# Security and privacy in wireless LAN

First Author: Raunak Joshi, Department of Computer Engineering,
PVPIT, Pune University, India, E-mail: raunakjoshi007@gmail.com

**Abstract**—. Wireless data networks have spread between home users and companies in an increasing fashion. The main reason behind this fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lack. The increasing of bandwidth capabilities has inspired people to think seriously about replacing wired networks with wireless networks especially in places where it is hard or expensive to have wired networks. One of the main places that can benefit from these ideas are rural areas, where wired networks infrastructure is either difficult or impossible to create due to physical obstacles.
With continual advances in technology, coupled with increasing price/performance advantages, wireless accessibility is being deployed increasingly. This topic discusses the security threats and risks associated with wireless networks, and outlines a number of best practices for deploying wireless networks and home Finally, a set of security tips is provided for end-users surfing the Internet using wireless networks.

**Index Terms**— Wireless, LAN, Protocols, Threats , Attacks.

## 1 INTRODUCTION

Security in computer world determines the ability of the system to manage, protect and distribute sensitive information. Data Security was found many years before the advent of wireless communication due to the mankind's need to send information (in war or in peace time) without exposing its content to others. The first and most known machine (Enigma) was used in WWII by the German military to encrypt their messages. The machine was something similar to a simple typing machine with a scrambler unit to obfuscate the content of the messages . From that time till now, many solutions to security threats have been introduced, and most of them were abandoned or replaced by better security standards. These ongoing changes promoted the security field to be a permanent hot topic. In the wireless world security threats were not known to public people till prices of wireless equipment went down around 2000. Before that date, the military was the number one client for wireless security products especially during the cold war.. This report aims to give a better understanding of security measures and protocols available in the market, along with a brief analysis of each security scheme's weaknesses and points of strength. This report starts with an introduction to security and privacy wireless worlds to give the right background for understanding the evolution of security standards. Chapter 3 gives a brief description about security standards in wireless LANs. Section 4 describes WMAN 802.16 protocol and the current security schemes used with it. Thoughts on wireless security section (Chapter 5) explores some of the practical suggestions to increase the level of network security. Since security in wireless networks is still a working progress, Chapter 6 discusses one of the recent proposals to enhance current security standards, a protocol called PANA (Protocol for carrying Authentication for Network Access). Finally, chapter 7 concludes this paper.

## 2 SECURITY AND WIRELESS OVERVIEW

An overview of security and wireless communications is presented in this section. Although this introduction will not cover all the aspects of both worlds, it will give a descent amount of information that allows the reader to go through the paper without the necessity of referring to other books or papers. Section 2.1 gives a crash course in security for both wired and wireless worlds. Section 2.2 describes the current wireless systems and infrastructures. Finally, a list of the common security threats and attacks are discussed in section 2.3.

### 2.1 Introduction to Security

This section outlines some of the basic conceptions in the security world. It starts by defining the goals behind implementing security in the computer world (Section 2.1.1). Then it discuss encryption and decryption concept (Section 2.1.2), the implementation of both block and stream ciphers (Section 2.1.3), and finally a brief description of the most common encryption standards.

#### 2.1.1 Security Goals

Every security system must provide a bundle of security functions that can assure the secrecy of the system. These functions are usually referred to as the goals of the security system. These goals can be listed under the following five main categories:

Authentication: This means that before sending and receiving data using the system, the receiver and sender identity should be verified.

Secrecy or Confidentiality: Usually this function (feature) is how most people identify a secure system. It means that only the authenticated people are able to interpret the message (date) content and no one else.

Integrity: Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.

Non-Repudiation: This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.

Service Reliability and Availability: Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

2.1.2 Data Encryption: Symmetric and Asymmetric Encryption

To send data securely between two nodes, the system must encrypt the data or "systematically scramble information so that it cannot be read without knowing the coding key".This operation determines to a certain level the strength of the security system, the harder it is to break the encrypted message the more secure the system is to be. Figure 1 shows the common use of encryption/decryption techniques, where unsecured messages (plain text) are encrypted using a special encryption technique, sent over the network, then decrypted at the destination to viewed back as unencrypted messages.

Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data. These two categories are: Asymmetric and Symmetric encryption techniques.

Symmetric Encryption

In this type of encryption, the sender and the receiver agree on a secret (shared) key. Then they use this secret key to encrypt and decrypt their sent messages. Fig. 2 shows the process of symmetric cryptography. Node A and B first on the encryption technique to be used in encryption and decryption of communicated data. Then they agree on the secret key that both of them will use in this connection. After the encryption setup finishes, node A starts sending its data encrypted with the shared key, on the other side node B uses the same key to decrypt the encrypted messages.

