International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

"Viable Means Using Which Wireless Network Security Can Be Jeopardized"

Adish.N.Joshi

[1]*Undergraduate 3rd year, Department of Computer Science & Engineering,*
[2]*DRIEMS, Mumbai University,*
Mumbai, Maharashtra, India

Abstract - *As wireless networks have provided practicality they are used avidly on a humongous scale. Which brings the concern of security & integrity of data manoeuvring over this networks. Perhaps this data can be accessed by a hacker or intruder easily due to keen-high implementation of protocols. Wireless security protects the wireless network from unauthorized access but even a tiny fallacy may lead to hampering of network or even exacerbate. Irrespective of the standard encryption & protocols attacker may hack the network which culminates that these protocol & encryption secures network to a certain extent & does not provides complete security.*

Key Words: **Malicious, Hacking, Security, Encryption, Protocols, Fallacy, Unauthorized, Jeopardized.**

1. INTRODUCTION

Wireless security is forestall of illegitimate access to the network or any damage to the computer systems within the network. The main objective of wireless security is to provide utmost security to the network intern to avoid a malicious attack to the network. As such attacks can completely or partially hamper the network and the crucial data can be accessed, which is highly undesired by the secured network. According to a survey conducted in year 2016 shows a rise in cybercrimes to extremely high levels in past years creating a global security threat. Most attacks are done unknowingly due to lack of knowledge, rest are done by professional hijackers. To avoid all this vexation there are certain protocols & standards which protects network & data, but these should be properly implemented according to the need. Since past few years the WI-FI (wireless fidelity) security algorithms have gone through multiple upgradations. It is always advisable to use the latest security version. A look through over the history of Wi-Fi security versions what flaws were there in past versions and how they are eradicated in the latest version.

Different security Protocols & Encryption Standards used in wireless security are listed below:

1. Wired Equivalent Privacy (WEP).
2. Wi-Fi protected access (WPA).
3. Wi-Fi protected access (WPA2).

1.1 Wired Equivalent Privacy (WEP).

Wired Equivalent Privacy (WEP) is a security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 standard ratified in 1997, its intention was to provide data confidentiality comparable to that of a traditional wired network. WEP, recognizable by its key of 10 or 26 hexadecimal digits (40 or 104 bits), was at one time widely in use and was often the first security choice presented to users by router configuration tools. Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets. On the contrary the WEP is a very weak encryption standard as it was maliciously attacked numerous times also did it security had several fallacies in it. Initially WEP was 64-bit encryption which then was improvised to 128-bits & 256-bits. Even after such ameliorations WEP still remain vulnerable to attacks. WEP encryption is secured by using WEP KEY.A WEP key is a kind of security passcode for Wi-Fi devices. WEP keys enable a group of devices on a local network to exchange encrypted (mathematically encoded) messages with each other while hiding the contents of the messages from easy viewing by outsiders. In the year August 2001, Scott Fluhrer, Itsik Mantin, Adi Shamir researchers published a cryptanalysis of WEP that shows manner in which RC4 ciphers and IV are used in WEP, intern causing a passive attack that can recover the RC4 key after eavesdropping on the network. How severe was the network traffic, and thus accordingly the number of packets which are available for inspection, a successful key recovery could take as little as one minute. If an insufficient number of packets are being sent, there are ways for an attacker to send packets on the network and thereby stimulate reply packets which can then be inspected to find the key. The attack was quickly implemented, and automated tools since then have been released. It is possible to perform the attack with a personal computer, off-the-shelf hardware and freely available software such as air-crack-ng to crack any WEP key in minutes. After such incidents the WEP was finally discarded in the year 2004 & more advanced algorithms were implemented since then like WAP.

1.2 Wi-Fi protected access (WPA).

Wi-Fi Protected Access (WPA) is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. This authority then decided to replace WEP by WAP, as the result of serious weaknesses that researchers had found in the previous system. So WPA is outcome of failure of WEP. The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP. The most commonly used WPA is WPA-PSK (Pre-shared Key) where 256-bits of encryption as it is more efficient than 64-bits & 128-bits used in WEP. TKIP (Temporal Key Integrity Protocol) The RC4 stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.

