Basic security measures for IEEE 802.11 wireless networks

Fundamentos prácticos de seguridad en redes inalámbricas IEEE 802.11

Oscar P. Sarmiento[1], Fabio G. Guerrero[2] and David Rey Argote[3]

ABSTRACT

This article presents a tutorial/discussion of three commonly-used IEEE 802.11 wireless network security standards: WEP, WPA and WPA2. A detailed analysis of the RC4 algorithm supporting WEP is presented, including its vulnerabilities. The WPA and WPA2 encryption protocols' most relevant aspects and technical characteristics are reviewed for a comparative analysis of the three standards in terms of the security they provide. Special attention has been paid to WEP encryption by using an educational simulation tool written in C++ Builder for facilitating the understanding of this protocol at academic level. Two practical cases of wireless security configurations using Cisco networking equipment are also presented: configuring and enabling WPA-Personal and WPA2-Personal (these being security options used by TKIP and AES, respectively).

Keywords: 802.11i, 802.1x, CCMP, TKIP, WEP, WLAN, WPA, WPA2.

RESUMEN

Este artículo presenta una discusión tutorial de tres estándares de seguridad de uso común en las redes inalámbricas IEEE 802.11: WEP, WPA y WPA2. Se realiza un análisis detallado del algoritmo RC4 que soporta a WEP y se indican sus vulnerabilidades. También se revisan los aspectos y características técnicas más relevantes de los protocolos de cifrado WPA y WPA2 con la finalidad de hacer un análisis comparativo de los tres estándares en términos de la seguridad que ellos proporcionan. Se ha dado especial atención al aspecto didáctico del funcionamiento del cifrado WEP mediante el desarrollo y uso de una herramienta de simulación escrita en C++ Builder para facilitar su comprensión a nivel académico. Igualmente, se presentan dos casos prácticos de seguridad de red inalámbrica con equipos del fabricante Cisco, habilitando y configurando WPA Personal y WPA2 Personal, opciones de seguridad que usan TKIP y AES, respectivamentements.

Palabras clave: 802.11i, 802.1x, CCMP, TKIP, WEP, WLAN, WPA, WPA2.

Recibido: enero 15 de 2008
Aceptado: junio 19 de 2008

Introduction

En Resources from the wired network side are exposed to unknown users if no action is taken to protect wireless local area network (WLAN) security; the Internet connection can be used by third parties for illegal activities and wired network traffic can be captured, leaving legitimate users at potential risk of identity theft. Some basic measures securing the network against casual access by inexperienced intruders but offering no real protection against expert intruder attacks are: changing both the access points (AP), factory default administration key and service set identifier (SSID), updating the APs to support Wi-Fi protected access (WPA) or Wi-Fi protected access 2 (WPA2) security, disabling the SSID broadcast to prevent connecting non-authorised users, filtering the media access control (MAC) address to allow known station only connection and adjusting transmitting power to restrict coverage to that which is strictly required. Truly effective measures for protecting a wireless network must include encryption and authentication.

Regarding encryption, WLAN hardware options are (in order of security encryption strength) wired equivalent privacy (WEP), WPA and WPA2. WEP is considered unsafe whilst WPA and WPA2 provide suitable security levels. The main difference between WPA and WPA2 is that the former supports encryption using temporal key integrity protocol (TKIP) whilst the latter supports encryption using advanced encryption standard (AES). Both WPA and WEP use the Rivest Cipher 4 or Ron's Code 4 (RC4) algorithm but WPA outperforms WEP because the encryption key changes dynamically for WPA.

The "Personal" version of WPA and WPA2 is known as a pre-shared key (WPA-PSK). The "Enterprise" version of WPA or WPA (known as WPA RADIUS) requires a RADIUS server

[1] Ingeniero electricista, Universidad del Valle, Colombia. Experto, Redes de Computadores. Profesor Auxiliar, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Colombia. Investigador, grupo de investigación SISTEL-UV. opolanco@univalle.edu.co
[2] Ingeniero en Electrónica y Telecomunicaciones, Universidad del Cauca, Colombia. Magíster, Sistemas Electrónicos, Bradford University, Reino Unido. Profesor asistente, Escuela de Ingeniería Eléctrica y Electrónica, Universidad del Valle, Colombia. Investigador, grupo de investigación SISTEL-UV. fguerrer@univalle.edu.co
[3] Ingenieo Electrónico, Universidad del Valle, Colombia. Ingeniero de Soporte, ZTE Corporation, Cali, Colombia. davidrey20@hotmail.com

to work in coordination with it.

