International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 25 Issue 5 – APRIL 2018 (SPECIAL ISSUE).

A SURVEY ON SECURITY ATTACKS AND COUNTER MEASURES IN WIRED AND WIRELESS NETWORKS

*[#1]Dr. D.C.Jullie Josephine,[*2]Mrs. C. Annapoorani,[*3]Mrs. Gracia Nissi S*

[#1]Professor and Head of CSE,Kings Engineering College
*[*2,*3]Assistant Professor,Kings Engineering College*

***Abstract*-Security is the important aspect of most networks and many companies implement a comprehensive security policy encompassing the OSI layers, from application layer all the way down to IP security. OSI Model is built to allow different layer to work collectively, but without the knowledge of each other. If one layer is hacked, the other layers will be compromised indirectly. To avoid this problem, we need to be aware about, how Attacks works and what techniques can be used to mitigate this type of attacks in each layer. The main objective of the paper is to present different types of security attacks, and counter measures in wired and wireless network layer. Security attacks are classified based on OSI Model Layers.**

I.INTRODUCTION

Many people rely on the computer for many of their professional, social and personal activities. But there are also people, who attempt to damage our Internet-connected computers, violate our privacy and security of the Internet services.

Given the frequency and variety of existing attacks as well as the threat of new and more destructive future attacks, network security has become a central topic in the field of computer networking.

The network and internet are working based on wired and wireless network concepts. In the wired networks the OSI model layers are prone to various attacks, which halts the performance of a network.

According to the ISO standards, networks have been divided into 7 layers depending on the complexity of the functionality each of these layers provide.

Our modern networks are increasingly moving towards wireless technologies. As convenient as they are, wireless connections have one major

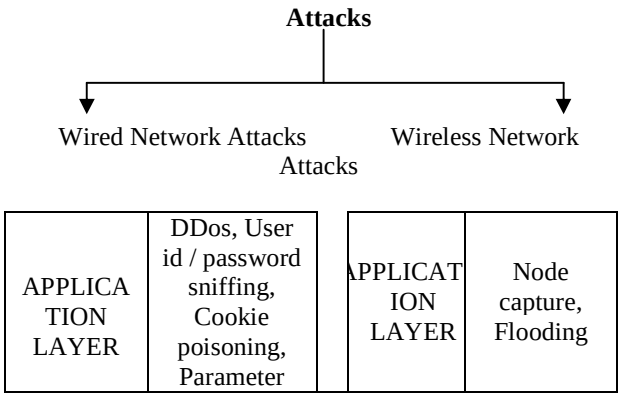
drawback is security. Compared to the wired counterparts, securing wireless technologies poses a bit of an extra challenge.

Network attacks are launched every hour of every day, and they evolve at an astounding pace. Every year brings new attacks and trends. Below are various layers in network and their attacks.

APPLICATION LAYER ATTACK:

1) Distributed denial of service attack: In which multiple compromised computer systems attack a target, such as a server, website or other network resource, and denies the service for users of the targeted resource. DoS attacks mostly focus on bandwidth consumption, target specific characteristics and vul-nerabilities of application layer protocols (e.g. HTTP, DNS).

The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.



	tampering, Cross-site scripting, SQL injection, Buffer overflows.		
PRESENTATION LAYER	SSL DoS, SMB Attack,	TRANSPORT LAYER	Malicious flooding, De-Synchronization
SESSION LAYER	Session Hijacking, DNS Poisoning,		
TRANSPORT LAYER	TCP SYN flood, UDP flood, Eavesdropping, Port scan, Replay attack, Man-in-the-Middle, TCP Session hijacking, Land attack, Denial-of-Service.	NETWORK LAYER	Sinkhole attack, Sybil attack, Selective forwarding
NETWORK LAYER	Ping flood, Fingerprinting, Worm hole, Sinkhole, Sybil attack, Black hole	MAC LAYER	Jamming, Tampering
DATA LINK LAYER	Packet Sniffing, MAC Address spoofing, ARP cache poisoning		
PHYSICAL LAYER	Keystroke logging, Lock picking	LINK LAYER	Collision, Exhaustion

2) User id / password sniffing: Theft or interception of data by capturing the network traffic using a sniffer. When data is transmitted across networks, if the data packets are not encrypted, the data within the network packet can be read using a sniffer. Sniffing involves capturing, decoding, inspecting and interpreting the information inside a network packet on a TCP/IP network. The purpose is to steal information, usually user IDs, passwords, network details, credit card numbers, etc.

