IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

STUDY ON WIRELESS NETWORK SECURITY

Nidhi Mishra[1]
Student M.Tech(IT),IET
Dr.Rammanohar Lohia Awadh University Ayodhya(UP)

Rajesh Kumar Singh[2]
Deptt. of I.T, IET
Dr.Rammanohar Lohia Awadh Unversity Ayodhya (UP)

Rajneesh Pandey[3]
Deptt. of IT
Dr.Rammanohar Lohia Awadh University Ayodhya(UP)

ABSTRACT

This is study on wireless network security. Since wireless communication has a different form of physical transport than a wired communication environment, we have to use different measures to secure the network in a wireless environment. Wireless networks have more threats and security vulnerabilities and we need effective management for this technology.

Wireless networks have very important features, as they provide the company and the user with flexibility and portability within budget. It allows users to access networks without physical cabling tied between them.

Keywords: Wireless network; Communication wireless network ;Network security

1. INTRODUCTION

Wireless securities stop unauthorized access cause damage to computers and device using wireless networks. Today, Companies and individuals use wireless technology for important communication progressively they want to keep private and secure, such as e-commerce transactions, email, and other corporate data transmissions. Same time Wireless platforms mature, become more popular, and store Valuable information; hackers are increasing their attacks on these new goals. Security Mechanisms in Wireless Networks are required to protect and provide security for data integrity, access control, and authentication, quality of service, user privacy, and continuity of service. They also play a fundamental role in Protect wireless network functionality The popularity of wireless networks is primarily a testament to their convenience, cost Efficiency integration with other networks and it's components. The computers sold to consumers today due to security purpose . Network technology The benefits of wireless networks include convenience, mobility, Productivity, implementation, expandability, and cost.

Keywords: Wireless network; wireless technology*; Network security*

2. Wireless Vulnerabilities

A wireless network consists of four basic components: data transmission. using radio frequencies; Access points that provide a connection to the organization. the client's network and/or device (laptop, PDA, etc.); and user. each of these components provide an opportunity for attack that may result in the compromise of one or exceed the three fundamental security objectives of confidentiality, integrity and Availability.

Common vulnerabilities in wireless networks are as follows:

End users are not security experts and may not be aware of the risks that occur by wireless LANs.

Almost all access points that have default settings have not enabled WEP protection.

Most users do not change the default access point password used by all factory vendor products.

Wireless access points enabled with WEP can be easily cracked.

To access the Internet over a wireless network, the clients are connected to the access point and the AP is connected to the wireless router. The function of a wireless router is to transmit a signal over the air and all wireless clients within range can connect to the wireless network.

3. WIRELESS EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is a security standard for wireless or WiFi networks. It was part of the original IEEE 802.11 protocol. Since wireless networks transmit data over radio waves, eavesdropping on wireless data transmission is relatively easy compared to wired networks connected by cables. WEP aims to provide the same security and privacy as its wired counterparts on wireless networks.

3.1 WIRELESS EQUIVALENT PRIVACY FEATURES

WEP Features WEP was introduced in 1997 as part of the IEEE 802.11 standard. It was available for 802.11a and 802.11b devices. WEP uses data encryption to make it unrecognizable to spies. It uses RC4 for encryption, a stream cipher, and a CRC-32 checksum for confidentiality and integrity. The two most widely used standards were WEP-40 and WEP-104. In WEP-40, a 40-bit WEP key is combined with a 24-bit initialization vector to generate a 64-bit RC4 key. In WEP-104, the 104-bit WEP key is combined with a 24-bit initialization vector to generate a 128-bit RC4 key. WEP always works on data link and physical layer. It includes two authentication methods: open system certification shared key authentication In 2001–2003, critical security flaws were identified with WEP, indicating that transmitted data was susceptible to malicious changes to wireless networks. In 2004, Wireless Protocol (WPA2), the IEEE WEP-40 and WEP-104 standards.

