International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 10 | Oct -2016 www.irjet.net p-ISSN: 2395-0072

COMPUTER NETWORKS AND SECURITY : A REVIEW

V.Mamatha Reddy[1], P.Poornima[2]

[1]*Assistant Professor, Department of Computer Science and Engineering, KITS(S), Huzurabad, Telangana, India*
[2] *Assistant Professor, Department of Computer Science and Engineering, KITS(S), Huzurabad, Telangana, India*

Abstract - *Network security refers to any activities designed to protect the network, which includes the authorization of information access in a network, which is controlled by the network administrator. Network security has turned out to be more important to personal computer users, Organizations, and military and it covers an assortment of computer networks, both public and private, that are utilized as a part of everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Network security is the procedure by which digital information resources are protected, the objective of security are to ensure confidentiality, maintain integrity, and assure availability, so viable network security focuses on a variety of threats and prevents them from entering or spreading on the network. Social network sites created a new way of communication, it brought about new information security issues such as identity theft, privacy leak and junk information. In This paper we mainly concentrate on the network security also we present some major issues that can influence the network along with existing problems of the online security of the computer, and precautionary measures.*

Key words: **Network Security, Threats, Privacy Protection, Preventive Measures, Cryptography.**

1. INTRODUCTION

Network Security comprises of the provisions and approaches adopted by a network administrator to avert and monitor unauthorized access, misuse, modification, or denial of a computer network and network accessible resources [1]. To secure the information and the entire network system, one specific methodology is required which can be capable of providing the complete security solutions-Cryptography is an emerging technology, which is essential for network security. It is the study of Secret(crypto-) Writing(-graphy) and is a strategy for storing and transmitting information in a particular form so that only those for whom it is deliberate can read and process it. Cryptography is an key technique for present computer and communications networks, protecting everything from business e-mail to bank transactions and online shopping, which avoid eavesdroppers from learning the contents of encrypted messages.

1.1 Network Security Attributes:

When developing a secure network, the following need to be considered [2].

1) Access: authorized users are provided the means to communicate to and from a particular network.

2) Confidentiality: Information in the network remains private.

3) Authentication: Ensure the users of the network are who they say they are.

4) Integrity: Ensure the message has not been modified in transit

5) Non-repudiation: Ensure the user does not refute that he used the network

2. NETWORK SECURITY PROBLEMS

Due to the lack of security control mechanisms and the lack of network security policies and protection, awareness of these risks is increasing (Fig-I).

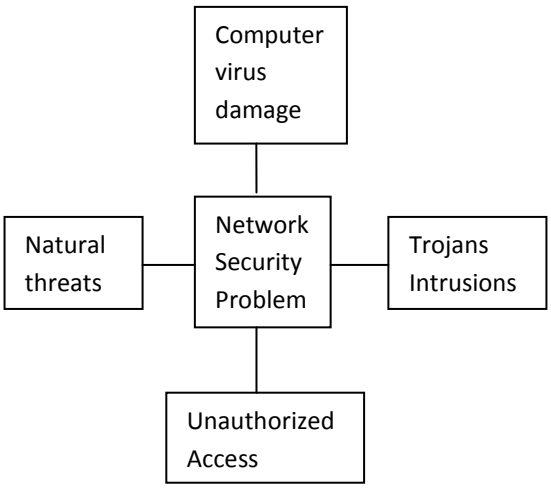

Fig-I Computer Network Security Problems

Natural threats may originate from different natural disasters, poor site environment, electromagnetic radiation and obstruction, network equipment and other natural aging. They will impact the storage and exchange. Trojan

horse is a hacking tool based on remote control, covert and unauthorized characteristics.

In general, there are two Trojans programs, one is a server program and the other is the controller program. A Trojan server program is required if the controller program is installed in a computer [3]. Unauthorized access is the use of a computer or network without authorization. A cracker, or hacker, is someone who tries to access a computer or network illegally. A computer virus attaches itself to another program or replaces it by overwriting it so that it can replicate itself without you knowing it. It can rapidly go through all the available memory on your computer and seriously slow down the system, and even stop it completely. Viruses can damage data files.

2.1 Common Internet Attack Methods

Common internet attacks methods are broken down into categories (Table-1).Some attacks gain system knowledge or personal information, such as eavesdropping and phishing. Attacks can also interfere with the system's intended function, suchas viruses , worms and trojans. The other form of attack is when the sys tem's resources are consumes uselessly, these can be caused by denial of service (DoS) attack.

