University of New Orleans

ScholarWorks@UNO

University of New Orleans Theses and Dissertations

Dissertations and Theses

5-21-2004

Security and Authentication for 802.11 Wireless Networks

Michel Getraide
University of New Orleans

Follow this and additional works at: https://scholarworks.uno.edu/td

Recommended Citation

Getraide, Michel, "Security and Authentication for 802.11 Wireless Networks" (2004). *University of New Orleans Theses and Dissertations*. 88.
https://scholarworks.uno.edu/td/88

This Thesis is protected by copyright and/or related rights. It has been brought to you by ScholarWorks@UNO with permission from the rights-holder(s). You are free to use this Thesis in any way that is permitted by the copyright and related rights legislation that applies to your use. For other uses you need to obtain permission from the rights-holder(s) directly, unless additional rights are indicated by a Creative Commons license in the record and/or on the work itself.

This Thesis has been accepted for inclusion in University of New Orleans Theses and Dissertations by an authorized administrator of ScholarWorks@UNO. For more information, please contact scholarworks@uno.edu.

SECURITY AND AUTHENTICATION FOR 802.11 WIRELESS NETWORKS

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of
the requirements for the degree of

Master of Science
in
The Department of Computer Science

by

Michel Getraide

B.Sc, M.Sc, Université de Marne La Vallée, 2002

May 2004

Acknowledgments

First of all, I want to express my gratitude to my advisor Dr. Golden Richard for supervising my thesis and for his help.

I would also like to thank the members of my committee Dr. Adlai DePano and Dr. Shengru Tu.

Venkata Mahadevan has been a great help for me during the practical part of my work. I owe him a special thank.

Finally, my achievements would not have been possible without the support of my parents. I am greatly thankful for their love and patience.

Table of Contents

List of Figures

List of Tables

Abstract

Wireless Networks is a very growing market. However, the security measures are not strong enough; the WEP security protocol is flawed. The 802.11 Task Group I is working on new security measures in order to strengthen the access control of users, the privacy and the integrity of data.

We will describe the WEP flaws and the new security measures of 802.11 Task Group I. Finally, we will propose a new architecture to improve user identification for the wireless network of our department.

Chapter 1: Introduction

1. Advantages of wireless networks

Productivity and profitability have become a key problem for businesses today. Return on investment is one of the deciding factors in any business decision. This is true for investment in IT infrastructure. Wireless networks present some advantages for businesses: [18]

- Stay connected.

According to surveys, using wireless LANs allows users to stay connected to their network more time each day. A user with a laptop and a wireless connection can roam their office building without losing their connection, or having to log in again on a new machine in a different location. This translates to a very real increase in productivity.

- Accurate information:

In the healthcare field, a study showed that the fact to have information "anywhere, anytime" allows increased access to accurate information.

- Simplicity and increase of productivity:

The simplicity to set up a wireless network (no need to open a trench to bury network cables beneath the ground) is a gain of time and allows a company to save money. The installation is quick and can also be removed easily (in case if the company moves location often). According to a study, "wireless networking has a measurable impact on return on investment, with organizations saving an average of $164,000 annually on cabling costs and labour". “While the initial investment required for WLAN may be higher than the cost of traditional wired LAN hardware, overall installation expenses and life-cycle costs can be significantly lower. Long-term cost benefits are greatest in dynamic environment requiring frequent moves and changes”. [19]

- Flexibility and increase productivity:

Wireless networks give a better quality of life to employees and a more productive and flexible working environment.

- Convenience

Sometimes, physical cable networks are not appropriate. There are some places where it is not convenient or even dangerous to connect wires. In that case, wireless deployment is a better solution and often cheaper.

- Mobility advantages:

The world has changed. People have become more mobile. The development of transportation and the global economy are the main reasons of this mobility. Most of the big companies have offices worldwide and their employees need to travel more often. They need access to the Internet or to the company's network while being out of their office (airports, meetings, congress).
Other mobility advantages include: students attending class on campus accesses information in the Internet, managers or professors can do lectures without carrying papers.

- Costs and technologies:

The cost of access points and wireless cards has reduced considerably. The technology helps making the wireless network a reality: the capacity of batteries has increased and laptops can be autonomous for a longer amount of time.

So, we see that wireless networks are simpler, more convenient, cost saving and thus very attractive for businesses but also for personal use. This market is growing.

2. What is 802.11?

IEEE standard 802.11 is a series of specifications for wireless local area network (WLAN). The goal of 802.11 is to define an Ethernet-like communication channel using radio waves instead of cables.

802.11 is divided into 2 layers: The Media Access Control (MAC) layer, and the Physical media (PHY) layer. The MAC layer is a set of rules to determine how to access the medium and send the data but the details of transmission is left to the PHY layer [8]. Different variations of 802.11 correspond to different PHY layers. *Frequency hopping spread spectrum* (FHSS) and *direct sequence spread spectrum* (DSSS) were the first two techniques used. 802.11b uses DSSS where as 802.11a uses another radio technique called *orthogonal frequency division multiplexing* (OFDM). Those different techniques use different frequency band and generates different speeds: 802.11b has a maximum bandwidth of 11 Mbps and operates in the 2.4 GHz frequency band where as 802.11a has a maximum bandwidth of 54 Mbps and operates in the 5 GHz frequency band.
However, all those PHY layer variations use the same MAC layer. Since 802.11 security mechanisms reside entirely in the MAC layer, there is no need to distinguish between security for 802.11a and 802.11b [2].

3. Wireless security requirements

Due to its insecure medium of communication, wireless networks need more security than traditional wired networks. We can distinguish three different areas of security.

3.1. Strengthen authentication

With wireless networks, there is no physical access to the network infrastructure (e.g. access points); that is you can associate with an access point without the knowledge of its location. For that reason, users need to ensure they are connecting to *legitimate* access points that are part of the organization's network, not "rogue" access points. Thus, not only the user has to authenticate to the network but the network also need to authenticate to the user. This is called *mutual authentication*.

3.2. Encrypt all traffic

Wireless networks are much easier to perform traffic analysis on because physical access to the network does not require physical access to the equipment since transmissions are broadcasted over radio waves. Frames can be easily intercepted in transit with wireless network analysis software. All the communication between access points and stations need to be encrypted.

3.3. Ensure integrity

Since a third party can intercept the data, there is a risk of malicious modification of the data. The receiver would have no way of knowing if the data received is the original data sent or if the data has really been sent by the specified sender. So, a mechanism to ensure integrity is necessary.

Chapter 2 will present the WEP scheme.
Chapter 3 will show that the WEP scheme is flawed and that none of the 3 basics foundations are enforced. Chapter 4 presents the new security protocols designed to improve (short term solutions) or replace (long term solutions) WEP. In the chapter 5, we will see other security measures. Chapter 6 is a practical part: it is the installation of a RADIUS server in the campus wireless network in order to improve access control.

Chapter 2: WEP Security Scheme

1. Introduction

Because of the broadcast transmission of data, the main concern with radio communication is that anyone can eavesdrop with a receiver. So the primary goal of WEP[1] is to protect the confidentiality of user data from eavesdropping and other attacks. WEP protects the link-layer communication. It is used by stations to protect data as it traverses the wireless medium, which means all the communication exchanges between a wireless station and an access point. However, it provides no protection past the access point. See figure 1.

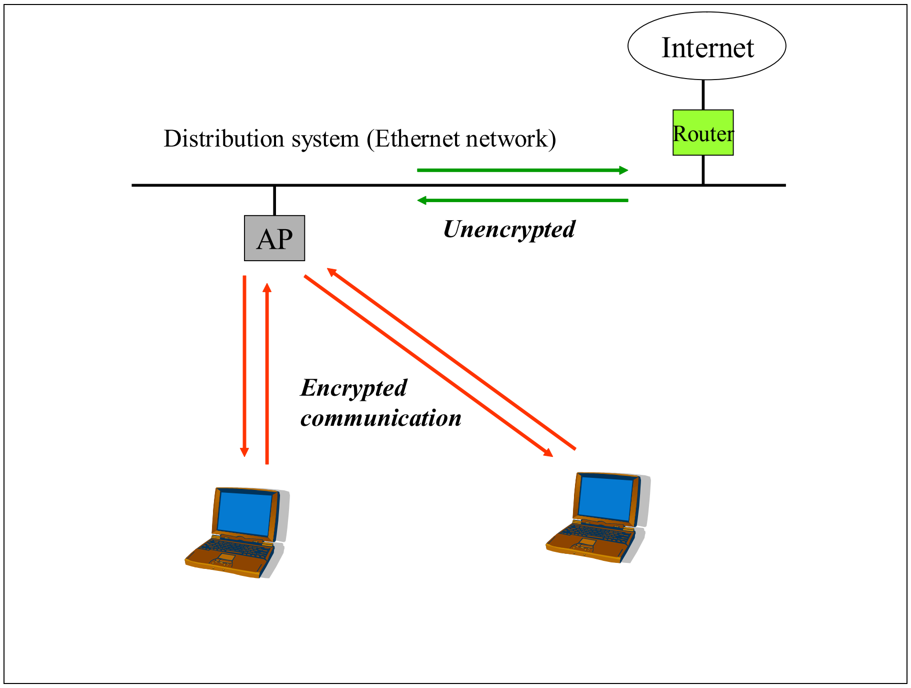


Figure 1: All the communications between access points (AP) and wireless stations have to be encrypted. However, access points decrypt the data intended to the wired network.

WEP make use of a 40-bit or 128-bit key for encryption and decryption. The encryptor (station or access point) encrypts the data with a key. Then the decryptor (access point or station) decrypts the data with the *same* key. So, both the key of the stations and the key of the access points have to be identical. We will see in the next

[1] WEP = Wired Equivalent Privacy. It is aimed at make a wireless LAN equivalent to an unsecured wired LAN. "Create the privacy achieved by a wired network" [Jesse Walker]

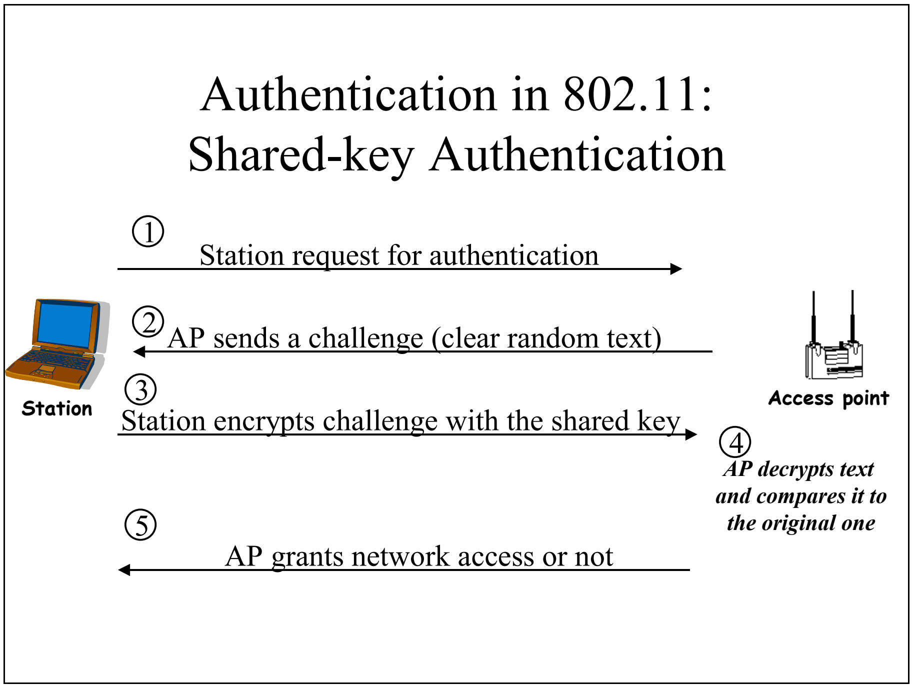
section that this is precisely what the authentication scheme is checking: the station will be authenticated if and only if it has the same key as the access point.
However, 802.11 does not provide any mechanism to manage the keys. So, most of the time, they are entered manually in the device drivers and access points.

The 3 services that WEP provides are authentication (access control), confidentiality, and data integrity. Each of theses services is reviewed in the next 3 sections.

2. Access Control / Authentication

The goal of authentication is to identify users in the network and prevent unauthorized access. 802.11 uses the *Shared-key authentication* scheme. Actually, shared-key authentication uses WEP encryption and therefore can be used only on products that implement WEP. Any stations implementing WEP have to implement shared-key authentication.
The protocol will check if the mobile station has the same set of keys[2] as the access point. (In a given service set, the set of keys are shared among all the stations.) So, it requires that those default keys be distributed to stations *before* attempting authentication. When a mobile station sends a request for authentication, the access point sends to the station a challenge. The wireless station encrypts this challenge text with its shared key and sends the message back to the access point. The access point decrypts the message using its key. If the original challenge text is recovered, then both the station and the access point share the same secret key and the station will be authenticated. Otherwise, the network access will not be granted. Figure 2 depicts the different steps of the authentication process.

[2] WEP uses a set of up to four default keys



Authentication in 802.11:
Shared-key Authentication

① Station request for authentication

② AP sends a challenge (clear random text)

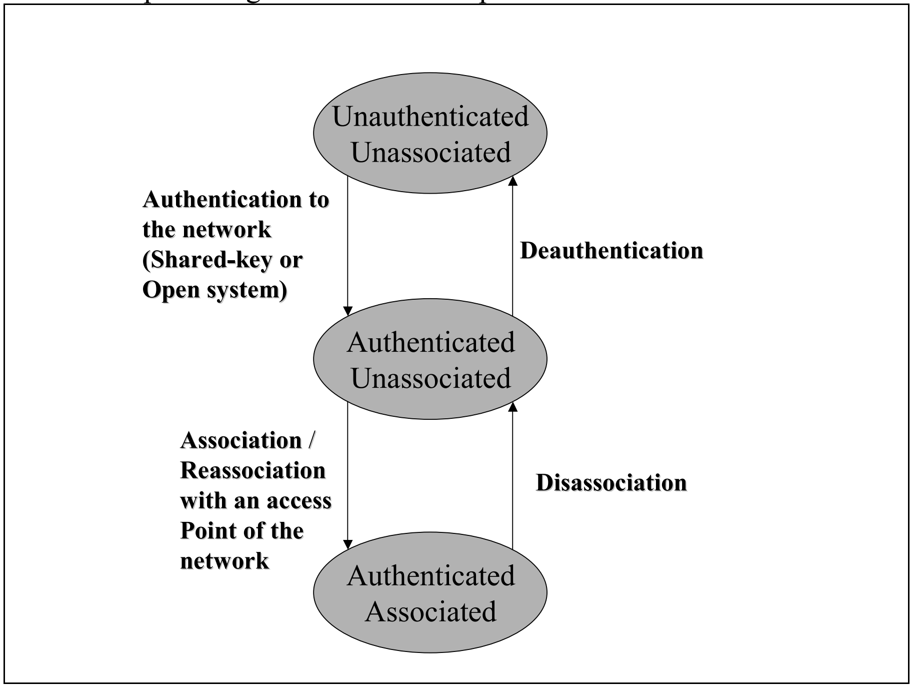
③ Station encrypts challenge with the shared key

④ *AP decrypts text and compares it to the original one*

⑤ AP grants network access or not

Figure 2: Shared-key authentication

802.11 provides another authentication scheme called *open-system authentication*. But it provides no security since the access is granted if the name of the network (SSID) is known!
Once the network has authenticated the station, the station has to associate with a specific access point. Figure 3 shows the 3 possible states of 802.11 state machine.



Unauthenticated Unassociated
Authentication to the network (Shared-key or Open system)
Deauthentication
Authenticated Unassociated
Association / Reassociation with an access Point of the network
Disassociation
Authenticated Associated

Figure 3: The 3 possible state machine of 802.11 (a station has to authenticate before associating with an access point)

Both the problems of data integrity and confidentiality are due because of the broadcasting transmission over the air. An eavesdropper could record traffic – called passive attack – or even modify the data – called active attack. To prevent those attacks, WEP provides means for data integrity and confidentiality.

