ISSN No. 0976-5697

Volume 7, No. 6(Special Issue), November 2016

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Different Security Threats and its Prevention in Computer Network

Mukesh Kumar
Assistant Professor
Dept.of Computer Science, Baba Farid College, Bathinda, Punjab
mukesh.pup@gmail.com

Navpreet Kaur
Assistant Professor
Dept. of Computer Science, Baba Farid College, Bathinda, Punjab

Sukhjinder Kaur
Assistant Professor
Dept. of Computer Science, Baba Farid College, Bathinda, Punjab

Rajpal Singh
Assistant Professor
Dept. of Computer Science, Punjabi University TPD Malwa College, Rampura Phula, Punjab

Abstract-Nowadays the computer network technology is growing rapidly. The computer network is used for transferring large volume of data and information these days including sensitive information like credit card details, passwords, online banking, account numbers and other confidential data so there are chances of leakage of that information while transferring over the network especially on the internet. Hackers are the programmers who are expert in breaching security are constantly looking for loopholes in network security and whenever they find any loophole they try to access or change the sensitive information that is being transferred over the network. It is very important to secure computer network by using firewalls, anti-viruses and other tools while transferring data through the computer network. The purpose of this paper is to understand about the various attacks that the intruder can do and other harmful programs like viruses, worms, Trojan horses etc that can breach the security of the network and affect the data and performance of our system and also understand about the various solutions to these attacks and harmful programs. In this paper we will discuss about the various threats like active and passive attacks, other malicious software that can affect the security of the computer network and their possible solutions.

Keywords—attacks, data, information, network, security, threats

I. INTRODUCTION

Information Technology has changed the way of communication. Earlier the communication was not effective and it takes lots of time for transferring data from one place to another place but with the emergence of information technology the way of communication has totally changed and it become now possible for transferring information from one location to another location in the world in no time. Also communication methods have improved drastically. We can transfer audio, video, text, images and almost any type of information through computer network. Computer Network is an interconnection of large amount of communication devices including computers and other devices that are capable of processing data and can transmit data from one device to another device through communication medium. Communication medium can be wired or wireless. Computer Network is being used for transferring large amount of data and information these days. As sensitive information like passwords, credit cards details, confidential data are also transferred over the network so there is a great possibility of hacking that data and information by some intruder or third party. There are lots of security threats to the computer network like different types of attacks and other malicious programs that can affect the information transferred through computer network. It is very important to aware about the various possible solutions and prevention methods from these threats while transferring data and information over the public networks.

II. VARIOUS ATTACKS IN COMPUTER NETWORK

An attack in computer network security is an attempt to breach the security of the computer system and to monitor, alter or delete data files or to gain unauthorized access to the system. Following are the major attack that an intruder can do while transferring data over the public network.

A. Passive Attack

A passive attack is a type of network attack in which the intruder monitors the information that is being transferred but does not alter the information. The main motive of passive attack is to obtain data and information that is being transferred. Major passive attacks like Traffic analysis and Eavesdropping are given as follow.

Traffic Analysis: In this attack an intruder analyze the traffic and monitor the packet transfer information to know about the source or destination or the pairing between the source and the destination.

Eavesdropping: In Eavesdropping attack an intruder try to monitor confidential information like passwords, private or secret key that is being transmitted over the network.

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

B. Active Attack

An Active attack is a type of network attack in which the intruder can access, modify, delete or can send false messages. Active attacks include attacks like masquerade attack, message modification attack, session replay attack, denial of service attack and distributed denial of service attack.

Masquerade attack: A masquerade attack is an attack in which an unauthorized user pretends to be an authorized user and by using fake identity the unauthorized user try to gain access to the system. A masquerade can be attempted through the stolen login ID and passwords or through bypassing the security mechanism.

Message Modification: Modification of message simply means to change some portion of the message.

Session Replay attack: A Session Replay attack is an attack where an intruder replays the authentication process to fool the computer in the granting access. In this attack data transmission is either repeated or delayed.

Denial of Service attack (DoS): The Denial of Service attack prevents the normal use of communication facilities over the computer network to the intended receiver. This attack may direct all traffic toward the particular destination or may send an erroneous route message to the originator node to disrupt the service and making resource unavailable to intended user [1]. The Denial of Service can be performed in several ways including flooding the network, disrupting the information state by resetting TCP session information, disrupting the connection among two or more machines or preventing a service from individual user.

Distributed Denial of Service attack (DDoS): In Distributed Denial of Service (DDoS) attack online services are prevented by overwhelming with traffic from multiple computers. In DDoS multiple sources targeted to a single system causing Denial of Service (DoS) attack.

