Security in Wireless Data Networks: A Survey Paper

Abdel-Karim R. Al Tamimi

abdelkarim.tamimi@gmail.com

Abstract

Both security and wireless communication will remain an interesting subject for years to come. They represent the need of ease of use and flexibility of communications in the computer world without jeopardizing the communicated content. This paper illustrates the key concepts of security, wireless networks, and security over wireless networks. Wireless security is demonstrated by explaining the main specifications of the common security standards like 802.11 WEP, 802.11 WPA and WPA2 (802.11i). Moreover, it explains the concept of WMAN (Wireless Metropolitan Access Network) and its security specifications. Finally, it sums up with thoughts and suggestions about wireless security, along with a chosen example of the current proposals in wireless security.

See Also: In-Building Wireless LANs , Recent Advances in Wireless Data Networking , IP Security : A Brief Survey

---

Table of Contents:

- 1. Introduction
- 2. Security and Wireless Overview
    - 2.1 Introduction to Security
        - 2.1.1 Goals
        - 2.1.2 Symmetric and Asymmetric Encryption
        - 2.1.3 Block Cipher and Stream Cipher
        - 2.1.4 DES, AES and RC4
    - 2.2 Introduction to The Wireless World
        - 2.2.1 Wireless LAN (WLAN)
        - 2.2.2 Wireless MAN (WMAN)
    - 2.3 Security Attacks
- 3. Security in WLAN (802.11)
    - 3.1 Introduction to 802.11 Standard
    - 3.2 WEP
    - 3.3 WEP Weaknesses

  - 3.4 802.1x: EAP Over LAN (EAPOL)
  - 3.5 Security in 802.11i
  - 3.6 RSN
- 4. Security in WMAN (802.16)
  - 4.1 Protocol Layers
  - 4.2 Security Concerns
- 5. Thoughts on Wireless Security
  - 5.1 Best Practices
  - 5.2 Security Policy
  - 5.3 Security … Problem Solved?
- 6. Recent Proposals
  - 6.1 PANA
- 7. Summary
- References
- List of Acronyms

Back to Table of Contents

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 [Enigma] [NIST98].

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.[Edney2003] [Hardjono2005]

This paper 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 paper starts with an introduction to security and wireless worlds to give the right background for understanding the evolution of security standards. Section 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 (section 5) explores some of the practical suggestions to increase the level of network security. Since security in wireless networks is still a working progress, section 6 discusses one of the recent proposals to enhance current security standards, a protocol called PANA (Protocol for carrying Authentication for Network Access). Finally, section 7 concludes this paper.

Back to Table of Contents

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[Earle2005][Imai2006]:

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" [Sabc]. 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.

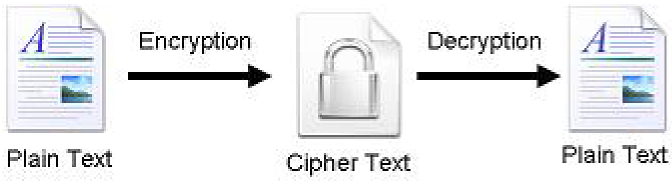


Fig.1 Data Encryption and Decryption

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.

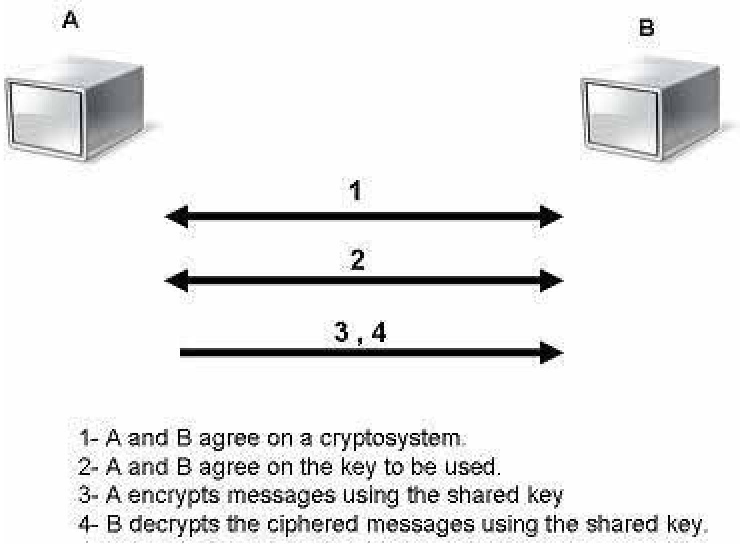
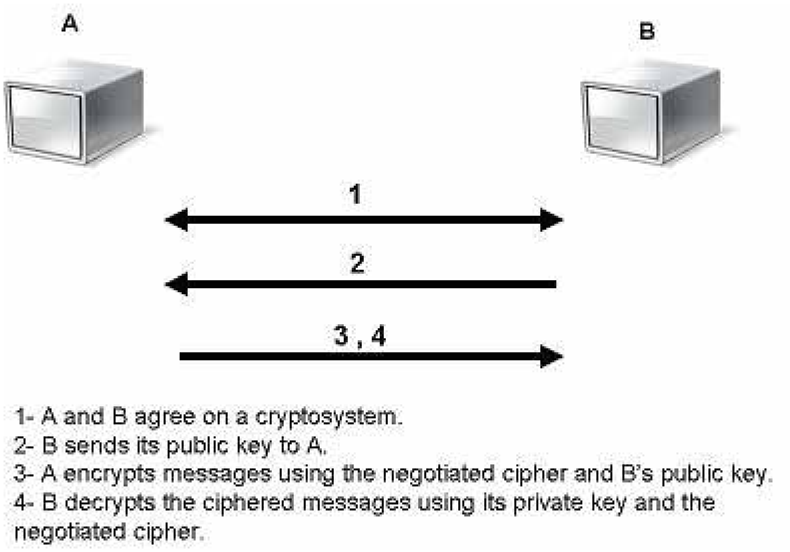

A
B
1
2
3 , 4
1- A and B agree on a cryptosystem.
2- A and B agree on the key to be used.
3- A encrypts messages using the shared key
4- B decrypts the ciphered messages using the shared key.