3. Data Integrity

The role of data integrity is to prevent modification of data by a third (unauthorized) party. An integrity check value (ICV) is computed over the unencrypted message to insure that the data has not been modified during its transmission. The ICV is added to the unencrypted message. They both are encrypted[3] before being sent. The ICV is a function of the data. If a third party modifies the data, the ICV will no longer correspond to the data. The receiver basically computes the ICV over the data received (and decrypted) and compares it with the ICV computed by the transmitter. If they don't match, then the data was modified during the transmission. (The ICV is encrypted to prevent a third party from modifying the data and the ICV accordingly). The *CRC-32* algorithm is used to compute the ICV.

4. Confidentiality

The goal of confidentiality is to prevent eavesdropping. As we said in the chapter 2, frames on wireless networks can be easily intercepted because of the broadcast nature of the wireless medium. For this reason, we need to encrypt all data communication over the wireless network. The algorithm used to encrypt and decrypt traffic is *RC4 stream cipher*. Let's explain what a stream cipher is and then, we will introduce the RC4 stream cipher.

4.1. Stream ciphers

Stream ciphers convert plaintext to ciphertext one bit at a time. A pseudo-random[4] number generator (PRNG) uses a specific algorithm to expand the key (seed). The keystream produced (as long as the plaintext) is xored with the plaintext to produce the ciphertext. During the decryption process, the same keystream is xored with the ciphertext to recover the plaintext. It works since $(P \oplus k) \oplus k = P$. The generator that decrypts the message should use the same key and the same algorithm in order to get the same keystream. Cf. figure 4.

[3] See section 4 below.

[4] It is called pseudo-random since a real random generator is impossible. The closer the keystream produced is random, the better the security.

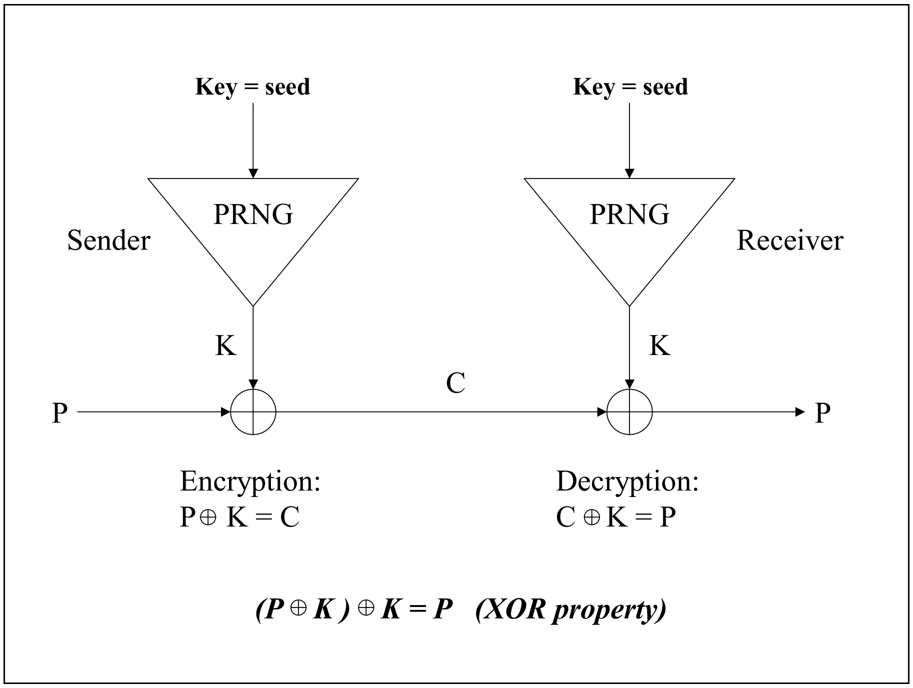


Figure 4: Stream cipher [1]

4.2. RC4 stream cipher

The stream cipher used to encrypt data is RC4. The key used is the concatenation of a 40-bit shared key[5] with a 24-bit initialization vector (IV). The RC4 pseudo-random number generator will take the 64-bit key (seed) as input and will expand it into a keystream. The generator uses a specific algorithm to expand the key. Both the message and the ICV[6] are encrypted. The encryption simply consists of doing a XOR with the RC4 keystream. The knowledge of the IV is necessary to decrypt the message, so it is not encrypted. Before the frame is sent over the air, the PHY layer adds a checksum (It is not part of the WEP processing though). (Cf. figure 5 below)

[5] There is a newer version of WEP that uses a 104-bit shared key.

[6] See section 3 above.

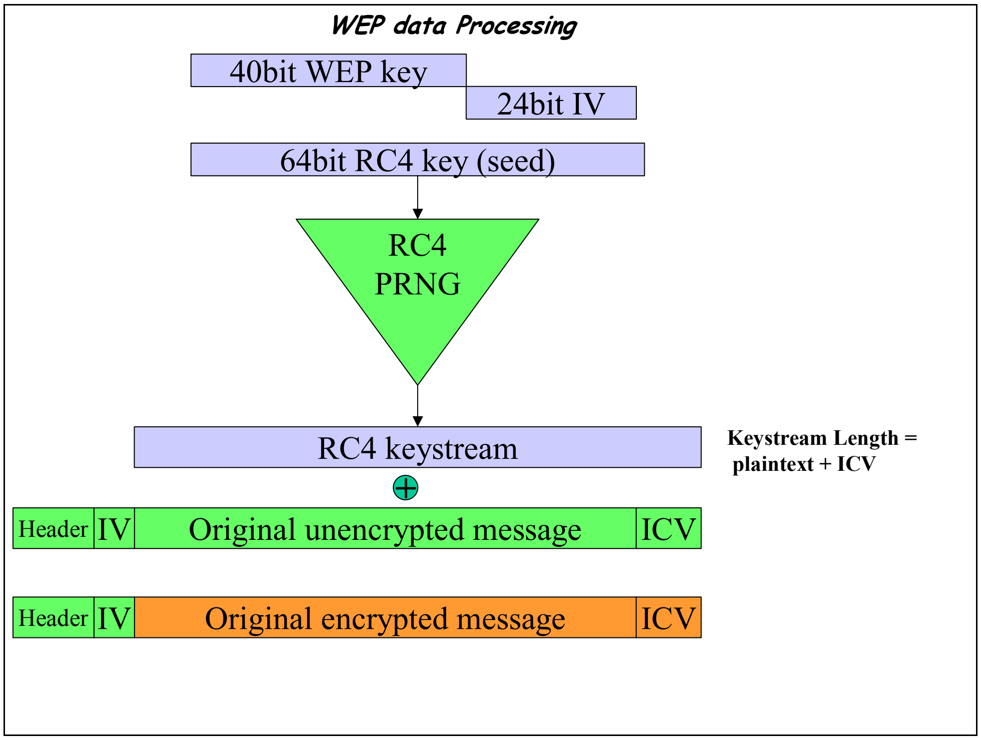


Figure 5: WEP data processing

5. Conclusion

We described the 3 services that WEP is supposed to provide. We will see in the next chapter that they all have flaws. Here is an overview of these flaws:

Authentication flaws:

- The authentication is of user's MAC addresses and not users themselves.
- There is no mutual authentication: only the user is authenticated but not the access point. So, there is a risk of "*rogue* access points".

Encryption flaws:
The keystream is a function of the tuple (key, IV). We will see in the next chapter that it is very insecure to encrypt 2 different frames with the same keystream. That is why a different IV is needed for each frame. However, it happens that the same IV is reused along with the same key (Cf. next chapter). A keystream reuse could lead to a *collision* attack.

Data integrity flaws:
The algorithm used to compute the ICV is CRC-32. It is a linear algorithm and we will see that it is not cryptographically secure. An elaborate attack could modify packets and the ICV accordingly. This is called *forgery* attack.

Chapter 3: WEP flaws

1. Introduction

In the previous chapter, we explained the WEP scheme. Here, we will describe the WEP flaws and the possible attacks to recover the WEP key or the original plaintext. Let's recall that WEP uses a stream cipher – RC4 - to encrypt and decrypt data and that the plaintext is xored with the generated pseudo-random stream to produce ciphertext. The decryptor uses the same generated keystream to recover the plaintext.

```
C = P ⊕ K  Plaintext encryption
C transmitted over the air
P = C ⊕ K  Plaintext decryption
```

If C is modified during the transmission over the air – it is possible since 802.11 Media Access Control (MAC) is not reliable, the decryptor could use the wrong byte of keystream for decryption and then the recovered plaintext would be wrong. Since, the encryptor and decryptor cannot remain synchronized there is a need for a random access property stream cipher[7]. But RC4 does not have this property. So a per-packet key has been introduced in order to thwart this problem [2]. The per-packet key solves this specific problem since the plaintext will be encrypted by blocks (the encryption process should start for each packet) but it raises another problem: if 2 ciphertexts encrypted with the same key are xored then the result is equivalent to the 2 xored plaintexts. (P1 + K) + (P2 + K) = P1 + P2 and thus reveals a lot of information about the plaintext. So, each packet should be encrypted with a different key. The reason why an initialization vector has been introduced is to make every per-packet key unique. But we will see that this idea is not sufficient. The IV that is used to construct the per-packet key is transmitted in clear - lead to weak key attack, Cf. 4.2 - and also is too small which lead to collision attack, Cf. 4.3-. An automatic management of keys would solve the collision problem by updating keys as often as necessary.

A stream cipher cannot be safely used in a datagram environment without a key management to replace keys before they can be reused [2].

We will also see that the integrity check value (ICV) is not cryptographically secure and does not protect against a malicious message modification: the forgery attack Cf. 4.4. The forgery attack leads to another type of attack: replay/bit-flip attack, Cf.4.5. The weak key attack and collision attack are called passive attacks: the attacker only

[7] A random access property stream cipher can generate any specified byte of the keystream in a constant time.

has to eavesdrop and record traffic. On the other hand, forgery attack and replay attack is called active attack since the attacker modifies the data.

2. Weak key attacks

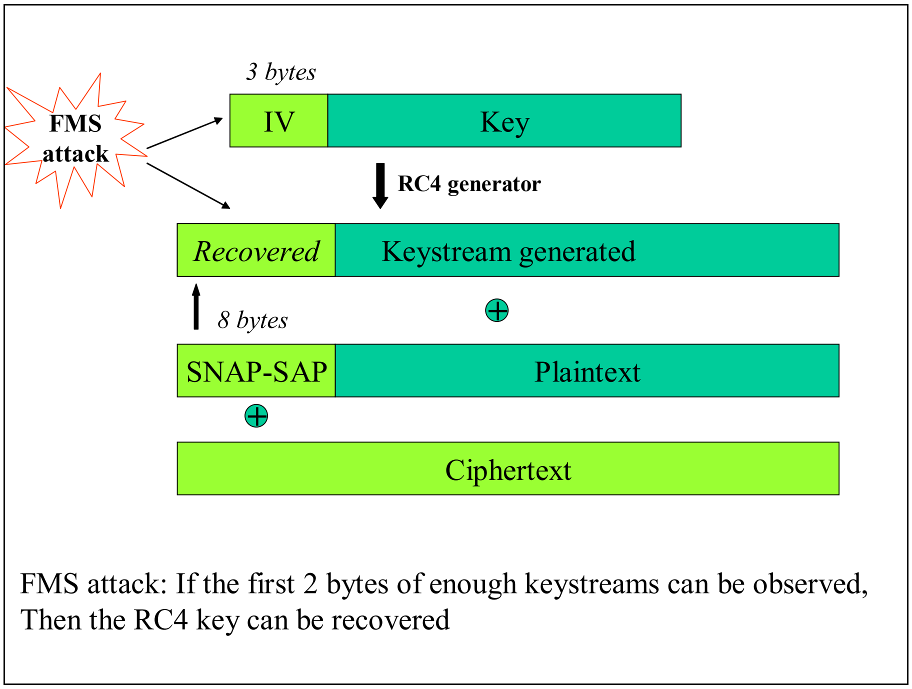

3 bytes
FMS attack
IV
Key
RC4 generator
Recovered
Keystream generated
8 bytes
⊕
SNAP-SAP
Plaintext
⊕
Ciphertext
FMS attack: If the first 2 bytes of enough keystreams can be observed, Then the RC4 key can be recovered

Figure 6: Weak keys, the FMS attack.

A drawback in WEP implementation is that the 24-bit IV is transmitted in the clear with the encrypted data. This transmission in clear is mandatory because the decryptor needs to know the IV in order to generate the same keystream. In August 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir noticed a weakness in the way that RC4 PRNG generates the keystream. When a portion of the RC4 key is known – in our case the IV – *the RC4 key schedule construct reflects patterns in the keys themselves by producing patterns at the beginning of the generated keystream. If the first two bytes of enough key streams can be discovered, then the RC4 key can be recovered.* [2] This technique is called FMS. It would be difficult to mount such an attack since we need to recover the beginning of the keystream. But another flaw in the WEP design will be helpful! The first eight bytes of every plaintext are known to be the LLC (logical link control) encapsulation, (the first byte is a particular header -the SNAP-SAP header- and always starts with 0xAA). So, we just need to XOR the first bytes of the ciphertext with the first bytes of the plaintext in order to recover the first bytes of the generated keystream! Then, the FMS attack can be executed[8]. Cf. figure 6.

[8] AirSnort is a software that implements the FMS attack. It currently requires about 20000 packets to recover the RC4 key which represents less than 11 seconds of 802.11b traffic. (AirSnort source)

3. Collision attacks (keystream reuse)

In WEP, the secret key is static[9], which means that the user or the manager will not change the key often. Therefore, the RC4 algorithm (keystream) is only function of the initialization vector (IV). The numbers of different possible IVs (space) is limited to 2^24. To prevent a frame to be encrypted with the exact same key, the key must be changed at least every 2^24 packets to avoid collisions.
Some statistics show that there is a 99% collision after 12430 packets which correspond to 3 seconds in 11Mbps traffics [5]. It means that keys cannot be updated as frequently as necessary without an automatic key management. Let's say someone knows a frame in clear and its associated encrypted frame. He could be able to decrypt another encrypted frame (with the same IV) without the knowledge of the key! A reuse of IV leads to a reuse of RC4 keystream! In general, stream ciphers are not appropriate for packets environment. The example below shows how to decrypt a ciphertext frame with the knowledge of a pair (ciphertext-plaintext).

Let's call: P = plaintext frame
C= ciphertext frame
K = key
IV = initialization vector
RC4(k, IV) = keystream
⊕ = exclusive or

```
C1 = P1 ⊕ RC4(k, IV)
C2 = P2 ⊕ RC4 (k, IV)
C1 ⊕ C2 = [P1 ⊕ RC4(k, IV)] ⊕ [P2 ⊕ RC4 (k, IV)]
C1 ⊕ C2 = P1 ⊕ P2
```

This means that the addition of 2 plaintext frames is equivalent to the addition of 2 ciphertext frames given the same key. Let's do an example:

```
P1 = 10101010
C1 = 01100110

C2 = 01000001
P2 = ???

C1 ⊕ C2 = 00100111 = P1 ⊕ P2
```

We can now deduce P2:

```
P1 ⊕ P2 = 00100111  → 10101010 ⊕ P2 = 00100111  → P2 =
10001101
```

There is another way to recover P2:
by computing the keystream thanks to P1 and C1:

```
P1 ⊕ RC4(k, IV) = C1→    RC4(k, IV) = 11001100
```

Then, `P2 ⊕ RC4(k, IV) = C2→    P2 = 10001101`

[9] WEP does not provide automatic key management. If a network has a lot of access points, we can presume that a network administrator would not update the keys very often.

4. Forgery attacks (Message modification, injection)

We saw in chapter 3 that to ensure the integrity of the message, we add to the plaintext message an integrity check value (ICV). The algorithm used is CRC-32. Although this algorithm is useful for detecting bit errors, it does not prevent malicious attacks. It is not cryptographically secure because of its linear property:

```
CRC(A ⊕ B) = CRC(A) ⊕ CRC(B)
```

Recall that both the plaintext message and the ICV are encrypted.

The ICV is only function of the data. It does not depend on the key. If an attacker knows the plaintext of the message, he can compute the ICV.

A possible attack a hacker could do is to produce a new ciphertext that will not be discarded by the “ICV test”. He would modify the ciphertext and would compute the ICV accordingly. This message modification is called *forgery* attack.