WPA-PSK can provide adequate protection for a simple personal WLAN or a small office WLAN, provided the key (PSK) has been randomly chosen and its length is at least 20 characters (Mokowitz, 2003).

Both WPA and WP2 have eliminated many WEP weaknesses but it is still vulnerable to attacks, particularly in the PSK version.

Authentication should be used to avoid more serious attacks; it adds another level of security because the client station is required to authenticate on the network. IEEE 802.1x is the access control framework for both WPA and WPA2. IEEE 802.1x supports different types of extensible authentication protocol (EAP), in turn being responsible for carrying out the actual authentication. The network manager can decide whether the RADIUS server will be installed on a computer from the internal wired network or within the access point to provide authentication (if the AP allows such option).

Despite WEP's weakness, RC4 operation and characteristics must still be understand because WPA (reasonably safe and still frequently used) is based on the RC4 encryption algorithm, using regularly changing keys. WPA and WPA2 operation must also be considered.

It should be noted that WPA2 should be used with AES encryption for corporate WLAN and any of the authentication options supported by the 802.1X standard enabled. Furthermore, when some access restrictions must be applied to computers which are going to access a WLAN system, then these computers can be registered into any virtual local area network (VLAN) in the wired network and such VLAN be treated as an insecure network through a firewall.

Wired equivalent privacy (WEP)

WEP is an optional security mechanism for protecting wireless networks (IEEE Computer Society LAN MAN Standards Committee, 1999). WEP was included in clause 8.2 of the first version of 802.11 IEEE and has remained unchanged in newer versions of IEEE 802.11 b, 802.11g, 802.11a for ensuring compatibility amongst different versions. WEP is a standard encryption system implemented at the MAC level and is supported by most wireless solutions.

IEEE 802.11 standard security aspects

IEEE 802.11 provides security through encryption and authentication. Authentication can be done through an "open system" or "shared key" in either *ad hoc* mode or infrastructure mode.

A network station or an access point (AP) can grant permission to any station requesting connection in the open authentication system, or only those included in a predefined list. Only those stations having an appropriate encryption key will be authenticated in a shared-key system.

Encryption represents an effective means of preventing jeopardising transmitted data in wireless transmissions. 802.11 specifies an optional encryption capability called WEP; this establishes a similar level of security to that of wired networks using encryption of the data being transported by the radio signals. WEP uses the RC4 algorithm developed by RSA Data Security. WEP is also used for preventing unauthorised users from gaining access to WLANs (i.e., provides authentication); such purpose is not explicitly set out in 802.11 but is considered an important feature of WEP.

WEP is a critical element in obtaining minimum confidentiality and data integrity in WLAN systems based on 802.11 as well as providing access control through authentication. Consequently, most 802.11-compatible WLAN products support WEP as an optional feature.

Encryption

WEP uses a secret key shared between a wireless station and an access point. All data sent and received between station and access point can be encrypted by using the "shared key." 802.11 does not specify how the shared key should be established but allows for a table associating a unique key with each station. However, the same key is usually shared in practice amongst all stations and access points within a given WLAN system.

WEP applies a cyclic redundancy check (CRC-32) to plain text to protect cipher-text against unauthorised modifications while it is in transit, producing an integrity check value (ICV). ICV is a type of fingerprint for plain text; it is added to plain text and the result is encrypted with a "key stream" and sent to the recipient along with the initialisation vector in plain text (Figure 1).

The receiver combines the cipher-text with the key stream to retrieve both the plain text and the ICV. It is possible to verify that the decryption process has been correct and that the data has not been altered by applying the integrity check to the plain text and comparing the output with the ICV value received; if the two ICV values are identical (i.e. matching fingerprints) the message is authenticated.