3) Cookie poisoning: Cookie poisoning attacks are a process involving the manipulation and forging of cookies, designed to achieve illicit access to web applications and user accounts. Modification of a cookie by an attacker is to gain unauthorized information about the user for purposes such as identity theft.

4) Parameter tampering: Parameter tampering is a simple attack targeting the application business logic In a parameter tampering attack, an attacker may manipulate the values of hidden fields by changing the value of a GET or POST variable in the URL address bar

5) Cross-site scripting: Cross-site scripting (XSS) is a security breach that takes advantage of dynamically generated Web pages. In an XSS attack, a Web application is sent with a script that activates when it is read by an unsuspecting user's browser or by an application that has not protected itself against cross-site scripting. Because dynamic Web sites rely on user input, a malicious user can input malicious script into the page by hiding it within legitimate requests.

These **attacks** are not only used to gain user information, but can also alter the behavior of the web applications functionality. Along with that it also has the ability to read the web applications content and post data

6) SQL injection: SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application.

A successful SQL injection can read sensitive data from the database, modify database data, execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system.

7) Buffer overflows: It is one of the most serious cyber security threats.

In which a program overwrites memory adjacent to a buffer that should not have been modified intentionally or unintentionally.

PRESENTATION LAYER ATTACKS:

1) SSL DoS : SSL is a method of encryption used by various network communication protocols. SSL DDoS attacks and SSL DoS attacks target the SSL handshake mechanism, send garbage data to the SSL server, or abuse functions related to the SSL encryption key negotiation process.

2) SMB Attack: SMBRelay and SMBRelay2 are computer programs that can be used to carry out

SMB man-in-the-middle mitm) attacks on Windows machines.

SMB Relay Attack is a type of attack which relies on NTLM Version2 authentication that is normally used in the most of the companies. This kind of attack is very dangerous because anybody with access to the network can capture traffic, relay it and get unauthorized access to the servers.

SESSION LAYER ATTACKS:

1) Session Hijacking: It is also called as IP Spoofing. The Session Hijacking attack consists of the exploitation of the session key, to gain unauthorized access to information or services in a computer system.

2) DNS Poisoning: DNS cache poisoning, also known as DNS spoofing, is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.

One of the reasons DNS poisoning is so dangerous is because it can spread from DNS server to DNS server.

TRANSPORT LAYER ATTACK:

1) TCP SYN: flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

2) UDP flooding: UDP flood" is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagram.

3) Eavesdropping: Eavesdropping is unauthorized real-time interception of a getting MAC Address; sniff clear text passwords and keys crack password hashes crack WEP keys, SSID.

4) Port scan: port scan attack, occurs when an attacker sends packets to your machine, varying the destination port. Hackers will know the IP address and port status to start attack.

5) Replay attack: are the network *attacks* in which an attacker spies the conversation between the sender and receiver and takes the authenticated information e.g. sharing key and then contact the receiver with that key.

6) Man-in-the-Middle attack: Man-in-the-middle attack. It is also known as a bucket brigade attack, or sometimes Janus attack in cryptography. The attacker keeps himself / herself between two parties, making them believe that they are talking directly to each other over a private connection, when actually the entire conversation is being controlled by the attacker.

7) TCP Session hijacking: TCP session hijacking" is a technique that involves intercepting a TCP session initiated between two machines in order to hijack it..

8) Land attack: A land attack is a remote denial-of-service (DOS) attack caused by sending a packet to a machine with the source host/port the same as the destination host/port.

10) Denial-of-Service attack "These attacks try to overwhelm the network or server resources so that legal users or hosts cannot get service timely

NETWORK LAYER ATTACK

1) Ping flood: is a denial-of-service attack in which the attacker attempts to overwhelm a targeted device with ICMP echo-request packets, causing the target to become inaccessible to normal traffic.

