Overview of Wireless Network attacks and Security measures

[1]Prof. Svapnil Vakharia,
Assistant Professor
Department of Information Technology
Gandhinagar Institute of Technology

[2]Bandi Vamsi Dharma Teja
Department of ECE,
Hindustan University, Chennai,
Tamil Nadu, 603103, India,

***Abstract*: Wireless networks has been facilitating numerous emerging applications that require packet delivery from one or more senders to multiple receivers. They are vulnerable to different type of attacks due to lack of security in the modern technology. The more we use the technology, more the chances of getting attacked by cyber criminals. In this paper we have introduce types of attacks and counter measures. The wireless networks are use in many commercial and private companies. Surveys shows that cyber-attacks are increasing every year. An attacker uses powerful operating systems like Kali linux or parrot os to target the attack.**

***Keywords*: wireless networks, attacks, counter measures, packets.**

I. Introduction

A wireless network is a flexible data communications system, which uses wireless media such as radio frequency technology to transmit and receive data over the air, minimizing the need for wired connections. Wireless networks are used to augment rather than replace wired networks and are most commonly used to provide last few stages of connectivity between a mobile user and a wired network.

Wireless networking has important as one of the most promising concept for auto configurable and self-organizing wireless networking to provide adaptive and flexible wireless connectivity to mobile users. This concept can be used for very different wireless access technologies such as wireless local area network (WLAN), wireless metropolitan area network (WMAN), and wireless personal area network (WPAN) technologies.
Wireless devices are more vulnerable to security threats. Security does not come free, it needs lot of equipment, money and time to create the anti-viral programs, which is very essential these days

II. Wireless LAN overview

Wireless LANs based on the IEEE 802.11 standards allow wire- free networking in the local area network environment using the unlicensed 2.4 or 5.3 GHz unlicensed radio band. They're used everywhere from homes to Fortune 500 companies to hotspot Internet access

A. Access point

An access point is a station that transmits and receives data. An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. Each access point can serve multiple users within a defined network area; as people move beyond the range of one access point, they are automatically handed over to the next one. A small WLAN may only require a single access point; the number required increases as a function of the number of network users and the physical size of the network.

B. Channels

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

C. WEP

Wired Equivalent Privacy (WEP) is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm. The shared-secret key is either 40 or 104 bits long. The key is chosen by the system administrator. This key must be shared among all the stations and the AP using mechanisms that are not specified in the IEEE 802.11.

D. Authentication:

Authentication is the process of proving identity of a station to another station or AP. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. In the closed network architecture, the stations must know the SSID of the AP in order to connect to the AP. The shared key authentication uses a standard challenge and response along with a shared secret key

E. Association

Data can be exchanged between the station and AP only after a station is associated with an AP in the infrastructure mode or with another station in the ad hoc mode. All the APs transmit Beacon frames a few times each second that contain the SSID, time, capabilities, supported rates, and other information. Stations can chose to associate with an AP based on the signal strength etc. of each AP. Stations can have a null SSID that is considered to match all SSIDs.

The association is a two-step process. A station that is currently unauthenticated and unassociated listens for Beacon frames. The station selects a BSS to join. The station and the AP mutually authenticate themselves by exchanging Authentication management frames. The client is now authenticated, but unassociated. In the second step, the station sends an Association Request frame, to which the AP responds with an Association Response frame that includes an Association ID to the station. The station is now authenticated and associated.

III. Types of wireless attacks

A.DDOS

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

Attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge, and used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Botnets can generate huge floods of traffic to overwhelm a target. These floods can be generated in multiple ways, such as sending more connection requests than a server can handle, or having computers send the victim huge amounts of random data to use up the target's bandwidth. Some attacks are so big they can max out a country's international cable capacity.

Specialized online marketplaces exist to buy and sell botnets or individual DDoS attacks. Using these underground markets, anyone can pay a nominal fee to silence websites they disagree with or disrupt an organization's online operations. A week-long DDoS attack, capable of taking a small organization offline can cost few hundred dollars

B. Wi-Fi ATTACKS:

There are two programs which are basically used for Wi-Fi attacks. They are Air crack and Pixie wps.

These little powerful tools are usually used to crack the WEP and WPA/WPA2 encrypted Wi-Fi Networks with an ease. Generally it take couple of minutes to few hours to crack a Wi-Fi with these tools Aircrack is a complete suite of tools to assess Wi-Fi network security.