C. Other Common Security Attacks

Phishing attack: In this type of attack an intruder creates a fake website that looks like a website that is very popular and has heavy traffic on that website such as SBI bank website. In this attack the hacker sends an email containing the link of the fake website and playing the trick that the user will think that this is the real website and the user tries to logon to that website with their account number and password which is recorded by the hacker and then the hacker can apply this account number and password on the real website. [4]

Hijack attack: In Session Hijack attack an intruder or hacker takes over of the entire session between the sender and the receiver and disconnect the communication between sender and the receiver and the users are completely unaware about this attack and can send private messages to the hacker thinking that he is sending message to the original party. [4]

Spoofing attack: In spoofing attack an intruder pretends to be some other computer over the network in order to trick other devices to share sensitive data with that computer. There are several spoofing attacks that the attacker can use to attack on the network. Major spoofing attacks like IP spoofing, DNS spoofing or ARP spoofing that is discussed below. [6]

1. IP Spoofing

IP Spoofing is normally used to gain unauthorized access to other computer. In this method the attacker hide his identity and get the IP address of the legitimate user and change the header part of the IP packet and user is thinking that it is coming from the trusted source.

2. DNS spoofing

The DNS stands for Domain Name System is responsible for converting domain name into IP address. When the user enters the URL it will be converted to IP address by the DNS and then the request is sent to the server. In Spoofing attack hacker reroute the DNS translation to different server. [6]

3. ARP spoofing

Address Resolution Protocol is used to map IP address into MAC address. In ARP spoofing an attacker attaches its MAC address with IP address of other computer or organization. This type of attack results in intercept of the data by the attacker that is meant for other computer or organization.

Man in the Middle Attack: Man in the Middle attack also called MitMA or MitM or MiM attack is an attack where a hacker insert itself between the communication between the two parties and access the messages that is transferred between the two parties.

Ping of Death: Ping of Death is a kind of Denial of Service (DoS) attack in which hacker sends a request that is more than the maximum size of IP packet (65,536 bytes). When the request size is more than the allowed size of IP packet then it can not be transmitted. To transmit packet it is fragmented into pieces and reassembled at the receiver end and this advantage is took by the attacker and when these fragments are reassembled at the receiver end it results in buffer overflow and operating system does not know what to do.

Password Attack: In this type of attack an intruder tries to steal the password that is stored in the password protected file or in the database over the network [4]. Dictionary attack, brute-force attack and hybrid attack are the example of password attacks which are discussed below.

1.Dictionary attack

In Dictionary attack or guessing attack the hacker tries to guess the password of the user by using common names, names of their loved one, date of birth, addresses, username, pet name or common pattern like abcdef, 123456 setc.

2. Brute-force attack

In this attack the hacker uses the computer program which tries to logon to the system by possible password combination starting with those passwords that are easy to guess.

3. Hybrid attack

In hybrid attack an attacker start with the dictionary file and then assign symbols and numbers in the password in place of characters. This attack is more advance form of the dictionary attack.

III. OTHER MALICIOUS PROGRAMS

There are some system and program threats that breach the security of the system and affect the performance of the system including modifying, deleting or corrupting the files of the computer system. Following are some major malicious programs that affect the performance of the system.

Virus: VIRUS is abbreviated as Vital Information Resources under Seize. A virus is a computer program that attaches itself to some other program and replicates over the network to some other computers. The viruses are usually spread over the internet and users who are unaware of the viruses may download the files containing viruses. A virus can change, delete or corrupt the files in the computer system. During its lifetime a virus normally goes through a number of stages like dormant phase where the virus is usually in the idle state but may be activated at some later stages, propagation stage where a virus normally replicates itself, triggering phase where a virus is activated and execution stage where a virus is executed and performs its intended function like corrupting files, deleting files etc.

Worms: A Worm is a malicious program that can spread itself to other computers by using computer network. Worms usually consume large amount of resources by replicating itself and ultimately the resources are exhausted and services are denied to the users. A Worm usually replicate itself by mailing a copy of itself to large number of users or by using remote login facility through which it logon to the remote system and execute commands to replicate itself.

Trojan Horse: A Trojan horse also called Trojan is a program that contains harmful code and command procedures which when executed performs harmful and unwanted functions like theft or loss of data. It is actually a security breaching program which acts upon the principle of allowing unauthorized software into the computer system and allowing other authorized users to run it. A Trojan horse does not replicate itself. To spread Trojan horse a user must invite it onto their computer. To spread these programs they can be placed over the internet as a music file, game, movie or as an e-mail attachment so that user can easily download it. It can easily damage the security system by modifying, deleting or encrypting files.

Logic Bomb: A logic bomb is actually a code that is normally attached with the program that is designed to do some malicious act. Logic bomb is triggered automatically when some particular conditions met. The most common examples of conditions for the triggering of logic bomb are met of particular date or time, presence or absence of certain files etc.

Trapdoor: Trapdoor also called the backdoor is the code that are embedded within the software by the software developers to gain access to the software without following the normal security access procedures but this trapdoor become problem when some unauthorized user try to gain access to the system by bypassing the security mechanism.

Stack and Buffer Overflow: Stack is a location in the memory which is used to store function parameters, local variables etc. Buffer is a temporary location in the memory where data is stored temporarily while transferring between main memory and secondary storage. Through network connection stack and buffer overflow threat helps an intruder or third party to gain access to the system. It also bypasses the firewall security system which provides an opportunity to an intruder to enter into the system.

Key logger: Key logger is a program that tries to track the key stroke of all the users.

Spyware: It is a kind of program or an application that collects user personal information over the internet without any information to them.