The main concern behind symmetric encryption is how to share the secret key securely between the two peers. If the key gets known for any reason, the whole system collapses. The key management for this type of encryption is a troublesome, especially if a unique secret key is used for each peer-to-peer connection, then the total number of secret keys to be saved and managed for n-nodes will be n(n-1)/2.

Asymmetric Encryption

Asymmetric encryption is the other type of encryption where two keys are used. To explain more, what Key1 can encrypt only Key2 can decrypt, and vice versa. It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is know to the public, and private key which is known only to the user. Figure 3 below illustrates the use of the two keys between node A and node B. After agreeing on the type of encryption to be used in the connection, node B sends its public key to node A. Node A uses the received public key to encrypt its messages. Then when the encrypted messages arrive, node B uses its private key to decrypt them.

This capability surmounts the symmetric encryption problem of managing secret keys. But on the other hand, this unique feature of public key encryption makes it mathematically more prone to attacks. Moreover, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques, because they require more computational processing power.

To get the benefits of both methods, a hybrid technique is usually used. In this technique, asymmetric encryption is used to exchange the secret key, symmetric encryption is then used to transfer data between sender and receiver.

2.1.3 Block and Stream Ciphers

Another categorization method for encryption techniques is commonly used based on the form of the input data they operate on. The two types are Block Cipher and Stream Cipher. This section discusses the main features in the two types, operation mode, and compares between them in terms of security and performance.

Block Cipher

In this method data is encrypted and decrypted if from of blocks. In its simplest mode, you divide the plain text into blocks which are then fed into the cipher system to produce blocks of cipher text.

There are many variances of block cipher, where different techniques are used to strengthen the security of the system. The most common methods are: ECB (Electronic Codebook Mode), CBC (Chain Block Chaining Mode), and OFB (Output Feedback Mode). ECB is the basic form of clock cipher where data blocks are encrypted directly to generate its correspondent ciphered blocks (shown in Fig. 4). CBC mode uses the cipher block from the previous step of encryption in the current one, which forms a chain-like encryption process. OFB operates on plain text in away similar to stream cipher that will be described below, where the encryption key used in every step depends on the encryption key from the previous step

Stream Cipher

Stream cipher functions on a stream of data by operating on it bit by bit. Stream cipher consists of two major components: a key stream generator, and a mixing function. Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique. For example, if the key stream generator produces a series of zeros, the outputted ciphered stream will be identical to the original plain text.

To start the series of Key Stream, an Initialization Vector (IV) is sent to set the initial value. A common IV between the sender and the receiver is usually imposed to keep both of them synchronized. The IV can be auto-generated or incremented on each packet, which depends on the capabilities of the system.

The stream cipher technique can be categorized into two modes: Synchronous Stream Cipher, and Self-Synchronizing Stream Cipher. In Synchronous Stream Cipher the Key Stream Generator depends only on the base key used for encryption. Fig.5 Show how Sync. Stream Mode (the "simple" mode) operates on the both sender and receiver sides. The sender uses only the base (shared) key to encrypt the outgoing stream, on the other side the receiver decrypts the stream using the same key. The main disadvantage of this method is that if the base key gets known the whole system is compromised.

The other mode is called Self-Synchronizing Stream Cipher. In this mode, the state of Key Stream Generator (the Key Used for that

instant of time) depends on the previous states of cipher text bits. The previous states number is fixed and defined by the algorithm. Self-Synchronizing method is more secure than the previous mode, but it is slower. Fig 6 below shows the process undertaken by self-synch stream cipher to encrypt/decrypt data.

Fig.6 Stream Cipher : Self-Synch. Mode

Stream cipher has a well known advantage over block cipher because of its speed and simplicity of analysis. But in the same time it is a known fact that stream cipher is less secure than block cipher. That's why most of the recommendation of today's standards recommends using block cipher techniques over stream cipher ones

2.1.4 Data Encryption Standards: DES, AES and RC4

After taking a quick look at the major classification of data ciphers (both stream and block ciphers). In this section we will describe briefly some of the well known and used encryption standards. Moreover we will mention the key features and disadvantages of each standard .

DES

DES (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology). It is based on the IBM proposed algorithm called Lucifer. DES became a standard in 1974 . Since that time, many attacks and methods recorded that exploit the weaknesses of DEC, which made it an insecure block cipher. As an enhancement of DEC, the3DEC (Triple DES) encryption standard was proposed. In this standard the encryption method is similar to the one in original DES but applied 3 times to increase the encryption level. But it is a known fact that 3DES is slower than other block cipher methods.