Table-1: Attack methods and Security Technology [4]

Security Attributes	Attack Methods	Technology for Security
Confidentiality	Eavesdropping, phishing, Denial of Service	IDS, Firewall, Cryptographic systems, SSL
Integrity	Viruses, worms, Trojans, Eavesdropping, Dos	IDS, Firewall, Anti malware software, SSL
Privacy	Email bombing, spamming, hacking, Dos and cookies	IDS, Firewall, Anti malware software, SSL
Availability	Dos, Email bombing, spamming, and systems Boot record infectors	IDS, Firewall, Anti malware software

2.1.1. Eavesdropping: Interception of communications by an unauthorized party is called eavesdropping. Passive eavesdropping is when the person only secretly listens to the networked messages. Active eavesdropping is when the intruder listens and inserts something into the communication stream [4].

2.1.2. Viruses: viruses are self replication programs that use files to infect and propagate [4]. Once a file is opened, the virus will activate within the system.

2.1.3. Worms: A worm is similar to a virus because they both are self-replicating, but the worm does not require a file to allow it to propagate [4].

2.1.4. Trojans: Trojan is any malicious computer program which is used to hack into a computer by misleading users of its true intent [4].

2.1.5. Phishing: Phishing is an attempt to obtain confidential information from an individual, group, or organization [5]. Phishers trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information.

2.1.6. IP Spoofing Attacks: IP spoofing is the creation of Internet Protocol (IP) packets with a false source IP address, for the purpose of hiding the identity of the sender or impersonating another computing system [4].

2.1.7. Denial of Service: A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service.

2.2 Social Networking Sites and Privacy Issues

Social media is conceivably the most crucial area of the internet, in any case, being open and social creates legitimate concerns about protection and security. Social networking sites offer security measures and empower sharing of individual data.
Some of the major problems faced by the users are as follows:

2.2.1. Identity theft: Some users are forced to delete their profiles on account of identity theft due to the embarrassment they face thereafter. Sometimes, fake profiles are being made and the actual user does not even know that a fake user is updating and posing things that are disgraceful. Cases of identity theft and hacking of the profile and all shared personal is quite commonly faced by the young users [6].
2.2.2. Hacking: Hacking is an attempt to exploit a computer system or a private network inside a computer. Simply put, it is the unauthorized access to or control over computer network security systems for some illicit purpose.
2.2.3. Clicking on enticing Ads: viruses and malware often find their way onto the computer through those annoying, but sometimes enticing ads.
2.2.4. Failing to utilize security settings: social media sites provide with the ability to restrict who has access to the information. One practice to increase the account's security is to disable most of the options.
2.2.5.Clickjacking: Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious

technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages

3. SECURITY TIPS

3.1 Solutions to Computer Network Security Problems

This section talks about solutions to computer network security problems when we have an existing network. It also applies to people who are considering building small networks [7].

First of all, we need to develop a plan to assess the vulnerabilities of the network. A vulnerability assessment plan should cover the key areas that, if affected, can bring down the network or create huge data loss. These items include

1. Server protection (the main computer in case of peer to peer networks),

2. Firewalls and antivirus on the server,

3. The method your server employs to communicate with other computers, and

4. How other peripherals on the network (computers, printers, etc) can pose a danger to the network.

3.2 Technology for Internet Security

Internet threats will continue to be a major issue in the global world as long as information is accessible and transferred across the internet. Different defense and detection mechanisms were developed to deal with these attacks.

3.2.1. Cryptographic Systems: cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

3.2.2. Firewall: A firewall is the front line defense mechanism against the intruders. It is a system designed to prevent unauthorized access to or from a private network [4].

3.2.3. Intrusion Detection System: IDS systems can be software and hardware devices used to detect an attack. IDS products are used to monitor connection in determining whether attacks are been launched. Some IDS systems just monitor and alert of an attack, whereas others try to block the attack.

3.2.4. Anti-Malware Software and Scanners: These are used to detect and removes malware like worms, Trojans, viruses.

3.2.5. Secure Socket Layer (SSL): SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

4. CRYPTOGRAPHIC SYSTEM

A cryptographic system (or a cipher system) is a method of hiding data so that only certain people can view it. Cryptography is the practice of creating and using cryptographic systems. Cryptanalysis is the science of analyzing and reverse engineering cryptographic systems. The original data is called plaintext. The protected data is called ciphertext. Encryption is a procedure to convert plaintext into ciphertext. Decryption is a procedure to convert ciphertext into plaintext. A cryptographic system typically consists of algorithms, keys, and key management facilities [8].