Adware: It is a program that displays unwanted pop-up ads to the user which slowdowns the processing speed of your computer and may also track users' data without any information to them.

IV. SOLUTION OF SECURITY THREATS

There are various solutions to the security threats like anti-viruses, firewall and cryptography through which we can secure our data over the network. All of these solutions are discussed below.

Anti-Virus: An Anti-Virus is a program that helps our system to protect from malicious programs like viruses, worms, Trojans etc. It is recommended that an anti-virus should be installed on our systems while using internet or downloading some file from the internet.

Firewall: A firewall is a network security system that is constantly monitors all the traffic of the network that is incoming or outgoing to the network of an organization [9][10]. Firewall can be implemented as either in software or hardware or combination of both.

Cryptography: Cryptography is the way of encrypting the data at the source side and decrypting the data at the receiver side so that an intruder in between can not understand the message.

978-93-85670-72-5 © 2016 (RTCSIT)

CONFERENCE PAPER
International Conference on
Recent Trends in Computer Science & Information Technology (RTCSIT-2016)
21st August 2016
Guru Nanak College Budhlada, Punjab India

Cryptography ensures secure transactions over the internet such as funds transfer, online banking, filling online tax returns etc. Cryptography is broadly divided into two categories.

1. Symmetric Key Cryptography

In Symmetric key Cryptography same key is shared between sender and the receiver. In the source side shared key is used to encrypt the message and at the destination side same shared key is used to decrypt the message. Most common examples of symmetric key cryptography are DES, 3DES and AES.

2. Asymmetric Key/Public Key Cryptography

In Asymmetric key Cryptography different key is used for encryption and decryption process. This method of cryptography is also known as public key cryptography. In this method two keys are basically used named as public and private keys. The sender uses the public key of the receiver which is announced to the public to encrypt the message and the receiver uses its own private key to decrypt the message. The most common examples of the asymmetric key cryptography are Knapsack algorithm, RSA algorithm and Diffie-Hellman algorithm.

Other Security tools: There are other so many security tools available over the internet that helps the user to protect their system and data from malicious programs.

5.CONCLUSION

This paper presents an overview about the various attacks and security threats in the computer network that breach the security of the network. In this paper various attacks like passive attack, active attack, other security attacks and different types of malicious programs like Viruses, Worms, Trojan horses, Trapdoors etc are discussed that are harmful to the network and the system and can alter, delete or corrupt the files of the computer system and also discussed the ways how we can secure our system from these threats. Passive attacks like eavesdropping monitor the secret information during the transmission in the computer network like passwords; private keys etc but cannot alter the information. On the other hand in Active attack an intruder can alter, delete or can send false messages over the network. Some of the major active attacks are masquerade attack, message modification attack, session replay attack, Denial of Service (DoS) attack and Distributed Denial of Attack (DDoS). By using security mechanism like anti-viruses, firewalls, encryption and decryption of the messages and other security tools we can secure our data from these attacks while transferring over the network.

6.REFERENCES

[1] Garg,A.; Beniwal,V," A Review on Security Issues of Routing protocols in Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer Science and Software Engineering vol 2 Issue 9, September 2012, pp 145-148 ISSN:2277-128X

[2] Kumar,M.;Agrawal,N,;"Analysis of different Security Issues and Attacks in Distributed System: A Review " International Journal of Advanced Research in Computer Science and Software Engineering vol 3 Issue 4, April 2013 ISSN:2277-128X

[3] https://www.techopedia.com/definition/4020/masquerade-attack

[4] Mohammad, I.; Pandey, R.; Khatoon, A.; "A review of types of security attacks and malicious software in network security", International journal of Advanced research in computer science and software engineering, vol.4, iss.5, pp.413 – 415, May 2014.

[5] Kaur, J.; Nagpal, P.;" Review paper on Security Challenges and Attacks in Mobile Ad-hoc Networks" International Journal of Advanced Research in Computer Science and Software Engineering vol 4 Issue 5, May 2014 ISSN:2277-128X

[6] https://www.checkmarx.com/glossary/spoofing-attack/

[7] Lone,I,A.; Ataullah,M," A Survey on Various Solutions of ARP Attacks" International Journal of Advanced Research in Computer Science and Software Engineering vol 3 Issue 2, February 2013, pp 299-303 ISSN:2277-128X

[8] http://www.comptechdoc.org/independent/security/terms/replay-attack.html

[9] Boudriga, Noureddine (2010). Security of mobile communications. Boca Raton: CRC Press. pp. 32–33. ISBN 0849379423

[10] https://en.wikipedia.org/wiki/Firewall_(computing)

[11] Manimegalai,C; Sumithra,A.;" An Overview of Attacks in Network Security System" International Journal of Advanced Research in Computer Science and Software Engineering vol 5 Issue 10, October 2015 ISSN:2277-128X

[12] Stallings, W.;"Cryptography and Network security", Vth edition.

[13] http://insights.scorpionsoft.com/3-types-of-password-security-attacks-and-how-to-avoid-them

[14] Kahate, A.;"Cryptography and Network security", IIIrd edition.