Fig.2 Symmetric Encryption

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 [Edney2003] .

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.



1- A and B agree on a cryptosystem.
2- B sends its public key to A.
3- A encrypts messages using the negotiated cipher and B's public key.
4- B decrypts the ciphered messages using its private key and the negotiated cipher.

Fig.3 Asymmetric Encryption

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[Edney2003] [Hardjono2005] .

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[Chandra2005] [Edney2003] .

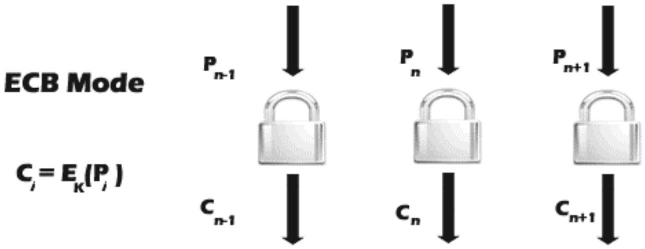


Fig.4 Block Cipher : ECB MODE

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.

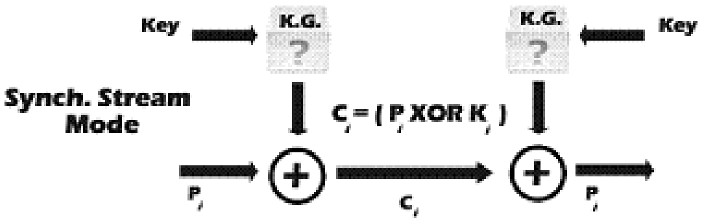


Fig.5 Stream Cipher : Simple Mode

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.

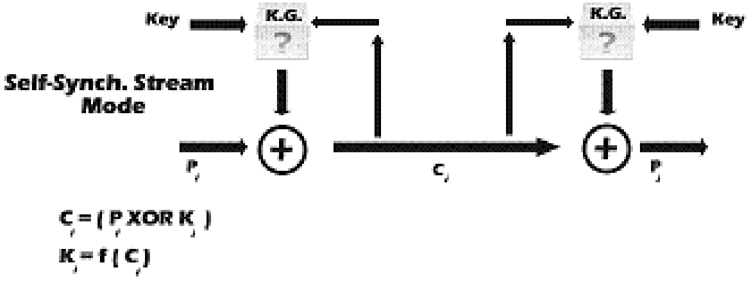


Fig.6 Stream Cipher : Self-Synch. Mode

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 [Chandra2005] .

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 [TropSoft] . 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 [Chandra2005] .

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.

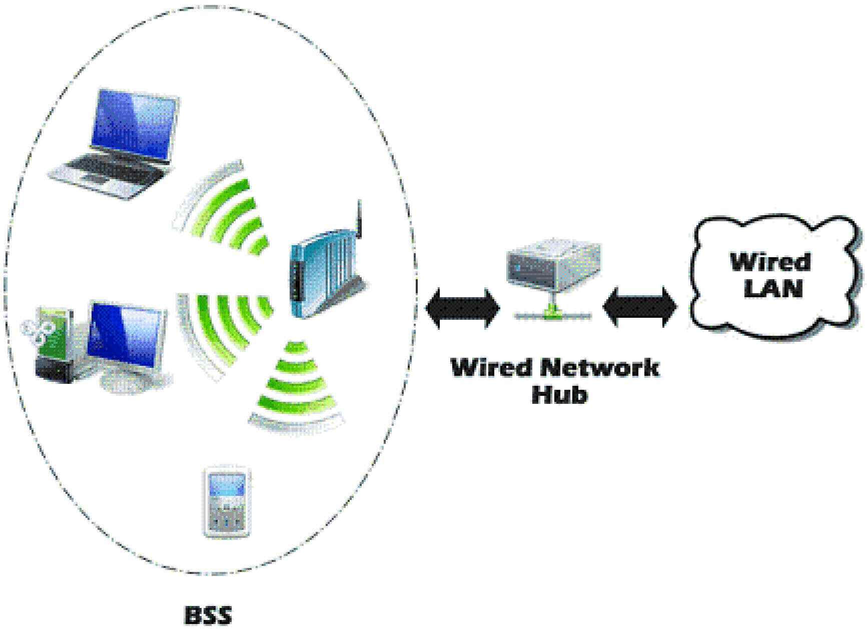


Fig.8 WLAN : BSS Structure

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.

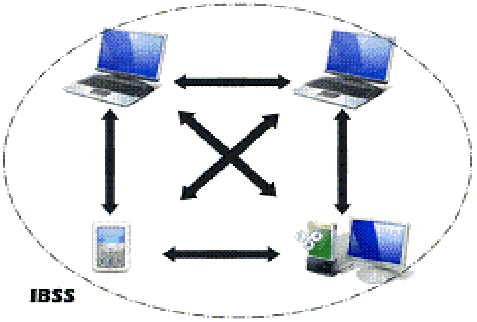


Fig.9 WLAN : IBSS Structure

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[Hardjono2005] .

