International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 49-58
© International Research Publication House
http://www.irphouse.com

Compare Various Routing Securities Strategies of Wireless Networks

[1]Er. Shikha Bansal and [2]Er. Manish Mahajan

[1]C.G.C Landran, Chandigarh, India
[2]Assistant Professor, Department of IT, C.G.C. Landran, Chandigarh, India

Abstract

Wireless technology has been very popular now days. This is because 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 security standards has caused companies to invest millions on securing their wireless networks. There are three major types of security standards in wireless. The aim of this paper is to make the non-specialist reader aware of the disadvantages and threats of the wireless security protocols. WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) and security protocols are examined in this respect. Then they are compared via the common features in order to give some insight to those who work with WLANs. We hope this paper give boost to the IT security staff and clarify the common questions of the non specialist reader.

Introduction

The major difference between wired and wireless networks is the way that how they transmit data. As for the security risks, the main difference between wired and wireless networks is how to access to the transmitted data. In wired networks this is only possible by tapping the media that is used for the network communication. In wireless networks the media used for communication is air. The transmitted data via the radio frequency can be accessed by equipment that is readily available in the market for a cheap price.

From the initial development stages of wireless technology and its security needs, experts knew that security would be the major issue. Wireless Networks are inherently less secure than traditional wired networks, since they broadcast information into the air and anyone within the range of and with the right equipment can easily intercept those transmissions. It is for sure that matching all security needs of a wireless network is not an easy task. There are a number of security issues that make securing a WLAN difficult.

There have been three major generations of security approaches, which is mentioned below

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

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

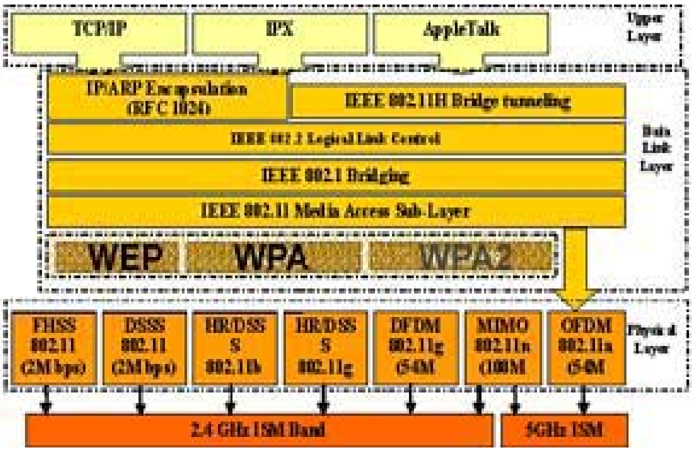


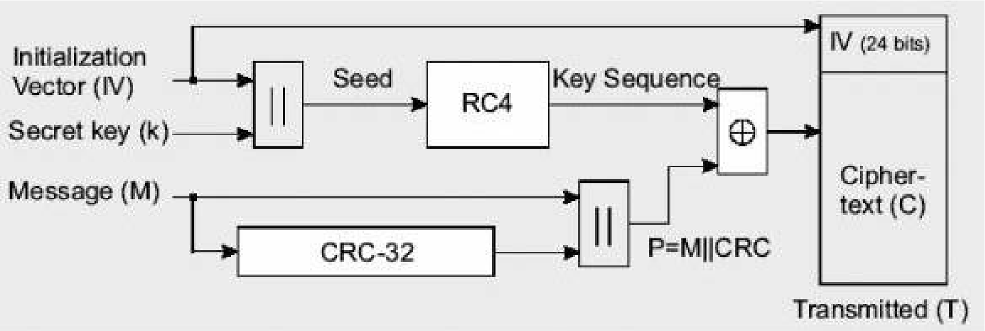
Figure 1: 802.11 AND OSI MODELL

Wired Equivalent Privacy (WEP)

The 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.

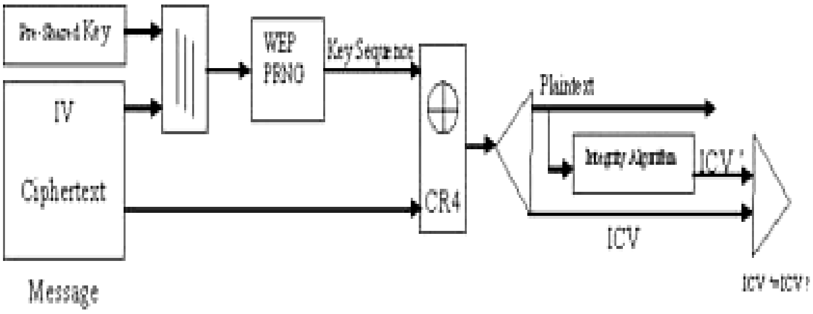
In the sender side

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 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.