The example below shows how this attack is possible: [12]

```
M = message
CRC(M) = ICV of the message
Plaintext P = [M, CRC(M)] = concatenation of M and CRC(M)

K = WEP key
IV = initialization vector
RC4(k, IV) = keystream produced by the RC4 generator
⊕ = exclusive or (1+1=0; 0+0=0; 1+0=1; 0+1=1)


Ciphertext C:
C = RC4(k, IV) ⊕ Plaintext  P
C = RC4(k, IV) ⊕ [M, CRC(M)]
```

How to find a new ciphertext C’ that will decrypt to a message M’ desired by the attacker? In general, the attacker does not know the original plaintext but he still needs to know the original ciphertext (traffic recording) and the desired plaintext difference (*diff*) in order to calculate C’ (encrypted desired plaintext)

```
M’ = M + diff
```

What happens if we add the plaintext difference to the original ciphertext?

```
C’ = C ⊕ [diff, CRC(diff)]
C’ = RC4(k, IV) ⊕ [M, CRC(M)] ⊕ [diff, CRC(diff)]
C’ = RC4(k, IV) ⊕ [(M ⊕ diff), CRC(M) ⊕ CRC(diff)]
C’ = RC4(k, IV) ⊕ [(M’, CRC(M’))]
```

The result is the message M’ encrypted!

This is the bit-flip attack: if `M2 = M1 ⊕ diff`, then `C2 = C1 ⊕ diff`

Example of bit-flip attack:

```
M        1010101010        ← Original plaintext
⊕ RC4 1101001100
---------------------------
C        0111100110        ← Original ciphertext
⊕diff   1000000000        ← Diff between M and M' = Diff between C and C'[10]
---------------------------
C'       1111100110        ← Forged ciphertext
⊕ RC4 1101001100
---------------------------
M'       0010101010        ← Forged plaintext
```

5. Replay attacks

The forgery attack can help to mount another type of attack: the replay attack.
Let's say there is an authorized WEP communication between a station and an access point. A hacker could eavesdrop and record traffic between the station and the AP. He could then resend the data to a station A – by modifying the destination address - on the wired network. The access point will decrypt[11] the message and then send it to the station A. The attacker uses the access point to decrypt the message! WEP provides no mechanism to avoid replay attack. WEP only verifies that the message is encrypted with the right key. Connectionless protocols – like UDP – can be exposed to this kind of attack [2]. To avoid replay attacks, each frame should be assigned a sequence number and the access point should discard any out-of-order received frames. Cf. chapter 5.

6. Rogue access points

Shared-key authentication (chapter 2, section2) does not provide mutual authentication since the network does not prove its identity to the user. Only the user authenticates to the network. There is a risk of *rogue* access points installed by a hacker. Users trying to authenticate are fooled into believing that the rogue access point is a legitimate one. The hacker can get authentication information from users that authenticate themselves through this rogue access point. The hacker would then reuse that information to connect to the network.

7. Absence of automatic key management

802.11 provides no automatic key management. Keys have to be entered manually either in the driver software or the firmware on the wireless card. Either way, the key cannot be protected from a local user who wants to discover it. If keys are accessible

[10] To flip the bit, we should add 1 and to keep the same bit, we should add 0.

[11] Recall that the WEP encryption only occurs on the wireless part of the network. The access point decrypts all the data intend to the backbone network.

to users, then all keys must be changed whenever a staff member leave the organization [8]. The absence of automatic key management leads to collision (section 3) and indirectly to weak key (section 5) attacks.

8. Conclusion

The use of the same key to encrypt two different messages leaks to a great amount of information about the plaintext because of the properties of XOR and stream cipher. A requirement is that the keystream generator in the encryptor side and in the decryptor side should be synchronized. The RC4 generator does not have the random access property that enforces synchronization. To remedy to this problem, they defined a per-packet RC4 key. The main problem is that the WEP IV used to construct the per-packet key is a bad implementation because the IV is transmitted in clear (leads to weak key attack) and also because the IV space is too small (leads to collision attack). An automatic management of keys would solve the problems described above but 802.11 and WEP provide no key management. A manual rekeying every few minutes - or even every few seconds to thwart those attacks - is administratively impossible. The new security protocol must include a key management. Also, the mechanism to protect integrity (ICV) is not strong enough and can cause forgery attacks. This lack of integrity helps mounting a replay attack by modifying the destination address of packets.

Chapter 4: Improving security

1. Introduction

We have just seen in the previous chapter several flaws in the WEP protocol. Actually RC4 is a robust encryption method but WEP is a poor implementation of it. The wireless community is working hard in order to fix those flaws.
The requirements for the new protocols are:

- Eliminate repetition of keystream to avoid collision attacks
- Provide a stronger message integrity code to avoid forgery attacks
- Mutual authentication to avoid rogue access points

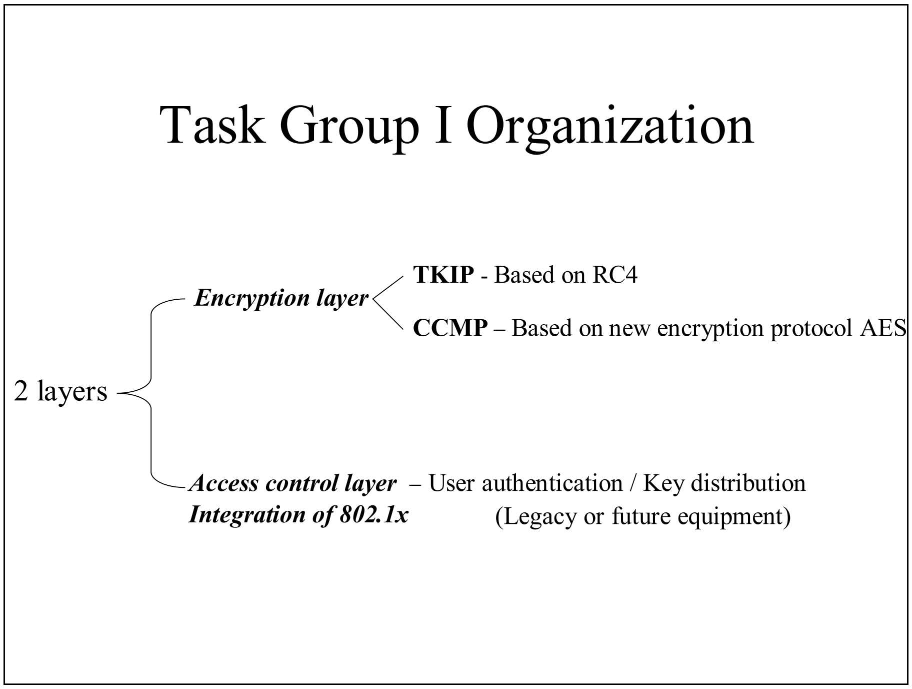
2. Task Group I

The role of *Task Group 802.11i* (TGi) is to develop an enhanced security standard to replace WEP called Robust Security Network (RSN).[12]
TGi incorporates a number of techniques used to improve or to replace WEP security protocol. It addresses WEP flaws and known attacks described in the previous chapter.

Right now, TGi propose solutions for both legacy devices as well as future Wi-Fi equipment. These protocols are Temporal Integrity Key Protocol (TKIP) based on legacy equipment – make use of RC4 - , and Counter Mode with CBC-MAC (CCMP) designed for future equipment- based on the new encryption protocol AES. TGi also includes 802.1X, a port-based access control for user and device authentication. It replaces 802.11 authentication and provides cryptographic key distribution.[13] Cf. 802.1x section.

These protocols can be divided in 2 layers: one for encryption and one for access control. The encryption layer includes TKIP and CCMP. The access control layer is made possible by 802.1x. Cf. Figure 7.

[12] RSN is also called WPA2 or simply 802.11i.
[13] 802.1x standard is not part of the 802.11i draft.



Task Group I Organization

2 layers

Encryption layer

TKIP - Based on RC4

CCMP – Based on new encryption protocol AES

Access control layer – User authentication / Key distribution

Integration of 802.1x (Legacy or future equipment)

Figure 7: Areas of development of TGi.

We can distinguish two kinds of fixes; short-term solutions and long-term solutions. Short-term solutions improve the existing protocol while making use of legacy hardware. Those solutions are also software or firmware[14] upgradeable. Long-term solutions generally use new protocols (authentication protocols, encryption protocol). It sometimes requires new hardware.

3. WPA before RSN

Short-term solutions may be less secure (patch – make use of legacy algorithms etc...) compared to long-term solutions but they have the advantage to address the immediate needs of the market. Since 802.11 networks are already widely deployed, and the new protocol RSN is not yet ratified, it is important to have a security solution - that replaces WEP - available today. This stopgap measure between WEP and the new stronger protocol is called Wi-Fi Protected Access (WPA) and has been created by the Wi-Fi Alliance[15] in collaboration with TGi. WPA takes the techniques

[14] Programming that is inserted into programmable read-only memory, thus becoming part of a computing device.

[15] Industry organization that certifies the interoperability of devices based on the 802.11 standard. It includes a group of vendors: Cisco Systems, Enterasys, Microsoft, Proxim/Agere, and Symbol Technologies.

"It will give TGi the time to complete and finalize the full 802.11i RSN amendment to the existing wireless LAN standard." *Wi-Fi Alliance Chairman Dennis Eaton* proposed by TGi that use legacy equipment and that are software/firmware upgradeable. Cf. figure 8.

WPA increases the level of authentication, confidentiality and integrity. It is designed for both home and enterprise users. Another requirement of WPA is that it has to be compatible with the future 802.11i standard.

WPA uses TKIP along 802.1x. TKIP enhances data privacy and data integrity. 802.1x enhances the user authentication, the access control and provides key distribution.

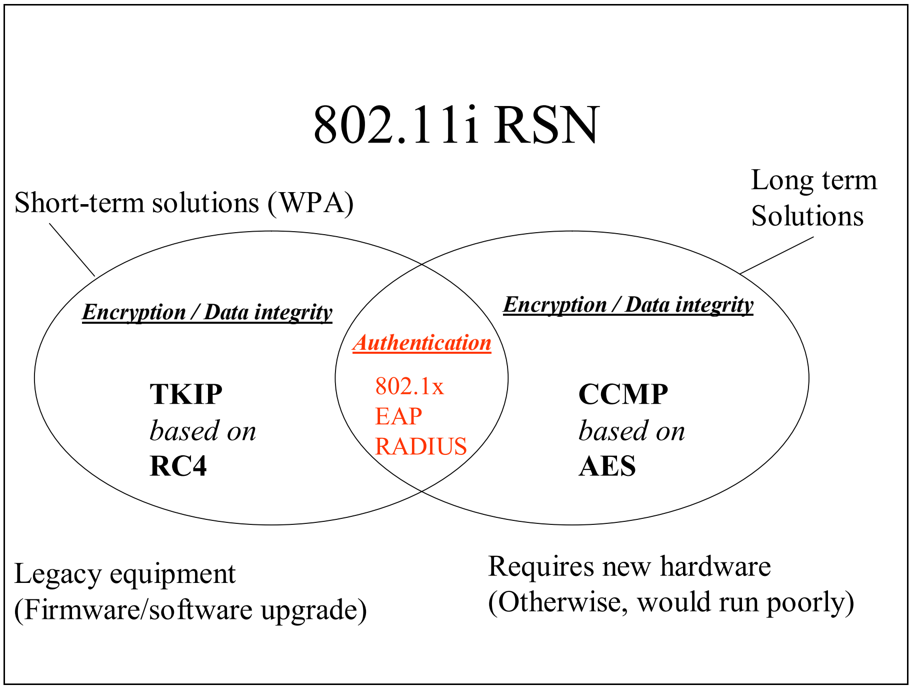

802.11i RSN
Short-term solutions (WPA)
Long term Solutions
Encryption / Data integrity
TKIP based on RC4
Authentication
802.1x
EAP
RADIUS
Encryption / Data integrity
CCMP based on AES
Legacy equipment (Firmware/software upgrade)
Requires new hardware (Otherwise, would run poorly)

Figure 8: Overview of 802.11 Robust Security Network. It includes both short term and long-term solutions. WPA takes the legacy solutions (left part) from the 802.11i draft plus 802.1x.

802.1x stands in the middle: it needs upgraded software drivers in Wi-Fi clients, firmware upgrades or replacement of access points, and the installation of a RADIUS server (software) in the wired network. See section 6 on 802.1x below.

4. TKIP

Temporal Key Integrity Protocol (TKIP) is a part of 802.11i. As we said above, TKIP fixes WEP flaws using existing hardware and thus keeps the original encryption protocol RC4. It changes the way keys are derived and rotates keys more often for security. Unlike WEP, TKIP provides a dynamic key management. TKIP can be viewed as an encapsulation of WEP.
Based on WEP flaws, here are the foundations of TKIP:

- Never reuse the same initialization vector (IV) with a particular session key.

We said in chapter 4.5 that 2 different packets should not be encrypted with the same key in order to avoid collision attacks (keystream reuse).

- Use a sequence number and discard packets which are not received in order

Each packet must have a sequence number. If a packet is received with a sequence number less or equal to the last successfully received packet, then it is discarded in order to prevent replay attacks.

- Automatic generation of new random keys

In order to enforce the foundation 1, session keys should be generated before the IV counter rolls over.

- New per-packet key generation

In order to avoid weak keys, session keys go through a complex mixing algorithm to produce per-packet keys used for the RC4 generator.

- New message integrity function

To avoid forgery attack as seen in chapter 4.3, a cryptographically secure hash function is used instead of the linear CRC in WEP.

We will describe the mechanisms that enforce the foundations of TKIP. It can be divided in 4 main components:

- Message Integrity Code (MIC)
- IV sequencing / Extended IV
- Per packet key construction
- Key distribution (rekeying mechanism)

The four next sections will describe those algorithms.

4.1. Message Integrity Code (MIC)

The Integrity Check Value (ICV) in WEP was a linear algorithm and was only function of the data. We have seen that ICV was not secure. To remediate, TKIP uses a cryptographically secure hash called MIC. It makes use of a key (*MIC key*). The requirements of the MIC key are [10]:

- Different keys for the two directions of communication
- Keys computationally independent of the encryption keys used
- Keys unpredictable for a third party

Furthermore, MIC is also function of the MAC addresses. See figure 9.

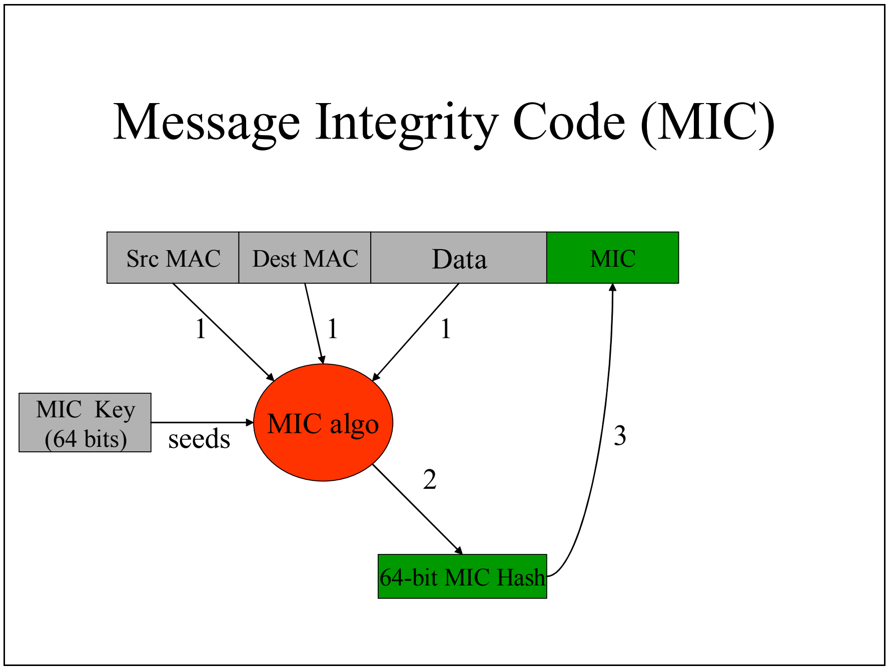


Figure 9: MIC computation

1) The MIC algorithm is function of the source MAC address, the destination MAC address, and the data. The MIC key seeds the MIC algorithm.
2) A 64-bit MIC hash is generated
3) The MIC hash is appended to the frame (before WEP encryption starts).

Figure 10 shows how the MIC is integrated in TKIP and its encapsulation in WEP.
By computing the hash over the source and destination MAC addresses, the frame is linked to the sender and the receiver thwarting forgery attacks.
The receiver of an encrypted frame computes the MIC = function (MAC ad. source, MAC ad. destination, Data). If the result is the same as the MIC sent, then the message is presumed to be authentic. Otherwise, the message has been forged.