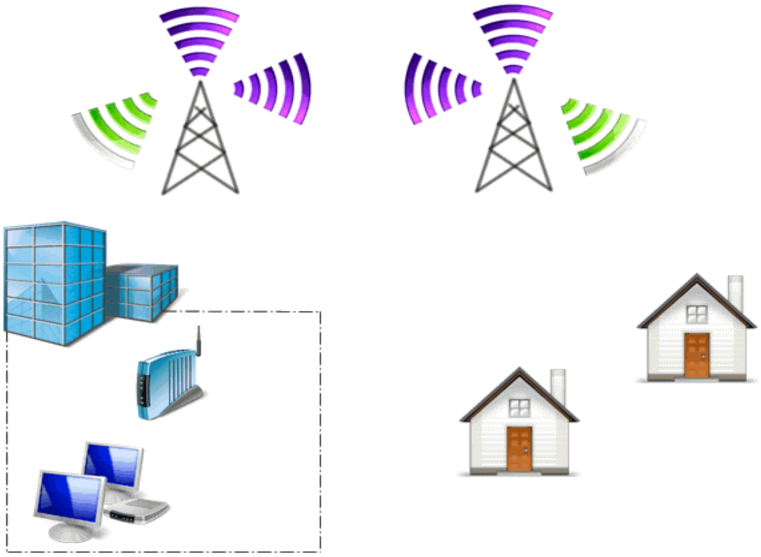


Fig.10 Wireless MAN

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 [Arbaugh2003] .

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[Welch2003] .

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[Earle2005] . 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[Potter2003] .

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[Welch2003] .

Session High-Jacking

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

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 [Welch2003] .

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.

Back to Table of Contents

3. Security in WLAN 802.11

In this section, we will go through the steps wireless LAN security took to achieve its current status of implementing 802.11i security protocol . First we will talk about the difficulties faced in creating the standard, then describe the standard 802.11 itself. After that we will take a journey through the different security modules that have been proposed to solve the security issues related to wireless networks starting from WEP and ending with WPA2.

Wireless media is more difficult to secure because of its broadcast nature[Arbaugh2003] . This property makes creating a well secured protocol that is similar to wired security modules a very hard task. In addition to that, mobile units that use wireless security protocols differ from regular PCs in many aspects. There are constraints related to processing power, battery capacity, and flexibility to facilitate inter-operability. In addition to that, there is a need for tampering proof techniques in case mobile units fall into the hands of malicious entities [Ravi2002] .

3.1 802.11 Standard

The 802.11 IEEE standard was standardized in 1997. It consists of three layers: Physical layer, MAC (Medium Access Control) layer, and LLC (Logical Link Control) layer (Fig.

11). The first version of the standard supported only 2 Mbps bandwidth, which motivated the developing teams to come up with other standards to support up to 54Mbps.

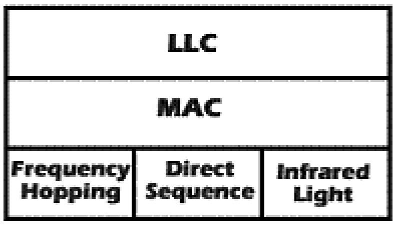


Fig.11 802.11 Layers

Designers took into consideration the necessity of making the physical layer supports more than one signaling technique and interface, as shown in Fig. 11 above. The physical layer is responsible for providing an interface to exchange frames with the upper MAC layer, transmitting and signaling packets, and works as a media activity sensor for MAC layer.

The MAC layer supports the functionality needed to allow reliable transfer to the upper layers, and it is very similar to the data link layer in the OSI (Open System Interconnection) model. It provides the functionality to control media access, and it is connectionless oriented. The LLC provides addressing and data link control, and it is independent from the lower layers (MAC and PHY). LLC provides connection oriented service to the upper layers.

802.11 Authentication

To allow clients to access the network they must be go through two steps: getting authenticated by the AP, then getting associated. There are two types of authentications used: Shared Key Authentication and Open Key Authentication [Earle2005].

In the WEP (Wired Equivalent Privacy) standard (the first security module used with 802.11) both of the authentication modes were supported. In the new security standards, it is not recommended to use shared key authentication. Fig. 12 below shows how Shared Key Authentication works.

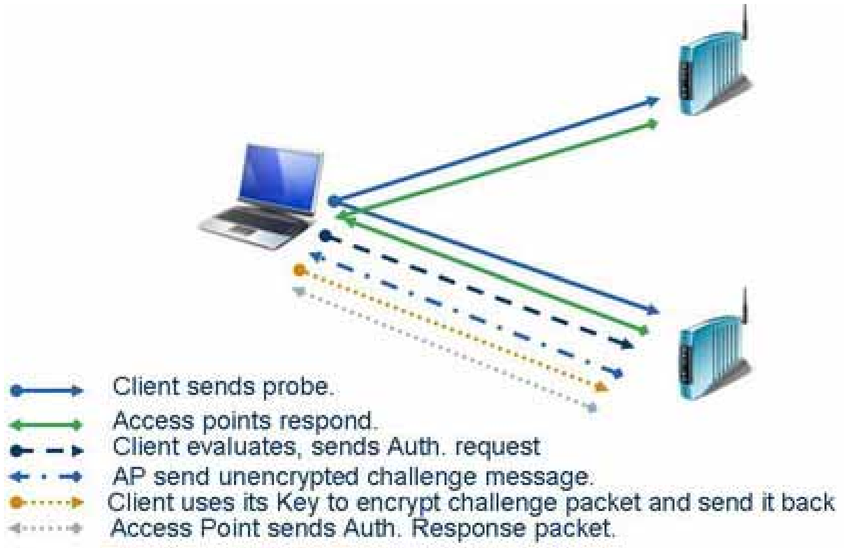

Client sends probe.
Access points respond.
Client evaluates, sends Auth. request
AP send unencrypted challenge message.
Client uses its Key to encrypt challenge packet and send it back
Access Point sends Auth. Response packet.

