ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

A Study of Consequences and Countermeasures of attacks in Computer Networks

Cheshta Rani, Shivani Goel

Student, Department of Computer Science and Engineering, Thapar University, Patiala, India

Assistant Professor, Department of Computer Science and Engineering, Thapar University, Patiala, India

ABSTRACT: Many different types of attacks are present in the computer networks. The attackers find the vulnerabilities present in the system application or operating system and use that to exploit the system. For removing the attack we need to identify the attack and then apply the appropriate countermeasure to remove that. This paper categorizes different types of attacks based on information modification; identify the consequences of the attacks and their countermeasures.

KEYWORDS: Attacks taxonomy, Active attacks, Passive attacks, Classification, Consequences, Countermeasures

I. INTRODUCTION

Usage of internet is increasing day by day almost at exponential rate. Nearly all organizations, government people and business firms use internet today for their businesses and activities. Internet is used for a wide variety of businesses, communication, online exams etc. for this a large amount of data exposed to the external users and we need to protect that information from the attackers or bad guys. These attacks hamper principles of security these principles are: confidentiality, integrity and availability [1-3]. Confidentiality means information is available only to the person who is authorized to access that. Integrity means that only authorized persons can modify or delete data. Availability means that information must be available to the authorized person when needed. Additionally access control, authentication and non-repudiation are included in the principles of security. Access control means that access to information is restricted only to the authorized person. Authentication means to confirm the identity of both the parties involved in communication. Non repudiation is sender or receiver cannot later deny the transmission.

Attacks are classified as: active attacks and passive attacks. Passive attacks occur as interception and categorized as release of message content, traffic analysis, packet sniffing and key logger. Active attacks can be categorized as modification, interruption and fabrication. Technique that can be used in modification is man-in –the-middle (MITM) attack. Techniques used in fabrication are replay attack and identity spoofing. The techniques used under the heading interruption are Denial of Services (DoS), Distributed Denial of Service (DDoS) and SQL injection attacks.

The paper is organized as follows Section 2 defines taxonomy of attacks and consequences of attacks. Section 3 defines research findings, here consequences and countermeasures of each attack are discussed. Conclusion and future scope is present in section 4.

II. CLASSIFICATION OF ATTACKS

Attacks in computer networks can be classified into two main categories: Active attacks and passive attacks[1, 2]. The taxonomy of attacks is shown in figure 1.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

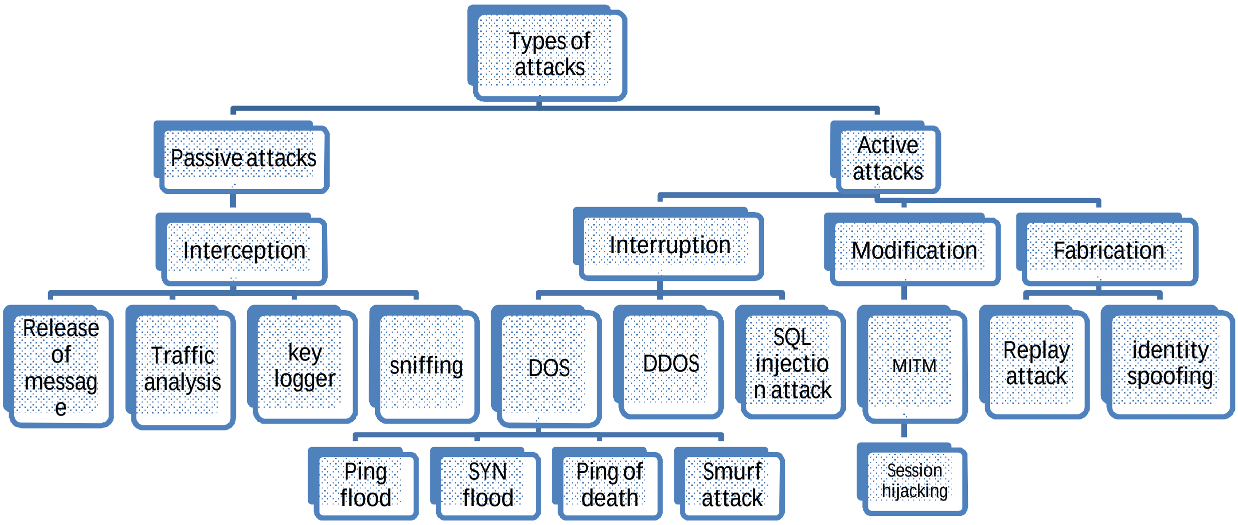

Figure 1 Attack classification

A. Passive attacks

In passive attacks, attacker's aim is to obtain the information flowing through the network. Attacker monitors the unencrypted traffic and looks for the clear-text passwords and sensitive information. Attacker does not modify the information present in the packet on the network so these attacks are difficult to detect. Common techniques under passive attacks are traffic analysis, packet sniffing, key loggers and release of message content.

