A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)

ARASH HABIBI LASHKARI
FCSIT, University of Malaya (UM)
Kuala Lumpur, Malaysia
a_habibi_l@hotmail.com

MIR MOHAMMAD SEYED DANESH
Faculty of Management (FOM), Multimedia University (MMU)
- 63100 Cyberjaya Malaysia
Mir_1362@yahoo.com

BEHRANG SAMADI
Faculty of Knowledge Management, Multimedia University (MMU) - 63100 Cyberjaya Malaysia
behrang_samadi@Yahoo.com

***Abstract*— Wireless technology has been gaining rapid popularity for some years. Adaptation of a standard depends on the ease of use and level of security it provides. In this case, contrast between wireless usage and security standards show that the security is not keeping up with the growth paste of end user's usage. Current wireless technologies in use allow hackers to monitor and even change the integrity of transmitted data. Lack of rigid security standards has caused companies to invest millions on securing their wireless networks. There are three major types of security standards in wireless. In our previous papers which registered in ICFCC 2009 Malaysia and ICCDA 2009 Singapore [1] [2], we explained the structure of WEP and WPA as first and second wireless security protocols and discussed all their versions, problems and improvements. Now, we try to explain WPA2 versions, problems and enhancements that have done solve the WPA major weakness. Finally we make a comparison among WEP and WPA and WPA2 as all wireless security protocols in Wi-Fi technology. In the next phase we hope that we will publish a complete comparison among wireless security techniques by add the WiMax security technique and make a whole comparison among all security protocols in this area.**

Keywords— Wireless Security, WEP, WPA, WPA2, 802.11i, 802.11X

I. INTRODUCTION

With reference to our previous paper in WEP (ICFCC2009 Conference), The 802.11 WLAN standards specify the two lowest layer of the OSI network model which are physical and data link layers. The major goals of IEEE for creating these standards were made different approach to the physical layer, for example different frequencies, different encoding methods, and share the same higher layers. They have succeeded, and the Media Access Control (MAC) layers of the 802.11a, b, and g protocols are considerably identical. At the next higher layer still, all 802.11 WLAN protocols specify the use of the 802.2 protocol for the logical link control (LLC) portion of the data link layer. As you can see in "Fig.1", in the OSI model of network, such protocols as TCP/IP, IPX, NetBEUI, and AppleTalk, still exist at higher layers. Each layer utilizes the services of the underside layers. "Fig. 1"

In WLANs, privacy is achieved by data contents protection with encryption. Encryption is optional in 802.11 WLANs, but without it, any other standard wireless device, can read all traffic in network. There have been three major generations of security approaches, which is mentioned below:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fa Protected Access)
- WPA2/802.11i (Wi-Fa Protection Access, Version 2)

Each of these protocols has two generations named as personal and enterprise template.

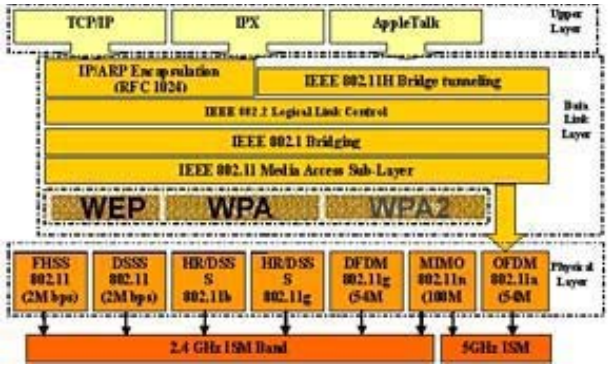

Fig-1: 802.11 AND OSI MODELL

II. WEP STATIC OR PERSONAL

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.