Fig.12 Shared Key Authentication

When the client wants to connect to the AP, it sends a request. Upon that request the AP sends a challenge packet in clear text (unencrypted). The client then encrypt it with its WEP key and sends it back. The AP tries to decrypt the message using its WEP key. If the decryption process succeeded that means the client is an authenticated user, otherwise the access is denied. In this case if someone is sniffing the traffic, they will get a copy of the encrypted and clear text versions of the message. With some time and processing power the WEP key can be found.

Open Key Authentication does not involve challenge/response messages exchange. The client will get authenticated always, but to send and receive messages she needs to have the correct WEP key. Although Open Key Authentication does not offer any kind of authentication, it is more secure. The reason behind the last statement is that Open Key Authentication does not expose the WEP key to traffic sniffers.[startawisp]

3.2 WEP (Wired Equivalent Privacy)

WEP has three goals to achieve for wireless LAN: confidentiality, availability and integrity [Earle2005] . WEP is now considered insecure for many reasons, nonetheless it served its purpose for a certain amount of time.

WEP uses encryption to provide confidentiality. The encryption process is only between the client and the AP, meaning that packet transfers after the AP (wired LAN) are unencrypted. WEP uses RC4 (discussed earlier) for the encryption purposes. Since RC4 is a stream cipher it needs a seed value to start its key stream generator. This seed is called IV (Initialization Vector). The IV and the shared WEP key are used to encrypt/decrypt transferred packets (Fig. 13). In the encryption process, the Integrity check (IC) value is computed and attached to the payload, then the payload is XORed with the encryption key consisting of two sections (IV and WEP Key). The packet is then forwarded with the IV value sent in plain text (Fig. 14).

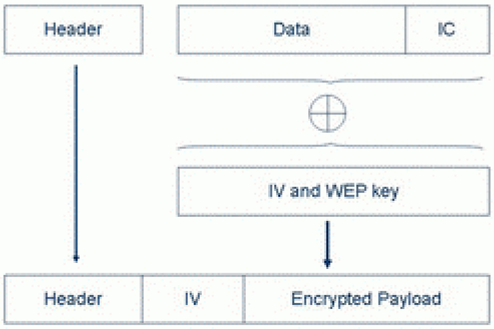


Fig.13 WEP Packet Encryption

WEP uses CRC (Cyclical Redundancy Checking) to verify message integrity. On the other side (receiver: AP) the decryption process is the same but reversed. The AP uses the IV value sent in plain text to decrypt the message by joining it with the shared WEP key. To get a better understanding of the operation, Fig. 14 below shows both encryption and decryption process between the client and AP.

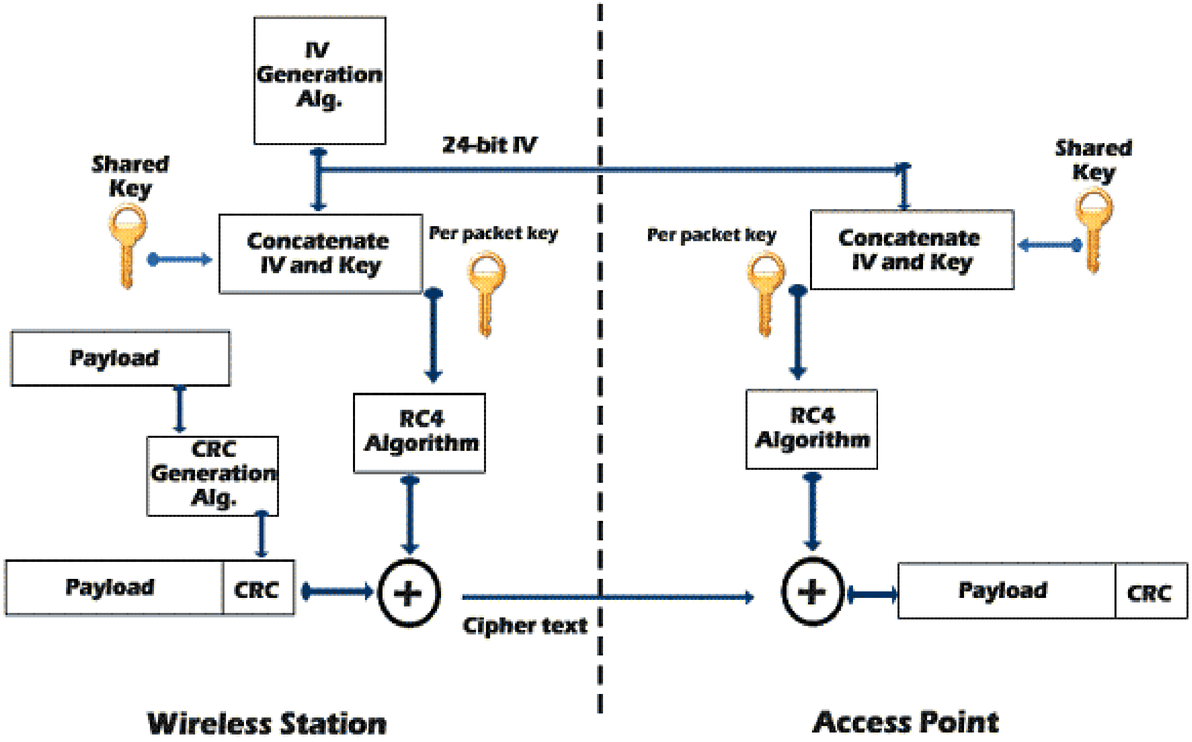


Fig.14 WEP Encryption / Decryption

In this section we have described the way the WEP security protocol operates and the main features or properties it possesses. In the following section we will go through WEP weaknesses and flaws.

3.3 WEP Weaknesses

Many people still think that WEP is secure. They argue that because no big accident has occurred, that is related to wireless security yet, means "no news is good news". The argument completely contradicts with the meaning of security, where you have to predict the risk and work to secure yourself from it before it happens.