Despite of all such security measures WPA is vulnerable to attacks TKIP being the important core component of the WPA protocol it was designed such that it could be upgraded over-the-air (OTA) firmware upgrades to the current system during which it was necessary to reprocess certain components of WEP & apparently they were exploited. Similar to WEP public demonstration was done proving the vulnerability of the WPA.

1.3 Wi-Fi protected access (WPA2).

WPA2 is an IEEE 802.11i standard which was finalized in the year 2004. The most significant advancement or enhancement in the WPA2 over WPA was the use of Advanced Encryption Standard (AES) for encryption. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. Advanced Encryption Standard (AES) technique is more secure than any other wireless protocols and standards. Another significant change that was made in WPA2 was introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP

CCMP is the encryption protocol which is used with Wi-Fi Protected Access II (WPA2) standard as it is much more secure than the Wired Equivalent Privacy (WEP) protocol and Temporal Key Integrity Protocol (TKIP) of Wi-Fi Protected Access (WPA). Data confidentiality; means that only authorized parties/personnel can access the information, Authentication; provides proof of genuineness of the user, Access control in conjunction with layer management. Primary security concerns of security of the algorithm are dubious. And the security issues of WPA2 to be jeopardized are limited to enterprise level networks and very little to no empirical consideration in home networks.

Despite of being secure it is vulnerable to attacks in the Wi-Fi Protected Setup (WPS), though breaking into a WPA /WPA2 networks using this vulnerability may require sensible amount of time approximately 2 to 14 hours of continuous effort with a modern computer having excellent hardware which can satisfy the resources required for such breaking. It is still a vulnerable aspect and WPS should be ceased for better security.

2. PRACTICES OF UNAUTHORIZED ACCESS.

There exist various methods using which malicious attacker can gain complete control over entire wireless network which are classified under “Practices of unauthorized access”. A refined attacker will always find a loophole to hack a network but the most common ways using which network can be hacked are listed below.

1. Ad-hoc networks.
2. Non-traditional network.
3. Traffic analysis.
4. Denial-Of-Service (DOS).
5. Session Interception & Message Modification.
6. Spoofing.
7. Delegation.
8. Forced De-authentication.

1. Ad-hoc networks: Ad-hoc networks are usually defined as peer-to-peer network i.e networks between wireless computers that do not have an access point in between them. In this types of networks encryption methods can be used to provide some security. The security flaw provided by the Ad-hoc networking is not the Ad-hoc network itself but the bridge it provides into the other networks. Thus the user may not even know about the insecure networks in operation on their computer. But due to convenience of the Ad-hoc networks they are used avidly.

2. Non-traditional networks: Non-traditional network includes any point to point communication example Bluetooth devices. Personal networks such as Bluetooth devices are not safe from hacking and should be regarded as security risk. Even wireless devices like barcode reader & wireless printer should be secured. As these networks are not that sophisticated can be easily trade-off buy a common man with some basic knowledge. These non-traditional networks are easily overlooked by IT personnel who have narrowly focus on laptops, office systems and access points.

3. Traffic analysis: Listening to & analysing traffic in a wireless environment is easy. In order to do this, the attacker only needs to have a device with a wireless card & listen to traffic flow through the channel. The attacker can then easily monitor the transmission of data measure the

load on wireless communication channel capture packets & read source & destination fields. By this the attacker can locate & trace user information & gain access over it.

4. Denial-Of-Service: DOS attacks are common in all kind of networks but they are particularly more threatening in the wireless context. This is because in wireless environment the attacker does not require any physical infrastructure. At same time the attacker gets the necessary anonymity very easily in a wireless environment. The attacker floods the communication server or access point with a large no of connection requests so that server responds to attacker alone. A distributed denial-of-service (DDoS) is a cyber-attack where the perpetrator uses more than one unique IP address, often thousands of them. The scale of DDoS attacks has continued to rise over recent years, by 2016 exceeding a terabit per second. This prevents the legitimate user from connecting & receiving normal network services.