Countermeasure:
Given the very seldom accidental MIC failure, the first MIC failure encountered should be the result of an active attack. However, it has been decided to "ignore" the first MIC failure and wait for a second failure to take active countermeasures [10]. So,

if 2 forgeries occur in one second, then the keys are deleted and the station is disassociated and has to reassociate.

4.2. Extended IV / New IV sequence counter

TKIP uses an extended 48-bit IV.
The classical WEP makes use of a 24-bit IV. It turned out the number of different IVs was too small to have a unique couple (key, IV) during the lifetime of the key.
Let's recall how the WEP frame is:

WEP frame: (IV = 3 bytes)

WEP IV 3 bytes	Key Id	Data N bytes	ICV 4 bytes

So it has been decided to extend the size of the IV in order to extend the IV space. The new IV in TKIP is constructed from the first and last bytes of the WEP IV and the 4 bytes of a new extended IV (Cf. TKIP frame below). The frame in TKIP is 12 bytes longer than WEP's one. (4 bytes for the extended IV and 8 bytes for the MIC.)

TKIP frame: (IV = 6 bytes)

ICV = CRC(Data, MIC)

1st byte		Last byte	Key Id	***Ext IV 4 bytes***	Data N bytes	MIC 8 bytes	ICV 4 bytes

WEP IV

The extended IV (4-bytes) has 2 roles:
It is used to prevent *collision* attacks (keystream reuse).
With 6 bytes, the IV space is largely expanded and defeats collision attacks. 2^48 packets can be exchanged using a single session key. Thus, it ensures that given a session key, the same IV is used at most once[16].

The 2-bytes IV taken from WEP IV is called TKIP sequence counter (TSC). It is used as a sequence counter. The receiver will discard any packets – for a given key - with a sequence number less or equal than the previously received packet. This prevents *replay* attacks.

Here are the IV management rules of the TSC:

- Initialize sequence to zero whenever the base keys are established, and not at every restart.
- The TSC is increased by one on each packet.
- Data traffic stops if the TSC reaches its maximum value
- Receiver discards any packets received out-of-sequence

[16] Under steady, heavy traffic conditions, it would take approximately 100 years for key reuse to occur. [18]

So, the use of an extended IV prevents 2 majors known attacks on WEP: The collision attack and the replay attack. Thanks to the expansion of the IV, no rekey should be required during a single association. Figure 10 shows at what step of the TKIP processing the new IV is used. The 48-bit IV is also used in the per-packet key construction, described in the next section.

4.3. Per-packet key construction

The goal of the per-packet key construction is to correct the WEP's misuse of RC4 that lead to weak key attacks.
The per-packet key is computed by mixing the transmitter address, the 48-bit IV and a 128-bit key called *temporal key*. The per-packet key is then used to encrypt the data, the MIC and the ICV. Each data or each fragment of data is encrypted with a unique key. Cf. figure 10. The use of the 48-bit IV extends the life of the temporal key and eliminates the need to re-key the temporal key during a single association.
The temporal key is named so since it is changed as soon as the sequence number rolls out.

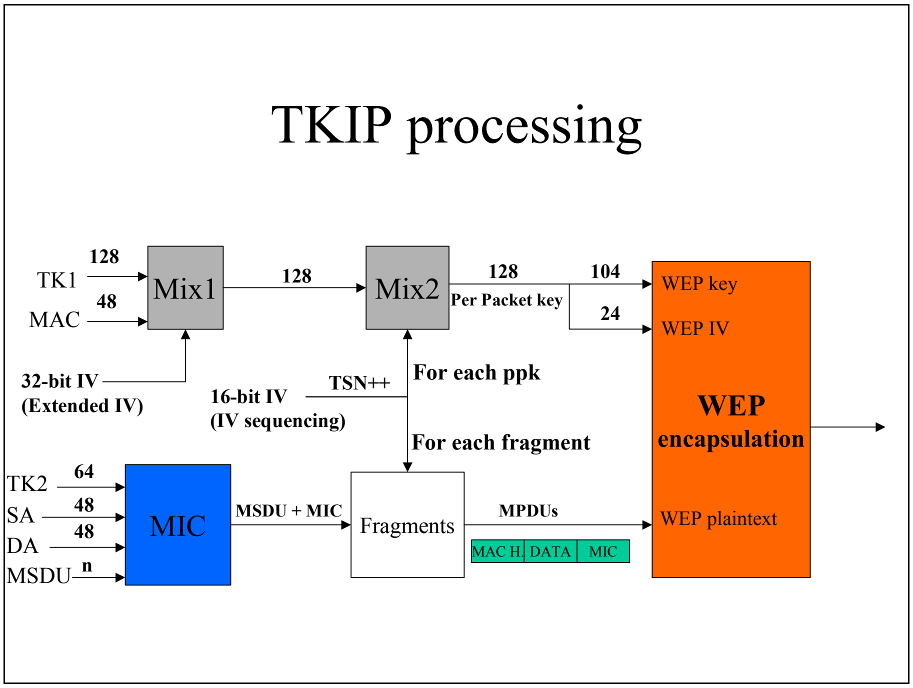


Figure 10: TKIP: Per packet Key construction and MIC computation

The complexity of the per-packet key construction prevents weak key attacks (see chapter 4, section 2). The temporal key is not used directly for the encryption. It goes

through a complex process that eliminates the patterns that are used to mount weak key attacks.
Phase 1 of the mixing function (Mix 1 in the figure 10) is used to eliminate the same key for use by all links.
Phase 2 of the mixing function (Mix 2 in the figure 10) is used to de-correlates the IV from know the per-packet key. [3]

4.4. Sum up of WEP fixes

Algorithm	Fixes (Prevents/Improves)
MIC (TKIP)	Prevents forgery
Extended IV (TKIP)	Prevents Collision/key reuse
IV sequencing - TSC (TKIP)	Prevents replay
Per-packet key const. (TKIP)	Prevents weak keys
802.1x (see next section)	Improve access control/ authentication, and key management

Table 1: Summary of WEP fixes

The 3 basic components to ensure security are confidentiality, integrity and authentication. We saw that the confidentiality is ensured by RC4 encryption, the integrity by an integrity check value (CRC-32 or MIC). Regarding the authentication, WEP provides an optional authentication called *Shared-key authentication*[17] (SKA). We’ve seen that SKA authenticates user’s MAC addresses and not users themselves. Moreover, there is no mutual authentication: the access point does not authenticate to the wireless station. When a user connects to a wireless network, he does not know where the access point is. He could connect to a rogue access point set up by a hacker who has a connection to the network. In this case, the user may not even know that the traffic is routed through the rogue access point! Another problem specific to wireless network: the communication channel between the user and the access point should be secure. Also, there is no centralized user authentication. In order to strengthen authentication, 802.11 TGi integrates the 802.1x standard described in the next section.

[17] Actually, the default is Open System Authentication that authenticates any stations. So, it cannot be considered as an authentication.

5. 802.1x: Standard for port-based network access control

The standard IEEE 802.1x defines a port-based network access control. It is based on Extensible Authentication Protocol (EAP)[18], which provides a wide variety of authentication mechanisms. 802.1x is designed to collect authentication information from users – credentials - and grant or deny access based on this information. The access control is performed at the MAC level (it is PHY-independent). 802.1x provides network access control through the concept of a port. A port is any kind of controlled access (router, switch, modem line for dial-up etc). 802.1x was not initially designed for wireless networks. So, to adapt this concept to 802.11, we need to define what a port in this context is: The IEEE community defines a *virtual port* as an association between a station and an access point. To associate with an access point, the station has to authenticate first (802.11 authentication[19]). Once associated with a specific access point, the station can go through 802.1x authentication.

802.1x provides per-station, per-session keys, and causes these keys to be changed often, solving reuse issues.

The use of EAP and RADIUS along with 802.1x provides a user-based identification, a choice of authentication methods and a centralized user management as well as a dynamic key management. EAP and RADIUS are described later in the chapter.

5.1. 802.1x authentication at a glance

When a client device attempts to connect with an access point, the access point responds by enabling a port for passing only EAP traffic from the client to an authentication server (typically a RADIUS server) located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the authentication server can verify the client's identity. Once authenticated, the access point allows other types of traffic on the client's port. In general, the protocol of communication between the client and the access point is EAP over LAN[20] (EAPOL) and the one between the access point and the authentication server is EAP over RADIUS[21] (or RADIUS).

5.2. 802.1x architecture and terminology

There are 3 principal entities in 802.1x. Each of them has a specific role to make the mechanism work. The client that desires the service is called a *supplicant* and the access point is referred as an *authenticator*.

1) The authenticator is responsible for:

- Enforcing the authentication of the device that attaches to its controlled port.
- Controlling the authorization state of its ports accordingly
- Route the traffic to an *authentication server*

[18] EAP is described later in the chapter.

[19] Open System Authentication or Shared-key authentication

[20] Encapsulate EAP messages in Ethernet frames.

802.1x was not specifically design for WLAN. For wireless networks, it is referred as EAPOW (EAP over WLAN)

[21] Encapsulate EAP messages in RADIUS attributes.

2) The supplicant is responsible for communicating its credentials - via a port on the authenticator – to the authentication server. (The supplicant may either initiate the authentication exchange or being requested by the authenticator). A supplicant is a network adapter; typically an Ethernet card adapter running 802.1x compliant client software or a WLAN client that supports 802.1x.
3) The *authentication server* performs the authentication function to check the credentials of the supplicant. It is usually a RADIUS server with EAP support (Cf. next chapter).
Figure 11 shows the 3 components of 802.1x. Figure 12 illustrates the port-based authentication.

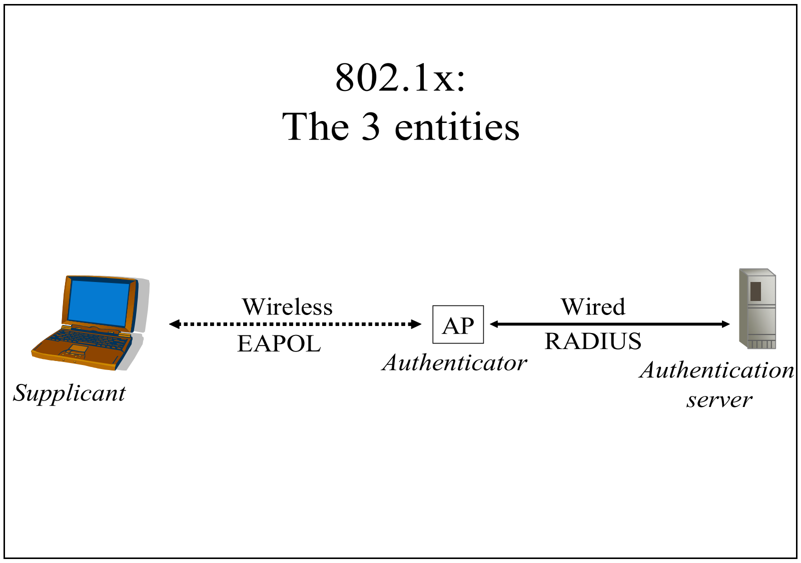

802.1x:
The 3 entities

Figure 11: The 3 components of 802.1x

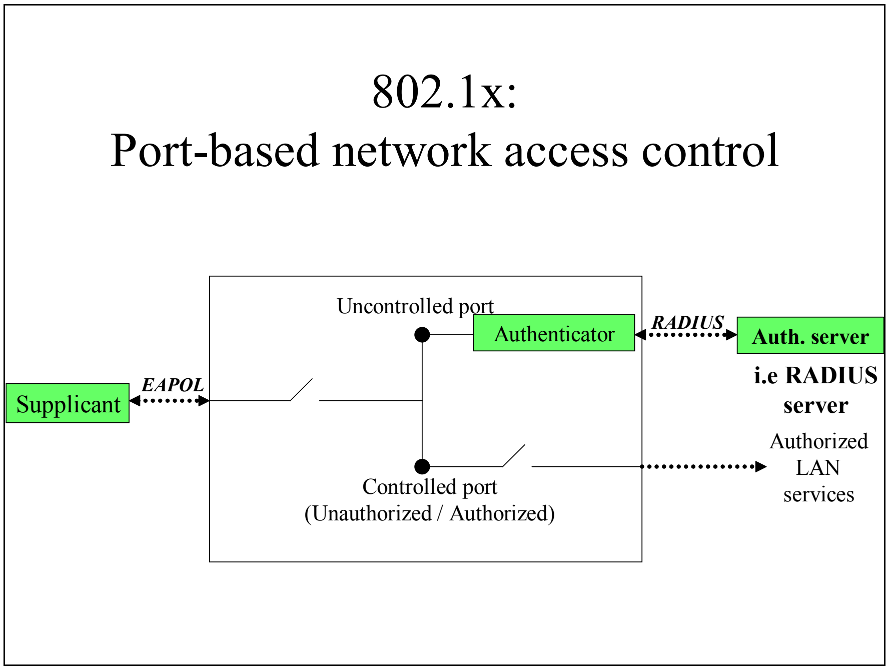

802.1x:
Port-based network access control

Figure 12: Port-based network access control

5.3. RADIUS

RADIUS (Remote Authentication Dial-In User Service) has been widely used by business and Internet Service Providers (ISPs) to control remote access.

A RADIUS client is a type of network access server (NAS) – in our case this is an access point, and sends authentication and accounting[22] requests to the RADIUS server (authentication server) in order to gain network access. Communications between the RADIUS server and the RADIUS client are authenticated through a shared secret. Each access point has its own shared secret with the RADIUS server. In general the transport protocol used is UDP and the RADIUS server listens on the port 1812. RADIUS supports a variety of authentication protocols (CHAP, MS-CHAP, and EAP). The main advantage of EAP is that it supports different methods of authentication. The choice of EAP method is negotiated by the client and RADIUS server during the authentication phase.

Figure 13 shows a typical RADIUS exchange. The RADIUS server sends Access-Challenge messages depending on the authentication method. The RADIUS client sends Access-Request to provide its identity or to respond to challenges. Eventually, the RADIUS server authenticates or not the client (Access-Accept / Access-Reject).

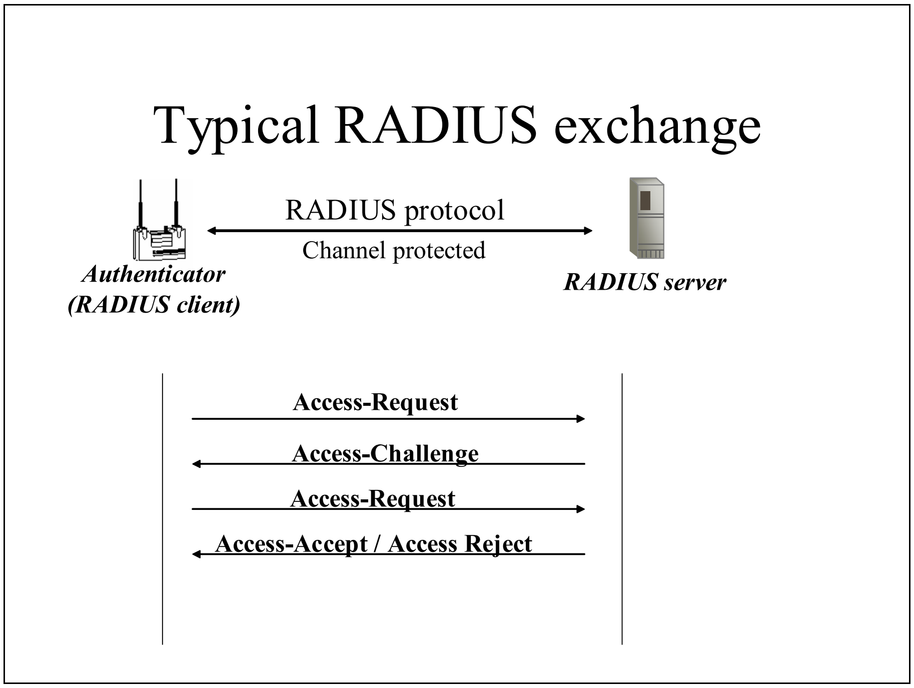


Figure 13: A typical RADIUS exchange.