Other people believe that attacking a wireless network is expensive and complex, it requires high processing power and complex techniques to break into the network. Today's computers have high processing power and they are continuously becoming cheaper . A wireless attacker does not need to now much about cryptography or security modules; there are many online tools that can ease the process for them [WarDrive] .

One of the major reasons behind WEP weaknesses is its key length. WEP has a 40-bit key , which can be broken in less than five hours using parallel attacks with the help of normal computer machines[Brown2003] . This issue urged vendors to update WEP from using 40-bit to 104-bit key; the new release is called WEP2.

This update helped to resolve some security issues with WEP. The main disadvantage of WEP however, is the lack of key management. Some SOHO users (Small Office/ Home Office) never change their WEP key, which once known the whole system is in jeopardy. In addition to that, WEP does not support mutual authentication. It only authenticates the client, making it open to rouge AP attacks.

Another issue is the use of CRC to ensure integrity. While CRC is a good integrity provision standard, it lacks the cryptography feature. CRC is known to be linear. By using a form of induction, knowing enough data (encrypted packets) and acquiring specific plaintext, the WEP key can be resolved [Brown2003] .

RC4 suffers from a deadly symptom. It tends to repeat IV values (even if it is auto generated), making the exposing of the traffic easier. Mathematically, if the same IV is used to encrypt two packets (WEP key did not change also) and you have a pair of encrypted/plaintext message, then by applying the following simple rule:

$$C1 \text{ XOR } C2 = P1 \text{ XOR } P2$$

(you already know P1,C1 and C2), making it very easy to know the content of the new encrypted packet P2 . [Welch2003]

These weaknesses forced the designers of WLAN security modules to be more cautious. It demonstrates the result of not designing the security module from the ground up taking into consideration all applicable risks. In the next section we will go through the new standards that came after WEP to overcome its vulnerabilities.

3.4 802.1x : EAP Over LAN (EAPOL)

The 802.1x standard was designed for port base authentication for 802 networks. 802.1x does not care what encryption techniques is used, it is only used to authenticate users. EAP (Extensible authentication Protocol) was designed to support multiple authentication methods over point to point connections without requiring IP [RFC3748] . EAP allows any of the encryption schemes to be implemented on top of it, adding flexibility to the security design module. EAPOL (EAP over LAN) is EAP's implementation for LANs[EAPOL] .

The 802.1x framework defines three ports or entities: Supplicant (client want to be authenticated), Authenticator (AP that connect the supplicant to the wired network), and Authentication Server (abbreviated AS which performs the authentication process from the supplicant based on their credentials). [Hardjono2005] [Earle2005] [EAPOL]

The authentication server in the 802.1x framework uses RADIUS (Remote Authentication Dial-In User Service) protocol to provide AAA (Authentication, Authorization and Accounting) service for network clients [RADIUS][Imai2006] . The protocol creates an encrypted tunnel between the AS (Authentication Server) and the Authenticator (AP). Authentication messages are exchanged inside the tunnel to determine if the client has access to the network or not. Fig.15 below shows the network layout.

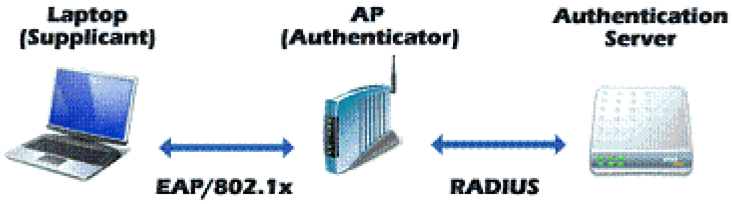


Fig.15 802.1x Authentication

3.5 802.11i Standard

The 802.11i (released June 2004) security standard is supposed to be the final solution to wireless security issue. It improves authentication, integrity and data transfer. Due to the market need of a better substitute to WEP vendors (WiFi Alliance) took a subset of it and market the new product before the final release under the name WPA (WiFi Protected Access), which was released in April 2003. After the final release of 802.11i the vendors implemented the full specifications under the name WPA2. This section will explore the details of 802.11i and its features [WPA] .

802.11i supports two methods of authentication. The first method is the one described before by using 802.1x and EAP to authenticate users. For users who can not or do not want to implement the first method, another method was proposed to use per-session key per-device. This method is implemented by having a shared key (like the one in WEP) called GMK (Group Master Key), which represent the base key to derive the other .GMK is used to derive PTK (Pair Transient Key) and PSK (Pair Session Key) to do the authentication and data encryption.

To solve the integrity problem with WEP, a new algorithm named Michael is used to calculate an 8-byte integrity check called MIC (Message Integrity Code). Michael differs from the old CRC method by protecting both data and the header. Michael implements a frame counter which helps to protect against replay attacks [Microsoft-WPA] [Tech-FAQ] .

To improve data transfer, 802.11i specifies three protocols: TKIP, CCMP and WRAP. TKIP (Temporal Key Integrity Management) was introduced as a "band-aid" solution to WEP problems[Brown2003] . One of the major advantages of implementing TKIP is that you do not need to update the hardware of the devices to run it. Simple firmware/software upgrade is enough.Unlike WEP, TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism [TKIP] . TKIP ensures that every data packet is sent with its own unique encryption key. TKIP is included in 802.11i mainly for backward compatibility.

WRAP (Wireless Robust Authenticated Protocol) is the LAN implementation of the AES encryption standard introduced earlier. It was ported to wireless to get the benefits of AES encryption. WRAP has intellectual property issues, where three parties have filed for its patent. This problem caused IEEE to replace it with CCMP.[Tech-FAQ2] [Brown2003] .

CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) is considered the optimal solution for secure data transfer under 802.11i. CCMP uses AES for encryption. The use of AES will require a hardware upgrade to support the new encryption algorithm.

3.6 RSN

RSN (Robust Secure/Security Network) is a part of 802.11i for providing a method to exchange the clients and the AP capabilities of implementing security methods . RSN uses RSN IE (Information Element) frames to exchange this type of information. RSN increases the flexibility of wireless security network standards and provides options to define the security policies implemented in organizations.[Earle2005]

This section described the security standards implemented in wireless LANs. It showed the difficulties the developers face to specify new standards to fill security holes from old standards. It also gave a glance about 802.11i standard features and improvements over WEP .

Back to Table of Contents

4. Security in WMAN 802.16

As mentioned before, the WMAN or WiMAX was proposed to solve the "last mile" problem. The 802.16 standard was released in Dec 2001. That gave the designers the time to learn from the mistakes made in 802.11 WEP security protocol. In the following sections the architecture of 802.16 will be discussed along with pointing out the security threats found in it.

4.1 The 802.16 Protocol Layers

802.16 protocol consists of four layers (Shown in Fig. 16):

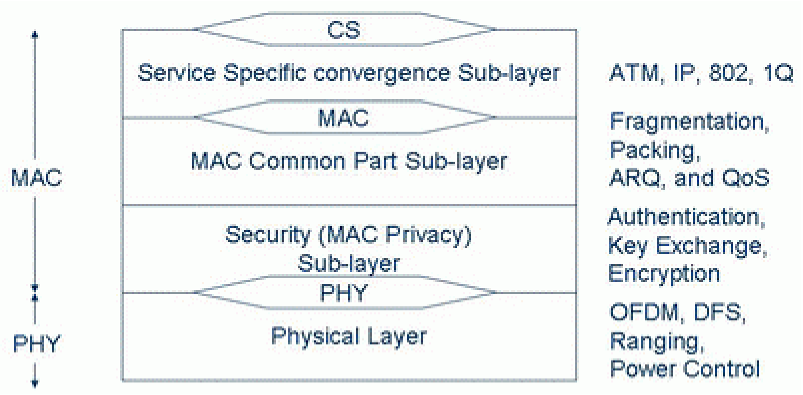

CS
Service Specific convergence Sub-layer
ATM, IP, 802, 1Q
MAC
MAC Common Part Sub-layer
Fragmentation, Packing, ARQ, and QoS
MAC
Security (MAC Privacy) Sub-layer
Authentication, Key Exchange, Encryption
PHY
Physical Layer
OFDM, DFS, Ranging, Power Control
PHY

Fig.16 802.16 Layers

Physical layer:
802.16 protocol operates in three major frequency bands:

1. 10 to 66 GHz (licensed bands)
2. 2 to 11 GHz (licensed bands)
3. 2 to 11 GHz (unlicensed bands)

To support these three bands, the protocol specifies multiple physical layers.
Security sub-layer or MAC sub-layer:
This layer focuses on the security functions in the MAC layer. It consists of two component protocols:
1. Encapsulation protocol: This component describes how the authentication is processed and the types of algorithms to be used in encrypting packets between the BS (Base Station) and the SS (Subscriber Station).
2. Key Management protocol: This component describes how to distribute and manage connection keys. The default protocol used here is PKM (Privacy Key Management). Each connection between the BS and SS or MS (Mobile Station) has a unique CID (Connection ID).
MAC common part sub-layer:
It is a connection oriented sub-layer, and it includes the mechanisms to request bandwidth. Authentication and registration is also a part of this layer functionality.

MAC convergence sub-layer (service specific convergence sub-layer):
Dividing the MAC layer into two sub-layers aims to solve the problem of having different protocols, where the common part sub-layer provides common functionality units to the above layer (MAC convergence sub-layer). The MAC convergence sub-layer implements different services on top of the common part sub-layer. It is also responsible about bandwidth allocation and QoS.[Cohen2003]

As mentioned before the key management protocol used in 802.16 is PKM. PKM is used by SS to obtain the needed authorization to use the media. PKM uses 3DES as its encryption algorithm. PKM protocol operates in two phases: AK (Authorization Key) phase, and TEK (Traffic Encryption Keys). AK represents the secret key used to obtain TEK in the exchanges between SS and BS in subsequent phases.

In each connection session between SS and BS, both of them keep track of two AK keys. The reason behind that is AK needs to be refreshed periodically. In order to keep all the packets during the reauthorization period, the two AK lifetimes must overlap. The same rule applies to TEK keys, where SS has to estimate the time period after which BS will invalidate the old TEK key[Hardjono2005] .

The security model in 802.16 ensures that specific requirements are supported. The first requirement is the ability of BS to identify the MS to allow it to access the network. Once done a master session key (MSK) is transferred securely between BS and MS. Secondly, WiMAX support a multicast and broadcast service (MBS) that allows the BS to distribute data to a certain group of registered users. The system must be able to control access to the distributed content by using a per-group secret key. Finally, WMAN security system provides per-MPDU (MAC Packet Data Unit) integrity protection and reply protection.

After we have briefed about WiMAX (WMAN) architecture, and explaining the main functionalities of each layer and summarized the security techniques used to keep the traffic secure, in the next section we summarize the security threats found in 802.16 security system.

4.2 WMAN Security Concerns

Although the designers of 802.16 security module have benefited from the loop holes found in 802.11 WEP design, they still had some shortcomings in their security design. Probably the reason behind this unexpected result is due to the fact that they incorporate the use of the pre-existing standard DOCSIS (Data Over Cable Service Interface Specifications) that was used to solve the "last mile" problem for cable communication. Since wired networks differ from wireless ones, 802.16 fails to protect the 802.16 link[Johnston2004] .