2) Fingerprinting: fingerprinting is a technique used to sniff the web traffic by analyzing the data packets' flow pattern- without removing the encryption.

Worm hole This attack is also called the tunneling attack. In this attack an attacker receives a packet at one point and tunnels it

to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network

4) Sinkhole attack: Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighboring node. Selective modification, forwarding or dropping of data can be done by using this attack

5) Sybil attack: In Sybil attack malicious nodes pretends to be multiple nodes by taking multiple identities.

6) Black hole: a packet drop attack or black hole attack is a type of denial-of-service attack in which a router that is supposed to create a false route through them and then perform malicious activities on the transmitted packets.

DATA LINK LAYER ATTACKS

1) Packet Sniffing: A packet sniffer is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network.

A packet analyzer used for intercepting traffic on wireless networks is known as a wireless analyzer or WiFi analyzer

2) MAC Address spoofing: MAC address spoofing, in which a malicious user changes a client's MAC address into his own, calling for a new detection method.

3) ARP cache poisoning and flooding: ARP is part of the Internet Protocol (IP) that is responsible for mapping a computer's IP address with its MAC address.

4) VLAN attack: **VLAN** hopping is a computer security exploit, a method of **attacking** networked resources on a virtual LAN (**VLAN**).

The basic concept behind all **VLAN** hopping **attacks** is for an **attacking** host on a **VLAN** to gain access to traffic on other **VLANs** that would normally not be accessible.

PHYSICAL LAYER ATTACKS

1) Keystroke logging: Keystroke logging, often referred to as key logging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.

2) Lock picking: These locks are much more resilient to brute force attacks and are impervious to shimming, but can fall victim to lock picking. Because these locks usually employ a pin tumbler locking mechanism you can test the security of your deadbolt through learning lock picking.

Cutting (cable disconnect) – disconnecting the cable.

WIRELESS NETWORK LAYERS AND ATTACKS

APPLICATION LAYER ATTACKS

1) Node capture: Direct physical access, capture and replace/subvert the sensor nodes.

2) Flooding: exhausting the resources of sensors.

TRANSPORT LAYER ATTACKS

1) Malicious Flooding: A UDP flood attack is a denial-of-service (DoS) attack using the User Datagram Protocol (UDP), a sessionless/connectionless computer networking protocol.

Using UDP for denial-of-service attacks is not as straightforward as with the Transmission Control Protocol (TCP). However, a UDP flood attack can be initiated by sending a large number of UDP packets to random ports on a remote host. As a result, the distant host will:

- Check for the application listening at that port;
- See that no application listens at that port;
- Reply with an ICMP Destination Unreachable packet.

2) De-Synchronization: The core objective of 3GPP Long Term Evolution (LTE) is to provide a secured communication and high data rate for 4G users. Even though 4G network provides security, there are loopholes which lead to several attacks in 4G network. One such attack is desynchronization attack in 3GPP handover key management.

NETWORK LAYER ATTACKS

1) Sinkhole attack: Sinkhole attack prevents the base station from obtaining complete and correct sensing data, and thus forms a serious threat to higher-layer applications. It is particularly severe for wireless sensor networks given the vulnerability of wireless links, and that the sensors are often deployed in open areas and of weak computation.

2) Sybil attack: In Sybil attack malicious nodes pretends to be multiple nodes by taking multiple identities.

In peer to peer systems, due to lack of central authorization authority these systems are vulnerable to these attacks.

3) **Selective forwarding**: Security and timely transmission of packets in wireless sensor network is its basic need of the network. The attack which affect this is the selective forwarding attack as in this attack malicious node drops the packet and make it unavailable to the destination.

MAC LAYER ATTACKS

1) Jamming: These types of attacks can easily be accomplished by an adversary by either bypassing MAC layer protocol or by emitting RF signals. Typically, jamming can be referred as intentional interference attacks on wireless networks. It is an attempt of making the users not possible to use network resources.

2) Tampering: it is the result of physical access to the node.

Parameter tampering is a form of Web-based attack in which certain parameters in the Uniform Resource Locator (URL) or Web page form field data entered by a user are changed without that user's authorization. This points the browser to a link, page or site other than the one the user intends.