978-1-4244-4520-2/09/$25.00 ©2009 IEEE

Secondly, the resulting key acts as the seed for a 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.2" define the objects and explain the detail of operations.[1]

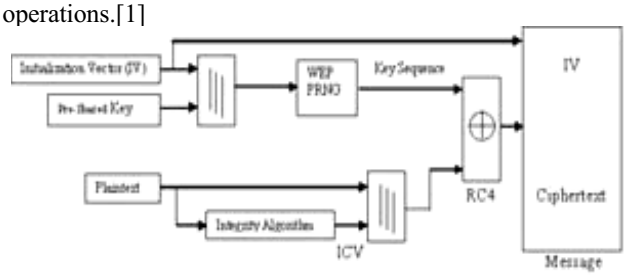

Figure 2: WEP encryption Algorithm (Sender Side)

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.3" you can see the objects and the detail of operations schematically [1]:

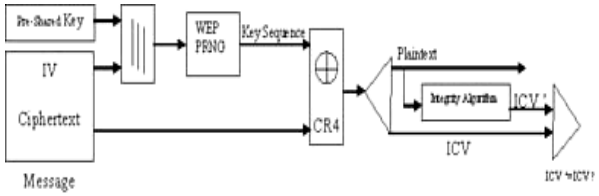

Figure 3: WEP encryption Algorithm (Recipient Side)

There are some other implementations of WEP that all of them are non-standard fixes and implemented by some companies. I will explain 3 of them here:

A. *WEP2*

This stopgap enhancement to WEP was present in some of the early 802.11i drafts. It was implement able on some (not all) hardware not able to handle WPA or WPA2, and extended both the IV and the key values to 128 bits. It was hoped to eliminate the duplicate IV deficiency as well as stop brute force key attacks. After it became clear that the overall WEP algorithm was deficient however (and not just the IV and key sizes) and would require even more fixes, both the WEP2 name and original algorithm were dropped. The two extended key lengths remained in what eventually became WPA's TKIP.

B. *WEP plus*

WEP+ is a proprietary enhancement to WEP by Agree Systems (formerly a subsidiary of Lucent Technologies) that enhances WEP security by avoiding "weak IVs". It is only completely effective when WEP plus is used at both ends of the wireless connection. As this cannot easily be enforced, it remains a serious limitation. It is possible that successful attacks against WEP plus will eventually be found. It also does not necessarily prevent replay attacks.

C. *Dynamic WEP*

Change WEP keys dynamically. Vendor-specific feature provided by several vendors such as 3Com. The dynamic change idea made it into 802.11i as part of TKIP, but not for the actual WEP algorithm.

III. WEP WEAKNESSES AND ENHANCEMENTS

With reference to our previous article in ICFCC 2009 Conference [1], we explain about problems and solutions on WEP, finally we can found these results from our previous article:

- *WEP does not Prevent forgery of packets.*
- *WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.*
- *WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.*
- *WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.*
- *WEP allows an attacker to undetectably modify a message without knowing the encryption key.*
- *Key management is lack and updating is poor.*
- *Problem in the RC-4 algorithm.*
- *Easy forging of authentication messages.*

And we found these Enhancements over WEP in that article:

Improved data encryption (TKIP), User authentication (Use EAP Method) and Integrity (Michael Method).

Now we try to explain the WPA structure and discuss about problems and improvements on it.

IV. WPA PERSONAL OR COMMERCIAL

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

1. *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.*

2. *Enterprise WPA or Commercial that the authentication is made by an authentication server 802.1x, generating an excellent control and security in the users' traffic of the wireless network. This WPA uses 802.1X+EAP 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.

Refer to the "Fig.2" and "Fig.3" you can see the whole picture of WEP processes in sender and receiver sides, now we draw a whole picture of WPA process "Fig. 4".

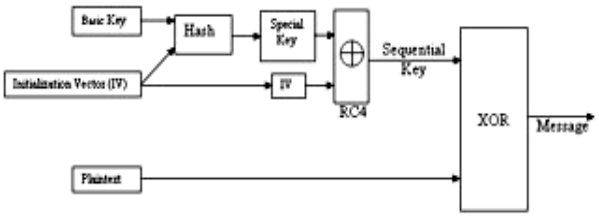

Figure 4: WPA Encryption Algorithm (TKIP)

As you see, 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.