Aircrack:

It focuses on different areas of Wi-Fi security:

- Monitoring: Packet capture and export of data to text files for further processing by third party tools.
- Attacking: Replay attacks, deauthentication, fake access points and others via packet injection.
- Testing: Checking Wi-Fi cards and driver capabilities (capture and injection).
- Cracking WPA-PSK keys

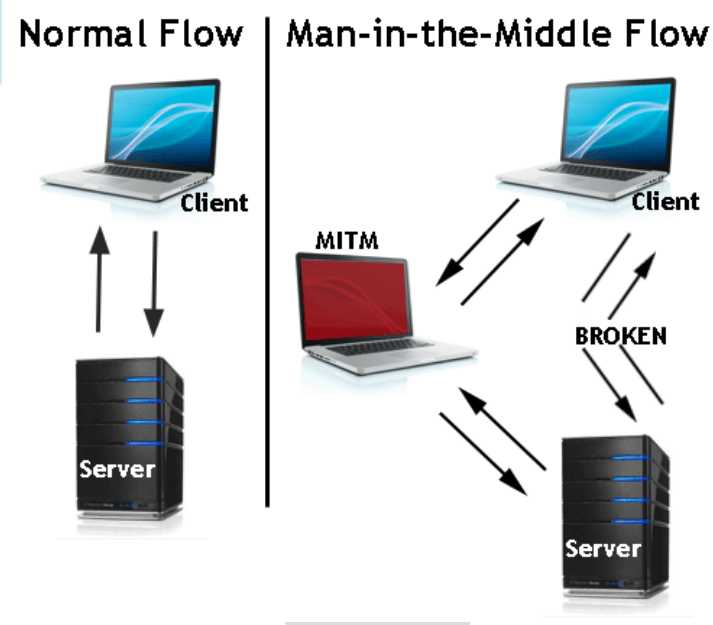
Pixie wps:

This is more advanced tool than any other Wi-Fi cracking setup. It focuses on the WPS pin of the Access Point (AP). some APs have weak ways of generating **nonces** (known as **E-S1** and **E-S2**) that are supposed to be secret. If we are able to figure out what these nonces are, we can easily find the WPS PIN of an AP since the AP must give it to us in a hash in order to prove that it also knowns the PIN, and the client is not connecting to a rouge AP. These E-S1 and E-S2 are essentially the "keys to unlock the lock box" containing the WPS pin. You can kind of think of the whole thing as an algebra problem, if we know all but 1 variable in an equation, we just have to solve for x. X in this case is the WPS pin

C. Man in the Middle attack:

A man-in-the-middle attack is a type of cyber-attack where a malicious actor inserts him/herself into a conversation between two parties, impersonates both parties and gains access to information that the two parties were trying to send to each other. A man-in-the-middle attack allows a malicious actor to intercept, send and receive data meant for someone else, or not meant to be sent at all, without either outside party knowing until it is too late. Man-in-the-middle attacks can be abbreviated in many ways, including MITM, MitM, MiM or MIM

- A MITM attack exploits the real-time processing of transactions, conversations or transfer of other data.
- Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.



D. EVIL TWIN

An evil twin is a fraudulent Wi-fi access point that appears to be legitimate, set up to eavesdrop on wireless communications. The evil twin is equivalent wireless LAN of the phishing scam. This type of attack may be used to steal the passwords of unsuspecting users, either by monitoring their connections or by phishing, which involves setting up a fraudulent web site and luring people.

The attacker snoops on Internet traffic using a bogus wireless access point. Unwitting web users may be invited to log in to the attacker's server, prompting them to enter sensitive information such as usernames and passwords. Often, users are unaware they have been duped until well after the incident has occurred.

When users log in to unsecured (non-HTPPS) bank or e-mail accounts, the attacker intercepts the transaction, since it is sent through their equipment. The attacker is also able to connect to other networks.

Fake access points are set up by configuring a wireless card to act as an access point (known as Host AP). They are hard to trace since they can be shut off instantly. The counterfeit access point may be given the same SSID and BSSID as a nearby Wi-Fi network. The evil twin can be configured to pass Internet traffic through to the legitimate access point while monitoring the victim's connection, or it can simply say the system is temporarily unavailable after obtaining a username and password

E. Jamming Attack:

Since RF (radio frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless network can no longer function. The complexity of jamming is the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well. Some widely used consumer products include cordless phones, Bluetooth enabled devices and baby monitors, all capable of disrupting the signal of a wireless network and faltering traffic

F. Bluetooth Attacks

Bluetooth hacking is also most common attacks used by criminals when they want to take the whole control of the device. BTscanner and Blue snarfing are the tools used for this attack.