5.4. EAP: Transport protocol between the supplicant and the access point

[22] Accounting is not in the scope of our paper, so we will not going through it.

EAP (Extensible Authentication Protocol) is essentially a transport protocol. Its main advantage is that it provides an authentication framework and can be used by a variety of different authentication types known as EAP methods[23]. It is supposed to head off proprietary authentication systems. It is designed to allow authentication methods to be deployed with no changes to the access point. EAP is used to pass the authentication information between the supplicant and the authentication server. The choice of authentication type is defined by the EAP type. The software supporting the EAP type resides on the authentication server and within the operating system of the client[24]. The access point can be seen as a bridge between the supplicant and the authentication server. One of the goals of EAP is to enable development of new authentication methods without modifying the access point. *One of the key points of 802.1X is that the authenticator can be simple and dumb---all of the brains have to be in the supplicant and the authentication server. This makes 802.1X ideal for wireless access points, which typically have little memory and processing power*. [11]
Since the authentication mechanism is independent of the access point[25], we can specify any EAP methods without updating access points.

5.5. Overview of EAP packets

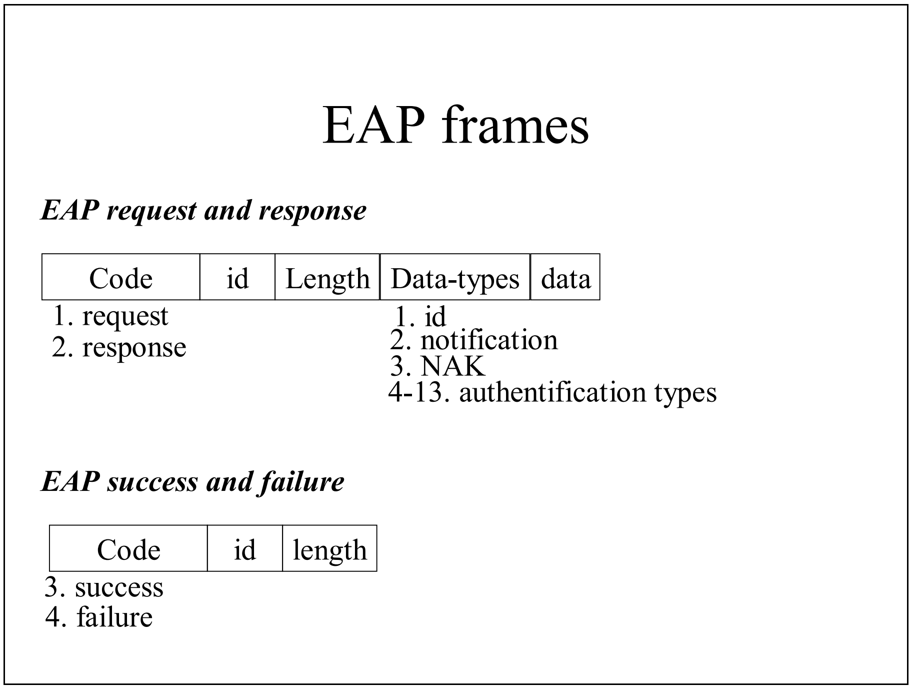
EAP exchanges are composed of requests and responses. The authenticator (access point) sends requests to the supplicant (wireless station that wants to access the network). The supplicant responds. Based on the credentials of the supplicant, the access will be granted or denied. There are two kinds of EAP packets (Cf. figure 14):

- EAP request and response
- EAP success and failure

The Data Type carried by the *EAP request and response* packets can be:
Data-type 1: The ID of the supplicant
Data-type 2: Notification: used to provide messages to the user
Data-type 3: NAK: used to suggest another authentication method
Data-type: 4-13 Kind of authentication type[26] (EAP-MD5, EAP-TLS, EAP-TTLS, EAP-PEAP, LEAP etc...)
At the end of the EAP exchange, the authenticator grants access or not to the network. The *EAP success and failure* packets do not contain data. It only specifies if the user has been authenticated or not following the requests and responses. The Data Type carried by the *EAP success and failure* packets are either Data Type 3 in case of a success and Data Type 4 in case of a failure.

NAK is used to suggest another authentication method. That is the client and RADIUS server negotiate the choice of authentication during the authentication phase. Figure 15 shows a typical EAP exchange.

[23] EAP supports both client-only authentication and strong mutual authentication.
[24] For example, Windows XP has integrated 802.1x and supports two EAP types: EAP-MD-5 and EAP-TLS
[25] However, the access point has to be 802.1x compliant.
[26] This is the key point of EAP. It provides an authentication framework. We can choose the authentication method. See next section for an overview of the EAP methods.



EAP frames

EAP request and response

Code	id	Length	Data-types	data

1. request
2. response

1. id
2. notification
3. NAK

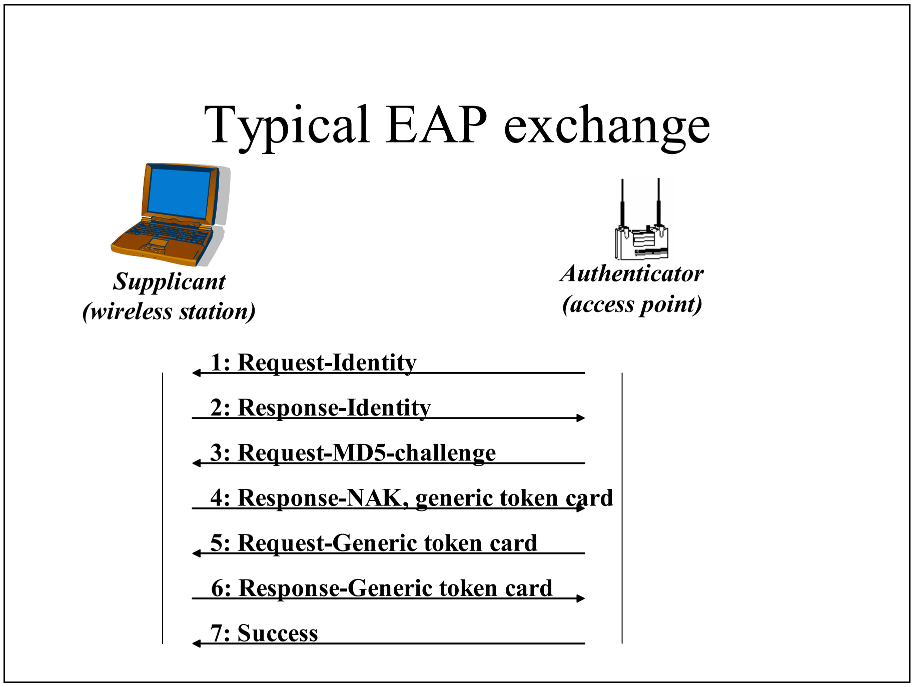
4-13. authentification types

EAP success and failure

Code	id	length

3. success
4. failure

Figure 14: Two kinds of EAP packets



Typical EAP exchange

Supplicant (wireless station)

Authenticator (access point)

1: Request-Identity

2: Response-Identity

3: Request-MD5-challenge

4: Response-NAK, generic token card

5: Request-Generic token card

6: Response-Generic token card

7: Success

Figure 15: A typical EAP exchange

The protocol used between the supplicant and the access point is EAPOL. It is an encapsulation of EAP and it provides start messages, session logoff notification and key negotiation.

5.6. 802.1x over 802.11

In this section, we show how 802.1x can integrate with 802.11.
1) The station must first associates with an access point[27]. In 802.11, the association follows the authentication (Open-system or Shared-key). Once the association is made, the dialogue between the station and the access point can start. (Cf. green part in figure 16).
The authentication server uses specific authentication techniques, to verify client's identity. (Passwords, digital certificates).
2.a) The supplicant can trigger the authentication process by sending an *EAPOL start* message. The authenticator allows only EAP traffic and blocks all other traffic, such as HTTP, DHCP, and POP3 packets
2.b) The authenticator sends an *EAP-Request/Identity* packet to the supplicant once it has associated with the access point.
3) The supplicant sends an *EAP-Response/Identity* packet to the authenticator to prove its identity. The packet is then routed to the authentication server encapsulated in RADIUS protocol (an EAP-Message attribute is used to encapsulate EAP packets for transmission from the authenticator to the RADIUS server).
4) The authentication server sends back a challenge to the authenticator. The challenge depends on the EAP method chosen. The authenticator unpacks this from RADIUS and re-packs it into EAPOL and sends it to the supplicant. At this point, the number of exchanged messages will vary according to the EAP method. Only mutual authentication is considered appropriate for wireless networks.
5) The supplicant replies to the challenge via the authenticator, which routes the response to the back-end server.
6) If the supplicant provides appropriate credentials, the authentication server responds with a success message -*Access Accept*-, which is then forwarded to the supplicant. The authenticator now unblocks the controlled port and allows normal traffic. However, RADIUS allows a per-user configuration. Certain users may have restricted access. In this case, the restrictions are specified in the RADIUS message *Access-accept* sent to the access point. For example, the authenticator might switch the supplicant to a particular VLAN or install a set of firewall rules.
EAP supports dynamic keying. That happens when the authentication succeeds.
7) EAPOW-key is used to transport the global keys. The section EAP keying – later in the chapter- describes the EAP key mechanism.
8) An EAPOL *logoff* notification can be sent to the authenticator to announce the end of the connection. 802.1X also defines a re-authentication timer, which can be used to periodically require the Supplicant to re-authenticate.
Figure 16 sums up the steps explained above. Figure 17 shows the encapsulation for both EAPOL and RADIUS protocol.

[27] This step can be viewed as the physical connection to the communication medium. It is similar as plugging an Ethernet NIC plugs into a jack in a wired network.

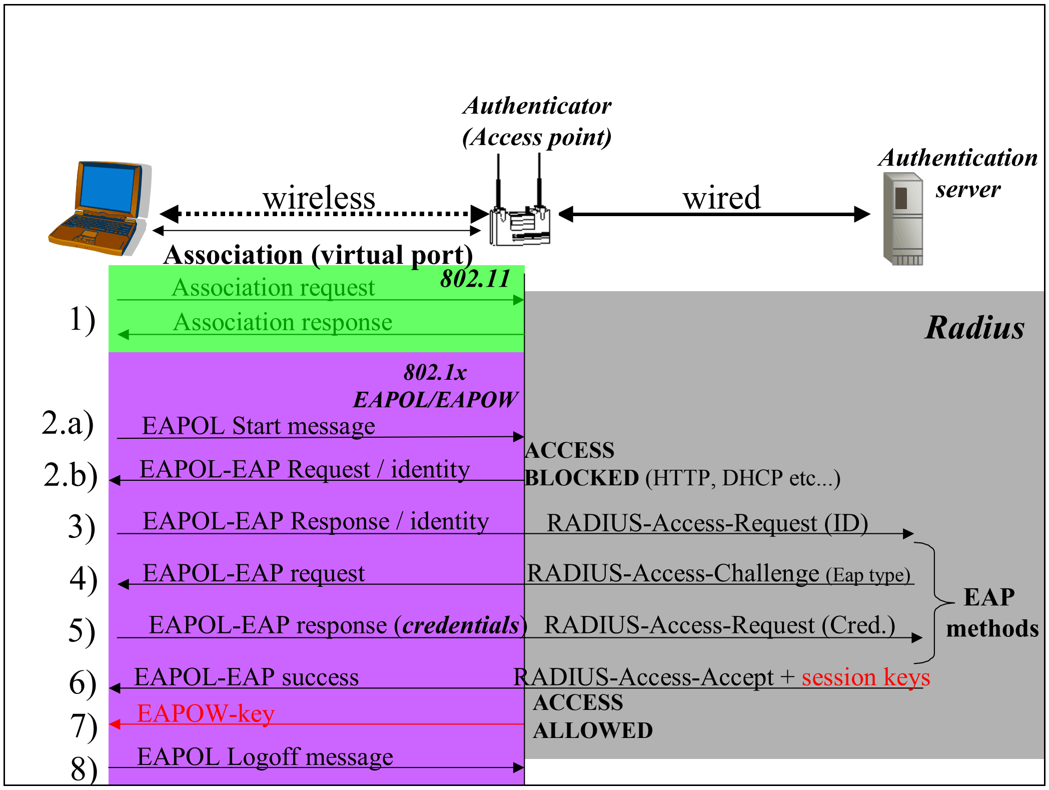

Authenticator
(Access point)
Authentication server
wireless
wired
Association (virtual port)
802.11
1)
Association request
Association response
Radius
802.1x
EAPOL/EAPOW
2.a)
EAPOL Start message
2.b)
EAPOL-EAP Request / identity
ACCESS
BLOCKED (HTTP, DHCP etc...)
3)
EAPOL-EAP Response / identity
RADIUS-Access-Request (ID)
4)
EAPOL-EAP request
RADIUS-Access-Challenge (Eap type)
EAP
methods
5)
EAPOL-EAP response (credentials)
RADIUS-Access-Request (Cred.)
6)
EAPOL-EAP success
RADIUS-Access-Accept + session keys
7)
EAPOW-key
ACCESS
ALLOWED
8)
EAPOL Logoff message

Figure 16: 802.1x over 802.11. Prior the 802.1x exchange, the station has to associate (in green in the figure – 802.11 part) to the access point (virtual port).

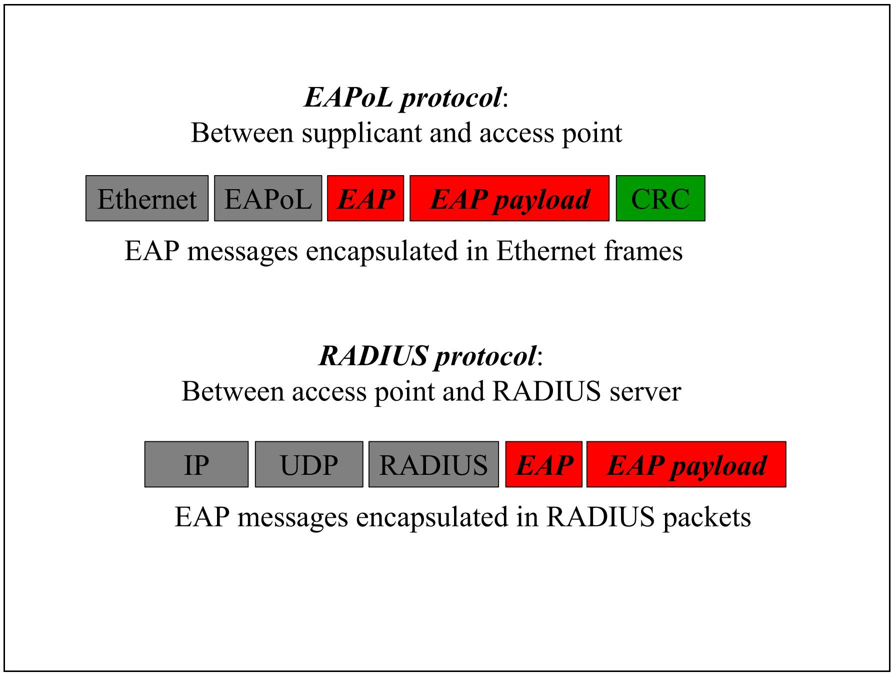

EAPoL protocol:
Between supplicant and access point
Ethernet
EAPoL
EAP
EAP payload
CRC
EAP messages encapsulated in Ethernet frames
RADIUS protocol:
Between access point and RADIUS server
IP
UDP
RADIUS
EAP
EAP payload
EAP messages encapsulated in RADIUS packets

Figure 17: Encapsulation in EAPOL and RADIUS protocol

5.7. Choice of EAP methods

802.1x was initially developed for authentication of users on wired LANs. So, the level of encryption needed was not as high as in wireless networks (easy to eavesdrop). Furthermore, wireless networks are subject to rogue access points, a problem that does not occur in a wired LAN. So, the client should ensure it connects a legitimate network. Both the client and the WLAN have to authenticate each other (*mutual authentication)*. Cf. Table 2.

New requirements for WLANs	*How to meet the requirements*
Stronger encryption to prevent eavesdropping	Encrypt communication between the client and the access point
Mutual authentication to prevent connection to rogue access points	Certificates to authenticate the network

Table 2: Two additional requirements for wireless networks

The EAP-MD5 method is the simplest to implement but is not recommended for wireless networks since there is no mutual authentication (network authentication) and no automatic keying.

