WIRELESS SECURITY

A SEMINAR REPORT

Submitted by

ANISH KUMAR

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

SCHOOL OF ENGINEERING

COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY

KOCHI- 682022

SEPTEMBER 2010

Division of Computer Engineering
School of Engineering
Cochin University of Science & Technology
Kochi-682022

CERTIFICATE

Certified that this is a bonafide record of the seminar work titled

WIRELESS SECURITY

Done by

ANISH KUMAR

of VII semester Computer Science & Engineering in the year 2010 in partial fulfillment of the requirements for the award of Degree of Bachelor of Technology in Computer Science & Engineering of Cochin University of Science & Technology

Dr.David Peter S
Head of the Division

Ms. Ancy Zachariah
Seminar Guide

ACKNOWLEDGEMENT

At the outset, I thank God almighty for making my endeavor a success. I am indebted to my respected teachers and supporting staffs of Division Of Computer Engineering for providing me inspiration and guidance for my seminar.

I am grateful to **Dr. David Peter S.,** Head of Division of Computer Engineering for giving such an opportunity to utilize all resources needed for the seminar.

I am highly obliged to my guide **Ms. Ancy Zachariah** and our seminar coordinator **Mr. Sudheep Elayidom M.** for their valuable instructions, guidance and corrections in our seminar and its presentation.

I also want to express sincere gratitude to all friends for their support and encouragement during the seminar presentation and their active participation in questioning session for the success of the seminar.

ANISH KUMAR

Reg.NO-12080012

CSE, S-7

ABSTRACT

Wireless network differ with the wired network at the data link layer and physical layer. Wireless transmission takes place through the open air. So it is more easy to eavesdrop. For secure transmission of data from the wireless network different types of encryption algorithms are used.

WEP was the first attempt at securing or providing confidentiality over wireless communications. In 2001, weaknesses in WEP were identified, and as a result, today WEP can be cracked within minutes.

WPA was an interim solution to the security flaws discovered in WEP. It implements most of what is found in the 802.11i specifications. It uses TKIP (Temporal Key Integrity Protocol) as the underlying security protocol which is based on RC4.WPA2 is improvement of WPA.

Wireless network has some advantage and disadvantages. But now a day it is widely used network type.

CONTENTS

01. INTRODUCTION.....01

02. WIRELESS NETWORK.....03

03 .802.11 WIRELESS LAN STANDARD.....05

3.1 802.11a……..05

3.2 802.11b……...05

3.3 802.11g……05

04. CONNECTION OF WIRELESS DEVICES TO ACCESS POINT.....06

05. WIRELESS SECURITY ENCRYPTION ALGORITHMS.....07

5.1 WIRED EQUIVALENT PRIVACY (WEP)……..……...08

5.1.1 WEP PROBLEMS……...10

5.2 WIRELESS PROTECTED ACCESS (WPA)……12

5.2.1 WEP IMPROVMENTS……...……....12

5.2.2 WPA WEEKNESSES…….....15

5.3 WIRLESS PROTECTED ACCESSS2 (WPA2)……...16

06. WIRELESS SECURITY PRECUATION.....17

07. ADVANTAGES AND DISADVANTAGES OF WIRELESS.....19

08. SUMMARY.....21

09. REFERENCES.....22

LIST OF TABLES:

Table 5.1 comparison between WEP, WPA and WPA2

List of figures:

Fig 2.1	OSI Reference Model of 802.11
Fig 4.1	connection of wireless device to AP
Fig 5.1	WEP encryption Algorithm (Sender Side)
Fig 5.2	WEP encryption Algorithm (Recipient Side)
Fig 5.3	RC4 Algorithm
Fig 5.4	TKIP Detail Encryption Algorithm

List of abbreviations:

WLAN-wireless local area network

FHSS-frequency hopping spread-spectrum

DSSS-direct sequence spread-spectrum

MAC-Media Access Control layer

LCC- Logical Link Control

WEP-Wired equivalent privacy

WPA-wireless protected access

WPA2- wireless protected access 2

IV- Initialization Vector

TKIP- Temporal Key Integrity Protocol

PRNG- Pseudo-Random Number Generator

CRC- Cyclic Redundancy Code

MIC- Michael

IEEE – Institute of Electrical and Electronic Engineers

CHAPTER 1

INTRODUCTION

Wireless networks are convenient and popular, but without security are easy to hack and leave your data at risk. This report gives a brief overview of the most popular forms of wireless security for home networks.

Hacking a computer network has been the plot of many a Hollywood movie, but the truth is that most wireless routers do not enable wireless security by default, and "hacking" an unsecured wireless network is as simple as viewing a list of available wireless networks in Windows and double clicking on any network that is unsecured. Not only does this make stealing bandwidth trivial, but if we have file sharing enabled you could find your personal photos, financial records or emails freely visible to anyone with a laptop within a few hundred feet.

The good news is that protecting your wireless network is not difficult, and there are a number of well supported standards that allow us to limit access to our wireless network.

Wired Equivalent Privacy, or WEP, was introduced in 1999. Its goal was to provide a wireless network with the same security inherent to the traditional wired networks. In a typical scenario implementing WEP is as simple as creating a key (which is basically a password) of 10 or 26 hexadecimal (i.e. between 0 and 9, A and F) characters which is saved in the router, and then used by any wireless client wanting to connect to it. An example WEP key is *74534b7126*.