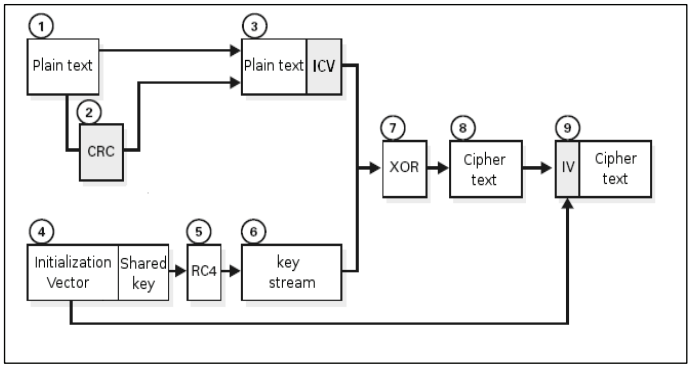

Figure 1. WEP encryption

Authentication

WEP provides two types of authentication: open system authentication (in which all users are allowed to access the WLAN) and shared key authentication controlling access to the WLAN and preventing unauthorised access to the network. Authentication through shared key is the safer of the two. The latter uses a secret shared key between all stations and access points in the WLAN system. When a station tries to connect to an access point this replies with a challenge random text. The station must use the copy of the shared secret key to encrypt the challenge text and return it to the access point for authentication. The access point decodes the response by using the same shared key and compares it to the challenge text sent earlier. If the two are identical texts, the access point sends a confirmation message to the station permitting access to the network; if the station does not have a key or it sends an incorrect answer, the access point prevents the station from accessing the network.

Shared key authentication only works if WEP encryption is enabled. If it is not enabled, the system reverts to open system default mode (unsafe), allowing (in practice) any station within the range of AP coverage to gain access to the network. This opens a window for an intruder entering the system and, therefore, permits sending, receiving, altering or falsifying messages; a minimum security measure when a secure authentication mechanism is required is thus to have WEP enabled.

Even though shared key authentication is enabled, all wireless stations on a WLAN system could have the same shared key, depending on how the system was installed. In such networks, it is not possible to make an individualised authenticcation; all users, including unauthorised ones, possesing the shared key will be able to access the network.

This weakness may result in unauthorised access, especially if the system includes a large number of users. The more users there are, the greater the likelihood that the key could fall into the wrong hands.

WEP features

According to the standard, WEP must provide WLAN confidentiality, authentication and access control. WEP uses the same symmetric and static key at the stations as in the access point. The standard does not provide any mechanism for automatic distribution of keys, forcing manual key writing on every network element. This creates several problems; if the key is stored in all stations this increases the chances that it could be compromised and manual key distribution leads to increased maintenance by the network administrator, usually meaning that the key is infrequently or never changed.

WEP encryption algorithm

The cryptographic algorithm used by the WEP encryption method (and the TKIP encryption method used by WPA) is RC4, according to the standard, with 64-bit keys (the seed). These 64 bits consist of 24 bits for the initialisation vector (IV) plus 40-bit shared key (secret). The 40-bit shared key has to be distributed manually. Instead, the initialisation vector is dynamically produced and should be different for every data frame. The initial IV goal was to encrypt 802.11 frames with different keys to prevent a potential attacker from capturing enough encrypted traffic with the same key and finally deducing the key. Unfortunately, new tools have been developed, such as BackTrack 2 (Aharoni *et al*., 2007) and "Klein's attack on RC4" have been expanded allowing an attacker to easily obtain the shared key in a few minutes, for example, as accomplished by the PTW attack (Pyshkin *et al*., 2007).

Both sides must know the secret key and the IV. The key is known by both sides since it is stored in the configuration of each network device; however, the IV is produced at one end and is sent in a frame to the other end.

WEP is encrypted via the following steps:

1. Calculate CRC-32 for 802.11 frame payload and concatenate the result (ICV);

2. Concatenate the 40-bit shared secret key to the 24-bit IV to form a 64-bit seed;

3. Input the seed obtained in step 2 into the RC4 pseudo-random number generator (PRNG) to generate a sequence of pseudo-random characters (called key stream) with a number of octets equal to the number of octets in step 1;

4. XOR the resulting characters from steps 1 and 3 to obtain the cipher-text; and

5. Send the IV (unencrypted) and the encrypted message within the IEEE 802.11 frame "frame body" field.

The decoding algorithm is similar to the previous one. As the other end will know the IV and the secret key then it will have the seed and can thus generate the key stream. XOR operation of encrypted received data with the key stream will unencrypt the message (payload and ICV). CRC is done. It should be noted that WEP has come to be considered unsafe (Ioannidis *et al*., 2001).

