Fall 2010

A Study of Wireless Network Security

Ningwei Sun
Governors State University

A Study of Wireless Network Security

By

Ningwei Sun

Master's Graduate Project

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science,
With a Major in Computer Science

Governors State University
University Park, IL 60484

2010

Contents

Abstract

I intend to make a survey in wireless data security since wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a wireless network has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired network. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources.

My survey research may involve these following aspects: wireless network architecture, data security in wireless networks, secure data storage in wireless networks and so forth.

1 Project Introduction

1.1 Overview Introduction

Wireless technologies have become increasingly popular in our everyday business and personal lives. Personal digital assistants (PDA) allow individuals to access calendars, e-mail, and phone number lists, and the Internet. Some technologies even offer global positioning system (GPS) capabilities that can pinpoint the location of the device anywhere in the world. Wireless technologies promise to offer even more features and functions in the next few years.

An increasing number of government agencies, businesses, and home users are using, or considering using, wireless technologies in their environments. Agencies should be aware of the security risks associated with wireless technologies. Agencies need to develop strategies that will mitigate risks as they integrate wireless technologies into their computing environments. This report discusses certain wireless technologies, outlines the associated risks, and offers security protect methods.

1.2 Report Purpose and Scope

The report addresses two wireless technologies that everyday business and personal lives are most likely to use: wireless local area networks (WLAN) and Bluetooth networks.

The report mainly addresses the wireless security issues and the methods to fix them. For the 802.11 standards, the security problems are evolving, so are the remedies. WEP (wired equivalent privacy) is used to be an important security algorithm in 802.11 standards, but it was soon replaced by WPA (Wi-Fi protected access). The other new

improving algorithms to replace WEP will not be mentioned in this report. I will introduce the WEP and its imperfections fist and then the WPA. On the other hand, Bluetooth security involves Pairing Mechanism and it's addressed in the second section of the report.

1.3 Report Organization

The document is divided into four sections. This subsection is a roadmap describing the report structure.

Section 1 is composed of an abstract, introduction, purpose, scope and report structure.

Section 2 provides an overview of 802.11 wireless technologies, includes WEP and WPA security algorithms.

Section 3 gives the Bluetooth technology and specifies its Pairing Mechanisms.

Section 4 the conclusion of this report.

2 Standards 802.11

2.1 IEEE 802.11 Introduction

IEEE 802.11 is a set of standards regards with wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. the IEEE LAN/MAN Standards Committee (IEEE 802) created it and IEEE 802.11-2007 is the current version.

The 802.11 family includes over-the-air modulation techniques that use the same basic protocol. The most popular are those defined by the 802.11b and 802.11g protocols, which are amendments to the original standard. 802.11-1997 was the first wireless networking standard, but 802.11b was the first widely accepted one, followed by 802.11g and 802.11n. Security was originally purposefully weak due to export requirements of some governments,[1] and was later enhanced via the 802.11i amendment after governmental and legislative changes.

802.11History

The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is today obsolete. It specified two net bit rates of 1 or 2 megabits per second (Mbit/s), plus forward error correction code. It specified three alternative physical layer technologies: diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum operating at 1 Mbit/s or 2 Mbit/s; and direct-sequence spread spectrum operating at 1 Mbit/s or 2 Mbit/s. The latter two radio technologies used microwave transmission over

the Industrial Scientific Medical frequency band at 2.4 GHz. Some earlier WLAN technologies used lower frequencies, such as the U.S. 900 MHz ISM band.

Legacy 802.11 with direct-sequence spread spectrum was rapidly supplanted and popularized by 802.11b.

2.2 802.11 Standards: a, b, g, n

802.11a

The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM based air interface (physical layer). It operates in the 5 GHz band with a maximum net data rate of 54 Mbit/s, plus error correction code, which yields realistic net achievable throughput in the mid-20 Mbit/s.

Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage. However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g. In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength and, as a result, cannot penetrate as far as those of 802.11b. In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5 Mbit/s or even 1 Mbit/s at low signal strengths). However, at higher speeds, 802.11a often has the same or greater range due to less interference.

802.11b

802.11b has a maximum raw data rate of 11 Mbit/s and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard. The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology.

802.11b devices suffer interference from other products operating in the 2.4 GHz band. Devices operating in the 2.4 GHz range include: microwave ovens, Bluetooth devices, baby monitors and cordless telephones.

802.11g

In June 2003, a third modulation standard was ratified: 802.11g. This works in the 2.4 GHz band (like 802.11b), but uses the same OFDM based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput. 802.11g hardware is fully backwards compatible with 802.11b hardware and therefore is encumbered with legacy issues that reduce throughput when compared to 802.11a by ~21%.

The then-proposed 802.11g standard was rapidly adopted by consumers starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs. By summer 2003, most dual-band 802.11a/b products became dual-band/tri-mode, supporting a & b/g in a single mobile adapter card or access

point. Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network.

Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output antennas (MIMO). 802.11n operates on both the 2.4GHz and the lesser used 5GHz bands. The IEEE has approved the amendment and it was published in October 2009.[2][3] Prior to the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal.

2.3 Wireless Network Protection Method

2.3.1 WEP

Wired Equivalent Privacy (**WEP**) is a deprecated security algorithm for IEEE 802.11 wireless networks. Introduced as part of the original 802.11 protocol in 1997, it was intended to provide confidentiality comparable to that of a traditional wired network, but is susceptible to eavesdropping. [4]

Since 2001, several serious weaknesses in the protocol have been identified by cryptanalysts with the result that today a WEP connection can be cracked with readily available software within minutes.[5] In response to vulnerabilities the IEEE created a

new 802.11i task force, by 2003 the Wi-Fi Alliance announced that WEP had been superseded by Wi-Fi Protected Access (WPA), which was a subset of the upcoming 802.11i amendment. Finally in 2004, with the ratification of the full 802.11i standard (i.e., WPA2), the IEEE declared that both WEP-40 and WEP-104 "have been deprecated as they fail to meet their security goals".[6] Despite its weaknesses, WEP is still widely in use and is often the first security choice presented to users by router configuration tools.[7][8]

Encryption details

WEP was included as the privacy of the original IEEE 802.11 standard ratified in September 1999. WEP uses the stream cipher RC4 for confidentiality,[9] and the CRC-32 checksum for integrity.[10] It was deprecated as a wireless privacy mechanism in 2004, but for legacy purposes is still documented in the current standard. [14]

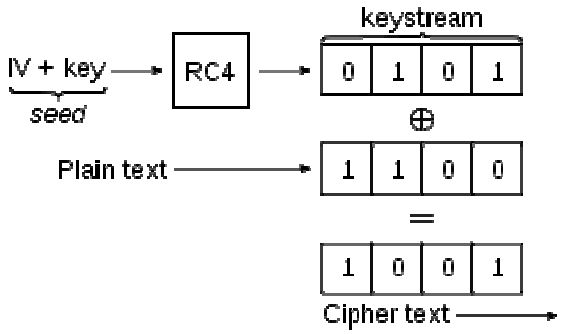

Figure 1, From Reference [14]

Basic WEP encryption: RC4 keystream XORed with plaintext

2.3.2 WEP Security Limitations

In many WLAN systems, the key utilized for authentication is the same key used for encryption. This presents a weakness which strengthens the problems mentioned above.

If the attacker has control of the shared key he can access the network in addition to decrypt the messages. The solution is to distribute separate keys throughout the system, one for authentication and one for encryption.(Barken 2004)

In addition Most WLANs share one key across all stations and APs in the network. It's not likely that a key shared among several users will remain secret forever. Some network administrators address this issue by configuring wireless stations with the secret key as opposed to allowing users to execute this task. A better solution is to assign a unique key to each station and to change keys frequently.

In cryptography, the **Fluhrer, Mantin, and Shamir attack** is a particular stream cipher attack, a dedicated form of cryptanalysis for attacking the widely-used stream cipher RC4. The attack allows an attacker to recover the key in an RC4 encrypted stream from a large number of messages in that stream.[11]

RC4 Weakness Background

The Fluhrer, Mantin and Shamir (FMS) attack, published in a 2001 paper titled Weaknesses in the Key Scheduling Algorithm of RC4, takes advantage of a weakness in the RC4 key scheduling algorithm to reconstruct the key from a number of collected encrypted messages. The FMS attack gained popularity in tools such as AirSnort and aircrack, both of which can be used to attack WEP encrypted wireless networks.[11]

This discussion will use the below RC4 key scheduling algorithm (KSA).

begin ksa(with int keylength, with byte key[keylength])

for i from 0 to 255

```
S[i] := i
endfor
j := 0
for i from 0 to 255
j := (j + S[i] + key[i mod keylength]) mod 256
swap(S[i],S[j])
endfor
end
```

The following pseudo-random generation algorithm (PRGA) will also be used.

```
begin prga(with byte S[256])
i := 0
j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256
swap(S[i],S[j])
output S[(S[i] + S[j]) mod 256]
endwhile
end
```

The Attack

The basis of the FMS attack lies in the use of weak initialization vectors (IVs) used with RC4. RC4 encrypts one byte at a time with a keystream output from prga(); RC4 uses the

key to initialize a state machine via ksa(), and then continuously modifies the state and generates a new byte of the keystream from the new state. Theoretically, the key stream functions as a random one time pad, as a pseudo-random number generator controls the output at each step.[11]

With certain IVs, an attacker knowing the mth byte of the keystream can derive the m+1th byte due to a weakness in the PRNG used to generate the keystream. Because the first byte of the plaintext comes from the WEP SNAP header, an attacker can assume he can derive the first byte of the keystream from B $\oplus$ 0xAA. From there, he only needs an IV in the form (a+3, n-1, x) for key index a origin 0, element value space n (256 since 8 bits make a byte), and any X. To start, the attacker needs IVs of (3, 255, x). WEP uses 24-bit IVs, making each value one byte long.[11]

To start, the attacker utilizes the IV as the first 3 elements in K[]. He fills the S-box S[] with sequential values from 0 to n as RC4 does when initializing the S-box from a known K[]. He then performs the first 3 iterations of ksa() to begin initializing the S-box.