V. WPA 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 Michae:** 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 $M_2 \ldots M_n$, and finally computes the tag from the key and the message words using a simple iterative structure:

$(L,R) \leftarrow (K_0,K_1)$
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 bit-wise 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 Replayd:

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.1" and "Fig.2" WEP constructs a per-packet 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. Temporal 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 per-packet 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 per-packet 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.5”

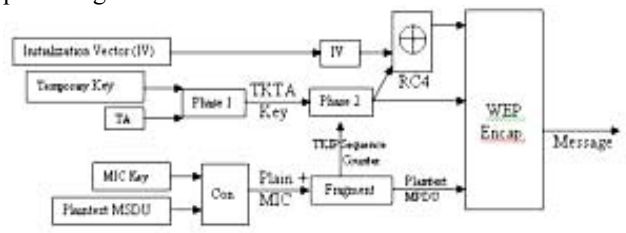

Figure 5: TKIP Detail Encryption Algorithm

VI. 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.”[10]

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 tools are 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. [11]

VII. WPA2 PERSONAL OR ENTERPRISE

The 802.11i standard is virtually identical to WPA2, and the terms are often used interchangeably 802.11i and WPA2 are not just the future of wireless access authentication - they are the future of wireless access. Wireless access is still in its infancy, in spite of the purchase and deployment of several million access points and wireless clients. The majority of these access points and clients are relatively immobile. Users sit down with their laptops at a conference table and connect, or a clerk stays within a relatively small area such as a warehouse, using wireless equipment to track inventory.

WPA was provided as an interim solution, and it had a number of major constraints. WPA2 was designed as a future-proof solution based on lessons learned by WEP implementers. Motorola is a key contributor and proponent of the WPA2 standard, and provides next generation products based on this standard.

WPA2 will be a durable standard for many reasons. One of the most important choices was that of the encryption algorithm. In October 2000, the National Institute of Standards and Technology (NIST) designated the Advanced Encryption Standard (AES) as a robust successor to the aging Data Encryption Standard. AES is an extremely well documented international encryption algorithm free of royalty or patent, with extensive public review.

WPA2, like WPA, supports two modes of security, sometimes referred to as “home user” and “corporate.” In “home user” mode a pre-shared secret is used, much like WEP or WAP. Access points and clients are all manually configured to use the same secret of up to 64 ASCII characters, such as “this_is_our_secret_password.” An actual 256-bit randomly generated number may also be used, but this is difficult to enter manually into client configurations.
The “corporate” security is based on 802.1X, the EAP authentication framework (including RADIUS), one of several EAP types (such as EAP-TLS, which provides a much stronger authentication system), and secure key distribution. “Home user” security introduces the same security problems present in WEP and WPA-PSK. Here we explain “corporate” security.

In security algorithm of 802.11i providing key enabler for secure and flexible wireless networks, allowing for client authentication, wireless network authentication, key distribution and the pre-authentication necessary for roaming. In using 802.1X in conjunction with 802.11i, it is strongly suggested to use EAP as a framework for authentication, and use an EAP type for the actual authentication that provides the optimal balance between cost, manageability and risk mitigation. Most often an 802.1X setup uses EAP-TLS for authentication between the wireless client (supplicant) and the access point (authenticator). In theory, several options may replace EAP-TLS, but in practice this is rare.

In 802.1X, no such port exists until the client connects and associates to the wireless access point. This immediately poses a problem, since beacon packets and probe request/response packets cannot be protected or authenticated. Fortunately, access to this data is not very useful for attackers, other than for potentially causing denial-of-service attacks, and for identifying wireless clients and access points by their hardware MAC addresses.