AES

AES (Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES. Rijndael (pronounced Rain Doll) algorithm was selected in 1997 after a competition to select the best encryption standard. Brute force attack is the only effective attack known against it, in which the attacker tries to test all the characters combinations to unlock the encryption. Both AES and DES are block ciphers.

RC4

RC4 or ARC-Four is the most widely used stream cipher. It is used with SSL (Secure socket Layer), which is used to secure identification information and money transfers over the Internet. Moreover, it is used in WEP (Wired Equivalent Privacy) which is responsible for securing wireless data. RC4 showed that is secure enough for certain systems, but it was found out that it does not offer that level of security to wireless communications, making it fall short for many security standards.

2.2 Introduction to the Wireless World

Wireless data networks have spread between home users and companies in an increasing fashion. The main reason behind this fast adaptation is due to the nature of wireless networks where it provides the flexibility and freedom that wired networks lack. The increasing of bandwidth capabilities has inspired people to think seriously about replacing wired networks with wireless networks especially in places where it is hard or expensive to have wired networks. One of the main places that can benefit from these ideas are rural areas, where wired networks infrastructure is either difficult or impossible to create due to physical obstacles.

The main standards in the wireless world are: 802.11, which describes the Wireless LAN architecture, and 802.16 which describes the Wireless MAN architecture. These two wireless networks are usually known by two acronyms: WiFi (Wireless Fidelity) to be a symbol of WLAN, and WiMAX (Worldwide Interoperability for Microwave Access) to describe WMAN.

2.2.1 Wireless LAN (WLAN)

Fig.7 Wireless LAN

Wireless LAN is simply trying to imitate the structure of the wired LANs, using another medium to transfer data rather than cables. This medium is electromagnetic waves which are mainly either radio frequency (RF) or infrared frequency (IR).

Wireless LANs consist mainly of two entities: clients or end-user devices and Access Points (AP). Clients' are equipped with devices that allow the user to use the RF medium to communicate with other wireless devices. AP functions like a regular switch or router in wired network for the wireless devices. Moreover, it represents a gateway between the wireless devices and a wired network.

The basic structure of a Wireless LAN is called BSS (Basic Service Set) shown in Fig. 8, in which the network consists of an AP and several wireless devices. When these devices try to communicate among themselves they propagate their data through the AP device. In order to form the network, AP keeps broadcasting its SSID (Service Set Identifier) to allow others to join the network.

If the BSS did not have an AP device, and the wireless devices were communicating with each other directly, this BSS is called an Independent BSS and works in mode called "ad hoc mode" (shown in Fig.9). Group of BSSs (either BSS or IBSS) can be combined to form an ESS (Extended Service Set). This set is created by chaining this group of BSSs to a single backbone system.

2.2.2 Wireless MAN (WMAN)

The idea behind using WMAN is to offer a broadband Internet service using wireless infrastructure. The idea is very similar to a TV broadcast network (shown in Fig.10). The theoretical speed of WMAN is 75Mbps extended to several miles, which offer a replacement to cable and DSL connections in the future.

WMAN is also called BWA (Broadband Wireless Access) as a formal title along with the industry icon acronym WiMAX. The main target of implementing WiMAX technology is to provide a convenient solution to the "last mile access", where the fast data backbone traffic is to be distributed among consumers. This also helps expand the Internet covered areas especially in rural areas.

2.3 Security Attacks

As mentioned before, the main difference between wired and wireless networks is the medium it transfers its data through. This difference made the burden of securing the network heavier. The broadcast nature of wireless networks makes it easy for everyone to attack the

network if not secured, due to the absence of physical barriers, where the range of wireless transmission ranges from 300 ft to half a mile .

The exponential growth of wireless networks add another obstacle on enhancing the network security. People tend to keep things the way they are instead of doing what is right. Also such enhancement of security is expensive in terms of time, money and effort that many users do not have or wish not to spend.

Below is a list of the most common attack types known in both wired and wireless networks. Most of the security attacks and threats are listed under the following categories:

Traffic Analysis

In this type of attacks the attacker uses the statistics of network connectivity and activity to find information about the attacked network. Information includes: AP location, AP SSID and the type of protocol used by the analysis of size and types of packets.

Passive Eavesdropping

Attackers in this type set themselves in sniffing mode, where they listen to all the network traffic hoping to extract information from it. This type of attack is only useful with unencrypted networks and stream cipher encrypted ones.

Active Eavesdropping

Similar to passive eavesdropping but the attacker tries to change the data on the packet, or to inject a complete packet in the stream of data.