However since its introduction a number of flaws have been discovered in WEP. The obscure nature of the WEP key may give WEP a false sense of security, but from a cryptographic standpoint it is a relatively easy system to break. A quick web search on "WEP cracking" will yield detailed instructions on how to crack a WEP wireless network in minutes using mainstream and freely available hardware and software.

The vulnerabilities inherent in WEP prompted the creation of Wi-Fi Protected Access (WPA) in 2003. WPA addresses WEP's insecurity, and is usually supported in older devices by way of a firmware update. In a typical scenario implementing WPA involves creating a key of between 8 and 63 characters. Just like WEP, this key is saved in the router and then used by any wireless client wanting to connect to it. But unlike WEP the WPA key is usually an ASCII string like *pa55w0rd*, which is much easier to remember. This form of WPA is known as WPA Pre-Shared Key (WPA-PSK). It is the most common usage of WPA in small networks and home networks. WPA Enterprise allows authentication against a RADIUS server, however the added complexity of having a dedicated server hosting user credentials restricts the usage of WPA Enterprise to larger networks.

WPA2 is the successor to WPA, and since 2006 support for WPA2 has been mandatory for all "Wi-Fi CERTIFIED" devices. WPA2 offers increased security over WPA, but its relatively recent introduction means that not all wireless devices support it.

Given how easy it is to connect to an unsecured wireless network it is imperative that you implement some form wireless security. In a home or small business environment WPA is just as easy to set up as WEP and provides better security. Should our network hardware support it, WPA2 offers even better security.

CHAPTER 2

WIRELESS NETWORK

In 1997, the IEEE ratified the 802.11 Wireless LAN standards, establishing a global standard for implementing and deploying Wireless LANS. The throughput for 802.11 is 2Mbps, which was well below the IEEE 802.3 Ethernet counterpart. Late in 1999, the IEEE ratified the 802.11b standard extension, which raised the throughput to 11 Mbps, making this extension more comparable to the wired equivalent. The 802.11b also supports the 2 Mbps data rate and operates on the 2.4GHz band in radio frequency for high-speed data communications

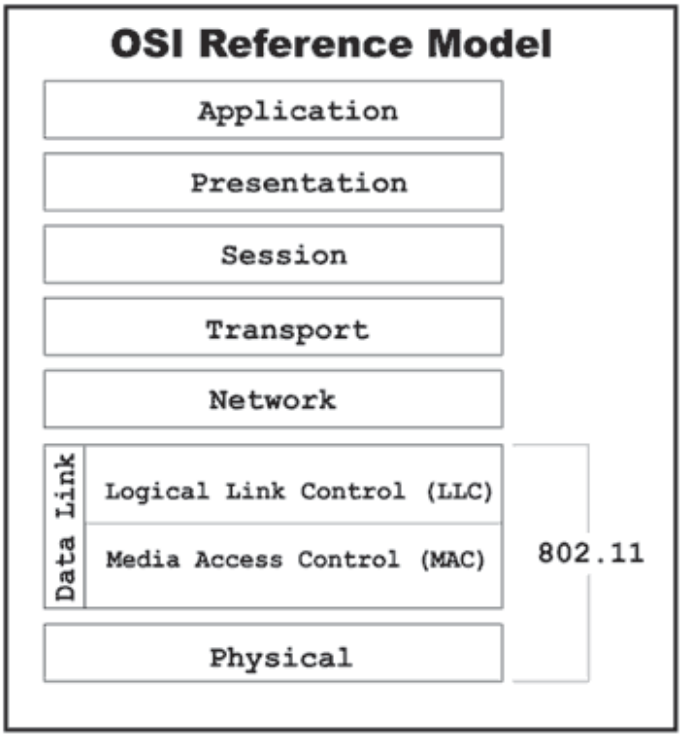

Figure 2.1: OSI Reference Model of 802.11

As with any of the other 802 networking standards (Ethernet, Token Ring, etc.), the 802.11 specification affects the lower layers of the OSI reference model, the Physical and Data Link layers.

The Physical Layer defines how data is transmitted over the physical medium. The IEEE assigned 802.11 two transmission methods for radio frequency (RF) and one for Infrared. The two RF methods are frequency hopping spread-spectrum (FHSS) and direct sequence spread-spectrum (DSSS). These transmission methods operate within the ISM (Industrial, Scientific, and Medical) 2.4 GHz band for unlicensed use. Other devices that operate on this band include remote phones, microwave ovens, and baby monitors.

FHSS and DSSS are different techniques to transmit data over radio waves. FHSS uses a simple frequency hopping technique to navigate the 2.4GHz band which is divided into 75 sub-channels 1MHz each. The sender and receiver negotiate a sequence pattern over the sub-channels.

DSSS, however, utilizes the same channel for the duration of the transmission by dividing the 2.4 GHz band into 14 channels at 22MHz each with 11 channels overlapping the adjacent ones and three non-overlapping channels. To compensate for noise and interference, DSSS uses a technique called "chipping", where each data bit is converted into redundant patterns called "chips".

