in a timely manner. Technologies that are not in line with security policies are frequently used.

2.4 Anti-virus technology

Anti-virus technology not simply refers to anti-virus software technology. From the effects of its use, it can be classified into network anti-virus software and stand-alone anti-virus software. Online anti-virus software focuses on network connection against viruses. Once the virus has invaded the network or diffused to other network data, it will be promptly detected by online virus software, be killed and deleted.

III TYPES OF ATTACKS

Networks are subject to attacks from malicious sources. And with the advent and increasing use of internet attach is most commonly growing on increasing. The main categories of Attacks can be from two categories: "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation [6]. A system must be able to limit damage and recover rapidly when attacks occur. There are some more types of attack that are also essential to be considered:

3.1 Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. It includes traffic analysis, monitoring of unprotected communications, decrypting weakly encrypted traffic, and capturing authentication information such as passwords. Passive interception of network operations enables adversaries to see upcoming actions. Passive attacks result in the disclosure of information or data files to an attacker without the consent or knowledge of the user.

3.2 Active Attack

In an active attack, the attacker tries to bypass or break into secured systems in the going on communication. This can be done through stealth, viruses, worms, or Trojan horses. Active attacks include attempts to circumvent or break protection features, to introduce malicious code, and to steal or modify information. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. These attacks are mounted against a network backbone, exploit information in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks

result in the disclosure or dissemination of data files, DoS, or modification of data.

3.3 Distributed Attack

A distributed attack requires that the adversary introduce code, such as a Trojan horse or back-door program, to a ―trusted component or software that will later be distributed to many other companies and users. Distribution attacks focus on the malicious modification of hardware or software at the factory or during distribution. These attacks introduce malicious code such as a back door to a product to gain unauthorized access to information or to a system function at a later date.

3.4 Insider Attack

According to a Cyber Security Watch survey insiders were found to be the cause in 21 percent of security breaches, and a further 21 percent may have been due to the actions of insiders. More than half of respondents to another recent survey said it's more difficult today to detect and prevent insider attacks than it was in 2011, and 53 percent were increasing their security budgets in response to insider threats [7]. While a significant number of breaches are caused by malicious or disgruntled employees - or former employees - many are caused by well meaning employees who are simply trying to do their job. BYOD programs and file sharing and collaboration services like Dropbox mean that it will be harder than ever to keep corporate data under corporate control in the face of these well-meaning but irresponsible employees.

3.5 Close-in Attack

A close-in attack involves someone attempting to get physically close to network components, data, and systems in order to learn more about a network. Close-in attacks consist of regular individuals attaining close physical proximity to networks, systems, or facilities for the purpose of modifying, gathering, or denying access to information. One popular form of close in attack is social engineering. In a social engineering attack, the attacker compromises

the network or system through social interaction with a person, through an e-mail message or phone. Various tricks can be used by the individual to revealing information about the security of company. The information that the victim reveals to the hacker would most likely be used in a subsequent attack to gain unauthorized access to a system or network.

3.6 Spyware attack

A serious computer security threat, spyware is any program that monitors your online activities or installs programs without your consent for profit or to capture personal information. And this capture information is maliciously used as the legitimate user for that particular kind of work.

3.7 Phishing Attack

In phishing attack the hacker creates a fake web site that looks exactly like a popular site such as the SBI bank or PayPal. The phishing part of the attack is that the hacker then sends an e-mail message trying to trick the user into clicking a link that leads to the fake site. When the user attempts to log on with their account information, the hacker records the username and password and then tries that information on the real site.

3.8 Hijack attack

In a hijack attack, a hacker takes over a session between you and another individual

and disconnects the other individual from the communication. You still believe that you are talking to the original party and may send private information to the hacker by accidently.

3.9 Spoof attack

In the spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules.

3.10 Password attack

An attacker tries to crack the passwords stored in a network account database or a password-protected file. There are three major types of password attacks: a dictionary attack, a brute-force attack, and a hybrid attack. A dictionary attack uses a word list file, which is a list of potential passwords [9]. A brute-force attack is when the attacker tries every possible combination of characters

3.11 Buffer overflow

A buffer overflow attack is when the attacker sends more data to an application than is expected. A buffer overflow attack usually results in the attacker gaining administrative access to the system in a command prompt or shell.

3.12 Exploit attack

In this type of attack, the attacker knows of a security problem within an operating system or a piece of software and leverages that knowledge by exploiting the vulnerability.

IV TYPES OF NETWORK SECURITY

There are many components to a network security system that work together to improve your security posture. The most common network security components are discussed below.

4.1 Access Control

To keep out potential attackers, you should be able to block unauthorized users and devices from accessing your network. Users that are permitted network access should only be able to work with the set of resources for which they've been authorized.