Unauthorized Access

This type of attack is also known by many other names, such as war driving, war walking, and war flying.This is the most common attack type where the attacker tries to get access to a network that she is not authorized to access. Mainly the reason behind such attacks is just to get Internet access for free .

Man-in-the-middle Attacks

In this attack, the attacker gets the packets before the intended receiver does. This allows her to change the content of the message. One of the most known subset of this attack is called ARP (Address Resolution Protocol) attacks, where the attacker redirects network traffic to pass through her device.

Session High-Jacking

The attacker attacks the integrity of the session by trying to hijack an authorized session from an authorized user.

In this paper we reviewed how security and privacy in wireless data networks has evolved over the last years. We have discussed also how the difference in the data transfer medium between wired and wireless networks plays a key role in exposing the system to more possible attacks. Security hazards will always be around, they can only be avoided if the correct policies and standards are used. The 802.11i protocol promises to fix most of the security holes found in its predecessor WEP, but since the standard is relatively new, it did not have the proper period of time to be tested thoroughly. Only the future can tell us if the current standards are secure as they promise. Moreover, we mentioned some of the ways that can be utilized to improve the security of the wireless networks. PANA the new protocol proposed to work as a messaging protocol between network clients and network access authority was discussed . Security still evolves and it will remain a hot topic as long as there are ways to threaten data security.

Replay Attacks

In this type of attack the attacker uses the information from previous authenticated sessions to gain access to the network.

Rouge AP

Some of the devices allow the user to declare itself as an AP. This will make people confused and sometimes they may connect to this false AP exposing their information to it. This can be solved by imposing mutual authentication between AP and network devices.

DoS Attacks

DoS (Denial of Service) attacks are the hardest type of attacks to overcome. Attackers use frequency devices to send continuous noise on a specific channel to ruin network connectivity. It is known in the wireless world as RF Jamming .

There are many other threats that can be placed under one of the categories above. These different types of attacks make it harder for the standard regulators to find the best way to come up with the best solutions to the security hazards without sacrificing network usability or speed. In this section we discussed the common concepts in security, the wireless world and the common security attacks against networks in both wired and wireless networks. This section should have provided enough information to go through the following sections.

## 3 CONCLUSION

## Acknowledgments

First of all my sincere gratitude to HOD Prof.Y.B.Gurav, for his constant encouragement. Also thank I Prof Y. P. MURUMKAR, I am extremely grateful and indebted to him expert, sincere and valuable guidance and encouragement extended to me. I also take this opportunity to record my sincere thanks to all the faculty members of the department of Computer Engineering for their help and encouragement. I also place a record, my sense of gratitude to one and all who, directly or indirectly, have lent their helping hands in this venture.

## References

1. [Chandra2005]," BULLETPROOF WIRELESS SECURITY : GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering) ,". Newnes 2005
2. [Imai2006]," Wireless Communications Security ,". Artech House Publishers 2006
3. [Welch2003] "Wireless security threat taxonomy,". Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 - 83

