Wireless security: susceptibilities, assaults and defenses

[1]Kanika Sharma, [2]Namarta Kapoor
[1]Assistant Professor, [2]Assistant Professor
[1, 2] P.G Department of Computer Science, D.A.V College, Jalandhar, India

Abstract: *Wireless attacks have become a very widespread security matter when it comes to networks. There are numerous forms of security intimidation to wireless networks. For example, hackers know how to steal information from a corporation, attain unconstitutional access to applications, and even interrupt process of the network. Every wireless network is very susceptible to such kinds of molests and it is therefore very important that the essential security measures are taken so as to avoid the jumble that can be originate by these kinds of attacks. A skilled hacker, or even laid-back snooper, is able to easily monitor isolated wireless data packets using tools such as AirMagnet and AiroPeek, which fully disclose the contents of wireless data packets. In this paper, a survey has been prepared on the entire attacks that may possibly occur in present and future developments. This paper also discusses a number of available solutions for countering those threats.*

Keywords: *Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding.*

1. INTRODUCTION:

Wireless security will play a vital responsibility in wireless networks. In the current era, 3G networks and 4G networks contain separate security layers but still there is a chance of security attacks. On the behalf of access control, authentication, availability, confidentiality and integrity, wireless network attacks are classified. This paper is also being a sign of the next generation attacks like Man in the Middle Attack, Denial of Service Attack and Eavesdropping. This paper helps the managers to understand and evaluate the various threats allied with the use of wireless technology. The security methods and tools which help to find the protection against different types of attacks are also discussed in this paper.

2. WIRELESS NETWORK ATTACKS:

On the behalf of access control, authentication, availability, confidentiality and integrity, wireless network attacks are classified.

a) **Access Control Attacks**

Access control attacks occur in the system which requires an authorized access of some useful information. When an entrée control means is defective, the assailant will have the right of entry to get control of the supervision of the whole application. After that the hacker can have right to access the personal or sensitive data of the user. Below are some of the important types of access control attacks.

S.No	Name of Attack	Description
1.	**War driving**	It is also called access point mapping. With the use of Omni-directional antenna with geophysical positioning system war driver can orderly plot positions of WI-FI access points. With the availability of free Wi-Fi connection and other GPS functionalities, hackers can drive around and obtain a very huge amount of information over a very short period of time. Some special type of software can be used to view all the different access points around one.
2.	**Rogue Access Points**	A rouge access point is mainly an entrée point that has been supplementary to any user's network without his/her knowledge. The user totally has no idea that it is there. It is very simple for even a trainee to attain tools and set up a wireless network. If all this is prepared from surrounded by another network, it build what is acknowledged as a subnet, which can produce back doors to its owner. Persons who desire to interrupt a network can also set rogue access points themselves.
3.	**Ad Hoc Associations**	It includes a direct link to an unprotected location to demolish access point security or to attack the location. It can be protected with the help of any wireless card or USB adapter.

4.	**Medium Access Control (MAC) spoofing**	MAC address is reliably coded and cannot be misused easily on a Network Interface Controller (NIC) but by using some tools that can be done by the hackers easily[2]. A hacker can collect authorized MAC addresses and take bandwidth, corrupt the files sending through this route or download files, and inflict disorder on a complete network. An authorized list of MAC addresses for authentication will provide some security while establishing the wireless LAN.
5.	**Remote Authentication Dial in User Service (RADIUS) Cracking**	This type of molest occurs on a RADIUS authentication server, this server is used for validation of wireless network. This will enable user to place a unique usernames and passwords for accessing WI-FI. A WI-FI hacker can join to the venture secured wireless network by breaking the user passwords this can be done by using brute force dictionary attacks. The hacker can't be able to see the password but they can search this through a dictionary based cracker.

b) Authentication Attacks

These attacks can be applied by the trespassers or attackers to de-authenticate the user's confidential identities and records by thieving it and use these to access other personal services or networks.