The Data Link layer is made up of two sub-layers, the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The Data Link layer determines how transmitted data is packaged, addressed and managed within the network. The LLC layer uses the identical 48-bit addressing found in other 802 LAN networks like Ethernet where the MAC layer uses a unique mechanism called carrier sense multiple access, collision avoidance (CSMA/CA). This mechanism is similar to the carrier sense multiple access collision detect (CSMA/CD) used in Ethernet, with a few major differences. Opposed to Ethernet, which sends out a signal until a collision is detected before a resend, CSMA/CA senses the airwaves for activity and sends out a signal when the airwaves are free. If the sender detects conflicting signals, it will wait for a random period before retrying. This technique is called "listening before talking" (LBT) and probably would be effective if applied to verbal communications also.

To minimize the risk of transmission collisions, the 802.11 committee decided a mechanism called Request-To-Send / Clear-To-Send (RTS/CTS). An example of this would be when an AP accepts data transmitted from a wireless station; the AP would send a RTS frame to the wireless station that requests a specific amount of time that the station has to deliver data to it. The wireless station would then send an CTS frame acknowledging that it will wait to send any communications until the AP completes sending data. All the other wireless stations will hear the transmission as well and wait before sending data. Due to the fragile nature of wireless transmission compared to wired transfers, the acknowledgement model (ACK) is employed on both ends to ensure that data does not get lost in the airwaves.

CHAPTER 3

802.11 WIRELESS LAN STANDARD

Several extensions to the 802.11 standard have been either ratified or are in progress by their respective task group committees. Below are three current task group activities that affect WLAN users most directly.

2.1 802.11a

The 802.11a ("another band") extension operates on a different physical layer specification than the 802.11 standard at 2.4GHz. 802.11a operates at 5GHz and supports date rates up to 54Mbps. The FCC has allocated 300Mz of RF spectrum for unlicensed operation in the 5GHz range. Although 802.11a supports much higher data rates, the effective distance of transmission is much shorter than 802.11b and is not compatible with 802.11b equipment and in its current state is usable only in the US. However, several vendors have embraced the 802.11a standard and some have dual band support AP devices and network cards.

2.2 802.11b

The 802.11b ("baseline") is currently the de facto standard for Wireless LANs. As discussed earlier, the 802.11b extension raised the data rate bar from 2Mbps to 11Mbps, even though the actual throughput is much less. The original method employed by the 802.11 committee for chipping data transmissions was the 11-bit chipping encoding technique called the "Barker Sequence". The increased data rate from 2Mbps to 11Mbps was achieved by utilizing an advanced encoding technique called Complementary Code Keying (CCK). The CCK uses Quadrature Phase Shift Keying (QPSK) for modulation to achieve the higher data rates.

2.3 802.11g

The 802.11g ("going beyond b") task group, like 802.11a is focusing on raising the data transmission rate up to 54Mbps, but on the 2.4MHz band. The specification was approved by the IEEE in 2001 and is expected to be ratified in the second half of 2002. It is an attractive alternative to the 802.11a extension due to its backward compatibility to 802.11b, which preserves previous infrastructure investments

CHAPTER 4

CONNECTION OF WIRELESS DEVICES TO ACCESS POINT

The following steps explain the process of how a wireless station associates to an AP using shared key authentication.

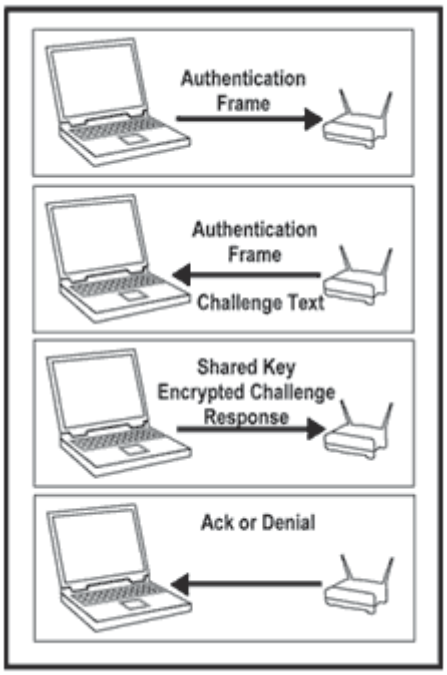

Figure: 4.1 connection of wireless device to AP

1) The wireless station begins the process by sending an authentication frame to the AP it is trying to associate with.

2) The receiving AP sends a reply to the wireless station with its own authentication frame containing 128 octets of challenge text.

3) The wireless station then encrypts the challenge text with the shared key and sends the result back to the AP.

4) The AP then decrypts the encrypted challenge using the same shared key and compares it to the original challenge text. If the there is a match, an ACK is sent back to the wireless station, otherwise a notification is sent back rejecting the authentication.

It is important to note that this authentication process simply acknowledges that the wireless station knows the shared key and does not authenticate against resources behind the AP. Upon authenticating with the AP, the wireless station gains access to any resources the AP is connected to.

CHAPTER 5

WIRELESS SECURITY ENCRYPTION ALGORITHM

Wired Equivalent Privacy (WEP) is better known as Wireless Encryption Protocol. The protocol was designed for offering security to wireless networks. WEP was initially built to offer almost the same level of security to the wireless networks as other protocols offer to the wired ones. It offers a widely supported security base for your networks but most of them are still susceptible as WEP is often disabled on local wireless systems. Though widely used, the Wireless Encryption Protocol or WEP, is not fully secure.

