Pranit Patil, Prof. Dr. B B Meshram, Pranav Ambavkar/ IOSR Journal of Engineering (IOSRJEN) www.iosrjen.org ISSN : 2250-3021
Vol. 2 Issue 2, Feb.2012, pp. 315-319

Analysis of Security in Wireless Network

Pranit Patil[1], Prof. Dr. B B Meshram[2], Pranav Ambavkar[3]
[1](Mumbai, India)
[2](Mumbai, India)
[3](Mumbai, India)

ABSTRACT
Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take. Information security can be categorized in various ways like in wired and wireless security. Wireless network security differs with implementation requirement. This paper proposes survey of insecurities and security mechanism levels available in wireless networks. The proposed models for wireless networks are based on different priorities for security and simplicity.

Keywords – Information security, wireless protocols, wireless security

I. INTRODUCTION
Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

Government, military corporations, financial institutes, hospitals and private businesses have a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is collected, processed and stored on electronic computers and transmitted across networks to other computers. Most of the organization uses wireless networks as their intercommunication media, which is easy target for eavesdropper. This paper presents the introduction to information security and types of attacks and security in wireless network.

II. INFORMATION SECURITY IN WIRELESS NETWORK
Wireless networks serve the same purpose of traditional wired networks. Whenever there is mid-air data transmission, there is higher chance of interceptions and illegal uses. However higher security carries higher price tags and companies must benchmark cost against their operational needs to rip financial advantages of wireless connectivity. To secure wireless networks various types of safe guard techniques can be used. Setting down a series of security plans in view of the each loopholes of wireless network can effectively prevent the security problems such as illegal terminal access, false AP (access point), midway data interception and so on.

Types of attacks on Wireless Network:
To avoid data loss and achieve security in wireless LAN we can use various types of safeguards discussed over here.
1. Prevent unauthorized user access : Because the wireless signal transmits in the air, the signal possibly can transmits to the place that is not hoped to arrive, in the signal coverage, without any physical connection the illegal user can gain the wireless network data, therefore, we must prevent the illegal terminal to access. Each wireless adapter card has an exclusive MAC address, we can establish access control table based on MAC address access control for AP to guarantee that only the equipment which has been registered can be able to enter the network [1].
2. Prevent network neighbor attack: In some situations (especially in public situation), the privacy of user's information appears especially important. The use of AP provided with the user isolation technology may avoid the network neighbor attacks. This can be done by configuring access point in client isolation mode.
3. Illegal user intercepting: The data in wireless link: Using advanced encryption technology to make the illegal user be unable to decrypt the code even if he has intercepted the data in

wireless link. To avoid illegal user encryption such as WEP / WPA can be used.
4. Prevent illegal AP access: When wireless AP is connected with the wired concentrator, it may suffer the attack from illegal AP. Illegal AP can harm the precious resources of the wireless network; therefore we must carry on the confirmation to the AP validity. Illegal AP uses can be avoided using the validity confirmation to AP as well as regular examination to station to prevent illegal AP access .Illegal AP uses can be find out using the receiving antenna to find the unauthorized network before the intruder uses the network. We must frequently carry on the physical station monitor as far as possible.

III. LEVELS OF SECURITIES IN WIRELESS NETWORKS

We can use various types of levels according to our need of security and usability from this list.

1. Level 1 security: The first level security is basic and is built into any wireless device that can be purchased today. It is based on an algorithm called 'Wired Equivalent Privacy (WEP), which is designed to overcome most security threats. Only recipient with correct WEP key can decrypt information. WEP is also used to prevent unauthorized access to wireless network. WEP (wired equivalent privacy): It provides two security key elements (authentication and confidentiality) [2] .

WEP used a shared key mechanism and encryption using RC4 algorithm and It used CRC-32 checksum for integrity. WEP try to use four operations to encrypt the data (plaintext) at first, the secret key used in WEP algorithm is 40-bit long with 24-bit initialization vector that is concatenated to it for acting as the encryption/decryption key.
The resulting key acts as the seed for a Pseudo-Random Number Generator (PRNG). Thirdly, the plaintext throws in an integrity algorithm and concatenate by the plaintext again. The result of key sequence and ICV will go to RC4 algorithm. A final encrypted message is made by attaching the IV in front of the Cipher text. A final encrypted message is made by attaching the IV in front of the Cipher text. WEP try to use from five operations to decrypt .At first, the pre-shared key (PSK) and Iteration Vector (IV) concatenated to make a secret key. Next, the Cipher text and Secret Key go to in CR4 algorithm and a plaintext come as a result. Thirdly, the ICV and plaintext will separate. Fourthly, the plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally the new ICV (ICV') compare with original ICV.