S.No	Name of Attack	Description
1.	**Shared Key Guessing**	Wireless networks that are equipped with Wired Equivalent Privacy (WEP) protocol will be attacked by the hacker. By shared key substantiation, the hacker will have the WEP encryption key of the destination workstation in advance and broadcasts the message back to the source computer. The targeted access point deciphers the message and match up to it with original characters then it will send the authentication code to the hacker. Then the hacker will become a part of the network to access it.
2	**Pre–Shared Key**	This attack engages the regaining of WI-FI Protected Access (WPA) pre-shared key from detained key handshake frames. It is all done with the help of a dictionary attack tool.
3	**Application login theft**	In this attack the username and passwords of the user's email ids is capturing by using clear text application protocols.
4	**Domain login cracking**	In this attack login and passwords of the windows of the targeted user are capturing by cracking NetBIOS password hashes. For this attack the Dictionary attack tool is used.
5	**Virtual Private Network (VPN) Login cracking**	In this attack Internet Protocol Security (IPSec) Pre-shared secret key (PSK) are regaining by using brute force attacks on VPN authentication protocols.
6	**Identity theft**	It involves capturing of user id's from clear text Identity response packets.
7	**Password guessing**	It is made by frequently trying to presume the user's password using a captured identity.
8	**Light weight Encrypted Authentication Protocol (LEAP) Cracking**	In this attack the user's id's recovering from seized LEAP packets, protected by NT password hash. For cracking it, a dictionary attack tool is used.
9	**Encrypted Authentication Protocol (EAP) Downgrade**	By forcing a wireless server to tender a weaker authentication using counterfeit EAP-response or NAK packets.

c) Availability Attacks

In this attack the wireless network service will be delivered to the hacker by denying the legitimate users with access to Wireless resources or by demolishing those resources. All this is done due to the faults in protocols, software designing and their employment.

S.No	Name of Attack	Description
1	**Access Point Theft**	In this attack availability is checked by physically removing an access point from a local space.
2	**Denial of Service (DOS) Attack**	A denial of service attack can also be used in combination with a rogue access point. It is one of the simplest network attacks to carry out because

		it only requires limiting access to services. This can be done by simply sending a large amount of traffic at an exact target. An attacker could use a radio frequency signal generator to jam the transmitter to jam the Wireless LAN. That's why Wireless LAN interference is accidental. There are some ways of denial of service attacks: Beacon flood, Associate/Authenticate flood, De-authenticate flood, EAP-Start flood, EAP-failure, EAP of Death and Length attacks.
3	**Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) exploits**	TKIP is a stop gap security protocol. In this method, an invalid TKIP data to exceed the target access point's MIC error threshold and thus suspending Wireless LAN service will generated by the hacker.

d) Confidentiality Attack

Confidentiality means securing useful data to leak from unauthorized access. A company will have to security against those malicious actions which will harm the confidentiality of their information. Below are some of the important types of confidentiality attacks.

S.No	Name of Attack	Description
1	**Eavesdropping**	Eavesdropping is the prohibited real time interception of a personal conversation like phone talk, personal messages or video-meeting. Many software's are used that will convert digital data of voice using some CODEC's to .WAV files on PC's.
2	**Wired Equivalent Privacy (WEP) Key cracking**	WEP performs this crosstalk function rather well then the eavesdropping by getting packets distorted among common pathways on a wireless network. Brute force attacks, which simply break down WEP's functionality forcing errors within the protocol and eventually causing it to open a door on its own. Other algorithms exist such as the dictionary attack which is also used to crack the WEP's functionality.
3	**Evil Twin Access Point**	A valid wireless access point is blocked in this threat. Users are redirected to a second access point without knowing it, which is managed by a hacker. Any information user broadcast is accessible to the hacker. Keystrokes are also able to be captured by the hackers. This type of threat is most common in public access points, such as restaurants and airports.
4	**Access Point Phishing**	Wi-Fi phishing is similar to the evil twin threat in that it takes you to what looks like a safe access point. In this threat, hacker gets the usernames, passwords and credit card number of the user. By using regular SSIDs of public Wi-Fi spots, user's computer will automatically connect to the hacker's network.
5	**Man in the Middle**	A hacker, there are several applications available as freeware that perform the tasks necessary to execute a proper MITM attack. It will fool the server as a client and client as server and manipulate the messages sent from both sides . The hacker can redirect the information to a official host, but only after they have had extensive access to the transaction.

e) Integrity Attacks

In this attack the changes to the user's personal data are to be made by authorized users through authorized methods. In this attack, an artificial control, management or data packets are sent over the wireless network to mislead the receiver and execute the attack.

S.No	Name of Attack	Description
1	**Frame Injection**	In this attack, the hacker will infuse his/her personal packets among the transmission and expertise the original one so that it can spend fake frames. When the user tries to input its login information, it is recorded by the hacker.
2	**Data Replay**	The hacker will take the data packets into his/her supervision getting important and personal information and save it for later use by changing it.