RC4 cryptographic algorithm

RC4 (or ARC4) is the most frequently used stream cipher in cryptography; it is used in some of the most popular protocols such as transport layer security (TLS) or secure socket layer (SSL) to protect Internet traffic and wired equivalent privacy (WEP) to add wireless network security. Using WEP is not recommended in modern systems; however, some RC4-based systems are safe enough for common use.

The RC4 cryptography algorithm was designed by Ron Rivest of RSA Security in 1987; its full name is Rivest Cipher 4, taking the alternative acronym RC for "Ron's Code" which is used by RC2, RC5 and RC 6 encryption algorithms.

RC4 is part of the most commonly used encryption methods such as WEP, TKIP (WPA) for wireless cards and TLS. RC4's

substantial speed and simplicity are among the main factors that have helped it to be used in such a wide range of applications. Implementing RC4 both in hardware and software is quite easy, requiring few resources to deliver high throughput (Baghaei and Hunt 2004).

RC4 (Schneier, 1996) generates a pseudorandom stream of bytes (key stream) which is XOR added to the plain text for encryption. Deciphering the message is done in the same way.

To generate the key stream, the encryption algorithm has an internal secret state consisting of the following:

-A permutation of 256 bytes called *S vector* or simply "S";

-Two 8-bit index pointers: *i* and *j*; and

-The permutation is initialised with a variable-length key, usually 40-256 bits, using a key scheduling algorithm (KSA). Once key scheduling is done, the ciphering "key stream" is produced by means of a pseudo-random generation algorithm (PRGA).

RC4 uses two blocks for encryption: KSA and PRGA. The following is RC4's pseudo-code:

/ * *S* = S VECTOR with fixed 256 bytes * /size
/ * *K* = VECTOR which contains the seed * /
/ * *L* = length of seed (IV length plus SK length) * /
/ * *N* = 256, S vector size * /

KSA (*K*, *S*)

FOR (*i* = 0 to *N* - 1)

S[*i*]= *i* (1)

j = 0
FOR (i = 0 to *N* - 1) (2)

j = (*j* + *S*[*i*] + *K*[*i* mod *L*]) mod *N*

SWAP(*S*[*i*], *S*[*j*])

PRGA(*S*)

i = 0 (3)
j = 0

Frame production loop

i = (*i* + 1) mod *N* (4)
j = (*j* + *S*[*i*]) mod *N*
SWAP(*S*[*i*], *S*[*j*])
OUTPUT = *S* [(*S*[*i*] + S[*j*]) mod *N*]

The previous pseudo-code assumed that the seed vector *K* [*i*] contained values [4, 5, 6, 7, 8, 9, C, Z] at the respective positions for *i* from zero to seven.

A 256 position memory block is allocated for the S vector for KSA. Part (1) of the pseudo-code initialises the array with values from 0 to 255.

In part (2), the two pointers to the S vector, *i* and *j* are initialised to zero. Then *j* is relocated into a pseudo-random position depending on seed vector *K* content.

j = *j* + *S*[0] + *K*[0] = 0 + 0 + 4 = 4

Then there is a swapping of the values in the S pointed by *i* and *j*. This is done 256 times for each frame which must be encrypted.

As a result, if the value of the seed vector *K* is not known, it is not possible to know the final contents of the *S* vector in advance.

Part (3) corresponds to the initialisation of pointers *i* and *j*.

A reordering or scrambling is done in Part (4) producing an output value (octet) which depends on the S vector obtained in part (2); this cycle is performed as many times as the frame to be encrypted has bytes.

For example, assuming that after the 256 iterations of part (2) completed *S* = [4, 3, 5, 1, 8, 0, 6 ,....., 255] then in part (4), *i* = *i* + 1 = 0 + 1 = 1 and *j* = 0 + *S* [1] = 0 + 3 = 3, after swapping the two positions S [i] and S [j], the contents of the *S* vector will be [4, 1, 5, 3, 8, 0, 6 ,....., 255].

Finally, the output value will be the position of *S* given by S [*i*] + *S* [*j*] = *S* [1] + S [3] = 1 + 3 = 4; then the output value will be S [4] = 8. The first octet of the message is then added using XOR to 8 and leading the first octet encrypted.