After the third step, the attacker can possibly, but not definitely, derive the fourth byte of the key using the keystream output O by computing (O - j - S[i]) mod n = K[i], with the value i = 3 at this step.[11]

At this point, the attacker does not yet have the fourth byte of the key. This algorithm does not regenerate the next byte of the key; it generates a possible value of the key. By collecting multiple messages—for example WEP packets—and repeating these steps, the attacker will generate a number of different possible values. The correct value appears

significantly more frequently than any other; the attacker can determine the value of the key by recognizing this value and selecting it as the next byte. At this point, he can start the attack over again on the fifth byte of the key.[11]

Although the attacker cannot attack words of the key out of order, he can store messages for later sequential attack on later words once he knows earlier words. Again, he only needs messages with weak IVs, and can discard others. Through this process, he can gather a large number of messages for attack on the entire key; in fact, he can store only a short portion of the beginning of those messages, just enough to carry the attack out as far as the word of the key the IV will allow him to attack.[11]

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.[11]

In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir published a cryptanalysis of WEP that exploits the way the RC4 cipher and IV is used in WEP, resulting in a passive attack that can recover the RC4 key after eavesdropping on the network. Depending on the amount of network traffic, and thus the number of packets available for inspection, a successful key recovery could take as little as one minute. If an insufficient number of packets are being sent, there are ways for an attacker to send packets on the network and thereby stimulate reply packets which can then be inspected to find the key. The attack was soon implemented, and automated tools have since been released. It is possible to

perform the attack with a personal computer, off-the-shelf hardware and freely available software such as aircrack-ng to crack any WEP key in minutes.[12]

Cam-Winget et al. (2003) surveyed a variety of shortcomings in WEP. They write "Experiments in the field indicate that, with proper equipment, it is practical to eavesdrop on WEP-protected networks from distances of a mile or more from the target." They also reported two generic weaknesses:

- the use of WEP was optional, resulting in many installations never even activating it, and
- WEP did not include a key management protocol, relying instead on a single shared key among users.

In 2005, a group from the U.S. Federal Bureau of Investigation gave a demonstration where they cracked a WEP-protected network in 3 minutes using publicly available tools. Andreas Klein presented another analysis of the RC4 stream cipher. Klein showed[7] that there are more correlations between the RC4 keystream and the key than the ones found by Fluhrer, Mantin and Shamir which can additionally be used to break WEP in WEP-like usage modes.

In 2006, Bittau, Handley, and Lackey showed that the 802.11 protocol itself can be used against WEP to enable earlier attacks that were previously thought impractical. After eavesdropping a single packet, an attacker can rapidly bootstrap to be able to transmit arbitrary data. The eavesdropped packet can then be decrypted one byte at a time (by transmitting about 128 packets per byte to decrypt) to discover the local network IP

addresses. Finally, if the 802.11 network is connected to the Internet, the attacker can use 802.11 fragmentation to replay eavesdropped packets while crafting a new IP header onto them. The access point can then be used to decrypt these packets and relay them on to a buddy on the Internet, allowing real-time decryption of WEP traffic within a minute of eavesdropping the first packet.

In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann were able to extend Klein's 2005 attack and optimize it for usage against WEP. With the new attack it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

In 2008, Payment Card Industry (PCI) Security Standards Council's latest update of the Data Security Standard (DSS), prohibits the use of the WEP as part of any credit-card processing after 30 June 2010, and prohibit any new system from being installed that uses WEP after 31 March 2009. The use of WEP contributed to the T.J. Maxx parent company network invasion.

2.3.3 802.11i

IEEE 802.11i-2004 or **802.11i** is an amendment to the original IEEE 802.11. The draft

standard was ratified on 24 June 2004. This standard specifies security mechanisms for wireless networks. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process it deprecated the broken WEP. The amendment was later incorporated into the published IEEE 802.11-2007 standard.[13]

802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. WPA implemented a subset of a draft of 802.11i. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as **WPA2**, also called **RSN** (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher. [14]

Protocol Operation

IEEE 802.11i enhances IEEE 802.11-1999 by providing a Robust Security Network (RSN) with two new protocols, the 4-Way Handshake and the Group Key Handshake. These utilize the authentication services and port access control described in IEEE 802.1X to establish and change the appropriate cryptographic keys. The RSN is a security network that only allows the creation of robust security network associations (RSNAs), which are a type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. It also provides two RSNA data confidentiality and integrity protocols, TKIP and CCMP, with implementation of CCMP being mandatory.