It is a challenge response authentication protocol using a one-way hash function to encrypt the response. The authentication server sends a challenge text to the supplicant. This latter encrypts the challenge text along with the password and sends it to the authentication server. Since MD-5 is a one-way hash function, it is not possible to decrypt the message. So, the authentication server also encrypt the challenge it produced but with its copy of the password. Eventually, he compared the two hash generated. If there are equals, it means that the password stored by the authentication server and the supplicant's one are the same. The fact that the password is not sent in clear over the air is the advantage of this technique.

A common way of authentication is *certificates*. Many EAP methods use certificates. Though we will not describe all the EAP methods using certificates, it is important to understand the basics principles of certificates. The next section will describe what a certificate is and how a client can verify the certificate of the server.

Some EAP methods based on public-key certificates and Transport Layer Security (TLS) protocol: EAP-TLS, EAP-TTLS, and PEAP.

EAP-TLS:

It provides mutual authentication since both the client and the server use digital certificates signed by a certificate authority. It can provide user-based and session-based WEP keys to encrypt the communication channel between the client and the access point. This is a very secure authentication method. However, it requires all the user devices to have certificates. So, the cost of administration is high. Another advantage is that the certificates can be replaced by smart cards thus authenticating the user instead of the device.

EAP-TTLS / PEAP:
It is a hybrid method combining EAP-TLS and a traditional password-based method or another legacy method. This is to remove the burden of managing user certificates. Only the server needs a certificate. Like with EAP-TLS, encryption keys are generated during the authentication exchange.

5.7.1. Certificates

A certificate is a file containing several information among them the name of the client or server. It also contains the public key of the certificate authority (CA) that delivers the certificate. The server or client should recognize this authority.

Signature of the certificate by the CA:
The certificate goes through a hash function - the algorithm (SHA, MD-5) is specified in the certificate. The hash is then encrypted with the private key of the CA (only known by the CA). This step corresponds to the CA's signature. This signature is then added to the certificate. Figure 18 shows the creation of a server certificate (i.e. a bank).

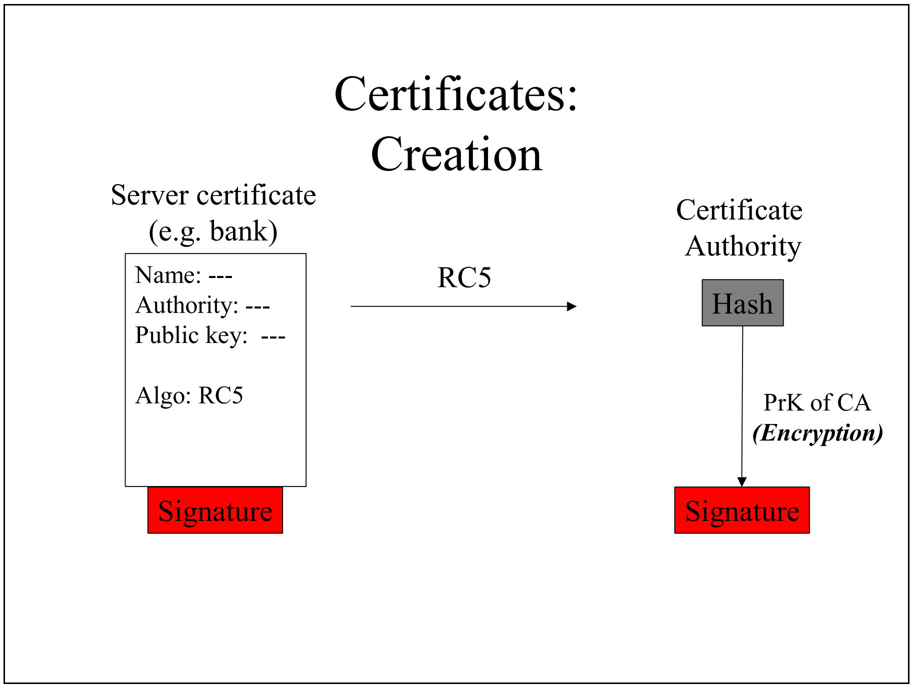
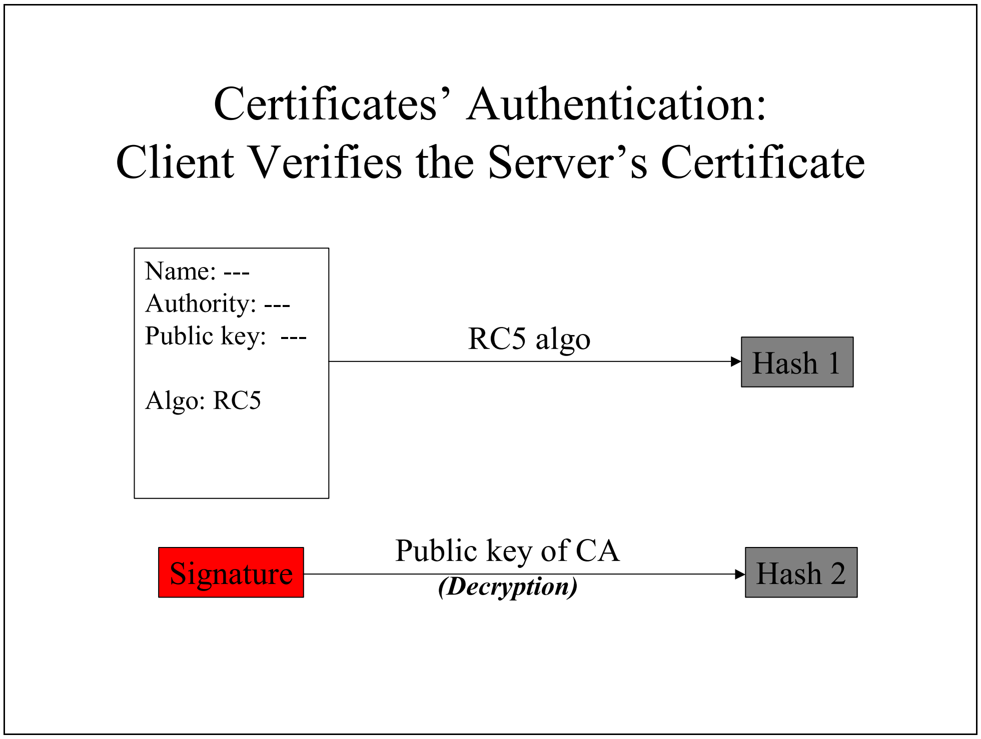


Figure 18: Creation of a server certificate: signature by the Certificate Authority

Verification of the certificate by the client:
When the client connects to the server, the server sends to the client the certificate. The client will verify that the content of the certificate is true. This is done in two steps. First, the client computes the hash algorithm and obtains a value x. It then decrypts the signature of the CA by using the public key of the CA – this is the reason why the client should recognize the CA. The decryption of the signature will reveal the value of the hash computed by the CA. If this hash matches the value x computed by the client, then the certificate is assumed to be true. Cf. figure 19.



Certificates' Authentication:
Client Verifies the Server's Certificate

Name: ---
Authority: ---
Public key: ---

Algo: RC5

RC5 algo

Hash 1

Signature

Public key of CA
(Decryption)

Hash 2

Figure 19: Verification of the certificate by the client – Two steps

5.8. EAP keying framework

We've seen that a lot of problems in WEP came from the absence of dynamic key management. Dynamic key management in 802.1x rectifies the drawbacks in the WEP security mechanism by deploying per-user session keys. Though 802.1x supports per-session keys (one session key for each user per session), most of the implementations only support global keys. But the difference is that if global keys are supported (WEP), the session key is only used to encrypt the global key and thus keeps the confidentiality of global keys unlike WEP.

EAP authentication involves the supplicant (EAP client), the access point and optionally the authentication server. We will describe the case where the authentication server is present (three-party exchange). When the authentication server is not present (two-party exchange), the EAP authentication method is implemented locally in the access point. This mode of exchange (called SOHO - Small Office Home office) is used in small networks. We will first describe the three-party exchange. In the next section, we will briefly describe SOHO.

5.8.1. Three-party exchange (with an authentication server)

There are 3 steps in the EAP keying framework [14][16]. They are:

✓ 802.1x authentication (EAP authentication protocol):
(Between the client and the authentication server)

During this phase, the EAP method is negotiated between the EAP client (supplicant) and the EAP server (authentication server).
An ***EAP master key (EMK)*** is derived between those two entities. Since this key is only held by the EAP client and EAP server, proof of possession of the EMK is a proof of mutual authentication and maybe used for fast reauthentication. This key must not be shared since it would enable a third party (e.g. access point) to impersonate the EAP client or server. To protect the EMK against compromising, EMK is not used directly (that's why TEKs are used to protect data) and should not be derivable from other keys like the MSK.
Transient EAP Keys (TEKs) are derived from EMK and are used to protect the EAP exchange itself.

EAP methods generate a **master session key (MSK)** directly from a successful EAP authentication. The MSK is either exported by the EAP method to the EAP client within the CS-Token[28] or is derived from the EMK, via a one-way function. This depends of the EAP method. For instance, EAP-TLS uses a one-way function. Whether the MSK is derived or transported, possession of the MSK must not provide information useful in determining the EMK and used in derivation of TSK.

✓ RADIUS-based key distribution – Token distribution (AAA[29] protocol)
(Between the access point and the authentication server)

Between the access point and the authentication server, a mutual authentication must be ensured to avoid rogue access points or rogue authentication server.
The communication channel between the access point and the authentication server must provide per-packet integrity protection, authentication and confidentiality. For example, RADIUS uses a static key to protect this channel. However, a session key is more secure like in RADIUS over IPSec [16]. The authentication server transports the MSK to the access point within the AN-Token[30].

✓ 802.1x key management (4-way handshake): TSK derivation
(Between the client and the access point)

[28] Package that provides integrity, authentication and encryption, in order to protect the MSK from compromise. Support for the CS-Token is optional and most current EAP methods do not support it, since they derive the MSK as part of the EMK (like EAP-TLS)

[29] Authentication, Authorization and Accounting

[30] Package within which the MSK and one or more AAA attributes (client MAC address, access point MAC and IP addresses, MSK lifetime etc...) is transported between the Authentication Server and the access point. [28]

After successful authentication and generation of the MSK, Both the client and the access point are supposed to possess the MSK. ***Transient Session Keys (TSKs)*** are derived from the MSK by a 4-way handshake: the 4-way handshake confirms that both the access point and the station possess the MSK. The TSK derivation should support mutual authentication so that the client will have the assurance that it is connected to the right access point.

The MSK is 192 bytes long. The first 32 bytes are called ***PMK (**or **pairwise master key)***. The MSK is ciphersuite independent. So that the MSK is usable with any ciphersuite (WEP-40, WEP-128, TKIP, CCMP etc…), it is often longer than necessary. So, it is cut to fit. For instance, TKIP and CCMP ciphersuites derive their TSK exclusively from the PMK.

The ciphersuite is negotiated between the EAP client and the access point using the link layer. The authentication server is not supposed to know the ciphersuite that will be used since it is not a party of the ciphersuite negotiation. So, the key generation in EAP methods should not be ciphersuite specific. This is the reason why the MSK is ciphersuite independent.

Figure 20 sums up the EAP keying framework.

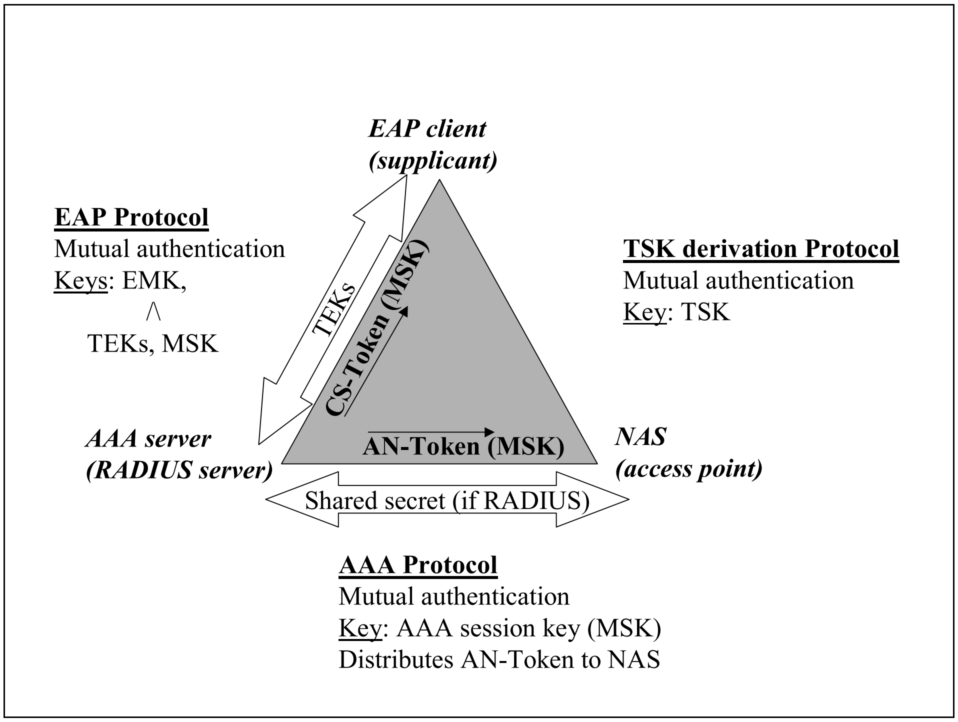


Figure 20: The 3 steps of EAP keying framework: The EAP authentication protocol, the AAA protocol and the TSK derivation protocol (adapted from [16])

Bernard Aboba and Dan Simon made some changes in a recent draft on EAP keying framework [17]:

During the EAP authentication, an ***EAP Master key (MK)*** is derived between the EAP client (station) and EAP server (AS). This key is kept local and is never exported to a third party. This key may be useful during fast resume. That is, since the MK possession is a proof of successful authentication, providing this key could shorten future EAP exchanges.

A ***Master session key (MSK)*** is derived between the EAP client and the authentication server. The MSK is chosen as the keying material (*AAA-key*) and the AAA-Key is transported to the authenticator (access point) (phase 1-b). The MSK is exported by the EAP method to the supplicant. The MSK is at least 64 bytes long and the first 32 bytes is called Pairwise Master Key (PMK). Another key is derived between the EAP client and server: the ***Extended Master Session Key (EMSK)***.

Like the MSK, the EMSK is exported by the EAP method but it is not transported to the authenticator. So, this key is only known by the supplicant and the authentication server. EMSK is not currently defined. It is reserved for future uses. For example, it could be used to derive additional keying material necessary against man-in-the-middle attack, or for fast handoff purposes.

Transient session keys (TSKs) are keys that are used by the ciphersuites (WEP-40, WEP-128, TKIP, CCMP etc...) 802.11i derive TSKs from the PMK only (first 32 octets of the MSK) where as WEP derive TSKs from the whole AAA-Key.

Transient EAP keys (TEKs) are used to establish a secure channel between the EAP client and server during the EAP authentication.

5.8.2. Two-party exchange (SOHO mode - without authentication server)

We’ve just seen that in a three-party exchange, an authentication server is present and there is a sophisticated authentication and distribution of keys. But in a two-party exchange (SOHO mode – Small Office Home office), a pre-shared key is entered manually. It is either entered as a stream of 256 bits or as a pass phrase. In the former case, those 256 bits correspond directly to the master key. In the latter case, the passphrase goes through an algorithm to convert the pass phrase into the master key:

Master key = Hash (pass phrase, SSID, SSID length) [13]

The output of this function is 256 bits corresponding to the master key.

The 4-way handshake (which occurs after a successful authentication and generation of the MSK in a three-party exchange) happens at the start of each session in a SOHO mode.

5.8.3. Advantage of using transient keys:

The keys generated by the authentication procedures or the pass phrase entered manually are not directly used for the TKIP encryption process. The master key is used to generate *transient* keys that will then be used in the negotiated cipher suite. For TKIP, we need one key for encryption function (cf. section 5.3) and one key for MIC computation (cf. section 5.1). For CCMP, only one key is needed for encryption and integrity. (Cf. section 7 below). Those transient keys help thwart any weak key attacks.