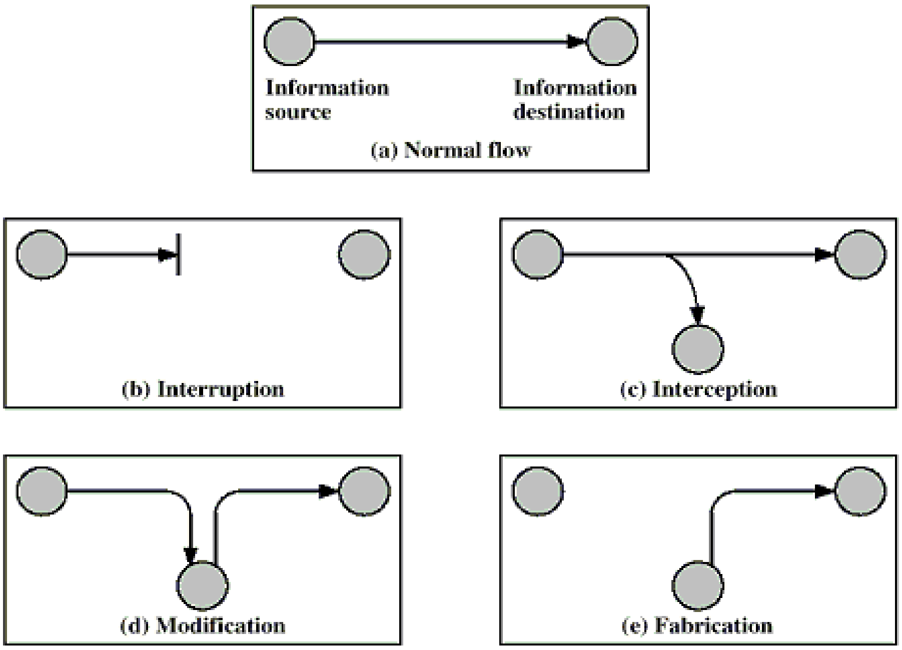

Figure 2 Different attack techniques

DOI: 10.15680/ijircce.2015. 0307096

a. Interception

It is the type of passive attack. In this attack attacker can intercept the messages or communication between two parties. This attack is done without user consent which results in loss of confidentiality of message. This attack technique can be classified as traffic analysis, packet sniffing, key logger and release of message content.

i. Traffic analysis

Traffic analysis is technique used in interception in order to deduce the information from packets being communicated. By monitoring the frequency and length of messages even encrypted nature of communication can be guessed. This technique is useful even when packets are encrypted and are not easy to decrypt. More the traffic obtained from the network more the information can be inferred.

ii. Packet sniffing

Packet sniffing is network attack which captures the network traffic and read that information. After capturing data, is analyzed for the sensitive information. This is done with the help of some sniffing tool e.g. Wireshark. If no encryption is used then sniffing tool provides full view of the data. Sniffing can be used by the IT professional to monitor the network or by the attacker to gain sensitive information flowing through the network. As a result of sniffing:

- Attacker can get valid user ID and passwords and can legally log on to the system.
- Unauthorized person can read confidential information

iii. Key logger

Keyloggers are software programs or devices that are designed to monitor and log keystrokes on a system. Keyloggers are primarily used to steal user data related to various online payment systems like credit card information and passwords. New keylogger Trojans are being written by virus writers for this purpose. Antivirus companies named such programs as Trojan or Trojan programs. Keyloggers are installed on the computer when use opens a file attached in email or file launched from open access network or installed from other malicious program present already on the victim machine or installed via web page vulnerability or automatically launched when a user visits an infected site.

iv. Release of message content

When two parties are communicating through any means for example through telephonic call or email or doing file transfer, these may contain confidential data. Attacker in between may capture all the data and confidential information also. So in order to prevent this all the communication between two parties should be encoded such that nobody is able to extract the data.