4. Wireless Security Basics

One of the most important basic fundamentals that an individual or company should know when implementing a wireless network is the importance of frequencies. The frequencies are used by the equipment being used and depending on the specific environment affect the amount of interference the network is subject to. As has been the case over the years, there are two main frequency bands used for wireless LANs (802.11): the 2.4 GHz and the 5 GHz bands. From a security point of view, the choice of frequency does not greatly affect the measurement of network security risk. What affects the number of available non-overlapping channels on the network. this will not affect any security. That's how an attacker tries to block a particular frequency to stop wireless endpoints to change access points (APs). The endpoint devices identify wireless networks by using a Service Set Identifier (SSID) along with a set of security parameters. During the implementations of wireless, the SSID is broadcast from the APs, giving clients the ability to easily work . The most secure technology is WPA3, which was released in 2018. This standard provides two different modes of working:

This standard provides two different modes of operation:

WPA3-Personal uses a 128-bit encryption key that is communicated to both parties (AP and client) before establishing a wireless connection. It’s a secret protocol that work for key exchange security and prevent offline attacks.

WPA3-Enterprise uses 192-bit key-based encryption. It also uses a 48-bit initialization vector which guarantees a minimum level of security.

5. THREATS IN WIRELESS NETWORK

This meant that the wireless network was made vulnerable to threats from attackers.

The two kind of security attacks are here:

Active attacks

Passive attacks

In active attacks, attackers alter information content and generate false information on the network to destroy network security as unauthorized. Access, Active Eavesdropping, Man-in-the-middle Attack (MITM), Session Hijacking, Denial of Service (DoS), Replay, whereas in Passive Attack, the attacker simply listens to the network traffic, gets information from the packet, it Passive listening and traffic analysis without changing. Such attacks are hard to detect.

5.1. Unauthorized access

Unauthorized access to the Company's wired and wireless networks a can come from many various methods and intentions. one among these methods is termed "Accidental Union". When a user activates the pc and a connects to A wireless access point of a neighboring company's overlay network, the user am i able to don't even know that this happened. However, this is often a security breach within the sense that Company proprietary information has been exposed and now a could also be a link to company to a different. this is often very true if the laptop is additionally connected by cable Network.

5.2 Denial of Service (DOS)

Anyone acquainted with network security knows the concept of denial of service (DoS), also called a "spoiler." this can be one amongst the best network attacks, because it requires only limited access to services. this will be done by placing virus or worm programs on your network, or by sending large amounts of traffic to a particular target with the intention of slowing down or stopping wireless services. this enables attackers to hijack resources, view unauthorized information disclosure, and introduce backdoors into systems. In wireless networks, the signal is intercepted under various varieties of techniques. Whenever a wireless LAN uses the two.4 GHz band, interference occurred like microwave or a competing access point on similar because it is channel. Since the two.4 GHz band is proscribed to only three channels that don't overlap (in the US), an attacker only has to interfere with these enough to cause a service disruption. A denial of service attack may occur in conjunction with an unauthorized access point. for instance, it will be set to a channel that's not employed by a sound access point. A denial of service attack can then be launched on a channel that's currently in use, causing endpoint devices to do to reconnect on a unique channel that's utilized by the rogue access point.
A Denial of Service (DoS) attack occurs when an attacker continuously bombs Target AP (Access Point) or network with bogus requests, premature success Connection messages, fault messages and/or other commands. this reason is valid Users are unable to access the network and might even cause the network to hold. These attacks are supported the misuse of protocols like extensible authentication. Protocol (EAP)

5.3 Malicious Companion

"Malicious associations" are those within which hackers can actively create wireless devices. to attach to the corporate network through your laptop rather than the corporate Access Point (AP). this sort of laptop is thought as a "soft AP" and is formed when A cracker runs software that creates your wireless network card look alike valid access point. Once the cracker has reached, it can steal the password, Launch attacks on wired networks, or Plant Trojans. Therefore wireless networks work of layer 2 level, layer 3 security like network authentication and personal networks (VPNs) doesn't offer any kind of barriers . 802.1x wireless authentication helps security, but are still liable

to cracking. the concept behind this kind of attack can be you must not enter a VPN or other security measures. possibly, the cookie is Layer 2 is trying to handle the client at the amount.