WEP simulation tool

The WEP encryption method's nine blocks (Figure 1) were developed in C++ Builder to practice and experiment through simulation with an educational goal. Figure 2 shows the application interface which allows entering and calculating values for WEP message encryption.

For example, when entering the following input values:

1: Vector initialisation (3 bytes in decimal) = 922
2: Shared key (5 bytes in ASCII): 2e3f4
3: Message (up to 250 bytes in ASCII): hello

The following output results are obtained:

4: Key stream (hex): 65E27CDCEF7FF5C7
5: CRC32 (hex): 6FA0F988
6: Encrypted text (hex): 0D8D10BD80DF0C4F

These results can be verified by clicking button 12, "RC4 Validation" of the window.

Temporal key integrity protocol (TKIP)

WPA encryption and integrity verification (Wi-Fi protected access) is based on the temporary key integrity protocol (TKIP) defined in clause 8.3.2 of the original IEEE 802.11i (IEEE Computer Society LAN MAN Standards Committee, 2004) and added later to current IEEE 802.11-2007 standard. TKIP creates a frame key for each frame before being cipher-

red using WEP. The frame key is based on a temporal key (data encryption key) and the value of the TSC (TKIP sequence, also called IV). TKIP also uses the Michael integrity check (MIC) algorithm with the message integrity check key (MK) to generate a frame integrity value or MIC. TKIP requires the following elements to perform encryption and data integrity verification:

-A temporal key (TK), being a previously-agreed data encryption key;

-The TSC (TKIP Sequence) or initialisation vector (IV) which starts at 0 and increases for each frame sent; this IV allows the use of the same TK for several frames;

-The IEEE 802.11 frame MAC destination address (DA) and MAC source address (SA);

The value of the priority field which has been reserved for future use and defaults to 0;

-Message integrity check key; and

-The payload.

Figure 2. WEP simulation tool GUI

Figure 3 shows TKIP encryption and integrity carried out on a frame, summarised as follows:

1. The IV (TSC), MAC destination address (DA) and TKK are introduced into a key mixing function which is a hash function, exchanging certain blocks of bytes several times, depending on IV value. This step produces a 128-bit block, equivalent to having a new 24-bit IV and a 104-bit key per frame as input to the RC4 algorithm.
2. The DA, SA, priority, data (802.11 unencrypted payload) and MIC keys are introduced into the Michael function which performs a one-way hash calculation as specified in RFC 1423 (Balenson, 1999), producing the MIC value.
3. The ICV is calculated with the CRC-32.
4. The new IV and the key obtained at step 1 are introduced into the RC4 generator (PNRG) to produce a key stream which is the same size (in bytes) as the data, MIC and ICV.
5. An XOR function is applied to the combination of data, MIC, and ICV with the key stream to produce the encrypted part of the 802.11 payload.
6. The encrypted part obtained in step 5 is encapsulated along with the IV and IEEE 802.11 frame headers.

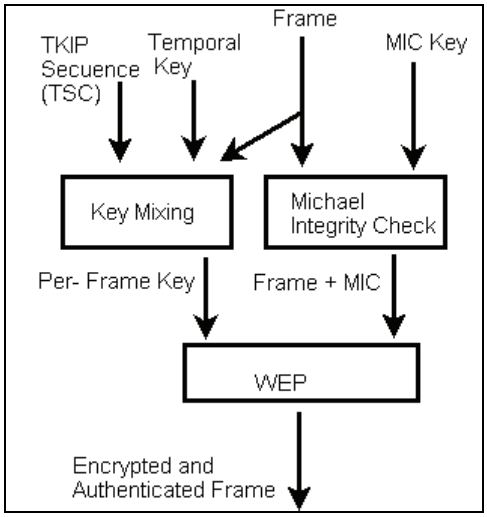

Figure 3. WPA encryption and integrity check

WI-FI protected access 2 (WPA-2)

WPA-2 introduced by the Wi-Fi Alliance was ratified in IEEE 802.11i clause 9.3.3 in June 2004. The WPA2 protocol includes the following features [8]:

-IEEE 802.1X authentication;
-Extensible authentication protocol (EAP); and
-Encryption using advanced encryption standard (AES) (NIST, 2001).

WPA2 is used in CCMP (counter with CBC MAC protocol) mode for implementing AES in 802.11i, including:

-128-bit keys;
-Using AES in CBC-MAC mode for calculating MIC and AES in counter mode for data encryption; and
-Guaranteeing 48 bit initialisation vector.