B. Active attacks

In active attacks, attacker first obtains the information flowing through the network i.e. guess the communication and then modifies the actual message or creates a new false message these types of attacks can be detected but are difficult to prevent. Active attack techniques are interruption, modification and fabrication. A detail of these is given below:**.**

a. Modification

If an unauthorized party not only accesses but tamper with the asset the threat is called modification. For example someone might change the values in the database or modify the data being communicated electronically. Modification is done without the knowledge of sender or receiver. This results in loss of integrity. Technique that is used in this attack is man-in-the-middle (MITM) attack.

i. Man-in-the-middle (MITM)

A MITM attack is defined as an attack in which the intruder is able to read and write messages communicated between two parties without either party being conscious of this fact[8]. This is done in three steps:

1. Get victim talk to you
2. Get target talk to you

DOI: 10.15680/ijircce.2015. 0307096

3. Sniff the traffic and forward the packets received on both sides.

This type of attack is done using more than one type of attack. For example this can also include ARP poisoning, masquerading, spoofing, forwarding etc. One common example of this type of attack is session hijacking. Figure 3 shows how MITM attack takes place [17].

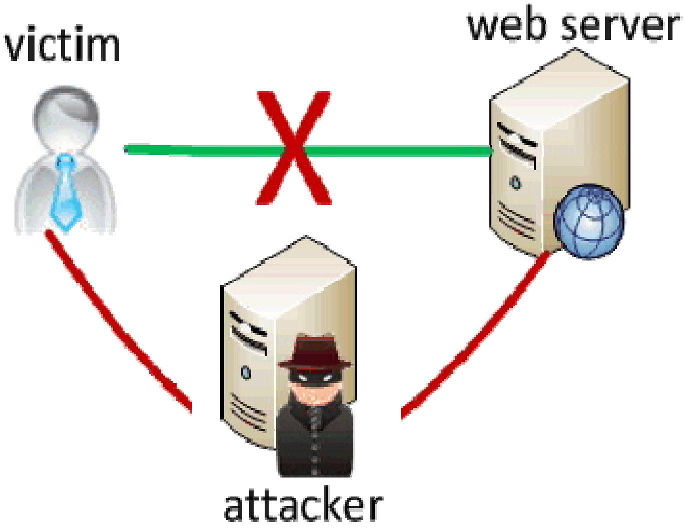

Figure 3 Man- In –The-Middle (MITM) attack

ii. *Session hijacking:*

In session hijacking [7], attacker takes an authorized and authenticated session away from the legitimate owner. Target only knows that he no longer has access to the session but in fact session may be taken over by the attacker. This type of attack occurs in real time but can continue long after that. Two tasks are done in this:

1. Masquerade as a target to the network done using high level packet crafting.
2. Stop the target from resuming the session using sequence of disassociate packets

b. *Interruption*

Interruption refers to the situation in which some information or service becomes unavailable, destroyed or unusable. This results in loss of availability [4]. Examples of interruption are cutting cable, disabling a file management server etc. techniques that are used under this category are Denial of Services (DoS), Distributed Denial of Service (DDoS) and SQL injection attack.

i. *Denial of Services (DoS)*

DoS attack prevents the normal use of computer or network by legitimate users is attack against availability. In this attacker sends invalid data to application or network, floods a computer or network with traffic or blocks traffic [5,12]. These result in

- Abnormal termination or behavior of application or services.
- Computer or network shutdown due to abnormal load.
- Blocks traffic which results in loss of access to network by authorized user or valid user.
- Randomize the attention if internet information system (IIS) staff so that they don’t see the intrusion immediately.