LINK LAYER ATTACKS

1) Collision: Stealthy packet dropping in multihop wireless sensor networks can be realized by the colluding collision attack. Colluding collision attack disrupts a packet from reaching its destination by malicious collusion at intermediate nodes.

2) Exhaustion: In power exhaustion attack more battery power of · the node consumption takes place, so node becomes inactive.

OSI Layer Attacks and Counter Measures		
Layers	**Attacks**	**Counter measures**
Application	Distributed denial of service attack	Authentication
	User id / password sniffing	Encryption
	Cookie poisoning	Web application Firewall
	Parameter tampering	Encryption and Hashing
	Cross-site scripting	HTTPS,SSL
	SQL injection	secure hash algorithms ,
	Buffer overflows	Dynamic Memory Allocation
Presentation	SSL DoS	Authentication,
	SMB(Server Message Block)	Authentication
Session	Session Hijacking	Antivirus, anti-malware software
	DNS Poisoning	SSH encryption,sniffing detection tools
Transport	TCP SYN flood	SYN Cookies,backlog Queue
	UDP flood	Port Blocking, Filtering, Monitoring
	Eavesdropping	Encryption,Segmenting Network
	Port scan	Filter inbound packets and outbound packets,Firewall,IDS
	Replay attack	Authentication,MAC,Timestamping
	Man-in-the-Middle	Public key infrastructure
	TCP Session hijacking	Encryption,HTTPS,SSL connections
	Land attack	Firewall
	Denial-of-Service	Firewall,Antivirus,Update OS
Network Layer	Ping flood	Distributed Defence Approach
	Fingerprinting	Text based retrieval, Image based retrieval
	Worm hole	Key management, Secure routing,True link
	Sinkhole	Authentication
	Sybil attack	Identity based validation technique
	Black hole	Secure Routing Protocol
Data Link Layer	Packet Sniffing	Encryption, PGP,S/MIME
	MAC Address spoofing	Encryption, Dynamic IP Address Allocation
	ARP cache poisoning	Monitoring ARP table Database
Physical Layer	Keystroke logging	Anti-Malware programs
	Lock picking	Install security pins

Wireless Network Layer Attacks and Counter Measures		
Layers	**Attacks**	**Counter measures**
Application Layer	Node capture	Adaptive antennas, Spread Sprecturm
	Flooding	Client Puzzles
Transport Layer	Malicious flooding	Packet Leashes, Authentication

	De-Synchronization	Client Puzzles Authentication
Network Layer	Sinkhole	Identity Certificate
	Sybil attack	Authentication
	Selective forwarding	Multihop Acknowledgement
Mac Layer	Jamming	Spread spectrum, region mapping, lower duty cycle.
	Tampering	Tamper proofing, Hiding nodes
Link Layer	Collision	Error Correction Code
	Exhaustion	Rate limitation

IV.CONCLUSION

The security of networks has become an vital topic since data communication is around Internet.In this paper, a survey on different attacks in wired and wireless network.We have also covered the counter measures for the attacks in each OSI layer.

V.REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, 2002.

[2] Wireless sensor networks: a survey I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci

[3] D.W. Carman, P.S. Krus, and B.J. Matt, “Constraints and approaches for distributed sensor network security”, Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, 2000

[4]ATTACKS AT DATA LINK LAYER OF OSI MODEL: AN OVERVIEW Raminderpal Singh Associate Professor, Amanjeet Kaur Assistant Professor, Sania Sethi Assistant Professor, Department of Computer Applications &Management, SBSSTC, Ferozepur (India), International Journal of Advanced Technology in Engineering and Science, Volume No.03, Special Issue No. 02, February 2015.

[5]Http://wiki.cas.mcmaster.ca/index.php/The_FiveLayer_TCP/IP_Model:_Description/Attacks/Defense

[6] An Approach to Detect Packets Using Packet Sniffing Rupam1 , Atul Verma2 , Ankita Singh3 Department of Computer Science, Sri Ram Swroop Memorial Group of Professional Colleges Tiwari Gang Faizabad Road, Lucknow, Uttar Pradesh, India.