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.



There are some other implementations of WEP that all of them are non-standard fixes. I will explain 3 of them which are as follows:

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.

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.

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.

WEP Weaknesses and Enhancements

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker cans 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)
- Integrity (Michael Method)

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

WPA Personal or Enterprise

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

- 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

- 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”.

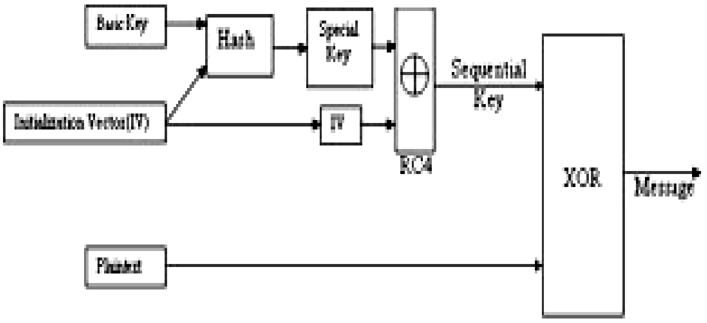


Figure 4: WPA Encryption Algorithm (TKIP)

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.

WPA Improvements

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

WEP

- A cryptographic message integrity code, or MIC, called Michael, to defeat forgeries.
- A new IV sequencing discipline, to remove replay attacks from the attacker's arsenal.
- A per-packet key mixing function, to de-correlate the public IVs from weak keys.
- 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-Endean words (K0, K1). 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 M1 M2 … Mn, and finally computes the tag from the key and the
Message words using a simple iterative structure:

```
(L, R) ← (N0, N1)
Do i from 1 to n
L ← L XOR Mi
(L, R) ← 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 the power –s+1packet.

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.1” and “Fig.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. 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 XO ring 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 aim. 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.

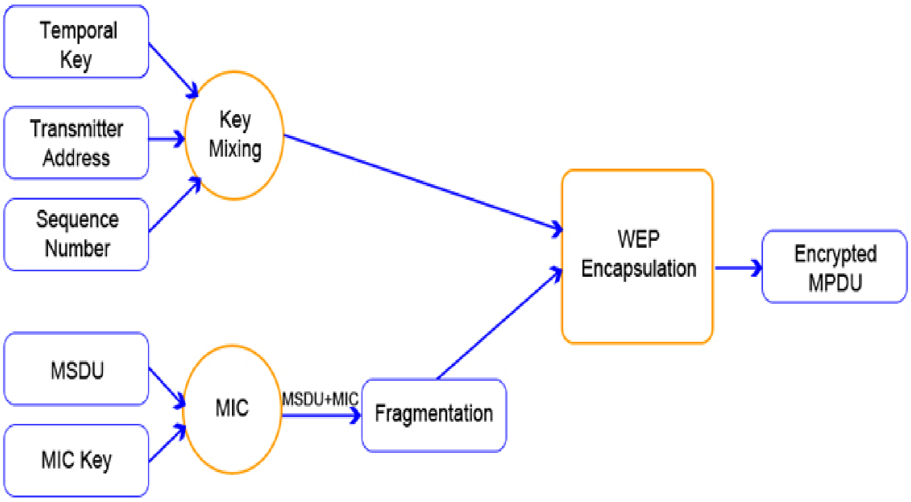
Phase 2: de-correlates the public IV from known theper-packet key:

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 aim, 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”



WPA Weaknesses

WPA and 802.11i provide for a Pre-Shared Key (PSK) as an alternative to 802.1X based key establishment. A PSK is a 256 bit number or a passphrase 8 to 63 bytes long. Each station MAY have its own PSK, tied to its MAC address. To date, vendors are only providing for one PSK for an ESS, just as they do for WEP keying.

When a PSK is used instead of 802.1X, the PSK is the Pairwise Master Key (PMK) that is used to drive the 4-way handshake and the whole Pair wise Transient Key (PTK) keying hierarchy. There is a straightforward formula for converting a passphrase PSK to the 256-bit value needed for the PMK.

This paper will look into the risks of using a PSK and particularly the risk associated with a passphrase-based PSK.

Comparison of WEP Mechanism, WPA Security Protocols

WEP has been regarded as a failure in wireless security, as it has been accepted by the IEEE that WEP was not aimed to provide full security. The original WEP security standard, using RC4 cipher is widely considered to be vulnerable and broken due to the insecure IV usage. It uses 40 bits of encryption key RC4 cipher by default (with vendor specific longer key support exceptions), concatenates key with IV values per packet sent over the air, with no key management mechanism embedded, having no automatic or periodic key change attribute associated with it, causing re-use and easy to capture small sized IVs that leads to key deciphering to the third parties. The data integrity check mechanism of WEP is not cipher protected and uses CRC-32, ICV providing no header integrity control mechanism and lack of replay attack prevention mechanism.