DoS attack is of following types[9]

- SYN flood attack
- Ping flood

- Ping of death attack
- Teardrop
- Smurf attack
- DNS poisoning

ii. *Distributed Denial of Services (DDoS)*

A Distributed Denial of Service (DDoS) attack is a coordinated attack on the availability of services of a given victim system or network and is launched indirectly through many compromised systems [10] these compromised system are called Zombies. In Distributed Denial of Service attack, multiple compromised systems, which are usually infected with some malicious program, are used to target a system causing Denial of Service attack [6]. Victim of this attack are end targeted system and all the system that are maliciously used by attacker in distributed manner. DDoS attack uses many computers and many internet connections which are often distributed globally and is referred as Botnet.

iii. *SQL injection attack*

SQL injection involves the modification of SQL statements that are used within web application with the data supplied by attacker[14]. Web applications are exposed to SQL injection attacks due to insufficient input validation and improper construction of SQL statements. SQL injection attack can result in Authentication bypass, information disclosure, privilege escalation, compromised availability and integrity of data [16].

c. *Fabrication*

In this type of attack, unauthorized person gains access to the system and inserts some false object into the system. It degrades the authenticity of the system. For example some attacker adds some record into the database, or the attacker gains access to victim's computer and sends messages from that system [4]. Recipient believes that message is from the victim but in fact it is not. Techniques that come under this attack are replay attack and identity spoofing.

i. *Replay attack*

In this type of network attack, valid data transmission is maliciously repeated or delayed[11]. This attack is carried out by attacker or adversary who intercepts the message between two parties and transmits messages. This can be used as the part of other attacks like masquerading or IP spoofing. As a result of this, user gets false information during communication.

ii. *Identity spoofing*

Most of the networks and operating systems use IP addresses to identify an entity as valid entity. In certain cases it is possible that IP addresses to be falsely assumed. This is called identity spoofing. Badguy may use specially constructed programs to construct the IP packets that appear to originate from legitimate users but in fact not. Spoofing can occur at MAC layer also [13]. this can launch other attacks also at various layers. For example IP address spoofing can lead to session hijacking.

As a result of this:

- Attacker can modify, delete or reroute the data after gaining access to the network.
- Attacker can also do other type of attacks like password based attack and DoS.

III. RESEARCH FINDINGS

To mitigate the risk of these attacks techniques, following methods can be used.

Table 1: Summary of Passive attacks

Attack name	Definition	Consequences	Countermeasures
Interception			
Traffic analysis	Deduce information from packets being communicated	- Unauthorized person can get the information	- Encryption - Masking channel
Packet sniffing	Tools collect information from network such as user id, passwords, content of email messages, credit card information etc.	-Attacker can get valid user ID and passwords and can log on to the system. -Unauthorized person can read confidential information	- Use strong cryptographic encryption
Key loggers	Software programs or devices that are designed to monitor and log keystrokes on a system.	- steal user's confidential data	- One time passwords - Virtual keyboards
Release of message content	Collect confidential data during telephonic call or email messages or during file transfer.	Attacker monitor the content of the transmissions	-Use encodings

Table 2: Summary of Active attacks

Attack Name	Definition	Consequences	Countermeasures
Modification			
Man-in-the-middle attack	Intruder is able to read and write messages communicated between two parties without user consent.	Attacker gets the information without user consent	- Use IDS - Use encrypted and authenticated channels
Session hijacking	Attacker takes away authorized and authenticated session between two parties	Attacker takes away the session and gets the information.	- Use encrypted and authenticated channels - Secure internal machines
Interruption			
DoS [12]	Prevents the normal use of computer or network by flooding the traffic or by blocking traffic	- Abnormal termination of application or services. - Computer or network shutdown due to abnormal load. - Loss of access to network by authorized user or valid user. - Randomize the attention of IIS staff so that they don't see the intrusion immediately.	- Files and folder hashes - DNS lookup - Firewall - Client puzzle - Use IDS and IPS
DDoS	Coordinated attack on the services of victim system and is launched through many compromised systems.	- Abnormal termination of application or services. - Computer or network shutdown due to abnormal load. - Loss of access to network by authorized user or valid user.	- Prevent secondary victims - Egress filtering - Load balancing - Throttling
SQL injection	Involves modification of SQL statements used within web	- Add or change information in database	- Input type checking - Identification of all

	applications with data supplied by attacker	- Perform privilege escalation - Launch other type of attacks like DoS	input sources
Fabrication			
Replay attack[13]	Valid data transfer is maliciously repeated or delayed	- User gets false information	- Session tokens - One time passwords - Time stamping - Disallow concurrent logins
Identity spoofing[13,15]	IP address is falsely assumed by attacker	- Attacker can steal data, destroy data and get control over the system. - Launch other type of attacks like password based attack and DoS attacks	- Packet filtering - Traceback - Use new protocols and services

IV. Conclusion and Future Work

This paper offers a classification of security attacks, their consequences and countermeasures to solve these attacks. These attacks hamper the principles of the security i.e. confidentiality, integrity and availability. Passive attacks using interception affect the confidentiality of information. Attacks due to modification like man-in the- middle attack and session hijacking result in loss of integrity of the messages and these can be removed by using the secure and encrypted channels or by securing systems. Attacks occurring due to interruption like DoS, DDoS and SQL injection affect the availability of information. Replay attack and identity spoofing affect the authenticity of the system. The solutions given in this paper can be applied to solve these attacks.