The Four-Way Handshake

The authentication process leaves two considerations: the access point (AP) still needs to authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived. The earlier EAP exchange has provided the shared secret key PMK (Pairwise Master Key). This key is, however, designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is generated by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. The product is then put through a cryptographic hash function.[13]

The handshake also yields the GTK (Group Temporal Key), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in the figure and explained below:

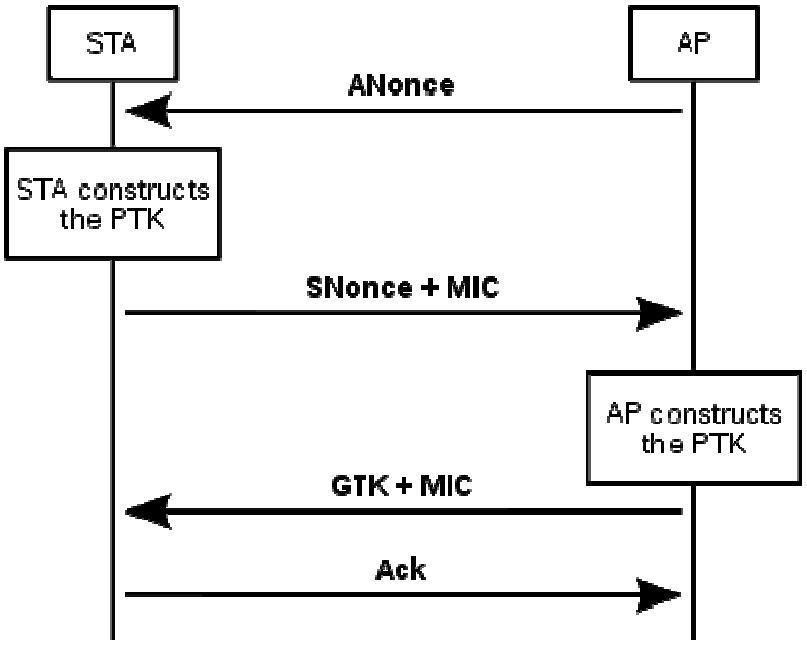

Figure 2, From Reference [13]

1. The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a MIC, including authentication, which is really a Message Authentication and Integrity Code: (MAIC).
3. The AP sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

All the above messages are sent as EAPOL-Key frames.

As soon as the PTK is obtained it is divided into five separate keys:

PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
2. 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP

5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.[13]

The Group Key Handshake

The GTK used in the network may need to be updated due to the expiry of a preset timer. When a device leaves the network, the GTK also needs to be updated. This is to prevent the device from receiving any more multicast or broadcast messages from the AP.[13]

To handle the updating, 802.11i defines a Group Key Handshake that consists of a two-way handshake:

1. The AP sends the new GTK to each STA in the network. The GTK is encrypted using the KEK assigned to that STA, and protects the data from tampering, by use of a MIC.
2. The STA acknowledges the new GTK and replies to the AP.

GTK (Groupwise Transient Key – 32 bytes)

1. 16 bytes of Group Temporal Encryption Key – Used to encrypt Multicast data packets
2. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on Multicast packet transmitted by AP

3. 8 bytes of Michael MIC Authenticator Rx Key – This is currently not used as stations do not send multicast traffic

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.[13]

2.3.4 WPA and WPA2

Wi-Fi Protected Access **Wi-Fi Protected Access** (**WPA** and **WPA2**) is a certification program developed by the Wi-Fi Alliance to indicate compliance with the security protocol created by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined the protocol in response to several serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy). [15]

The WPA protocol implements the majority of the IEEE 802.11i standard. The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the preparation of 802.11i. Specifically, the Temporal Key Integrity Protocol (TKIP), was brought into WPA. TKIP could be implemented on pre-WPA wireless network interface cards that began shipping as far back as 1999 through firmware upgrades. Because the changes required fewer modifications on the client than on the wireless access points (APs), most pre-2003 APs could not be upgraded to support WPA with TKIP. Researchers have since discovered a flaw in TKIP that relied on older weaknesses to retrieve the keystream from short packets to use for re-injection and spoofing. [15]

The later WPA2 certification mark indicates compliance with the full IEEE 802.11i standard. This advanced protocol will not work with some older network cards.