WPA-2 improves WEP shortcomings but, unlike WPA, incurporates AES encryption mechanisms to reduce vulnerabilities which could introduce hash functions with WPA TKIP. WPA-2 uses a TK and a packet number (PN) field to prevent attacks by repeating frames. The authentication phase and pair master key (PMK) derivation are performed according to IEEE 802.1X.

WPA-2 uses AES in CBC-MAC mode to calculate MIC and AES in counter mode to encrypt the payload. Figure 4 shows

these two processes performed in parallel.

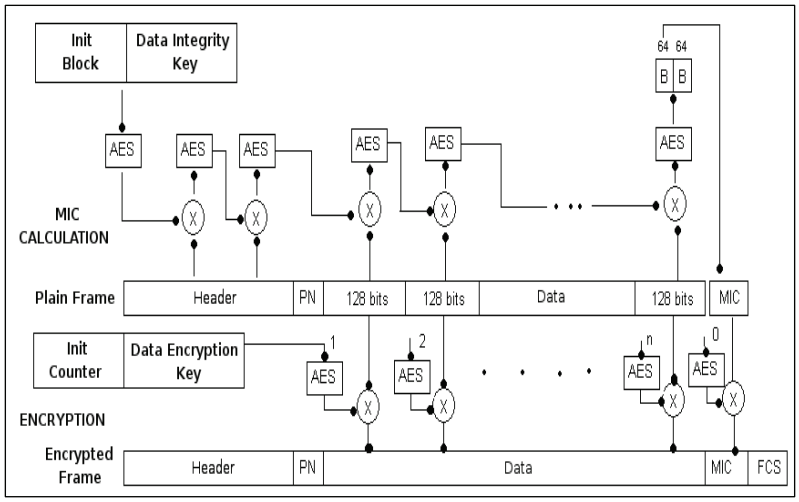

Figure 4. WPA-2 encryption and integrity check

Message integrity check (MIC): AES uses the data integrity key at this stage:

1. A 128 bit Init Block (starting block), as explained below, and the data integrity key are introduced into AES in CCMP mode producing a 128-bit block.

2. An XOR is applied to the result of the previous step with the first 128 bits of the IEEE 802.11 payload block, producing a 128-bit block.

3. The result from step 2 is introduced into AES in CCMP mode producing a 128-bit block.

4. Steps 2 and 3 are carried out with the remaining 128-bit payload blocks, except for the PN field, used for numbering the frame and already included on the starting block.

This is done until the last 128-bit block of the payload field. From the last 128 bits resulting from the AES-CCMP function, the 64 most significant bits are taken and named "R1." R1 corresponds to unencrypted MIC.

WPA-2 builds the starting block (used for calculating MIC) using the following information:

-The flag field (8 bits) is set at 01011001. This field contains several flags, including the one that specifies that a 64-bit MIC length is in use;
-The priority field (8 bits) which is fixed at 0 and is reserved for future use;
-The source address field (48 bits) from the IEEE 802.11 frame MAC header;
-The PN field (48 bit); and
-Data length field (16 bits).

There are two padding fields at the beginning and end of the payload frame used to complete the payload or the header to match 128-bit blocks.

Data encryption: AES uses the DEK obtained during the 802.1X authentication process.

AES is used in counter mode for payload encryption. An initial 128-bit counter is used with the following fields to start the process:

-Flag field (8 bits) set at 01011001 containing several flags, including the one which specifies that a 64-bit MIC length is in use;
-The priority field (8 bits) which is fixed at 0 and is reserved for future use;
-Source address field (48 bits) from the IEEE 802.11 MAC frame header;
-PN field (48 bits); and
-Counter field (16 bits) which is fixed at 1 and is only increased if the 802.11 frame payload is fragmented. It should be noted that this counter is only part of the counter that inputs to the AES function in counter mode, which is actually modified by the package number (field PN) if the payload is not fragmented.

The payload is encrypted as follows after this 128-bit initial counter has been built:

1. The initial counter is input into an AES function in counter mode along with the data encryption key producing a 128-bit block;

2. With this result, an XOR is applied to the first 128 payload bits (clear text payload) producing the first 802.11 frame payload 128 ciphered bits; and

3. The initial counter is increased in step 1 and step 2 is repeated with the following 128 bits of clear text payload. This is done until finishing the encryption of the entire frame's payload.