Even on networks that have active wireless encryption protocol, the chances of being compromised are high. Experienced hackers can easily break into the WEP security systems. Most of the modern wireless devices such as wireless routers, wireless Internet modems etc. carry the provision of using the protocol to offer a minimum level of protection.

Beginning the decade 2000, there was a rise in software capable of decrypting the WEP security. To counter this, IEEE came up with Wi-Fi protected access. This is popularly known as WPA. Soon after, another advancement of WPA was released under the name of WPA2. Though the WPA is based on the weaknesses of WEP, there is much difference among WEP, WPA, and WPA2. To be more precise, WPA is more oriented towards Wi-Fi connections and hotspots while WEP is concerned with the low level protection of data travelling through the different devices on any type of wireless network. These include routers, wireless data cards, and Wi-Fi devices as well.

Summarizing the difference in these protocols, WPA and WPA2 offer better protection to Wi-Fi connections while WEP is concerned with all kinds of wireless network components. If you cannot implement WPA2 or WPA on a network device, you can still use WEP to get minimal protection against eavesdropping (type of hacking).

4.1 **Wired Equivalent Privacy (WEP)**

The Wired Equivalent Privacy (WEP) was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication.

A. In the sender side:

WEP try to use from four operations to encrypt the data (plaintext).At first, the secret key used in WEP algorithm is 40-bit long with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key. Secondly, the resulting key acts as the seed for as Pseudo-Random Number Generator (PRNG).Thirdly, the plaintext throw in a integrity algorithm and concatenate by the plaintext again. Fourthly, the result of key sequence and ICV will go to RC4 algorithm. A final encrypted message is made by attaching the IV in front of the Cipher text. Now in "Fig. 3" define the objects and explain the detail of operations.

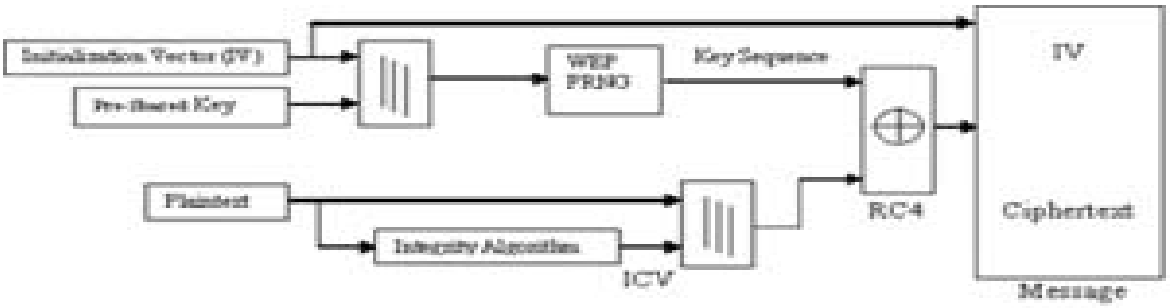

Figure 5.1: WEP encryption Algorithm (Sender Side)

B. *In the Recipient side:*

WEP try to use from five operations to decrypt the received side (IV+ Cipher text).At first, the Pre-Shared Key and IV concatenated to make a secret key. Secondly, the Cipher text and Secret Key go to in CR4 algorithm and a plaintext come as a result. Thirdly, the ICV and plaintext will separate. Fourthly, the plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally the new ICV (ICV') compare with original ICV. In "Fig. 4" you can see the objects and the detail of operations schematically:

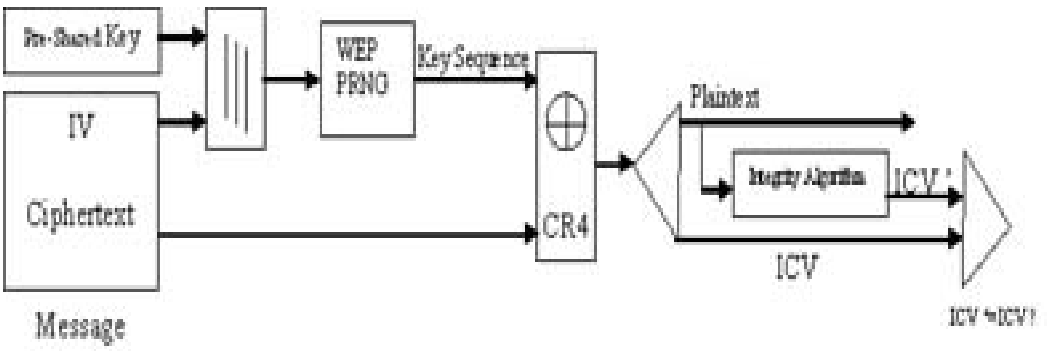

Figure 5.2: WEP encryption Algorithm (Recipient Side)

Now try to describe and define all of boxes in 2 previous diagrams:

Initialization Vector (IV):

is a randomly bits that size of it depends on the encryption algorithm and is normally as large as the block size of the cipher or as large as the Secret key. The IV must be known to the recipient of the encrypted information to be able to decrypt it that in WEP algorithm does this by transmitting the IV along with the packet. For two different lengths (64, 128 bit) of keys IV is 24-bit.