WPA2

The Wi-Fi Alliance name for IEEE 802.11i certification testing is *Wi-Fi Protected Access (WPA) 2* or *WPA2*. WPA2 resembles IEEE 802.11i but differs slightly to allow for interoperability concerns with WPA. WPA is the Wi-Fi Alliance's earlier certification, which was based on a draft of the IEEE 802.11i standard. If migration isn't a concern then WPA2 runs as defined by IEEE 802.11i. For instance, an access point and client card running only CCMP in WPA2 will be running IEEE 802.11i. However, an access point that allows CCMP and TKIP clients will be running a mixture of IEEE 802.11i and WPA. This enables the earlier WPA clients to associate to the new WPA2 access points. To users this is transparent. But developers will need to note the difference when designing to include earlier WPA systems.[16]

Wi-Fi Alliance tests for interoperability. WPA2 testing, however, doesn't test all configurations of IEEE 802.11i. The actual tests depend on product classification. Home products aren't expected to have the same features as enterprise products.[16]

Security & Insecurity in pre-shared key mode

Pre-shared key mode (PSK, also known as Personal mode) is designed for home and small office networks that don't require the complexity of an 802.1X authentication server. Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters. If ASCII characters are used, the 256 bit key is calculated by applying the PBKDF2 key derivation function to the passphrase, using the SSID as the salt and 4096 iterations of HMAC-SHA1. [15]

Shared-key WPA remains vulnerable to password cracking attacks if users rely on a weak passphrase. To protect against a brute force attack, a truly random passphrase of 13 characters (selected from the set of 95 permitted characters) is probably sufficient. To further protect against intrusion the network's SSID should not match any entry in the top 1000 SSIDsas downloadable rainbow tables have been pre-generated for them and a multitude of common passwords. [15]

In November 2008 Erik Tews and Martin Beck - researchers at two German technical universities (TU Dresden and TU Darmstadt) - uncovered a WPA weakness which relied on a previously known flaw in WEP that could be exploited only for the TKIP algorithm in WPA. The flaw can only decrypt short packets with mostly known contents, such as ARP messages. The attack requires Quality of Service (as defined in 802.11e) to be enabled, which allows packet prioritization as defined. The flaw does not lead to key recovery, but only a keystream that encrypted a particular packet, and which can be reused as many as seven times to inject arbitrary data of the same packet length to a wireless client. For example, this allows someone to inject faked ARP packets which makes the victim send packets to the open Internet. This attack was further optimised by two Japanese computer scientists Toshihiro Ohigashi and Masakatu Morii. Their attack doesn't require Quality of Service to be enabled. In October 2009, Halvorsen with others made further progress, enabling attackers to inject larger malicious packets (596 bytes, to be more specific) within approximately 18 minutes and 25 seconds. In February 2010, a new attack was found by Martin Beck that allows an attacker to decrypt all traffic towards the client. The authors say that the attack can be defeated by deactivating QoS, or by switching from TKIP to AES-based CCMP.[15]

The vulnerabilities of TKIP are significant in that WPA-TKIP was, up until the proof-of-concept discovery, held to be an extremely safe combination. WPA-TKIP is still a configuration option upon a wide variety of wireless routing devices provided by many hardware vendors.[15]

2.4 Summary

Included in the IEEE 802.11 standard is the requirement to provide for privacy of data transmission across wireless networks. The way that privacy is provided is by use of the WEP. WEP is a protocol that uses RSA's RC4 data stream encryption and CRC-32 integrity checking of data frames at the data link layer. WEP is usually implemented in the hardware and firmware of the wireless network interface cards. It is worth stressing that vulnerabilities in WEP will require a new generation of wireless interface cards.

However, the WEP security algorithm is extremely likely to be insecure. The aspects of security affected are the privacy, confidentiality and integrity of data transmitted across a WLAN, all connected devices or networks, and availability of the WLAN itself. The weaknesses in privacy and confidentiality relate to well-publicized vulnerabilities in the Wired Equivalency Privacy (WEP) protocol used to provide data link layer encryption. Moreover, the risks to privacy of data extend to wired systems connected to WLANs via wireless access points, as wireless access points are often configured by default not to use authentication mechanisms and hence can be used to gain illegitimate access to wired networks. The integrity of information from WLANs may have been compromised and should not be treated as trusted or genuine. It is possible to capture data in transit and to

alter that data without detection by the integrity checker. The threat to availability is that a wireless connection can be blocked by Radio Frequency (RF) jamming or by deliberate RF transmission.

The situation is liable to change because work is ongoing in the IEEE on the 802.11i standard (Media Access Control Enhancements for Enhanced Security) to resolve the cryptographic vulnerabilities that WEP has. Because IEEE 802.11i (WPA) has more than one data-confidentiality protocol, WPA provides an algorithm for the IEEE 802.11i client card and access point to negotiate which protocol to use during specific traffic circumstances and to discover any unknown security parameters.