This section will briefly highlight some of these threats:

Physical Layer Attacks

Since the security layer of 802.16 operates completely in the MAC layer, there is no protection for the PHY layer. Attacks like water torture where the attacker sends a series of packets to drain the receiver battery resources are possible[Johnston2004] . Not to forget that the known radio jamming attack is also applicable to 802.16 networks.

NO Specific Definition for SAA

SA (Security Association) holds a security state relevant to a certain connection. 802.16 designers did not specify the authorization SA, which led to making the system vulnerable to replay attacks.

No Mutual Authentication

One of the major flaws in the 802.16 security module is the lack of BS authentication, causing some undesirable circumstances like 802.11 had with rouge AP.

PKM Authorization Vulnerabilities

- Insufficient Key-Length and wrong choices in choosing the correct cipher modes: WiMAX uses DES-CBC cipher with 56-bit key length. This cipher requires a guarantee of unpredictable IV to initialize CBC mode. TEK uses 3DES encryption, but operates it in ECB mode which is not secure enough.
- Lack of Integrity Protection of MPDUs: PKM lacked the message integrity protection until 802.16-2004 specification.
- Small Key ID for AK and TEK: AK ID is only 4-bit long, where TEK ID is only 2-bit long. This opens the possibility of reusing keys without detection

These obvious vulnerabilities motivated people to come with PKMv2 . PKMv2 introduces a solution to mutual authentication and promote a key hierarchy structure to reduce the cost of key exchanges in PKM[Hardjono2005] .

In this section we mentioned the common and known threats in 802.16 security module. Moreover, we highlighted the motivation behind proposing a new key management system for 802.16, which is PKMv2.

Back to Table of Contents

5. Thoughts on Wireless Security

This section will briefly discuss the best practices for installing wireless security in your home or company taking into consideration all the security threats mentioned earlier. Moreover, we will discuss the main reasons behind the lack of security even with the existence of good security systems.

5.1 Best Practices

WEP has many flaws in its security system, but this is not the main reason why most of the wireless networks are attacked. Less than half of wireless networks are well configured and running correctly. In addition to that most APs default settings do not implement any type of encryption or authentication.[Manley2005]

One of the best practices in home networks is to change the WEP key on a regular basis; this will weaken the chances of getting attacked. One of the most common techniques to test your network security is to use what attackers use to hack your network. There are many tools online that you can use, and they are available for different operating systems [WarDrive] .

5.2 Security Policy

Such techniques are not feasible for companies where many computers are attached to the network. In this situation a security policy must be described and written down to allow managers as well as technicians to react correctly to undesired circumstances [Manley2005] . It is not surprising that the main reason for security breaches is the human error factor or what is known as social engineering. APs can also be configured to stop broadcasting its SSID which will make it harder for the attacker to forge a rouge AP.

There are three levels of security policy: Organization specific, Issue specific (for certain type of technologies), and Systems-specific for individual PCs that hold important information[Manley2005] . The availability of the wireless network and the downtime for the network must be taken into consideration while writing these specifications .

Switching to WPA and WPA2 technologies will solve many of the problems on both user and company levels. The user has to be cautious about implementing the new network, since WPA supports backward compatibility, devices that still implementing WEP will jeopardize the entire network security. It is due to the fact that a security system strength is determined by the strength of the weakest chain. Below is a list of some of the commercial routers that implement WPA2 [bbwexchange] .

Table 1 List of Commercial WPA2 Routers

Company Name	Equipment
Atheros Communications Inc.	Atheros AR5002AP-2X Concurrent 802.11a and 802.11b/g Dual-band Access Point
	Atheros AR5002X Universal 802.11a/b/g Wireless Network Adapter
Broadcom Corporation	Broadcom AirForce™ 802.11a/g CardBus Reference Design, BCM94309CB
	Broadcom AirForce™ 802.11a/g Access Point Reference

	Design,BCM94704-AGR
Cisco Systems	Cisco Aironet 1200 Series Access Point with integrated 802.11a and 802.11g radios
Instant802 Networks	Gateway 7001 Access Point
Intel	Intel® Pro/Wireless 2915 Network Connection
Realtek	Realtek RTL8185&8255 802.11a/g 54M WLAN NIC / RTL8185 8255-NIC

5.3 Security … Problem solved?

With all these proposed new technologies and security standards over the last years to solve the wireless security problems, we still can not say that our wireless networks are secure. The human factor is the major drawback. In spite the fact that people want security, they tend to prefer less secure system in favor of ease of use. Moreover, adding security features to wireless components make it more expensive than other less secure systems, and regular people prefer cheap equipments over good equipments.[Viega2005]

This section described what can the user or the administrator of the wireless network do to prevent most of the known threats. In addition to that we showed a list of the new routers that implements WPA2 to help neutralizing many of the security hazards.

Back to Table of Contents

6. Recent Proposals

This Section discusses one of the recent proposals working to enhance wireless security mechanisms. The chosen protocols is PANA . PANA (Protocol for Carrying Authentication for Network Access) target is to improve the authorization between WLAN clients and AAA servers.

6.1 PANA

PANA is a new method to authenticate WLAN users over IP based networks. The goal of this proposal is to identify a link-layer protocol to allow host and network to authenticate each other for network access. The protocol runs between PaC (PANA Client) and PAA (PANA Authentication Agent). The purpose of this protocol is to provide the carrier for the existed security protocols.

This protocol design is limited only to defining a messaging protocol that will allow authentication payload to be carried between the host/client (PaC) and an agent/server (PAA) in the access network for authentication and authorization purposes regardless of the AAA infrastructure that may (or may not) reside on the network[RFC4058] . As a network-layer protocol, it will be independent of the underlying access technologies and applicable to any network topology.