There are two basic types of cryptographic systems: symmetric ("private key") and asymmetric ("public key").

Symmetric key systems require both the sender and the recipient to have the same key. This key is used by the sender to encrypt the data, and again by the recipient to decrypt the data. Key exchange is clearly a problem.

Asymmetric cryptographic systems are considered much more flexible. Each user has both a public key and a private key. Messages are encrypted with one key and can be decrypted only by the other key. The public key can be published widely while the private key is kept secret.

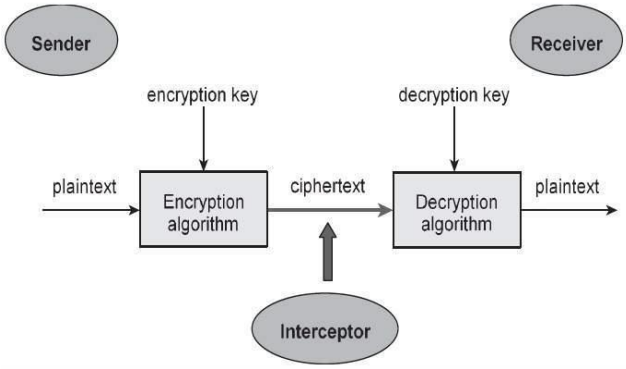

Fig-II Cryptography

There are various cryptographic algorithms in use. The following are amongst the most well-known [9]:

1) DES: This is the 'Data Encryption Standard'. This is a cipher that operates on 64-bit blocks of data, using a 56-bit key. It is a 'private key' system.
2) RSA: RSA is a public-key system designed by Rivest, Shamir, and Adleman.
3) HASH: A 'hash algorithm' is used for computing a condensed representation of a fixed length message/file. This is sometimes known as a 'message digest', or a 'fingerprint'.
4) MD5: MD5 is a 128 bit message digest function. It was developed by Ron Rivest.
5) AES: This is the Advanced Encryption Standard (using the Rijndael block cipher) approved by NIST.
6) SHA-1: SHA-1 is a hashing algorithm similar in structure to MD5, but producing a digest of 160 bits (20 bytes).Because of the large digest size, it is less likely that two different messages will have the same SHA-1 message digest. For this reason SHA-1 is recommended in preference to MD5.
7) HMAC: HMAC is a hashing method that uses a key in conjunction with an algorithm such as MD5 or SHA-1. Thus one can refer to HMAC-MD5 and HMAC-SHA1.

5. CURRENT DEVELOPMENT IN NETWORK SECURITY

The network security field is continuing down the same route. The same methodologies are being used with the addition of biometric identification. Biometrics provides a better method of authentication than passwords. This might greatly reduce the unauthorized access of secure systems. New technology such as the smart card is surfacing in research on network security. The software aspect of network security is very dynamic. Constantly new firewalls and encryption schemes are being implemented.

6. CONCLUSION

Network security is an important field that is progressively gaining attention as the internet expands. There are various ways, which ensure for the safety and security of the network. We have focused on security issues related to network security and social network sites, it also gives an essential thought to solve the security problems of the social network sites. Finally, the paper presents the two sorts of cryptographic systems and different algorithms to provide cryptography.

REFERENCES

[1]. Simmonds, A; Sandilands, P; van Ekert, L(2004)."Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317-323.

[2]. Dowd, P.W.; McHenry, J.T., "Network security: it's time to take it seriously," Computer, vol.31, no.9, pp.24-28, Sep 1998.

[3]. Z. Trabelsi, and K. Shuaib, "A Novel Man-in-the-Middle Intrusion Detection Scheme for Switched LANs," International Journal of Computers & Applications, vol. 30, no. 3, pp. 234-243, 2008.

[4]. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.

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

[6]. Privacy concerns with social networking services. (2014, March 27). Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Privacy_concerns_with_social_networking_services

[7]. www.brighthub.com/computing/smb-security/articles/115146.aspx

[8]. http://www.cgisecurity.com/owasp/html/ch13.html

[9]. http://www.cryptographyworld.com/algo.htm

BIOGRAPHIES

V.Mamatha Reddy
Assistant Professor of Computer Science and Engineering Dept, Kamala Institute of Technology & Science, Huzurabad. Area of interest- Computer Networks, Network Security and Cloud Computing.

P.Poornima
Assistant Professor of Computer Science and Engineering Dept, Kamala Institute of Technology & Science, Huzurabad. Area of interest- Network Security and Internet Of Things