3 Bluetooth

3.1 Bluetooth vs. Wi-Fi IEEE 802.11 in Networking

Bluetooth is an open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.[17]

Bluetooth and Wi-Fi have many applications: setting up networks, printing, or transferring files.

Wi-Fi is intended for resident equipment and its applications. The category of applications is outlined as WLAN, the wireless local area networks. Wi-Fi is intended as a replacement for cabling for general local area network access in work areas.

Bluetooth is intended for non-resident equipment and its applications. The category of applications is outlined as the wireless personal area network (WPAN). Bluetooth is a replacement for cabling in a variety of personally carried applications in any ambiance and can also support fixed location applications such as smart energy functionality in the home (thermostats, etc.).[17]

Wi-Fi is wireless version of a traditional Ethernet network, and requires configuration to set up shared resources, transmit files, and to set up audio links (for example, headsets

and hands-free devices). Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a faster connection and better range from the base station. The nearest equivalents in Bluetooth are the DUN profile, which allows devices to act as modem interfaces, and the PAN profile, which allows for ad-hoc networking.[17]

3.2 Bluetooth Devices

Figure 3, From Reference [17]

A Bluetooth USB covers with a 100 m range. The MacBook Pro, shown, also has a built in Bluetooth adaptor.

Bluetooth exists in many products, such as the iPod Touch, Lego Mindstorms NXT, PlayStation 3, PSP Go, telephones, the Wii, and some high definition headsets, modems, and watches. The technology is useful when transferring information between two or more devices that are near each other in low-bandwidth situations. Bluetooth is commonly used to transfer sound data with telephones (i.e., with a Bluetooth headset) or byte data with hand-held computers (transferring files).

Bluetooth protocols simplify the discovery and setup of services between devices.

Bluetooth devices can advertise all of the services they provide.[17] This makes using services easier because more of the security, network address and permission configuration can be automated than with many other network types.

3.3 Security Method in Bluetooth

3.3.1 Security Overview

Bluetooth implements confidentiality, authentication and key derivation with custom algorithms based on the SAFER+ block cipher. Bluetooth key generation is generally based on a Bluetooth PIN, which must be entered into both devices. This procedure might be modified if one of the devices has a fixed PIN (e.g., for headsets or similar devices with a restricted user interface). During pairing, an initialization key or master key is generated, using the E22 algorithm. The E0 stream cipher is used for encrypting packets, granting confidentiality and is based on a shared cryptographic secret, namely a previously generated link key or master key. Those keys, used for subsequent encryption of data sent via the air interface, rely on the Bluetooth PIN, which has been entered into one or both devices.[17]

An overview of Bluetooth vulnerabilities exploits was published in 2007 by Andreas Becker.

In September 2008, the National Institute of Standards and Technology (NIST) published a Guide to Bluetooth Security that will serve as reference to organizations on the security capabilities of Bluetooth and steps for securing Bluetooth technologies effectively. While Bluetooth has its benefits, it is susceptible to denial of service attacks, eavesdropping,

man-in-the-middle attacks, message modification, and resource misappropriation. Users/organizations must evaluate their acceptable level of risk and incorporate security into the lifecycle of Bluetooth devices. To help mitigate risks, included in the NIST document are security checklists with guidelines and recommendations for creating and maintaining secure Bluetooth piconets, headsets, and smart card readers.[17]

Bluetooth v2.1 - finalized in 2007 with consumer devices first appearing in 2009 - makes significant changes to Bluetooth's security, including pairing.

3.3.2 Pairing

Many of the services offered over Bluetooth can expose private data or allow the connecting party to control the Bluetooth device. For security reasons it is therefore necessary to control which devices are allowed to connect to a given Bluetooth device. At the same time, it is useful for Bluetooth devices to automatically establish a connection without user intervention as soon as they are in range.[17]

To resolve this conflict, Bluetooth uses a process called pairing, which is generally manually started by a device user—making that device's Bluetooth link visible to other devices. Two devices need to be paired to communicate with each other; the pairing process is typically triggered automatically the first time a device receives a connection request from a device with which it is not yet paired. Once a pairing has been established it is remembered by the devices, which can then connect to each without user intervention. When desired, the pairing relationship can later be removed by the user.[17]

Implementation

During the pairing process, the two devices involved establish a relationship by creating a shared secret known as a link key. If a link key is stored by both devices they are said to be paired or bonded. A device that wants to communicate only with a bonded device can cryptographically authenticate the identity of the other device, and so be sure that it is the same device it previously paired with. Once a link key has been generated, an authenticated ACL link between the devices may be encrypted so that the data that they exchange over the airwaves is protected against eavesdropping.[17]

Link keys can be deleted at any time by either device. If done by either device this will implicitly remove the bonding between the devices; so it is possible for one of the devices to have a link key stored but not be aware that it is no longer bonded to the device associated with the given link key.