4.2 Application Security

Application security includes the hardware, software, and processes that can be used to track and lock down application vulnerabilities that attackers can use to infiltrate your network.

4.3 Firewalls

A firewall is a device or service that acts as a gatekeeper, deciding what enters and exits the network. They use a set of defined rules to allow or block traffic. A firewall can be hardware, software, or both.

4.4 Virtual Private Networks (VPN)

A virtual private network encrypts the connection from an endpoint to a network, often over the Internet. This way it authenticates the communication between a device and a secure network, creating a secure, encrypted "tunnel" across the open internet.

4.5 Behavioral Analytics

You should know what normal network behavior looks like so that you can spot anomalies or network breaches as they happen. Behavioral analytics tools automatically identify activities that deviate from the norm.

4.6 Wireless Security

Wireless networks are not as secure as wired ones. Cybercriminals are increasingly

targeting mobile devices and apps. So, you need to control which devices can access your network.

4.7 Intrusion Prevention System

These systems scan network traffic to identify and block attacks, often by correlating network activity signatures with databases of known attack techniques. So, these are some ways of implementing network security. Apart from these, you'll need a variety of software and hardware tools in your toolkit to ensure network security, those are:

- Firewalls
- Packet crafters
- Web scanners
- Packet sniffers
- Intrusion detection system
- Penetration testing software

Network security is essential for overall cyber security because network is a significant line of defense against external attack. Given that, virtually all data and applications are connected to the network, robust network security protects against data breaches.

V SAFETY MEASURES TO IMPROVE SECURITY

5.1 Online anti-virus measures.

According to the characteristics of computer network virus, effective prevention on the virus is difficult and complex. It is a daunting task for network managers to monitor the prevention work. Previous work is only limited to every client computer, in which every user needs to install anti-virus software and on your machine, such as KV300 system, or Rising anti-virus software, etc. However, due to limited computer skill of users, this approach is hard to ensure the safety of the whole network system. As an effective solution to prevent the, the basic requirement is to meet the following demands:

1) Install anti-virus software on computers
2) Update the virus database in users' machines
3) Released the latest virus database upgrade file from the WAN connection
4) Coordination and management of remote users' virus scanning
5) Address user-reported problems timely
6) Download and preview scan report provided by users
7) Remote control user options

Improve the execution speed and zooming ability in large-scale networks. People are more capable of preventing online viruses. More anti-virus measures have emerged in order to effectively guarantee the network security. Network management personnel can install a complete set of virus software on any client server through one source server. As there are many types of software, network managers should take into account their own situation to achieve the "best use." When choosing solutions, managers should address current situation and leave room for further developments.

5.2 Measure to prevent hackers.

The invasion and attack can be divided into subjective and objective security issues. Subjectivity security issue mainly refers to errors made by network management personnel. Objectivity security issue mainly refers to loopholes in computers and the network where hackers exploit these

vulnerabilities to conduct various forms of attack.

5.2.1 Use safety tool

The above-mentioned basic techniques of computer network security can collect safety issues of host computers. Network management personnel identify these problems in a timely manner and install the patch. Network managers take the advantage of scanning tools (such as NAL's Cyber Cop Scanner) to scan host computers, learn about the weakness links take appropriate preventive and repair measures.

5.2.2 Firewall technology

This paper has described the firewall technology. In short, firewall technology is to prevent others from accessing your network device like a shield. There are three types of firewall technology, namely, packet filtering technology, agent technology, and status monitoring technology. Packet filtering technology is to verify the IP address by setting it. Those IP addresses that do not match those settings will be filtered by the firewall. But this is the first layer of protection. Agent technology is to verify the legitimacy of requests sent by accept client of proxy server to. This technology also involves with user authentication, login, simplified filtering criteria and shielding the internal IP addresses. Status monitoring technology is the third generation of network security technologies, which is effective for all levels of network monitoring. It makes it possible to make timely security decisions. Firewall technology can successfully prevent hacker from intrusion in the local network and protect the network.

5.2.3 Measures about switch

When designing a large-scale regional computer network, we need to ensure that the switch is connected to a network or in a separate network, so that the switch can form a separate management network. This will effectively reduce the number of network switches and narrow the scope of failure. By using search and location, it is also convenient for network managers to quickly handle remote network accidents.

VI SECURITY MECHANISMS

Encryption is an interesting piece of technology that works by scrambling data so it is unreadable by unintended parties

6.1 Triple DES

Triple DES was designed to replace the original Data Encryption Standard (DES) algorithm, which hackers eventually learned to defeat with relative ease. At one time, Triple DES was the recommended standard and the most widely used symmetric algorithm in the industry.Triple DES uses three individual keys with 56 bits each. The total key length adds up to 168 bits, but experts would argue that 112-bits in key strength is more like it.Despite slowly being phased out, Triple DES still manages to make a dependable hardware encryption solution for financial services and other industries.