6. CCMP

Sources: [4] [6] [9]
The long-term solution proposed by TGi is Counter Mode with CBC-MAC (CCMP). It is designed for future equipment based on the new encryption protocol AES. Traditionally, two different cryptographic algorithms are used for authentication and encryption, each requiring its own key. For example, authentication might be provided by HMAC-MD5 and encryption by Triple-DES. However, CCMP uses a block cipher to provide both authentication and encryption. It is often referred as *Authenticated Encryption*.

CCMP is based on AES in CCM mode. CCM mode is an Authenticated Encryption combining counter (CTR) mode and CBC-MAC, using a single key. Counter Mode provides privacy and CBC-MAC provides authentication by computing a Message Authentication Protocol (MAC) using Cipher Block Chaining (CBC). CBC uses feedback to feed the result of encryption back into the encryption of the next block. The plaintext is xored with the previous ciphertext block before it is encrypted. The encryption of each block depends on all the previous blocks. See next section and figure 21 upper part.

1. Authentication

The message blocks are formed by splitting the message m into 16-octets blocks, and then padding the last block with zeroes if necessary. The MIC of a block {Mo ... Mk} is the result of the AES encryption of the block Mk xored with the previous MIC (MIC of {Mo ... Mk-1}). See figure 21, upper part. We can notice than the MIC is computed over both the header and the plaintext.

Let’s call M1 ... Mm the m block message
Let’s call Ck, the MIC of the blocks Mo-Mk.

$Ck = AES(Mk \oplus Ck-1)$ for $k = \{2...m\}$
$C1 = AES(Mo)$ (Mo is the initial block and contains a 48-bit PN)

Reuse of the same packet number (PN) with the same key voids all security guarantees.

2. Encryption

Each {Ao … Am} block contains one flag byte, one byte of QoS information, a six bytes address field, a six byte packet number and a two byte counter. So, the size of each A block is 16 bytes. Each of these As blocks goes through the AES encryption. The result is then xored with a block of plaintext to produce the ciphertext. Notice that both the plaintext and the MIC are encrypted. See figure 21, bottom part.

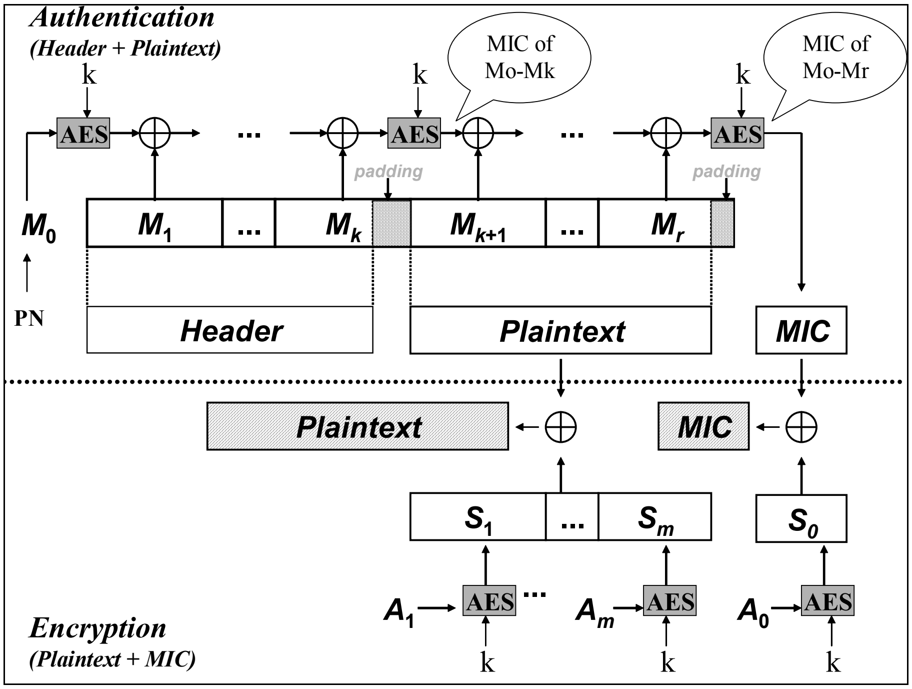


Figure 21: Authentication (upper part) and encryption (bottom part) with CCMP (adapted from [4])

Chapter 5: Other security measures

We have seen in the previous chapters that it is very difficult to have 100% security. There are always flaws in the protocols and algorithms but we should keep in mind that some known attacks described are not straightforward to mount. It is important to assess the motivation and the capability of the attacker. The protocols described (WEP, TKIP, CCMP, 802.1x) act at the MAC layer. Several other protections can be used on top of those protocols. Here are some examples.

1. Firewalls

If a hacker manages to access in the wireless network, he then could enter the wired network as well. To prevent such a scenario, it's recommended to put the wireless services outside of a firewall, so that in the worst case, the hacker would still gain little more than Internet access. [21]
See figure 22 below.

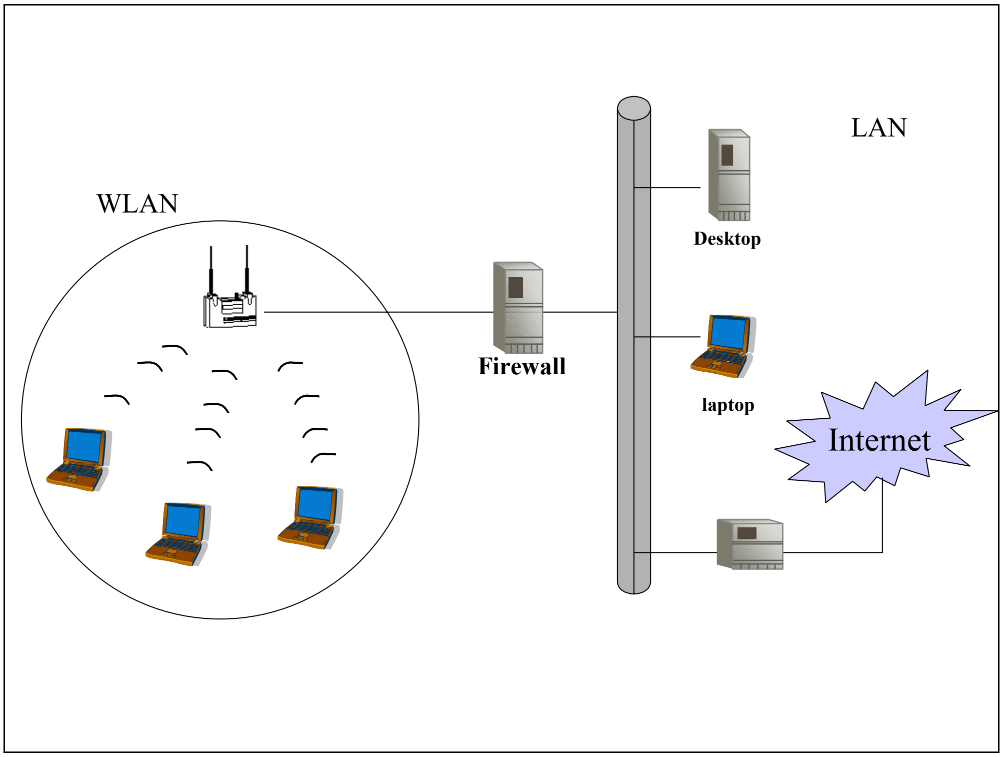


Figure 22: Separate the wireless network from the wired network

2. VPN

VPN technology provides secure data transmission over public networks such as Internet. Basically, the data is transmitted over the network by creating an encrypted, virtual point-to-point connection between the client and a VPN server that is located in a private network. VPN makes use of cryptography and allows user or device authentication. We can distinguish two categories of VPN. At the layer 2, we have L2TP whereas IPSec operates at the layer 3. IPSec is the most used today. [20]
Figure 23 shows how IPSec interacts with a WLAN.

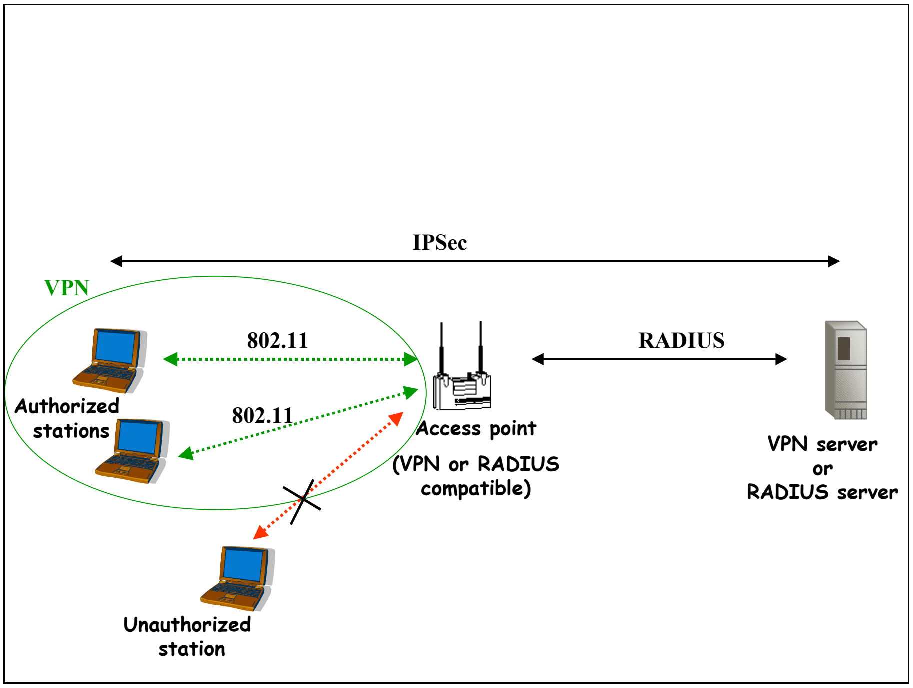


Figure 23: Integration of VPN in a WLAN

3. MAC address filtering

Most of the access points support MAC address filtering. Only a set of MAC addresses can associate with the access point. Each MAC address has to be manually entered in the access point. This is an interesting measure for very small networks. Otherwise, the cost of administration would be too high. However, like for the SSID, it is possible to sniff authorized MAC addresses with the help of a software. Then a hacker can reuse them since there is a way to change the MAC address by reprogramming wireless cards. So, this MAC-based authentication should only be used as a supplementary authentication method.

4. Closed network

Access points emit beacons continuously to show their presence to users. The frequency of broadcasting can be specified in the access point. However, it is possible to set up the access point so that it does not contain the SSID in the beacon frame. It forces the station to know the SSID in order to connect. However, the SSID is still broadcast by other stations during their associations with the access points. So, it is still possible to guess the SSID but it requires the use of a software to sniff the traffic. This adds a little protection to the wireless network but since the deployment of this security measure is so straightforward, it is worthy to do it.

All those techniques can be added on top of the protocols described in the paper. If those measures are all put together, it enhances the overall security of a wireless network.

Chapter 6: Security in practice: Installation of a RADIUS server

1. Introduction

The Mathematic building of the university is covered by a 802.11 wireless network. This allows Internet connectivity everywhere in the building. Students and professors can enjoy the wireless connectivity; students can access useful information while being in class and professors can access their slides online easily during their lectures.

The access control of the wireless network needs to be improved. After a description of the requirements and of the current security measures, we will explain the shortcomings and choose an appropriate method of access control (and data encryption). The last section will describe the deployment, tests and results of these new measures.

2. Identify the security requirements / strategy / policy

All the students and staff members can have access to the wireless network. However, for security reasons, we need to keep track of who is using the network at a given time.

3. Current security measures

The wireless network has 11 access points through the building. MAC address filtering is used. MAC access lists are stored in the access points. The WEP protocol is enabled. A key is required to gain access to the network. Students and staff members willing to access the network have to ask the WEP key to the network administrator. An IP address is statically assigned per MAC address. The reason why an IP address is bind to a MAC address is security: we want to keep track of people using the network.

4. Shortcomings

Every single user has to know the WEP key. Thus, the key is not a secret! Moreover, the wireless network uses one class C address, in other term it contains at most 255 IP addresses, which is a small number for our network. For each user (or each MAC address), we have to assign a static IP address. It wastes a lot of addresses since all the users may not be connected at the same time. But it is a security requirement to know who is using the network. The best thing would be to be able to keep track of users while having dynamic IP addresses.

5. New Security Measures Chosen

To fulfill the security requirement and having dynamic IP addresses, we will use 802.1x architecture in association with a RADIUS server.
The use of a centralized authentication server such as RADIUS will allow the user to enter a username and password. The authentication server checks the identity and a dynamic IP address will be assigned to the user. The user will not be identified by the MAC address. He will be identified with his username.

Besides that, the network administrator will no more interfere in the process. No more “pseudo-secret” WEP key is shared among the users! The authentication process will be simplified and the security will be improved.

6. Deploying these new Security Measures

6.1. Introduction

We will make use of FreeRADIUS as the RADIUS server on a UNIX server.

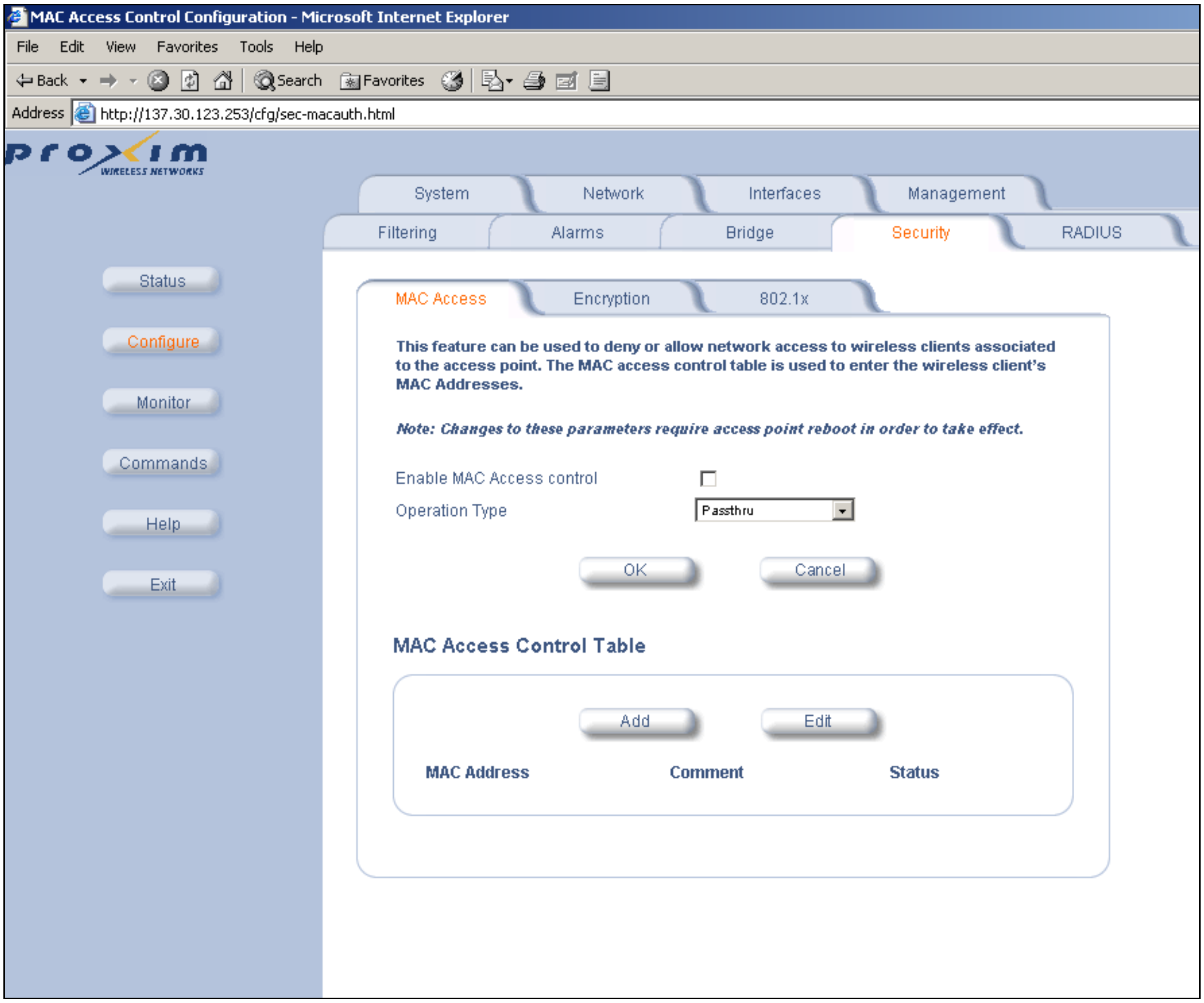
RADIUS (RFC 2138) is a protocol spoken between a network access server (NAS) and a RADIUS server. In our case (802.11) the NAS is an access point. When a user connects to the access point, he is asked for a username and a password. This credential is sent to the radius server. The server replies with *Access-Accept* or *Access-Reject message*. Besides authenticating users, a RADIUS server is also capable of doing accounting (login and logout records etc).
FreeRADIUS is an implementation of the RADIUS server program.
The work consists of installing the freeRADIUS server on a Linux machine on the wired side of the network.
An access point Proxim Orinoco AP-600 is used as the NAS. The user seeking access to the network has a station equipped with a wireless network interface card, running Windows XP operating system. The RADIUS server, the access point and the wireless station are the 3 basic components of the architecture. To enable the

communication between the access point and the RADIUS server, both the access point and the server needs to be configured. So, we will first show how to configure the access point and then we will explain the main configuration files of RADIUS server.