Pre-Shared Key:

is a simple 5- or 13-character password that is shared between the access point and all wireless network users. This key is available by administrator an bye system auto generation. For the 64-bit key the length of secret key is 40 bits and for 128-bit key the length is 104 bits.

PRNG:

In WEP defined a method to create a unique secret key for each packet using the 5- or 13-characters of the pre-shared key and three more pseudo-randomly selected characters picked by the wireless hardware (IV). For example, our Pre-shared key is "ARASH". This word would then be merged with "AHL" as IV to create a secret key of "AHLARASH", which would be used in encryption operations of packet. The next packet would still use "ARASH", but concatenate it this time with "ARA" to create a new secret key of "ARAARASH". This process would randomly continue during the transmission of data.

ICV & Integrity Algorithm (CRC-32):

is one of hashing algorithm and it is abbreviated of "Cyclic Redundancy Code". CRCs is a family of algorithms and CRC32 is one certain member of this family (other members are CRC16, XMODEM...) that 32 represent the length of checksum in bits (= 4Byte). The "CRC" term is reserved for algorithms that are based on the "polynomial" division idea. The base of the idea to compute the checksum in all CRC algorithms is the same.

RC4:

RC4 that is not specific to WEP; it is a random generator, also known as a key stream generator or a stream cipher, and was developed in RSA Laboratories in 1987. RC4 works by logically XORing the key to the data. In the fig.3you can see the operation of RC4 simply:

Figure 5.3: RC4 Algorithm

For example, if the data has the format 10010100 and the key is 1011, then RC4 (data, key) = 00101111. Since RC4 is a two-way algorithm, a second call to RC4 (encrypted data, key) is 10010100 which is the original data.

4.1.1 WEP PROBLEMS

Size of IV is short and reused

Regardless of the key size, 24-bit long of WEP's IV can only provide 16,777,216 different RC4 cipher streams for a given WEP key. On a busy network this number can be achieved in a few hours and reuse of the same IV then becomes unavoidable. In WEP the RC4 cipher stream is XOR.ed with the original packet and the IV is sent in the clear format with each packet. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV or can forge packets. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them, i.e., the key stream or the shared secret key. Because XORing two ciphertexts that use the same key stream would cause the key stream to be cancelled out and the result would be the XOR of the two plaintexts. Key management is lack and updating is poor. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access points and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is difficult, network administrators must personally visit each wireless device in use and manually enter the appropriate WEP key. Access points and client stations must be programmed with the same WEP key. Since the change of keys task is tedious and difficult, they are rarely changed by the system administrators. This may be acceptable at the installation stage of a WLAN or when a new client joins the network, but anytime the key becomes compromised or there is a loss of security, the key must be changed. This may not be a huge issue in a small organization with only a few users, but it can be impractical in large corporations, which typically have hundreds of users.

Problem in the RC-4 algorithm

RC4 implementation has been considered to have weak keys, meaning that there is more correlation between the key and the output than there should be. Determination of which packets were encrypted with weak keys is an easy job. Since the first three bytes of the key are taken from the IV that is sent unencrypted in each packet, this weakness can be exploited easily by a passive attack. Out of the 16 million IV values available, about 9,000 are interesting. They indicate the presence of weak keys. The attacker captures "interesting packets" filtering for IVs that suggest weak keys, then

analyses them and only has to try a small number of keys to gain access to the network. Because all original IP packets start with a known value, it's easy to know when he/she has the right key. To determine a 104-bit WEP key, he/she has to capture between 2,000 and 4,000 interesting packets. On a fairly busy network the capture of the interesting 5,000 packets might not pose any difficulty and can be achieved in a short period of time.

Easy forging of authentication messages

802.11 standards declare two types of authentication; Open System and Shared Key authentication. The theoretical idea was that an authentication would be better than no authentication. But in reality the opposite is emerged to be true. Turning on authentication with WEP, actually reduce the total security of the network and make it easier to guess WEP key for the intruders and attackers. Shared Key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. The problem here is, any monitoring attacker can observe the challenge and the encrypted response. From those, then can determine the RC4 stream used to encrypt the response, and use that stream to encrypt any challenge he/she would receive in the future. So by monitoring a successful authentication, the attacker can later forge an authentication. The only advantage of Shared Key authentication is that it reduces the ability of an attacker to create a denial-of-service attack by sending garbage packets (encrypted with the wrong WEP key) into the network. To handle the task of proper authenticating wireless users turn off Shared Key authentication and depend on other authentication protocols, such as 802.1x.

4.2 Wireless Protected Access (WPA)

The WPA came with the purpose of solving the problems in the WEP cryptography method, without the users need to change the hardware. The standard WPA similar to WEP specifies two operation manners:

A. Personal WPA or WPA-PSK (Key Pre-Shared) that use for small office and home for domestic use authentication which does not use an authentication server and the data cryptography key can go up to 256 bits. Unlike WEP, this can be any alphanumeric string and is used only to negotiate the initial session with the AP. Because both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air.