PANA is intended to be used in situations where no prior trust between PAA and PaC exists. PANA defines four integral parts : PaC, EP (Enforcement Point) the physical point where inbound and outbound traffic filters are applied, and PAA which represent the access authority on the network.

In this proposal if the client wishes to gain access to the network it has to go through a specific scenario. PaC must first discover the IP address of PAA, after that it starts sending authentication messages to authenticate itself on the network. Authentication can be granted from AAA server or from the local PAA depending on the network authentication infrastructure. Once the client is authenticated, PANA SA is created in both PAA and PaC. Furthermore, information filters are installed on the EP. Even after the client is authenticated, there might be other authentication messages exchanged between PaC and PAA during the connection session. Fig. 17 below shows the authentication process in PANA.

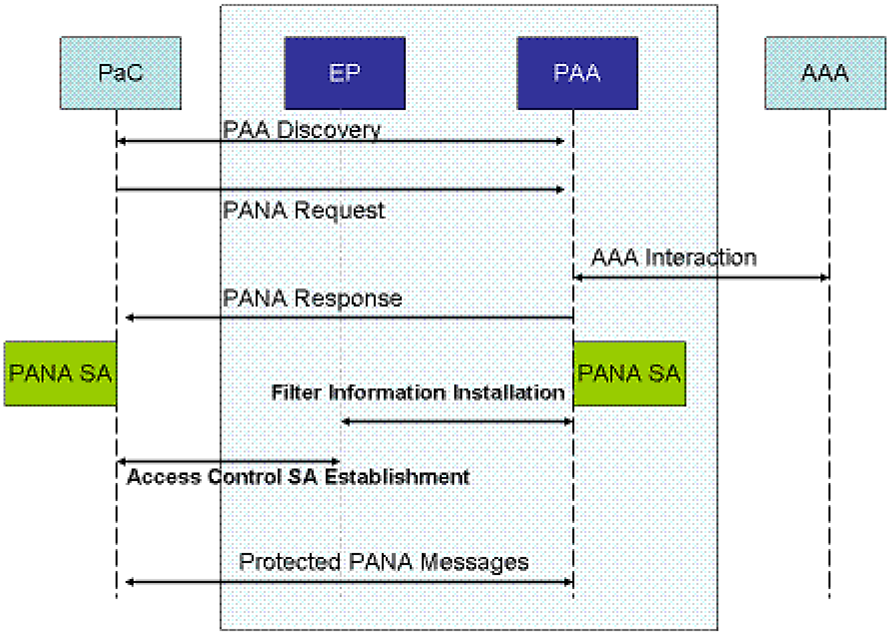


Fig.17 PANA Framework

It also provides a mechanism to prevent DoS attacks by using ISN (Initial Sequence Number), and cookie based authentication between PAA and PaC. It also works as a carrier to carry EAP packets..[RFC4058] [RFC4016] [Foresberg2005]

PANA is still being developed and there are many discussion about its strength and flexibility. These ongoing discussions are aiming to provide a very reliable substitute to the 802.1x/EAP authentication scheme.

Back to Table of Contents

7. Summary

In this paper we reviewed how security 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.

Back to Table of Contents

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
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]
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]
42. [RFC4058],[Yegin, et al.] ,Protocol for Carrying Authentication for Network Access (PANA) Requirements
43. [RFC4016],[Parthasarathy], PANA Threat Analysis and Security Requirments.
44. [Foresberg2005] [Foresberg, et al.]. "PANA", http://people.nokia.net/~patil/IETF56/PANA/PANA_Solution_Slides_7.pdf

Back to Table of Contents

List of Acronyms

Acronym	**Meaning**
WLAN	Wireless LAN
WMAN	Wireless MAN
PKC	Public Key Cryptography
ECB	Electronic Codebook Mode
CBC	Chain Block Chaining Mode
OFB	Output Feedback Mode
IV	Initialization Vector
KSG	Key Stream Generator
NIST	National Institute of Standards and Technology
DES	Data Encryption Standard
AES	Advanced encryption Standard
SSL	Secure Socket Layer
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
RF	Radio Frequency
IR	Infrared Frequency
AP	Access Point
BSS	Basic Service Set
IBSS	Independent BSS
ESS	Extended Service Set
SSID	Service Set ID
BWA	Broadband Wireless Access
Dos	Denial of Service
MAC	Medium Access Control
LLC	logical Link Control
WEP	Wired Equivalent Privacy
CRC	Cyclical Redundancy Checking
EAP	Extensible authentication Protocol
EAPOL	EAP over LAN
AS	Authentication Server
AAA	Authentication, Authorization and Accounting
RADIUS	Remote Authentication Dial-In User Service
WPA	WiFi Protected Access
GMK	Group Master Key

PTK	Pair Transient Key
PSK	Pair Session Key
MIC	Message Integrity Code
TKIP	Temporal Key Integrity Management
WRAP	Wireless Robust Authenticated Protocol
CCMP	Counter with Cipher Block Chaining Message Authentication Code Protocol
RSN	Robust Secure Network
RSN IE	RSN Information Element
BS	Base Station
SS	Subscriber Station
PKM	Privacy Key Management
MS	Mobile Station
TEK	Traffic Encryption Keys
AK	Authorization Key
MBS	Multicast and Broadcast Service
MSK	Master Session Key
DOCSIS	Data Over Cable Service Interface Specifications
SA	Security Association
MPDU	MAC Packet Data Unit
PANA	Protocol for Carrying Authentication for Network Access
PaC	PANA Client
EP	Enforcement Point
PAA	PANA Authentication Agent
ISN	Initial Sequence Number
ARP	Address Resolution Protocol
OSI	Open System Interconnection

Back to Table of Contents

Date Last Modified : 04/23/2006

Note This paper is available on-line at http://www.cse.wustl.edu/~jain/cse574-06/