An 802.1X wireless setup consists of three main components:

- Supplicant (the wireless client).
- Authenticator (the access point).
- Authentication server (usually a RADIUS server).

The supplicant initially connects to the authenticator, as it would to a WEP- or WPA protected network. Once this connection is established, the supplicant has in effect a network link to the authenticator (access point). The supplicant can then use this link to authenticate and gain further network access. The supplicant and authenticator first negotiate capabilities. These consist of three items:

- The pairwise cipher suite, used to encrypt unicast (point-to-point) traffic.
- The group cipher suite, used to encrypt multicast and broadcast (point-to-multiplepoints) traffic.
- The use of either a pre-shared key (PSK, or "home user" security, using a shared secret) or 802.1X authentication.

So, the main problem of WPA as a pairwise solved by divided the type of security to three categories witch just in one of them use pairwise and in two other use group cipher and pre-shared key.

CONCLUSIONS

In this research, continuing our previous papers in Conference ICFCC 2009 and ICCDA 2009:

At first, we explain the structure of WEP in sender and receiver side and describe all steps verbally and practically at the same time as a brief of our previous paper on the first generation of wireless security protocols.

Secondly, we discuss about the second generation of wireless security protocol as WPA and define the two modes and try to describe all major Improvements on WPA such as cryptographic message integrity code or MIC, new IV sequencing discipline, per-packet key mixing function and rekeying mechanism then make a whole diagram for WPA encryption and decryption. Finally, explain about the major problem on WPA that happed in the PSK part of algorithm.

Finally, we discuss about third generation of wireless security protocol as WPA2/802.11i and define two type of this security as home user and corporate. Then we explain the improvement that has done in this protocol for solve the WPA major problem. This is done by categorize the security to three groups and use group cipher and pre-shared key. We hope as continues papers in the next paper we will explain the WiMax and make a totally survey on wireless security protocols and try to design a whole diagram of security protocols and completely discuss on weaknesses and improvements of them.

ACKNOWLEDGMENT

We would like to express our appreciation to our parents and all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it.

REFERENCES

[1] Arash Habibi Lashkari, F. Towhidi, R. S. Hoseini, "Wired Equivalent Privacy(WEP)", ICFCC Kuala Lumpur Conference, 2009

[2] Arash Habibi Lashkari, Masood Mansoori, Amir Seyed Danesh;, "Wired Equivalent Privacy(WEP) versus Wi-fi Protected Access", ICCDA Singapore Conference, 2009

[3] Donggang Liu, P. N., "Security for Wireless Sensor Networks", Springer., November, 2006

[4] Garcia, R. H. a. M., "AN ANALYSIS OF WIRELESS SECURITY", CCSC: South Central Conference. 2006

[5] Kempf, J., "Wireless Internet Security: Architecture and Protocols ",Cambridge University Press. October, 2008

[6] Hani Ragab Hassan, Yacine Challal, "Enhanced WEP: An efficient solution to WEP threats", IEEE 2005

[7] Halil Ibrahim BULBUL, Ihsan BATMAZ, Mesut OZEL, "Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols"; e-Forensics January 2008, Adelaide ,Australia.

[8] Arunesh Mishra, William, A. Arbaugh, "An Initial Security Analysis of The IEEE 802.1X Standard", University of Meryland, 2002

[9] Vebjørn Moen, H˚avard Raddum, Kjell J. Hole; "Weaknesses in the Temporal Key Hash of WPA" ; Mobile Computing and Communications Review,2005

[10] John L. MacMichael ; " Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode"; Linux Journal, 2005

[11] Bhagyavati, Wayne C. Summers, Anthony DeJoie;"Wireless Security Techniques: An Overview"; InfoSec Conference, September 2004

[12] Yoshiaki Hori , Kouichi Sakurai ;"Security Analysis of MIS Protocol on Wireless LAN comparison with IEEE802.11i ";Mobility Conference , October 2006, Thailand