3	**Authentication Replay**	The hacker will get the Extensible Authentication Protocol (EAP) identity and Remote Authentication Dial in User Service (RADIUS) access and keep the certification information and now monitor the traffic for another authentication. By using this authentication packets information, it will try to gain access of a system.

3. SECURING WIRELESS NETWORKS:

S.No	Name	Description
1	**Encryption**	The effective way to protect wireless network from hackers is to encrypt, or scramble, communications over the network. There have a built-in encryption mechanism in most wireless routers, access points, and base stations. Consider wireless router that have an encryption feature and getting one that does. Companies often carry wireless routers with the encryption feature turned off. User of wireless network must turn it on for security purpose.
2	**Anti-virus and anti-spyware software, and a firewall**	Computers on a wireless network required the same protection software's as any computer associated to the Internet. Always use anti-virus and anti-spyware software, and make sure that the anti virus software must be up-to-date. If users firewall was crafted in the "off" mode, turn it on.
3	**Turn off identifier broadcasting**	Most wireless routers have a device called identifier broadcasting. It sends out a signal to any device in the surrounding area broadcast its existence. User doesn't need to transmit information regarding network. Hackers can use identifier broadcasting to weak user's wireless networks. If wireless router allows then disable the identifier broadcasting device.
4	**Change the identifier on your router from the default**	The manufacturer assigned a default ID to the route as identifier. Hackers know the default IDs of user's router and can use it to try to access the network. Change your identifier to something only user know, and use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.
5	**Change router's pre-set password for administration**	The manufacturer of wireless router most likely assigned a standard default password to it that allows setting up and operating the router. Hackers know these default passwords, so change it to something only user knows.
6	**Allow only specific computers to access the wireless network**	Each workstation that is able to converse with a network is allocated its own unique Media Access Control (MAC) address. Wireless routers frequently have a method to allow only devices with particular MAC addresses access to the network.
7	**Turn off wireless network when won't use it**	Attackers cannot right to use a wireless router when it is shut down. If user turns the router off when he/she not using it, user limit the amount of time that it is vulnerable to a hack.
8	**Don't assume that public "hot spots" are secure**	Many cafés, hotels, airports, and other unrestricted organizations offer wireless networks for their customers' use.

4. CONCLUSION:

The installation of wireless access points or devices in an open environment makes the networks vulnerable. Wireless networks are increasingly being used in commercial applications, public and private sectors. Security is an important feature for the installation of access points in Wireless Networks. This paper gives a rundown of the attacks and their categorization in wireless networks and also a small effort to analyze the security system for those attacks. This survey will surely inspire next generation researchers to come up with intelligent and stronger security mechanisms and make a safer network. This paper also described various commonly available countermeasures that could be used to mitigate those risks.

REFERENCES:

1. War Driving, http://www.worldwidewardrive.org

2. B. Haines, "802.11 Wireless – Infrastructure Attacks," in Seven Deadliest Wireless Technology Attacks, T. Kramer, Ed. New York: Elsevier, 2010, ch. 1, pp. 01–05.
3. M. Gast, "Introduction to Wireless Networks," in 802.11 Wireless Networks: The Definitive Guide,1sted. New York: O'Reilly, 2002, ch. 1, pp. 01–06.
4. Security Threats of Wireless Networks: *A Survey (PDF Download Available)*. Available from: https://www.researchgate.net/publication/277465990_Security_Threats_of_Wireless_Networks_A_Survey [accessed Aug 12, 2017].
5. Cisco Systems, Inc. "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite", http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf, 2002.
6. Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).
7. McDougall, P. (2004, March 25). Laptop theft puts GMAC customers'data at risk. Information Week Security Pipeline.
8. Nokia. (2003). Man-in-the-middle attacks in tunneled authentication protocols.
9. Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.
10. Slashdot. (2002, August 18). Wardriving from 1500ft Up.
11. Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems. NIST Special Publication 800-30.
12. Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.
13. "Wireless Security Recommendations for Rutgers", http://techdir.rutgers.edu/wireless.html, November 3, 2003. [14] Vladimirov, Gavrilenko, Mikhailovsky. Wi-Foo: The Secrets of Wireless Hacking. Boston: Addison-Wesley, 2004
14. Perez, Fabian Andre. "Security in current commercial wireless networks: A survey." School of Electrical and Computer Engineering, Purdue University West Lafayette (2004).
15. Le, Tung M., Ren Ping Liu, and Mark Hedley. "Rogue access point detection and localization." Personal Indoor and Mobile Radio Communications (PIMRC), 2012 IEEE 23rd International Symposium on. IEEE, 2012.