Bluetooth services generally require either encryption or authentication, and as such require pairing before they allow a remote device to use the given service. Some services, such as the Object Push Profile, elect not to explicitly require authentication or encryption so that pairing does not interfere with the user experience associated with the service use-cases.[17]

Pairing Mechanisms

Pairing mechanisms have changed significantly with the introduction of Secure Simple Pairing in Bluetooth v2.1. The following summarizes the pairing mechanisms:

- **Legacy pairing**: This is the only method available in Bluetooth v2.0 and before. Each device must enter a PIN code; pairing is only successful if both devices enter the same PIN code. Any 16-byte UTF-8 string may be used as a PIN code, however not all devices may be capable of entering all possible PIN codes.
    - **Limited input devices**: The obvious example of this class of device is a Bluetooth Hands-free headset, which generally have few inputs. These devices usually have a fixed PIN, for example "0000" or "1234", that are hard-coded into the device.
    - **Numeric input devices**: Mobile phones are classic examples of these devices. They allow a user to enter a numeric value up to 16 digits in length.
    - **Alpha-numeric input devices**: PCs and smartphones are examples of these devices. They allow a user to enter full UTF-8 text as a PIN code. If pairing with a less capable device the user needs to be aware of the input limitations on the other device, there is no mechanism available for a capable device to determine how it should limit the available input a user may use.
- **Secure Simple Pairing** (SSP): This is required by Bluetooth v2.1. A Bluetooth v2.1 device may only use legacy pairing to interoperate with a v2.0 or earlier device. Secure Simple Pairing uses a form of public key cryptography, and has the following modes of operation:
    - **Just works**: As implied by the name, this method just works. No user interaction is required; however, a device may prompt the user to confirm

the pairing process. This method is typically used by headsets with very limited IO capabilities, and is more secure than the fixed PIN mechanism which is typically used for legacy pairing by this set of limited devices. This method provides no man in the middle (MITM) protection.

- **Numeric comparison**: If both devices have a display and at least one can accept a binary Yes/No user input, they may use Numeric Comparison. This method displays a 6-digit numeric code on each device. The user should compare the numbers to ensure they are identical. If the comparison succeeds, the user(s) should confirm pairing on the device(s) that can accept an input. This method provides MITM protection, assuming the user confirms on both devices and actually performs the comparison properly.
- **Passkey Entry**: This method may be used between a device with a display and a device with numeric keypad entry (such as a keyboard), or two devices with numeric keypad entry. In the first case, the display is used to show a 6-digit numeric code to the user, who then enters the code on the keypad. In the second case, the user of each device enters the same 6-digit number. Both cases provide MITM protection.
- **Out of band** (OOB): This method uses an external means of communication (such as NFC) to exchange some information used in the pairing process. Pairing is completed using the Bluetooth radio, but requires information from the OOB mechanism. This provides only the level of MITM protection that is present in the OOB mechanism.

SSP is considered simple for the following reasons:

- In most cases, it does not require a user to generate a passkey.
- For use-cases not requiring MITM protection, user interaction has been eliminated.
- For numeric comparison, MITM protection can be achieved with a simple equality comparison by the user.
- Using OOB with NFC will enable pairing when devices simply get close, rather than requiring a lengthy discovery process.[17]

3.3.3 Security Concerns

Prior to Bluetooth v2.1, encryption is not required and can be turned off at any time. Moreover, the encryption key is only good for approximately 23.5 hours; using a single encryption key longer than this time allows simple XOR attacks to retrieve the encryption key.

- Turning off encryption is required for several normal operations, so it is problematic to detect if encryption is disabled for a valid reason or for a security attack.
- Bluetooth v2.1 addresses this in the following ways:
    - Encryption is required for all non-SDP (Service Discovery Protocol) connections

- A new Encryption Pause and Resume feature is used for all normal operations requiring encryption to be disabled. This enables easy identification of normal operation from security attacks.
- The encryption key is required to be refreshed before it expires.

Link keys may be stored on the device file system, not on the Bluetooth chip itself. Many Bluetooth chip manufacturers allow link keys to be stored on the device; however, if the device is removable this means that the link key will move with the device.

Bluetooth security is not all satisfactory and it has some limitations. First about the authentication: only the device is authenticated, not the user. Secondly BT doesn't define authorization separately for each service either. This can be applied in the Bluetooth architecture without changing the BT protocol stack, but changes in the security manager and the registration processes would be necessary.

At the moment BT only allows access control at connection set-up. The access check can be asymmetric, but once a connection is established, data flow is in principle bi directional. It is not possible within the scope of this architecture to enforce unidirectional traffic.