5. Session Interception & Message Modification: Attacker can easily enter the wireless network & intercept a session alter the messages of session. Another attack is man-in-the-middle attack intercepts the session by inserting a malicious host between access point & end host. All the data transmissions will go through the attacker's malicious host.

6. Delegation: A delegation is a powerful mechanism to provide flexibility & dynamic access control decisions. In wireless networks as devices move from one location to another they switch connections between different types of networks. During this process they issue some kind of delegations to different network access points. The attacker can hack the device during delegation process. As in wireless networks frequent delegations take place it becomes easy for attacker to hijack the device & data apparently hampering network security.

7. Spoofing: The attacker may hijack a session & impersonate as an authorized legitimate user to gain access to unauthorized information & services. Identity theft also called as (MAC Spoofing) occurs when the attacker is able to listen the packets on the network able to identify the MAC address of the computer with network privileges. Most systems allows MAC filtering which allows only authorized user to gain access over the system.

8. Forced De-authentication: In forced de-authentication the attacker transmits packets intended to convince a communication party to drop its network connection. It then reacquires a new signal, & inserts a crook device between the original device and wireless network so forcefully legitimate user is de-authenticated & attacker gains access over network and movement of all data within network.

3. WIRELESS INTRUSION PREVENTION TECHNIQUES.

To secure a wireless network can be an extremely troublesome task for a lay man without any prior knowledge or specialized skills about network. But here are some preventive measures which can be easily taken by an individual to secure there wireless network.

1.FOR CLOSED NETWORKS :- Most common way is to restrict the access point which includes encryption & check on MAC address, these type of networks include home users & organization. Another option for closed network is to disable ESSID broadcasting, making the access point difficult to detect for outsiders. Wireless intrusion systems can be used to provide wireless LAN security.

2. FOR COMMERCIAL NETWORKS: Commercial networks providers, hotspot & large organization; the preferred solution is often to have an open and unencrypted, but completely isolated wireless network. As isolation provides additional security to the network & data within. The users will at first have no access to the Internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to require the users to connect securely to a privileged network using VPN. If the need be such that user want to share its commercial business network then setting up a guest network is advisable, It would be bad form to deny friends and relatives access to your Wi-Fi network when they're visiting. But circulating the static passphrase to everyone is bad security. Instead, set up a separate wireless network under a second SSID, a feature supported by an increasing number of wireless routers. Having a separate network for guests allows you to routinely change the passphrase without affecting your own devices. You can even disable it entirely when not in use.

4. CONCLUSIONS

It can be culminated that distinct protocols & encryption standards are not the stand-alone solutions to the increasing security threats to wireless networks. With evolving technology the security issues are also getting acute, as regardless of using such advance algorithms for security there always exists a vulnerability of network being unsecured. With the advancements in technology attackers possess all the required tools to breach the wireless network & attack the data. So to prevent such attacks an individual on the network should must be completely aware about the security standards used in wireless systems to make network more secure.

REFERENCES

[1] Kevin Beaver, Peter T. Davis, Devin K. Akin. - "Hacking Wireless Networks For Dummies".

[2] What is an ad-hoc network? - http://news.mit.edu/2011/exp-ad-hoc-0310.

[3] Wi-Fi Protected Access, What is WPA? Wi-Fi Alliance.

https://web.archive.org/web/20070521092851/http:/www.wifialliance.org/knowledge_center_overview.php?docid=4486

[4] Most probable reasons why corporate Wi-Fi clients connect to unauthorized networks-(infosecurity) https://www.infosecurity-magazine.com/opinions/comment-top-reasons-why-corporate-wi-fi-clients/

[5] Bradley Mitchell "What is Ad-Hoc mode in Wireless Networking ? https://www.lifewire.com/ad-hoc-mode-in-wireless-networking-816560

[6] What is a WEP KEY?"- https://www.lifewire.com/what-is-a-wep-key-818305

[7] How to Secure your personal & small business Wireless Network - https://www.fcc.gov/consumers/guides/how-protect-yourself-online