B. Enterprise WPA or Commercial that the authentication is made by an authentication server 802.1x, generating an excellent control and security in the user's traffic of the wireless network. This WPA uses 802.1X+EAP for authentication, but again replaces WEP with the more advanced TKIP encryption. No preshared key is used here, but you will need a RADIUS server. And you get all the other benefits 802.1X+EAP provides, including integration with the Windows login process and support for EAP-TLS and PEAP authentication methods. The main reason why WPA generated after WEP is that the WPA allows a more complex data encryption on the TKIP protocol (Temporal Key Integrity Protocol) and assisted by MIC (Message Integrity Check) also, which function is to avoid attacks of bit-flipping type easily applied to WEP by using a hashing technique. We draw a whole picture of WPA process.

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

4.2.1 WEP IMPROVEMENTS

In the comparison between TKIP and WEP there are four improvements in Encryption algorithm of WPA that added to WEP:

1. A cryptographic message integrity code, or MIC, called Michael, to defeat forgeries.

2. A new IV sequencing discipline, to remove replay attacks from the attacker's arsenal.

3. A per-packet key mixing function, to de-correlate the public IVs from weak keys.

4. A rekeying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

Now we explain these four algorithms one by one:

***MIC* or Michael:**

Michael is the name of the TKIP message integrity code. It is an entirely new MIC designed that has 64-bits length and represented as two 32-bit little-Endian words (*K*0,*K*1). The Michael function first pads a message with the hexadecimal value 0x5a and enough zero pad to bring the total message length to a multiple of 32-bits, then partitions the result into a sequence of 32-bit words *M*1 *M*2 … *Mn*, and finally computes the tag from the key and the message words using a simple iterative structure:

$(L,R) \leftarrow (K0,K1)$

do *i* **from** 1 **to** *n*

$L \leftarrow L$ *XOR*

*M*i

$(L,R) \leftarrow \text{Swap}(L,R)$

return (*L*,*R*) as the tag

The Michael verification predicate reruns the tagging function over the message and returns the result of a bitwise compare of this locally computed tag and the tag received with the message. The security level of a MIC is usually measured in bits. If the security level of a MIC is *s* bits, then, by definition, the time required for an attacker to construct a forgery is, on average, after about 2^{-s+1} packet.

New IV sequencing discipline For Defeating Replayed:

One forgery a MIC cannot detect is a replayed packet. This occurs when an adversary records a valid packet in flight and later retransmits it. To defeat replays, TKIP reuses the WEP IV field as a packet sequence number. Both transmitter and receiver initialize the packet sequence space to zero whenever new TKIP keys are set, and the transmitter increments the sequence number with each packet it sends. TKIP requires the receiver to enforce proper IV sequencing of arriving packets. TKIP defines a packet as out-of-sequence if its IV is the same or smaller than a previous correctly received MPDU associated with the same encryption key. If an MPDU arrives out of order, then it is considered to be a replay, and the receiver discards it and increments a replay counter.

Key Mixing:

As you saw in "Fig.4.1" and "Fig.4.2" WEP constructs a perpacket RC4 key by concatenating a base key and the packet IV. The new per-packet key that called the

TKIP key mixing function substitutes a *temporal key* for the WEP base key and constructs the WEP per-packet key in a novel fashion. Emporal keys are so named because they have a fixed lifetime and are replaced frequently. The mixing function operates in two phases:

Phase 1 eliminates the same key from use by all links: Phase 1 combines the 802 MAC addresses of the local wireless interface and the temporal key by iteratively XORing each of their bytes to index into an S-box, to produce an *intermediate key*. Stirring the local MAC address into the temporal key in this way causes different stations and access points to generate different intermediate keys, even if they begin from the same temporal key—a situation common in ad hoc deployments. This construction forces the stream of generated per-packet encryption keys to differ at every station, satisfying the first design goal. The Phase 1 intermediate key must be computed only when the temporal key is updated, so most implementations cache its value as a performance optimization.

Phase 2 de-correlates the public IV from known the per-packet key: Phase 2 uses a tiny cipher to encrypt the packet sequence number under the intermediate key, producing a 128-bit perpacket key. Actuality the first 3 bytes of Phase 2 output are exactly mach to the WEP IV, and the last 13 to the WEP base key, as existing WEP hardware expects to concatenate a base key to an IV to form the per-packet key. This design accomplishes the second mixing function design goal, by making it difficult for a rival to be connected to IVs and perpacket keys.

Rekeying or Defeating key collision attacks:

Rekeying delivers the fresh keys consumed by the various TKIP algorithms. Generally there are three key types: temporal keys, encryption keys and master keys. Occupying the lowest level of the hierarchy are the temporal keys consumed by the TKIP privacy and authentication algorithms proper. TKIP employs a pair of temporal key types: a 128-bit encryption key, and a second 64-bit key for data integrity. TKIP uses a separate pair of temporal keys in each direction of an association. Hence, each association has two pairs of keys, for a total of four temporal keys. TKIP identifies this set of keys by a two-bit identifier called a *WEP key id*. Now we can drawing a new figure from TKIP process with details of these four parts. ”fig.6”