The counter is increased and its value is sent to the AES function. The result is XORed with the MIC (and of course with R1) and the most significant 64 ciphered bits are taken and encapsulated along with the frame check sequence (FCS) and IEEE 802.11 header.

Table 1. Main features of WEP, WPA, and WPA-2

	WEP	***WPA***	***WPA-2***
Authentication	N/A	IEEE 802.1X/ EAP/PSK	IEEE 802.1X/ EAP/PSK
Cryptographic algorithm	RC4	RC4	AES
Key size	40 O 104 bits	128 bits	128 bits
Encryption method	WEP	TKIP	CCMP
Data integrity	CRC32	MIC	CCM
Keys for packets	No	Yes	Yes
IV length	24 bits	48 bits	48 bits

Practical examples of wireless network security in IEEE 802.11

The following didactic examples show the steps carried out for configuring a Cisco AP model AIR-AP1242AG-AK9 and a Linksys WUSB54GC wireless card (installed in a PC) to create

a WLAN working both in personal WPA (TKIP) mode and personal WPA-2 (AES) mode.

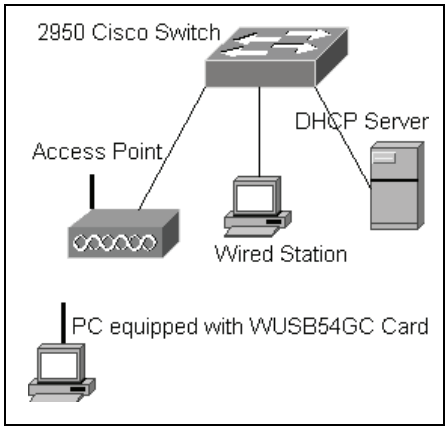

Figure 5. Network diagram to setup the access point in personal mode (WPA or WPA-2)

Setting the AP to operate in personal WPA (TKIP) mode with shared password

After basic setup of the access point, launch a browser from a wired station and log in to it. Once within the AP, select the **Security** option and in the **Encryption Manager** option conduct the following steps:

a. Choose Enable cipher for TKIP;
b. Delete the value of the encryption key 1;
c. Set the encryption key 2 as the key for transmission; and
d. Apply this setup to the Dot11Radio0 radio interface.

At the ***SSID Manager*** perform the following steps:

e. ssid = ap-with-psk-tkip (name assigned to the SSID);
f. Apply the configured ssid to the 802.11G radio;
g. Activate "Open authentication" and select <No addition>;
h. Choose "Key Management = Mandatory", select the box "Enable WPA" and select "WPA" at the immediate option;
i. Fill "WPA pre-shared Key = 0123456789" and flag the circular button "ASCII"; and
j. Apply the settings.

This generates the following lines on the AP's Dot11Radio0 radio interface configuration file:

```
 !
dot11 ssid ap-with-psk-tkip
 authentication open
 authentication key-management wpa
 wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
 encryption mode ciphers tkip
 !
 ssid ap-with-psk-tkip
```

Create a profile with ssid name matching the AP's ssid (ap-with-psk-tkip) to which you wish to connect in personal computers equipped with WUSB54GC cards; set the option "security = WPA-Personal" and fill in the shared key with the value "0123456789". Save the configuration and connect to the AP. Check that the WUSB54GC card associates with the AP, receives an IP address from the DHCP server and can communicate with other computers which are connected to the wired network.

Setting the AP to operate in Personal WPA-2 (AES) mode with shared password

Select the **Security** option and at the **Encryption Manager** option conduct the following steps:

a. Choose cipher for AES-CCMP;
b. Delete the value of encryption key 1;
c. Set the encryption key 2 as the key for transmission; and
d. Apply this setup to the Dot11Radio0 radio interface.

At ***SSID Manager*** perform the following:

e. ssid = ap-with-psk-aes;
f. Apply the configured ssid to the 802.11G radio;
g. Activate "Open authentication" and select <No addition>;
h. Choose "Key Management = Mandatory", select the box "Enable WPA" and select "WPA" at the immediate option;
i. Fill "WPA Preshared Key = 0123456789" and flag the circular button "ASCII"; and
j. Apply the settings.