5.4. Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that don't have an intermediate access point. Them. Although this kind of network has little security, encryption methods are often accustomed provide protection

5.5. Non-traditional networks

Non-traditional networks, like Bluetooth personal network devices, don't seem to be secure. against cracks and will be considered a security risk. even barcode scanners, Portable PDAs and wireless printers and copiers must be insured. Such non-traditional networks is totally moniter by IT expert who Focused on laptops and access points to prevent threats

5.6. Session Hijacking

Session hijacking is indirectly kind of like man within the middle attack (MITM) within which the attacker captures the session of the victim client [8] [11]. The victim simply assumes that their session ended for whatever reason during their session. was handed over to the attacker and he can exploit it at will. In session hijacking, the attacker first obtains the MAC address of the victim and also the AP, then sends a MAC separation message to the victim. Victim closes his session from the network while his actual session AP . is opened in

5.7. Man-in-the-middle attacks

The Man within the Middle may be a very dangerous attack within which the attacker spies on the communication and modifies it before sending it. Although the organization implemented VPN, SSH, IPsec security measures, these measures are revolutionary through the MITM attack as these measures can only protect against a knowledge privacy attack. during this way, all the user data is more matured the attacker to the Accesspoint and also the attacker can't only sniff the information but also can modify it excute the virus in download file, and then it the change web content settings easily. Techniques won't to deceive the user. Also, encryption doesn't play a security role between the access point and therefore the client user

6. Securing Wireless Transmissions

Although the WEP algorithm has several flaws, it is still possible for users to secure their respective wireless networks. To deal with the security threats mentioned above, the following techniques are recommended to reduce the security risks involved in wireless networks.

6.1. Exploring proper knowledge to user

The first step in wireless network security is to educate users about the security of the network. It is often observed that end users do not know how to implement security and leave many loopholes for attackers. Minimizing security risks is quite possible if users are well-versed about wireless tool settings/adjustments and the security of their respective networks.

6.2. Wireless Network Auditing

It is a powerful technique to secure a wireless network. The user should scan work through network scanner to know about the activities of the network. Several free network scanning software like Net Stumbler and Kismet is available over the internet.

6.3. Change the router's default password

Every wireless router/access point manufacturer sets a default username and password. If the user doesn't change it, it's a really sweet cake for the attacker because the attacker simply scans the access

point and accesses it through their default username and password, so it's highly recommended that you simply must first change the user, as an example, to the default username. and password

6.4. Change SSIDE

Each access point includes a default ID and also the attacker can easily find the access point by entering the default ID. All devices that connect with a wireless network use an identical SSID. If the user doesn't change the default SSID, it's like leaving the default password. Additionally, it's also an honest practice to vary the SSID within 30 days or earlier

7. CONCLUSION

Wireless networks offer many opportunities to extend productivity and reduce costs. It also changes the computer security risk profile of a corporation. Although it's impossible to completely eliminate all risks related to wireless technology A reasonable level of overall security will be achieved by adopting the network Systematic approach to risk assessment and management. This document discussed the risks and the vulnerabilities related to each of the three basic technology components Describes the wireless network (client, access point, and transmission medium) and various commonly available countermeasures which will be accustomed to mitigate those risks. He also emphasized the importance of coaching and educating users on secure wireless networks. Networking processes.

References

[1] Graham, E., Steinbart, P.J. (2006) Wireless Security

[2] Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.

[3] CSI. (2004). CSI/FBI Computer Crime and Security Survey.

[4] Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.

[5] Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.

[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