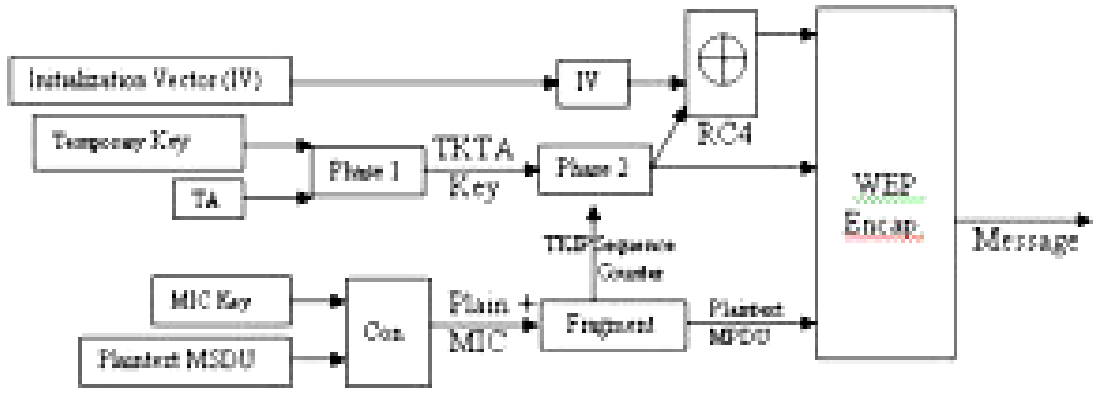

Figure 5.4: TKIP Detail Encryption Algorithm

4.2.2 WPA WEAKNESSES

In November 2003, Robert Moskowitz released "Weakness in Passphrase Choice in WPA Interface". In this paper he explains a formula that would reveal the passphrase by performing a dictionary attack against WPA-PSK networks. This weakness was based on the pairwise master key (PMK) that is derived from the concatenation of the passphrase, SSID, length of the SSID and nonces (a number or bit string used only once in each session). The result string is hashed 4,096 times to generate a 256-bit value and then combine with nonce values. The required information for generate and verify this key (per session) is broadcast with normal traffic and is really obtainable; the challenge then becomes the reconstruction of the original values. He explains that the pairwise transient key (PTK) is a keyed-HMAC function based on the PMK by capturing the four-way authentication.

Handshake, the attacker has the data required to subject the passphrase to a dictionary attack. Finally he found that "a key generated from a passphrase of less than about 20 characters is unlikely to deter attacks. For confirmation, in late 2004, Takehiro Takahashi, then a student at Georgia Tech, released WPA Cracker and Josh Wright, a network engineer and well-known security lecturer, released cowpatty around the same time. Both tool sare written for Linux systems and perform a brute-force dictionary attack against WPA-PSK networks in an attempt to determine the shared passphrase. Both require the user to supply a dictionary file and a dump file that contains the WPA-PSK four-way handshake. Both function similarly; however, cowpatty contains an automatic parser while WPA Cracker requires the user to perform a manual string extraction. Additionally, cowpatty has optimized the HMAC-SHA1 function and is somewhat faster. Each tool uses the PBKDF2 algorithm that governs PSK hashing to attack and determine the passphrase. Neither is extremely fast or effective against larger passphrases, though, as each must perform 4,096 HMAC-SHA1 related to the values as described in the Moskowitz paper.

4.3 Wireless Protected Access2 (WPA2)

As the name suggests, *WPA2* is a second, newer version of Wireless Protected Access (WPA) security and access control technology for Wi-Fi wireless networking. WPA2 is available on all certified Wi-Fi hardware since 2006 and was an optional feature on some products before that. It is designed to improve the security of Wi-Fi connections by requiring use of stronger wireless *encryption* than what WPA requires. Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations).

Most wireless routers for home networks support both WPA and WPA2 and administrators must choose which one to run. Obviously, WPA2 is the simpler, safer choice. Some techies point out that using WPA2 requires Wi-Fi hardware to work harder in running the more advanced encryption algorithms, which can theoretically slow down the network's overall performance compared to running WPA. Network owners can make their own choice but should run experiments to decide whether they notice any difference in their networks speeds with WPA2 vs. WPA.

COMPARISON BETWEEN WIRELESS SECURITY ALGORITHMS

	WEP	**WPA**	**WPA2**
Encryption	**RC4**	**RC4**	**AES**
Key rotation	**None**	**Dynamic session keys**	**Dynamic session keys**
Key distribution	**Manually typed into each device**	**Automatic distribution available**	**Automatic distribution available**
Authentication	**Uses WEP key as AuthC**	**Can use 802.1x & EAP**	**Can use 802.1x & EAP**

TABLE 5.1: comparison between WEP,WPA and WPA2

CHAPTER 6

WIRELESS SECURITY PRECAUTIONS

If you've just purchased an 802.11x router and you've plugged it in and it works, you are not done. You've just exposed your computers and network to anybody that drives by or might be in the next building. There are a couple things you can do to minimize security risk and even go so far as to eliminate it. Many of these precautions can be corrected simply by logging into your router configuration interface by pointing your browser to the IP address of your access point.

Change default names:

This is just good practice for ALL hardware and software. The default passwords are easily obtained and because so many people don't bother to take the simple step of changing them they are usually what hackers try first. Make sure you change the default password on your wireless router / access point to something that is not easily guessed like your last name.

Add passwords to all devices:

Protection of wireless device with the help of password is one way to secure wireless.

Disable broadcasting on network hubs:

Announcing that you have a wireless connection to the world is an invitation for hackers. You already know you have one so you don't need to broadcast it. Check the manual for your hardware and figure out how to disable broadcasting.