IJSER

4. [Edney2003]," Real 802.11 Security: Wi-Fi Protected Access and 802.11i ,". Addison Wesley 2003
5. [Earle2005] "Wireless Security Handbook,". Auerbach Publications 2005
6. [Hardjono2005]," Security In Wireless LANS And MANS ,". Artech House Publishers 2005
7. [Rittinghouse2004]," Wireless Operational Security ,". Digital Press 2004
8. [Prasad2005]," 802.11 WLANs and IP Networking: Security, QoS, and Mobility ,". Artech House Publishers 2005
9. [Manley2005] "Wireless security policy development for sensitive organizations,".Systems, Man and Cybernetics (SMC) Information Assurance Workshop, 2005. Proceedings from the Sixth Annual IEEE 15-17 June 2005 Page(s):150 - 157.
10. [Arbaugh2003] "Wireless security is different,". Computer Volume 36, Issue 8, Aug. 2003 Page(s):99 - 101
11. [Potter2003] "Wireless security's future,". Security & Privacy Magazine, IEEE Volume 1, Issue 4, July-Aug. 2003 Page(s):68 - 72
12. [Osorio2005] "Measuring energy-security tradeoffs in wireless networks,". Performance,Computing, and Communications Conference, 2005. IPCCC 2005. 24th IEEE International 7-9 April 2005 Page(s):293 - 302
13. [Johnston2004] "Overview of IEEE 802.16 security,". Security & Privacy Magazine, IEEE Volume 02, Issue 3, May-June 2004 Page(s):40 - 48
14. [Ravi2002],"Securing Wireless Data: System Architecture Challenges", in Proc. Intl. Symp. System Synthesis, pp. 195--200, October 2002
15. [Hole2005] "Securing Wi-Fi networks,". Computer Volume 38, Issue 7, July 2005 Page(s):28 - 34
16. [Chen2005] "Wireless LAN security and IEEE 802.11i,". Wireless Communications, IEEE Volume 12, Issue 1, Feb. 2005 Page(s):27 - 36
17. [Brown2003] "802.11: the security differences between b and i ,". " Potentials, IEEE Volume 22, Issue 4, Oct-Nov 2003 Page(s):23 - 27"
18. [Barbeau2005] "WiMax/802.16 threat analysis,". International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems
19. [Viega2005] "Security---problem solved? ,".Queue Volume 3 , Issue 5 (June 2005) Security: a war without end
20. [WirelessLAN]; Wireless LAN ," http://cnscenter.future.co.kr/hot- topic/wlan.html [ This page sums up all the organizations, papers, resources, … etc related to WLAN ]
21. [Unofficial802.11]" The Unofficial 802.11 Security Web Page ," http://www.drizzle.com/~aboba/IEEE/ [ This page tries to gather relevant papers and standards to 802.11 Security in a single place. ]
22. [CITA]" CTIA : Wireless Internet Caucus: Standards & Tech ," http://www.wirelessenterpriseinfo.org/wic/standardsandtech.htm [ Links to all groups that have been involved in the identification and development of standards and requirements for mobile data solutions ]
23. [WiFiPlanet] " Wi-Fi Planet ," http://www.wi-fiplanet.com/ [ The Source for Wi-Fi Business and Technology]
24. [ITtoolbox]" ITtoolbox Security Knowledge Base ," http://security.ittoolbox.com/ [ ITtoolbox Security Knowledge Base provides the latest community-generated content from the IT market. Share knowledge with your peers and work together to form experience-based decisions. ]
25. [Enigma]. "Enigma Machine", http://homepages.tesco.net/~andycarlson/enigma/about_enigma.html [Description about Enigma Machine and how it works]
26. [NIST98] "Security History", http://csrc.nist.gov/publications/history/ [Group of papers that explain security history in computer world]
27. [Sabc] "Glossary Terms", http://www.sabc.co.za/manual/ibm/9agloss.htm [Definition of security]
28. [TropSoft] "DES Overview", http://www.tropsoft.com/strongenc/des.htm [Explains how DES works in details, features and weaknesses]
29. [Cohen2003] "802.16 Tutorial" http://www.wi-fiplanet.com/tutorials/article.php/3068551 [Tutorial about 802.16 standard and about its security features]

IJSER

30. [WarDrive] "War Driving Tools", http://www.wardrive.net/wardriving/tools/ [War driving tools to hack/test wireless networks for different OSes]
31. [bbwexchange] "WPA2 Routers List". http://www.bbwexchange.com/publications/newswires/page546-1160883.asp [contains a list of the WPA2 routers from different companies]
32. [Wireless80211] "802.11 standards" , http://compnetworking.about.com/cs/wireless80211/a/aa80211standard.htm [Describe briefly 802.11 standards and their specifications]
33. [startawisp] " Shared vs Open authentication method", http://www.startawisp.com/index2.php?option=com_content&do_pdf=1&id=147 [Explains why shared Authentication is considered less secure than open authentication]
34. [RFC3748] "Extensible Authentication Protocol (EAP)", http://www.ietf.org/rfc/rfc3748.txt [RFC draft for EAP]
35. [EAPOL] "EEE 802.1X: EAP over LAN (EAPOL) for LAN/WLAN Authentication&Key Management",http://www.javvin.com/protocol8021X.html [Explanation of 802.1x, EAPOL]
36. [RADIUS],"RADIUS - Wikipedia, the free encyclopedia",http://en.wikipedia.org/wiki/RADIUS [Wikipedia definition and related resources about RADIUS]
37. [WPA],"Wi-Fi Protected Access - Wikipedia,", http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access. [Wikipedia definition and related resources about WPA]
38. [TKIP],"TKIP - Wikipedia", http://en.wikipedia.org/wiki/TKIP . [Wikipedia definition and related resources about TKIP]
39. [Microsoft-WPA] "Overview of the WPA wireless security update in Windows XP", http://support.microsoft.com/?kbid=815485 [Explains the security features in WPA]
40. [Tech-FAQ] "What is MIC ?", http://www.tech-faq.com/mic-message-integrity-check.shtml [Short definition for MIC and how it works]
41. [Tech-FAQ2] "What is WRAP ?",http://www.tech-faq.com/wrap-wireless-robust-authenticated-protocol.shtml , [Explaining why WRAP is not the recommended data transfer encryption standard for 802.11i]

IJSER

IJSER