With BTscanner, an attacker scan for an open Bluetooth ports and he use Blue snarfer to take control of the device,

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to calendars, contact lists, emails and text messages, and on some phones, users can copy pictures and private videos. Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge. While Bluejacking is essentially harmless as it only transmits data to the target device, Bluesnarfing is the theft of information from the target device.

G. Metasploit

Metasploit is a computer security tool which is used to find the information about security vulnerabilities. Its the most common and powerful tool used by any attacker to gain access to the target machine. Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.

The basic steps for exploiting a system using the Framework include:

1.Choosing and configuring an *exploit* (code that enters a target system by taking advantage of one of its bugs; about 900 different exploits for Windows, Unix/Linux and Mac OS X systems are included);
2.Optionally checking whether the intended target system is susceptible to the chosen exploit;
3.Choosing and configuring a payload (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);
4.Choosing the encoding technique so that the intrusion-prevention system (IPs) ignores the encoded payload;
5.Executing the exploit.

IV.SECURITY MEASURES

A. Prevention from DDoS attacks

1. Rate limit your router to prevent your Web server being overwhelmed
2. Add filters to tell your router to drop packets from obvious sources of attack
3. Timeout half-open connections more aggressively
4. Drop spoofed or malformed packages
5. Set lower SYN, ICMP, and UDP flood drop thresholds

B. Prevention from WI-FI attacks

Upgrade to WPA/WPA2 from WEP. Usually WPA2 are also vulnerable to attacks from advanced cracking algorithms. The only way to prevent is to turnoff the WPS pin, so that the attacker has no chance for brute forcing the WPS pin.

Besides that its always better to add MAC Filtering for extra protection, so that one can add the MAC addresses devices only which he uses.

It’s also advised to hide the network and not share the password with neighbors.

C. Prevention from Man In The Middle attacks

Method 1. VPN

The most common used for a secure connection is Virtual Private Network (VPN). A VPN extends a private network across a public network, e.g., the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols or traffic encryptions, such as PPTP (Point-to-point Tunneling Protocal) or Internet Protocol Security (IPSec).

Method 2. Proxy Server with Data Encryption

The 2nd technique is utilizing a reliable proxy server and encrypt the transmission between you and the proxy. Some privacy software like Hide My Ip provides proxy servers and option of encryption.

Method 3. Secure Shell Tunneling

The 3rd trick is to make use of Secure Shell(SSH), which is a network protocol for remote administration of UNIX/LINUX hosts. SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding TCP ports and X11 connections; A Secure Shell (SSH) tunnel consists of an encrypted tunnel created through an SSH protocol connection. Users may set up SSH tunnels to transfer unencrypted traffic over a network through an encrypted channel.

D. Prevention from evil twin

Not just relying on the name of a Wi-Fi network before deciding whether it can be trusted as legitimate or not.

•Where possible restricting browsing on public Wi-Fi networks to websites that do not require login credentials, and never using them for sensitive data. 3G mobile connections, for instance, can be typically considered much safer than public Wi-Fi.

•Running a VPN to ensure that any browsing and transmitted data is done through an encrypted tunnel that cannot be easily snooped upon by malicious parties.

E. Prevention from jamming attacks

The only way to prevent from jamming attacks is using 5ghz band instead of 2.4ghz.

Most advanced routers can be more pricey but they usually block all kind of unwanted singanls without being jammed

F. Prevention from Bluetooth attacks

Most of the advanced Bluetooth mobile devices have pin encryption, so need to worry about them. But for old devices its always better to turn off the Bluetooth for safe measures. However its also adviced to turn off the Bluetooth in the newer handsets too.

G. Metasploits

Payloads and exploits are always gaining to take over new programs like java, adobe etc. There is no full control to prevent from metasploits attacks. The only thing that is suggested is to update the operating system regularly and also by using the internet security softwares.

V. CONCLUSION

This research shows all the different kinds of wireless attacks and how the attackers take the advantage of weak security that is present in the technology. Every counter measure is also described in detail so that we can protect our self from these attacks.

REFERENCES

[1] AusCERT. AA-2004.02 - denial of service vulnerability in IEEE 802.11 wireless devices. http://www.auscert.org

[2] R. Bruno, M. Conti, and E. Gregori, IEEE 802.11 Optimal Performances: RTS/CTS Mechanism vs. Basic Access, PIMRC, 2002

[3] B. Dahill et al., "A Secure Protocol for Ad Hoc Networks," IEEE ICNP, 2002.

[4] X. Gu and R. Hunt, "Wireless LAN Attacks and Vulnerabilities" In the Proceeding of IASTED Networks and Communication Systems, April 2005.