Don't give the network a name that identifies your company:

Don't give the network a name that identifies your company so that anybody can accidentally know about your company wireless network.

Move wireless hubs away from windows:

Wireless signal has less area of propagation. Weaker wireless signal is not easy to detect so it not easy to eavesdrop.

Use the built-in encryption:

WEP and WPA encrypt your data so that only the intended recipient is supposed to be able to read it. WEP has many holes and is easily cracked. 128-bit keys impact performance slightly without a significant increase in security so 40-bit (or 64-bit on some equipment) encryption is just as well. As with all security measures there are ways around it, but by using encryption you will keep the casual hackers out of your systems. If possible, you should use WPA encryption (most older equipment can be upgraded to be WPA compatible). WPA fixes the security flaws in WEP but it is still subject to DOS (denial-of-service) attacks.

Disable the features you don't use:

Disable the features that you don’t want so that nobody can access without your knowledge.

Put a firewall between the wireless network and other company computers:

Many wired and wireless routers have built-in firewalls. They are not the most technically advanced firewalls, but they help create one more line of defense. Read the manual for your hardware and learn how to configure your router to only allow incoming or outgoing traffic that you have approved.

CHAPTER 7

ADVANTAGES AND DISADVANTAGES OF WIRELESS

Advantages

Mobility:

The main advantage of wireless computing is virtually limitless mobility. Wireless technology provides the ability for users to connect to the internet or their office networks from virtually anywhere, without the hassles of wires. The only restriction you have is the range of your wireless network. The mobility to connect from anywhere from a factory floor to the top of a skyscraper allows extreme ease of use in environments where wires are extremely impractical.

Flexible

The lack of wires and the restrictions which they entail allows extreme flexibility in the layout of a computing environment. Users can position themselves anywhere in an office or outdoor environment, with their only restrictions being a consistant power supply. This allows for dynamic network computing, and improved mobility in any environment.

Resilience, Maintenance, and Expansion

Wireless systems often are more resilient than wired systems due to the simple fact that wires can be damaged through various processes such as fire, accidental destruction, water damage, and general aging and corrosion of wires and infrastructure. In addition, maintenance of wireless systems is much simpler as there are generally fewer components to a wireless system and they are often easily accessible. The expansion of a wireless network is also much simpler as no addition hubs or wires are required, all that is needed is a wireless network card.

Ease of Installation:

WLAN are also easy to install, an entire network can be put together in a matter of hours rather than days. WLAN may be installed where rewiring is impractical. Wireless systems can be installed in different environments and users can communicate with the existing wired network through access points or wireless adapters.

Cost:

A wireless network may cost less than a traditional network because it requires fewer pieces of physical hardware to set up. All that is required for a wireless network is a wireless router and a wireless adapter installed in each computer that is going to connect to the router. Many new computers come with wireless adapters built in.

Disadvantages

Interference:

Wireless networks suffer from the persistent problem of signal interference. Our modern society provides a large number of conveniences which produce radio signals which may interfere with the frequency of the wireless signals being sent. There are generally two types of signal interference in an office network environment. Inward interference is caused by things such as microwaves, elevator motors, and cordless phones. This interference can cause delays in the network or in the worst case, render it completely unusable. Outward interference is when your network interferes with other wireless networks such as navigation systems on aircraft. These problems can be combated by using a frequency management committee who monitors and assigns unique frequencies to various wireless networks.

High power consumption:

A major problem with wireless computing is power management. Currently batteries in mobile computing devices have limited amounts of energy, which can be quickly expended in the effort of sending wireless signals. The farther your device is from the destination of your message, the more power it requires to send the message. A commonly used solution to this problem is to operate the devices in power saving modes. This however eliminates the ability of the user to obtain real-time data.

Security

The major disadvantage to wireless computing is security. Radio waves can easily penetrate walls and buildings and the signals may be passively retrieved with out being noticed. This allows hackers to easily penetrate your network causing large amounts of damage. Even if your wireless signals are encrypted, if you are sending data to a wired network, the signal must be temporarily unencrypted leaving it vulnerable to hackers and other unfriendly parties.

Speed:

Wireless devices are almost always slower than the same network using a wired configuration (about 4 to 6 megabits per second).

Limited range:

Wireless LANs can transmit up to 1,00 feet without losing connection. The rule of wireless transmission is higher the data rate, the shorter the range.

CHAPTER 8

SUMMARY

Wireless LANs provide new challenges to security and network administrators those are outside of the wired network. The inherent nature of wireless transmission and the availability of published attack tools downloaded from the Internet, security threats must be taken seriously. Best practices dictate a well thought out layered approach to WLAN security. Access point configuration, firewalls, and encryption should be considered. Security policies should be defined for acceptable network thresholds and performance.

CHAPTER 9

REFERENCE

www.ieee.org

1) Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, "Wired Equivalent Privacy(WEP)", ICFCC Kuala Lumpur Conference, Published by IEEE Computer Society, Indexed by THAMSON ISI, 2009
2) Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, Priva "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)", ICFCC Kuala Lumpur Conference, Published by IEEE Computer Society, Indexed by THAMSON ISI, 2009

www.cse.org

http://en.wikipedia.org/wiki/Wireless_LAN_security