WPA, an interim solution to the WEP vulnerability, uses a subset of 802.11i features and had been generally believed as a major security improvement in wireless environment. In the
light of critics done towards WEP, WPA has numerous enhancements over WEP. Namely, RC4 – TKIP encryption cipher mechanism, 128 bits of key size, mixed type of encryption key per packet usage, 802.1x dynamic key management mechanism, 48 bits of IV size, 802.1x – EAP usage for authentication, providing data integrity and header integrity, ciphering aspect via MIC that is inserted into TKIP and IV sequence mechanism to prevent replay attacks and support for existing wireless infrastructures.

Features of Mechanism	WEP	WPA
Encryption Cipher Mechanism	RC4 (Vulnerable - IV Usage)	RC4 / TKIP
Encryption Key Size	40 bits *	128 bits
Encryption Key Per Packet	Concatenated	Mixed
Encryption Key Management	None	802.1x
Encryption Key Change	None	For Each Packet
IV Size	24 bits	48 bits
Authentication	Weak	802.1x - EAP
Data Integrity	CRC 32 - ICV	MIC (Michael)
Header Integrity	None	MIC (Michael)
Replay Attack Prevention	None	IV Sequence

Conclusions

Wireless networks can be a significant tool in increasing business productivity. As more implementations of wireless networks emerge due to user demand, the IT staff responsible for the system security have to understand the security threats that wireless technology poses. People who are after this technology need to plan and take proper security measures before and after implementing wireless networks in their environment to protect data.

However, as discussed in this paper, wireless networks bring with them a totally new set of security risks which must be evaluated and countered proactively. Often IT staff overlooks the importance of wireless security. Therefore, they need to understand the strengths and weaknesses of wireless technology, so they can take the appropriate steps to address those security issues.

With current technology one may insist that there is no reason not to trust a well setup wireless network but the cost of possible vulnerability exploitation is worth considering proactively. WLANs that are not managed properly might cause very serious risks to companies. So before installing any such networks, all risks must be identified, evaluated, and based on the results, the necessary counter measures must be installed to Secure the network.

Although no security system can ever be considered totally unbreakable, 802.11i RSN security seems to be a dependable one. It suffers none of the problems of older mechanisms and protocols namely WEP and WPA. So 802.11i RSN is a wireless security protocol that anybody can rely on until its vulnerabilities are brought out

For the time being in terms of cost versus security options, if full security preferred then RSN must be employed, if minimum cost preferred WEP must be employed, otherwise usage of WPA is recommended.

References

[1] Borisov. N., Goldberg, I., Wagner, D., Intercepting Mobile Communications :The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

[2] Fluhrer, S., Mantin, I., Shamir, A., Weaknesses in the Key Scheduling Algorithm of RC4. http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pd f

[3] Arbaugh,W., Shankar N., Justin Wan,Y.C.,¯Your 802.11 Wireless Network Has No Clothes. http://www.cs.umd.edu/~waa/wireless.pdf

[4] Stubblefield A., Ioannidis J., D. Rubin A.,Using the Fluhrer, Mantin, and Shamir Attack. to Break WEP. Revision 2, August 21,2001, AT&T Laboroties and Rice University. http://www.uninett.no/wlan/download/wep_attack.pdf

[5] 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

[6] Donggang Liu, P. N., "Security for Wireless Sensor Networks",Springer., November, 2006Garcia, R. H. a. M., "AN ANALYSIS OF WIRELESS SECURITY",CCSC: South Central Conference. 2006

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