This generates the following lines at the configuration file of the AP's Dot11Radio0 radio interface:

```
 !
dot11 ap-with-psk-aes
 authentication open
 authentication key-management wpa
 wpa-psk ascii 7 055B575D72181B5F4E5D4E
!
interface Dot11Radio0
 !
encryption mode ciphers aes-ccm
 ssid ap-with-psk-aes
```

Create a profile with an ssid name, which must match the AP's ssid (ap-with-psk-aes) to which you wish to connect in the personal computers equipped with WUSB54GC cards; set the option "security = PSK2" and fill in the shared key with the value "0123456789". Save the configuration and connect to the AP. Check that the PC's WUSB54GC card associates with the AP, receives an IP address from the DHCP server and can communicate with other computers connected to the wired network.

Conclusions

The WEP protocol is vulnerable to attacks; the problem does not lie with the RC4 algorithm used by WEP but the way in which the encryption keys are managed and generated to be used as RC4 algorithm input. Other RC4 algorithm-based se-

curity protocols such as transport layer security, secure socket layer and WPA are more secure for practical uses.

Due to the weaknesses found in WEP, new alternatives such as WPA (based on RC4 and TKIP) and WPA-2 (based on AES/CCMP) have emerged to reduce the lack-of security stigma of wireless networks, ensuring confidence in their use in homes, businesses, schools, universities, etc. These new levels of security are achieved through greater security implementation providing strong encryption and incorporating authentication such as RADIUS or DIAMETER.

WPA and WPA-2 have two modes of operation in terms of authentication: pre-shared key (PSK) and IEEE 802.1x. The PSK operation mode (also known as WPA Personal mode) is aimed for small office/home office (SOHO) wireless networks which do not have authentication servers, this mode being quite easy to configure as shown in the two practical examples presented here. The IEEE 802.1x operation mode (also known as WPA Enterprise mode) is aimed at Corporations having existing authentication server infrastructure, such a RADIUS servers; as could be expected, this mode of operation is harder to configure.

Some wireless networks with old or legacy hardware are still using WEP; however, there are no reasons in terms of both security and performance to use anything less than WPA-2 or at least WPA in modern wireless networks.

It is expected that the basis for understanding the operation, main features, usage, advantages and disadvantages of the different security options available for IEEE 802.11 wireless networks discussed in this paper could contribute to enriching discussion on these matters.

Bibliografía

Aharoni, M., Moser, M., Muench, M. J., Grimchaw, D., Naepflin, A., Schroedel, P., Waeytens F., .BackTrack., Mar. 6, 2007. URL: http://www.remote-exploit.org/backtrack.html.

Baghaei, N., Hunt, R., Security performance of loaded IEEE 802.11b wireless networks., Computer Communications, Elsevier, U.K., Vol. 27, No. 17, 2004pp. 1746–1756.

Balenson, D., .Privacy Enhancement for Internet Electronic Mail. Part III: Algorithms, Modes, and Identifiers., Request for Comments (Standard) 1423, Internet Engineering Task Force, 1999.

Ioannidis, J., Rubin, A. D., Stubblefield, A., Using the Fluhrer, Mantin and Shamir Attack to Break WEP., AT&T Labs Technical Report TD-4ZCPZZ, Aug 6, 2001. URL http://www.isoc.org/isoc/conferences/ndss/02/papers/stubbl.pdf

LAN MAN Standards Committee of the IEEE Computer Society., Par 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications., IEEE Standard 802.11, 1999 Edition.

LAN MAN Standards Committee of the IEEE Computer Society., Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications., Amendment 6: medium access control (MAC) security enhancements. IEEE Standard 802.11i, 2004 Edition (2004).

Moskowitz, R., Weakness in Passphrase Choice in WPA Interface., Nov 4, 2003. URL: http://wifinetnews.com/archives/002452.html.

NIST (National Institute of Standards an Technology)., Announcing the Advanced Encryption Standard (AES) - Federal Information Processing Standards Publication 197., Nov. 26, 2001. URL. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

Pyshkin, A., Tews, E., Weinmann, R. P., Breaking 104 bit WEP in less than 60 seconds., Apr 1, 2007. URL: http://eprint.iacr.org/2007/120.

Schneier, B., .Applied Cryptography: Protocols, Algorithms, and source code in C., 2a ed., New York, John Wiley and Sons, Inc., 1996, pp 397-398.