WEP weakness: WEP does not prevent forgery of packets. WEP does not prevent replay attacks. Attackers can simply record and replay packets as desired and they will be accepted as legitimate. WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software such as 'aircrack-ng'. WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key. WEP allows an attacker to undetectably modify a message without knowing the encryption key.

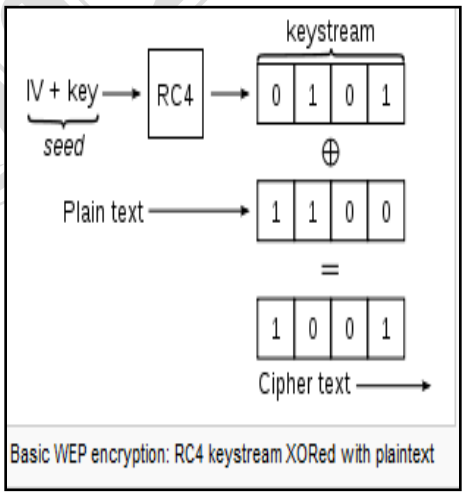

Fig.1: WEP encryption process

However there are still several outstanding security threats existing within a wireless network environment even with level 1 security.

2. Security threats in level 1 security:

2.1 Easy Access: Wireless LANs are extremely easy to find and connect if proper security measures are not implemented on the network. Attacker can intrude on the network without needing to a physical access to facility. SID (Secure System Identifiers are assigned to each wireless network) If the SSIDs are broadcasted

over the network, they might be intercepted and facilitate unauthorized access [3].

2.2 Rough access points: These are the access points installed within a company without the authorization of the network/system administrator. Access points can be easily purchased and installed anywhere. However, depending on the individual installing the access points, proper security measurements might not be implemented on the network, thereby setting up an entry point to attacker and hackers.

2.3 Eavesdropping: This implies the interception of the information being transmitted over wireless networks. Eavesdropping can be done via wireless sniffers such as airodump-ng software.

2.4 Traffic analysis: It enables gaining information about data transmission and network activity by monitoring / intercepting patters of wireless communication.

2.5 Data tampering: It describes the risk that wireless data can be captured and deleted during the course of transmission

2.6 Masquerading: It often occurs when the user attacker gains unauthorized access to the wireless networks and imitates an authorized user.

2.7 Denial of service (DoS): Attacker can block the entire frequency or bandwidth of communication channel by using strong frequency generator, thus disturbing access to the network.

3. Level 2 securities: It uses WPA (Wi-Fi protected access) WPA supports stronger network access control, better security technology and enforces data integrity. The WPA came with the purpose of solving the problems in the WEP cryptography method, without the user's needs to change the hardware. WPA is software/firmware improvement over WEP (no new hardware required).

Security Mechanism in Level 2 Security: The standard WPA similar to WEP specifies two operation manners:

3.1 Personal WPA or WPA-PSK: It's used in SOHO (small office/home office) for domestic use authentication. Personal WPA not uses an authentication server and the data cryptography key can go up to 256 bits. Keys can be any alphanumeric string and is used only to negotiate the initial session with the access points (APs). Here both the client and the AP already possess this key. WPA provides mutual authentication, and the key is never transmitted over the air.

3.2 Enterprise WPA: In this type of mode authentication is made by an authentication server 802.1x, generating an excellent control and security in the users' traffic of the wireless network. This WPA uses 802.1X+EAP (Extensible Authentication Protocol) for authentication, but again replaces WEP with the more advanced TKIP (Temporal Key Integration Protocol) encryption. Here no Pre Shared key (PSK) is used. TKIP uses the same WEP's RC4 Technique, but making a hash before the increasing of the algorithm RC4.A duplication of the initialization vector is made.

One copy is sent to the next step, and the other is hashed (mixed) with the base key. After performing the hashing, the result generates the key to the package that is going to join the first copy of the initialization vector, occurring the increment of the algorithm RC4. After that, there's the generation of a sequential key with an XOR from the text that you wish to cryptograph, generating then the cryptography text. Finally, the message is ready for send. Its encryption and decryption will performed by inverting the process.