There is no support of legacy applications: It will not make calls to the security manager. Instead Bluetooth aware "adapter" application is required to make security related calls to the BT security manager on behalf of the legacy application.[17]

3.4 Summary

Bluetooth is a short range (within 100m) wireless network technology, it's useful when transferring information between multiple devices that are near each other in low-bandwidth situations. Among computers and cell-phones we use USB Bluetooth adapter to get connections. Like WEP in WLAN, Bluetooth has its benefit, but it is hard to denial service attacks, eavesdropping, message modification and resource misappropriation. In 2009 Bluetooth's security made significant changes, including pairing. Two devices need to be paired to communicate with each other. In Bluetooth v2.0 and before, legacy pairing is the only available method. Each device must enter a PIN code in order to pair successfully. Security Simple Pairing is required by Bluetooth v2.1 and it uses a form of public key cryptography. Bluetooth is not perfect and it has limitations. One reason is that only the device is authenticated rather than the user. Secondly BT doesn't define authorization separately for each service either.

4. Project Conclusion

There were four sections in my project: Project Introduction, Standards 802.11, Bluetooth and Project Conclusion. Section one introduced wireless technologies and the reason why they are popular. Standards 802.11 and Bluetooth security protection methods were the main concerns in the report.

For 802.11 securities section, WEP algorithm and the reason why it is deprecated had been first mentioned, and then, the replacement algorithm WPA & WPA2 was described next. WEP has many security problems for example: WEP adopts the same key for authentication and encryption. If the attacker has control of the shared key he can decrypt the messages theoretically.WPA (Wi-Fi Protected Access) is a protocol implements the majority of the IEEE 802.11i standard and WPA2 resembles IEEE 802.11i but differs slightly to allow for interoperability concerns with WPA. Also, WPA has more than data-confidentiality protocol, it provides an algorithm for the IEEE 802.11i client card and access point to negotiate witch protocol to use during specific traffic circumstances and to discover any unknown security parameters.

In Bluetooth section, I have introduced in where Bluetooth and Wi-Fi 802.11 are different. Like 802.11 standards, Bluetooth also has its own security issues. The PIN code is necessary for Bluetooth devices to connect, Security Simple Pairing is required by Bluetooth v2.1 and it uses a form of public key cryptography. Bluetooth's security is not perfect and it has limitations. One reason is that only the device is authenticated rather than the user. Secondly BT doesn't define authorization separately for each service either.

References

[1] IEEE 802.11, http://en.wikipedia.org/wiki/IEEE_802.11 , retrieved 01/05/2010.
[2]IEEE Standards Association, http://standards.ieee.org/announcements/ieee802.11n_2009amendment_ratified.html, retrieved 01/05/2010.
[3] 802.11n-2009—Amendment 5: Enhancements for Higher Throughput., IEEE-SA. 29 October 2009. doi:10.1109/IEEESTD.2009.5307322, retrieved 01/18/2010.

[4] IEEE Standard for Information Technology, http://ieeexplore.ieee.org/search/freesrchabstract.jsp?arnumber=654749&isnumber=14251&punumber=5258&k2dockey=654749@ieeestds&query=%28802.11+1997%29%3Cin%3Emetadata&pos=0, retrieved 02/04/2010.

[5] Intercepting Mobile Communications: The Insecurity of 802.11, http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, retrieved 02/04/2010

[6] What is a WEP key?, http://lirent.net/wifi/what-is-a-wep-key.html, retrieved 03/02/2010.

[7] The Final Nail in WEP's Coffin, http://www.cs.ucl.ac.uk/staff/M.Handley/papers/fragmentation.pdf, retrieved 02/04/2010 .

[8] Wireless Adoption Leaps Ahead, Advanced Encryption Gains Ground in the Post-WEP, http://www.rsa.com/press_release.aspx?id=8451, retrieved 02/04/2010.

[9] WPA Part 2: Weak IV's, Last updated Dec 23, 2004. http://www.informit.com/guides/content.aspx?g=security&seqNum=85, retrieved 02/04/2010.

[10] http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm

[11] Fluhrer, Mantin and Shamir attack, http://en.wikipedia.org/wiki/Fluhrer,_Mantin_and_Shamir_attack, retrieved 03/04/2010.

[12] Wired Equivalent Privacy, http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy, retrieved 03/04/2010.

[13] IEEE 802.11i-2004, http://en.wikipedia.org/wiki/IEEE_802.11i-2004, retrieved 05/04/2010.

[14] GET IEEE 802®: LOCAL AND METROPOLITAN AREA NETWORK STANDARDS,

http://standards.ieee.org/getieee802/download/802.11i-2004.pdf, retrieved 07/04/2010.

[15] Wi-Fi Protected Access, http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access, retrieved 08/04/2010.

[16]IEEE 802.11i and wireless security, http://www.eetimes.com/discussion/other/4025006/IEEE-802-11i-and-wireless-security, retrieved 10/04/2010.

[17]Bluetooth, http://en.wikipedia.org/wiki/Bluetooth, retrieved 11/04/2010.