6.2 RSA

RSA is a public-key encryption algorithm and the standard for encrypting data sent over the internet. It also happens to be one of the methods used in our PGP and GPG programs.Unlike Triple DES, RSA is considered an asymmetric algorithm due to its use of a pair of keys. You've got your public key, which is what we use to encrypt

our message, and a private key to decrypt it. The result of RSA encryption is a huge batch of mumbo jumbo that takes attackers quite a bit of time and processing power to break.

6.3 Blowfish

Blowfish is yet another algorithm designed to replace DES. This symmetric cipher splits messages into blocks of 64 bits and encrypts them individually.Blowfish is known for both its tremendous speed and overall effectiveness as many claim that it has never been defeated. Meanwhile, vendors have taken full advantage of its free availability in the public domain.Blowfish can be found in software categories ranging from e-commerce platforms for securing payments to password management tools, where it used to protect passwords. It's definitely one of the more flexible encryption methods available.

6.4 Twofish

Computer security expert Bruce Schneier is the mastermind behind Blowfish and its successor Twofish. Keys used in this algorithm may be up to 256 bits in length and as a symmetric technique, only one key is needed.Twofish is regarded as one of the fastest of its kind, and ideal for use in both hardware and software environments. Like Blowfish, Twofish is freely available to anyone who wants to use it. As a result, you'll find it bundled in encryption programs such as PhotoEncrypt, GPG, and the popular open source software TrueCrypt.

6.5. AES

The Advanced Encryption Standard (AES) is the algorithm trusted as the standard by the U.S. Government and numerous organizations.Although it is extremely efficient in 128-bit form, AES also uses keys of 192 and 256 bits for heavy duty encryption purposes.AES is largely considered impervious to all attacks, with the exception of brute force, which attempts to decipher messages using all possible combinations in the 128, 192, or 256-bit cipher. Still, security experts believe that AES will eventually be hailed the de facto standard for encrypting data in the private sector.

VII THE FUTURE OF ENCRYPTION

Cyber attacks are constantly evolving, so security specialists must stay busy in the lab concocting new schemes to keep them at bay. Expert observers are hopeful that a new method called Honey Encryption will deter hackers by serving up fake data for every incorrect guess of the key code. This unique approach not only slows attackers down, but potentially buries the correct key in a haystack of false hopes. Then there are emerging methods like quantum key distribution, which shares keys embedded in photons over fiber optic, that might have viability now and many years into the future as well.

VIII CONCLUSION

Security is a very difficult and vital important topic. Everyone has a different idea regarding security policies, and what levels of risk are acceptable. The key for building a secure network is to define what security means to your need of the time and use. Once that has been defined, everything that goes on with the network can be evaluated with respect to that policy. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him

but Users who find security policies and systems too restrictive will find ways around them. There are different kinds of attacks on the security policies and also growing with the advancement and the growing use of internet. In this paper we are trying to study these different kinds of attacks that penetrates our system and security mechanisms against attacks. As the threats are increasing, so for secure use of our systems and internet there are various different security policies are also developing. In this paper we have mention some of the security policies that can be used mostly by number of users and some new advance qualities that fits to the today's more penetrating environments like Trend micro security mechanism, use of big data qualities in providing security, etc. Security is everybody's business, and only with everyone's cooperation, an intelligent policy, and consistent practices, will it be achievable.

IX REFERENCES

[1]Network Security [Online] available: http://en.wikipedia.org/wiki/Network_security.

[2]Network Security: History, Importance, and Future, University of Florida Department of Electrical and Computer Engineering, Bhavya Daya.

[3] Ateeq Ahmad, ―Type of Security Threats and its Prevention", Ateeq Ahmad, Int.J.Computer Technology & Applications, Vol 3 (2), 750-752.

[4] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257

[5] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ―A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.

[6] Network Security Types of attacks [Online]available:http://computernetworkingnotes.com/network-security-access-listsstandards-and-extended/types-of-attack.html.

[7] Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008.

[8]AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.

[9] Li Wenlong. Face to face with a hacker. internet world.1999(2):2~8

[10]Xiao Ze. Research on computer network security analysis model [J]. Journal On Communications, 2012(3):269.

[11]Zhang Cheng. Research on computer network security analysis model [J]. Practical Electronics, 20l3(v)=148-149.

[12]Hong Yaling. Research on computer network security analysis model [J]. Computer CD Software and Applications, 2013(z):1-152.

[13] Wang Yuan. Quantitative Evaluation Method of Network Security Situation [D]. Ph.D. Dissertation, university of science and technology, 2003.

[14]Cui Jing, Liu Guangzhong, the basics of computer network [J]. Tsinghua University Press, 2010.07.01.