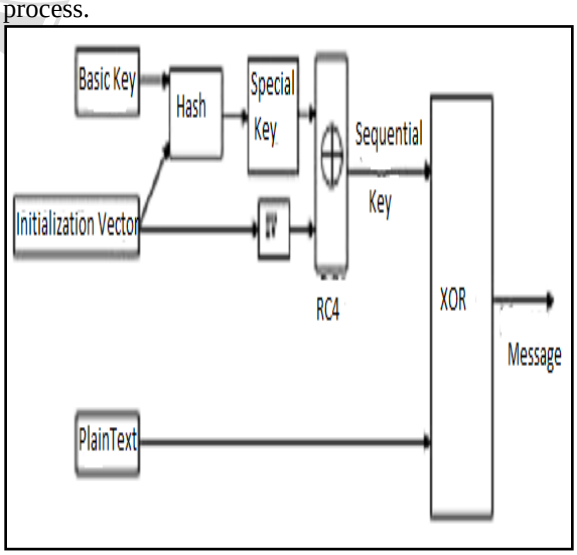

Fig.2: WPA Encryption Process

4. Security threats in level 2 security

4.1 Encryption Weaknesses: WPA has some encryption weaknesses; Therefore data

tampering and masquerading are not completely resolved by level 2 security.

4.2 Sacrificing performance: Due to intensive computations of authentication and encryption protocols, the system performance degrades and data transfers and communication speeds are dropped.

5. Level 3 Securities: Level 3 security includes 802.11i protocol. It eliminates most of the security flaws in WPA/WEP level and provides 128 bit encryption security for wireless networks. It also consists of 802.1X authentication and key management protocols. In this protocol generally, a successful authentication means that the supplicant and the authenticator verify each other's identity and generate some shared secret for subsequent key derivations. Based on this shared secret, the key management protocols compute and distribute usable keys for further data communication sessions.

Security Mechanism in Level 3 Security: WPA2 protocol is mainly used in this level of security. WPA2 provides stronger encryption mechanism through Advanced Encryption Standard (AES), which is requirement for some corporate and government users. Likewise WPA, WPA2 also offers both Personal pre shared key (PSK) and Enterprise modes. WPA2 requires hardware up gradation in router and or access points due to extensive computations in encoding and decoding frame is AES encryption. However , there is performance decrease occurs when every time user attempts to perform a transaction, as network runs scripts to perform security checks and encryption, thus slowing down the data transfer rate [7].

When we think about information security, we refer security breach by intruders and we falsely believe on authenticated users within our network but hardly anyone thinks about inside attackers.

IV. RECENTLY DISCOVERED INSECURITIES IN WIRELESS NETWORK

Recently discovered 'hole 196' vulnerability in WPA2 security protocol exposed WPA2-secured Wi-Fi networks to insider attacks. This allows insiders to send group addressed data traffic encrypted using Group Temporal Key. This data traffic only supposed to send by Access point and not by client nodes .But if malicious insider sends this GTK traffic, he/she can able to update other nodes ARP cache with help of ARP request broadcasted with GTK. This allows that insider to sniff all private data of user.

V. FACTORS CONSIDERED WHILE DESIGNING OF WIRELESS NETWORKS

In order to design a secure wireless network, we need to consider below factors when erecting the wireless network.

1. Pay attention to the physical location of Access Point: The wireless signal is disseminates in the air, its boundary certainly does not look to be clear as the wired network; the signal can exist outside the specific coverage at any moment. In the view of the physical security, the position of AP needs to be measured through special purpose instrument. We must reduce the possibility that wireless signals divulge outside the network coverage as far as possible [5].
2. Access Point control and Management: When there are many APs in a wireless network, how to carry on the management and the monitoring to these APs appear to be extremely important. If there does not have a reasonable effective AP management system, it will cause the network security gap and give an opportunity to the intruder to break in.
3. The user identification authentication: When designing wireless network, we must consider the authentication and authorization of the wireless network accessing to the wired network resources. IT network administrators of enterprise may integrate the wireless local area network into the already existed RADIUS construction to simplify the user management. It also helps to authenticate remote users of large scale companies.

VI. CONCLUSION

Wireless network security in telecommunication sector in one of the most important area in the information security. As day by day increasing users of wireless network technologies exposes increased risks of data theft and forging so it becomes urge need to secure any kind of communication methods either wired or wireless becomes very important. Methods used and

described in this paper can be used by various types of user levels and expertise to achieve information security in wireless networks at desired level. Also newly discovered insecurities are also discussed to show various types of insecurities still present in the security mechanisms.

REFERENCES

1) Analyze of Application Schemes for the Wireless Network Security by Quihua Wang and Jianwu Zhang.
2) Wireless network security – A discussion from a business perspective by Ankush Karnik and Katia Passerini
3) http://interscience.in/IJSSAN_Vol1Iss1 /paper25.pdf
4) http://www.cse-cst.gc.ca/its-sti /publications/itspsr-rpssti/itspsr21a-eng.html
5)http://www.airtightnetworks.com/WPA2-Hole196.
6)http://www.wifi.org/knowledge_center/ wpa2
7) An Integrated Security model for WLAN by Ondiwa Odhiambo, E. Biermann and G.Noe

IOSRJEN