References

1. K. Ahmad, S. Verma, N. Kumar and J. Shekhar, 'Classification of Internet Security Attacks', Proceeding of the 5th National Conference INDIACom-2011Bharti Vidyapeeth‟ s Institute of Computer Applications and Management, New Delhi, March 10-11, 2011.
2. M. Choi, Rosslin J. Robles, C. Hong, and T. Kim, 'Wireless Network Security: Vulnerabilities, Threats and Countermeasures', International journal of Multimedia and Ubiquitous Engineering, Vol. 3, Issue 3, 2008.
3. David A Wheeler, "Secure programming for Linux and Unix HOWTO", 2003.
4. Charles P. Pfleeger, and Shari Lawrence Pfleeger. 'Security in computing', Prentice Hall Professional Technical Reference, 2002.
5. Bicakci, Kemal, and Bulent Tavli. 'Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks', Computer Standards & Interfaces, Vol. 31, Issue 5, pp. 931-941, 2009.
6. Roger Needham, and Butler Lampson, 'Network Attack and Defense', Whitepaper, 2008.
7. A. Simmonds, P. Sandilands, and L. V. Ekert, 'An ontology for network security attacks', Proceedings of Asian Applied Computing Conference (AACC), Lecture Notes in Computer Science, Kathmandu, Nepal, Springer Berlin, Vol. 3285, pp. 317-323, 2004.
8. Benjamin Aziz and Geoff Hamilton, 'Detecting man-in-the-middle attacks by precise timing', 3rd International Conference on Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. IEEE, pp. 81-86, June 2009.
9. Donald Welch and Scott Lathrop, 'Wireless security threat taxonomy', IEEE Systems, Man and Cybernetics Society Information Assurance Workshop, IEEE, pp.76-83, 2003.
10. Stephen M. Specht, and Ruby B. Lee, 'Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures', Proceedings of 17th International Conference on Parallel and Distributed Computing Systems(PDCS. 04), September 2004.
11. Paul Syverson, 'A taxonomy of replay attacks [cryptographic protocols]', *Proceedings of the 7th IEEE Computer Security Foundations Workshop (CSFW 07)* , pp. 131 -136, 1994 .
12. XiaoFeng Wang, and Michael K. Reiter, 'Defending against denial-of-service attacks with puzzle auctions', Proceedings of IEEE Symposium on Security and Privacy, IEEE, pp.78-92, 2003.
13. K. Xing, S. Srinivasan , M. Rivera, Jiang Li , X. Cheng "Attacks and countermeasures in sensor networks: a survey."*Network Security*. Springer US, pp. 251-272. 2010.
14. Halfond, W. G., Jeremy Viegas, and Alessandro Orso, 'A classification of SQL-injection attacks and countermeasures', *Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA*. 2006.
15. Xiang, Yang, and Wanlei Zhou, 'IP spoofing attack and its countermeasures', P*roceedings of the 5th Australian Information Warfare and Security Conference*. Edith Cowan University, School of Management Information Systems, We-B Centre, 2004.

16. W. G. Halfond, Jeremy Viegas, and Alessandro Orso, ‘A classification of SQL-injection attacks and countermeasures’, *Proceedings of the IEEE International Symposium on Secure Software Engineering, Arlington, VA, USA*, March, 2006.
17. http://www.x-services.nl/certificate-pinning-plugin-for-phonegap-to-prevent-man-in-the-middle-attacks/734

BIOGRAPHY

Cheshta Rani is M.E Student in M.E. (Information Security) in Computer Science and Engineering Department, Thapar University, Patiala. Her research areas are computer security.

Dr Shivani Goel is Assistant Professor in Computer Science and Engineering Department, Thapar University, Patiala. Her research areas are artificial intelligence and algorithms. She has guided 24 M.E. thesis and is presently guiding 04 PhDs.