6.2. Access point configuration

It is possible to configure the access point via the web. To do so, we have to type the IP address of the access point (i.e. http://137.30.123.253). The GUI allows the configuration and the monitoring of the access point. In the configuration mode, there is a *Security* tab. (See picture 1 below).

Under the *Security* tab, we can configure the *MAC Access*, *Encryption* and *802.1x* (figure 24):



Address http://137.30.123.253/cfg/sec-macauth.html

This feature can be used to deny or allow network access to wireless clients associated to the access point. The MAC access control table is used to enter the wireless client's MAC Addresses.

Note: Changes to these parameters require access point reboot in order to take effect.

Enable MAC Access control □

Operation Type Passthru

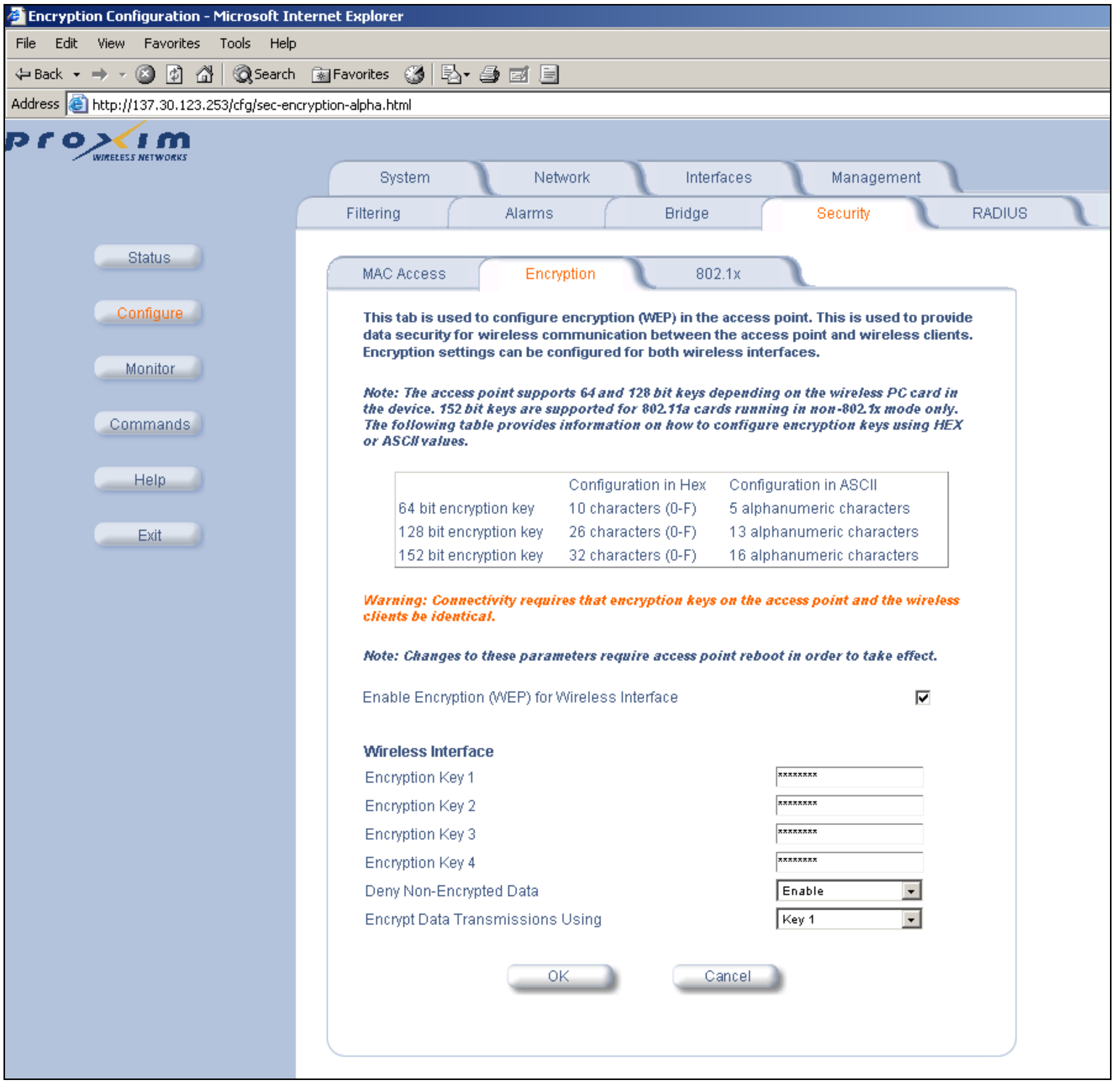
MAC Access Control Table

MAC Address Comment Status

Figure 24: Security configuration (MAC access)

The *MAC Access* tab (figure 24) allows the MAC address filtering. (Cf. chapter 6 section 3.). Authorized MAC addresses should be entered manually.

The *Encryption* tab (figure 25) is used to configure the WEP encryption of the access point. We can specify up to four encryption keys. The length of the keys can be 64 or 128 bits (or 152 for 802.11a cards).



This tab is used to configure encryption (WEP) in the access point. This is used to provide data security for wireless communication between the access point and wireless clients. Encryption settings can be configured for both wireless interfaces.

Note: The access point supports 64 and 128 bit keys depending on the wireless PC card in the device. 152 bit keys are supported for 802.11a cards running in non-802.1x mode only. The following table provides information on how to configure encryption keys using HEX or ASCII values.

	Configuration in Hex	Configuration in ASCII
64 bit encryption key	10 characters (0-F)	5 alphanumeric characters
128 bit encryption key	26 characters (0-F)	13 alphanumeric characters
152 bit encryption key	32 characters (0-F)	16 alphanumeric characters

Warning: Connectivity requires that encryption keys on the access point and the wireless clients be identical.

Note: Changes to these parameters require access point reboot in order to take effect.

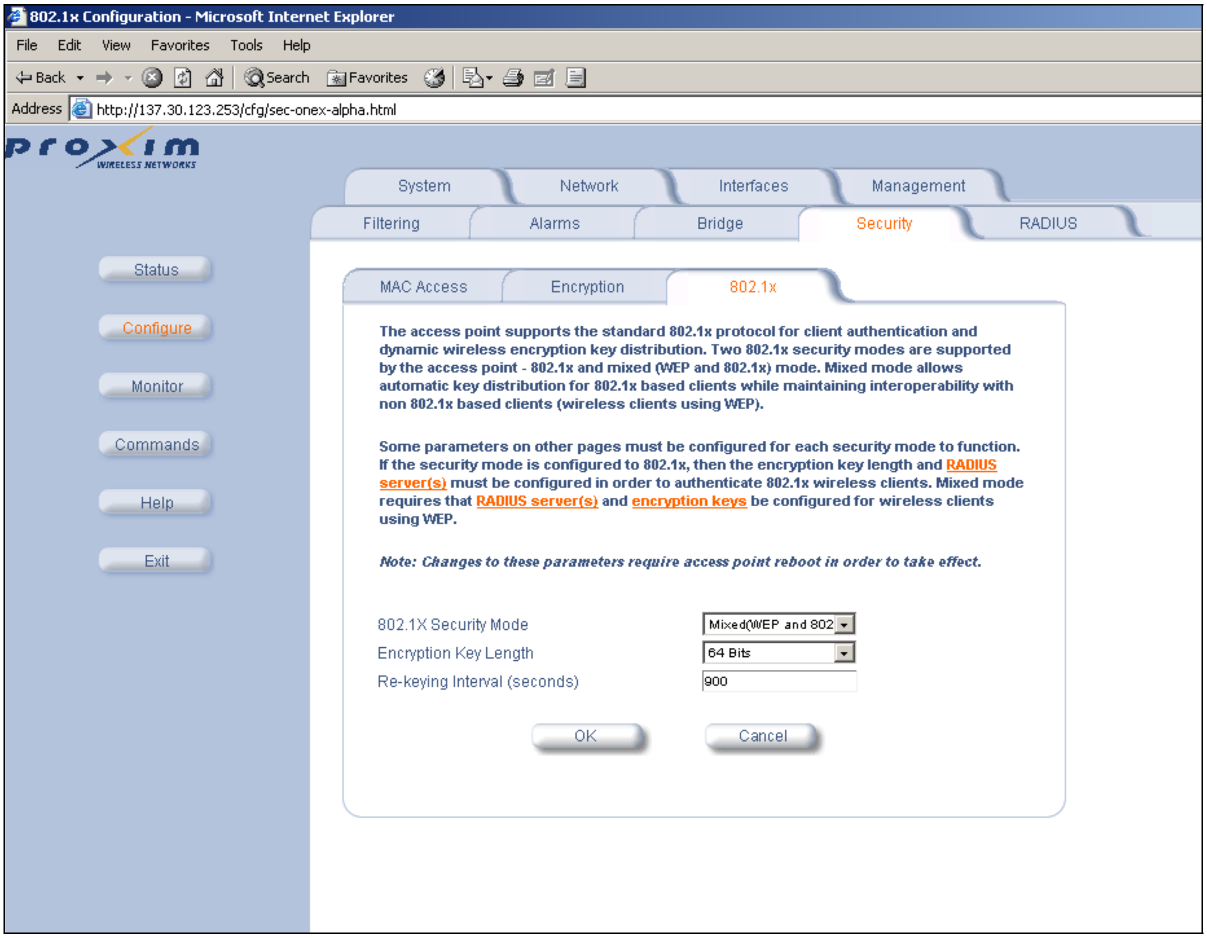
Enable Encryption (WEP) for Wireless Interface ☑

Wireless Interface

Encryption Key 1	*********
Encryption Key 2	*********
Encryption Key 3	*********
Encryption Key 4	*********
Deny Non-Encrypted Data	Enable
Encrypt Data Transmissions Using	Key 1

Figure 25: Security configuration (WEP encryption)

In the *802.1x* tab (figure 26) we can configure the 802.1x protocol. This access point supports two modes: 802.1x and mixed (WEP and 802.1x). In the former mode, only the RADIUS server has to be configured (along with the encryption key length). In the mixed mode, both the RADIUS server and encryption keys (*encryption* tab) should be configured.



The access point supports the standard 802.1x protocol for client authentication and dynamic wireless encryption key distribution. Two 802.1x security modes are supported by the access point - 802.1x and mixed (WEP and 802.1x) mode. Mixed mode allows automatic key distribution for 802.1x based clients while maintaining interoperability with non 802.1x based clients (wireless clients using WEP).

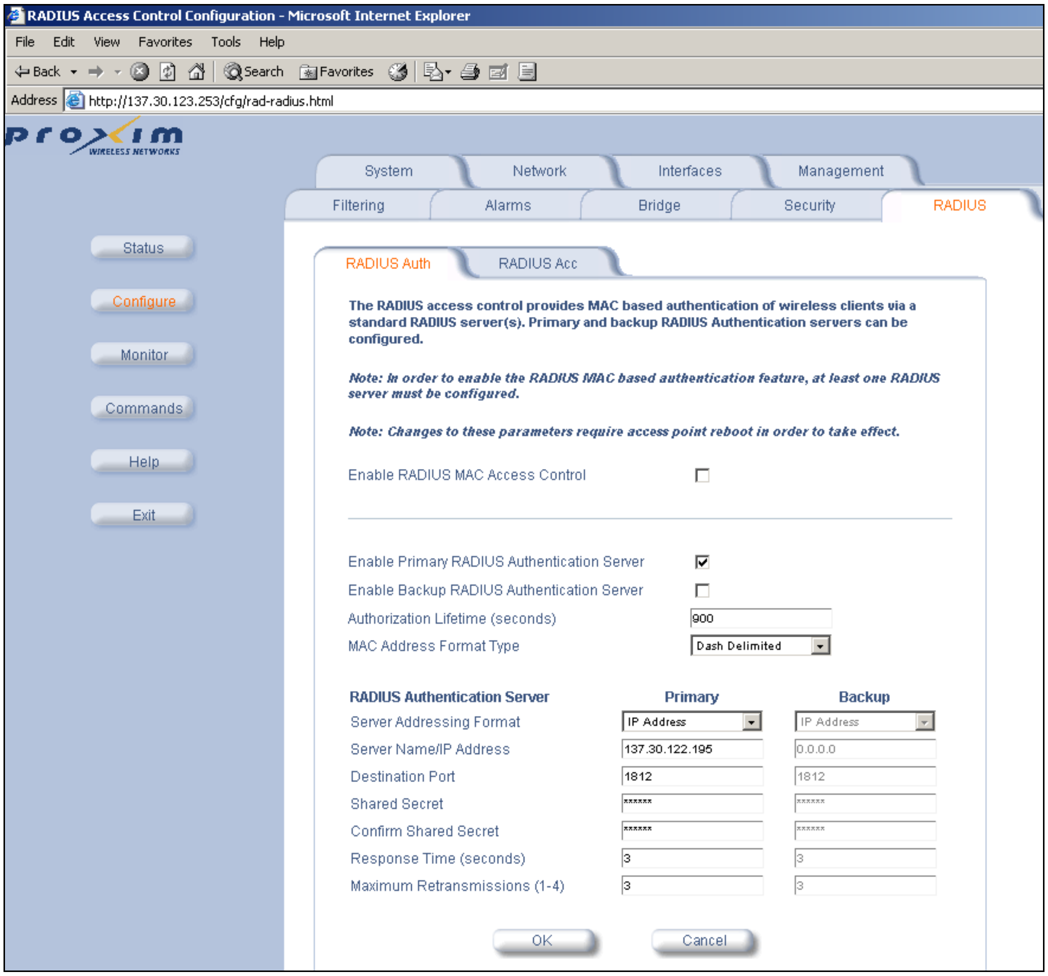
Some parameters on other pages must be configured for each security mode to function. If the security mode is configured to 802.1x, then the encryption key length and RADIUS server(s) must be configured in order to authenticate 802.1x wireless clients. Mixed mode requires that RADIUS server(s) and encryption keys be configured for wireless clients using WEP.

Note: Changes to these parameters require access point reboot in order to take effect.

802.1X Security Mode	Mixed(WEP and 802
Encryption Key Length	64 Bits
Re-keying Interval (seconds)	900

Figure 26: Security configuration (802.1x)

Under the RADIUS tab (figure 27), we can configure the RADIUS server. Both the RADIUS *authentication* and RADIUS *accounting* can be configured. We will explain only the RADIUS authentication. Up to 2 servers can be set up. For each server, we have to specify the address of the RADIUS server on the wired side of the network. Here, it is 137.30.122.95. Then, the port the RADIUS *authentication* is listening is 1812. As we said in chapter 5, section 5.3, the communication between the RADIUS and each access point is protected by a key called *shared secret*. This key has to be specified here and in the RADIUS server configuration (see next section).



The RADIUS access control provides MAC based authentication of wireless clients via a standard RADIUS server(s). Primary and backup RADIUS Authentication servers can be configured.

Note: In order to enable the RADIUS MAC based authentication feature, at least one RADIUS server must be configured.

Note: Changes to these parameters require access point reboot in order to take effect.

Enable RADIUS MAC Access Control	□
Enable Primary RADIUS Authentication Server	☑
Enable Backup RADIUS Authentication Server	□
Authorization Lifetime (seconds)	900
MAC Address Format Type	Dash Delimited

RADIUS Authentication Server	Primary	Backup
Server Addressing Format	IP Address	IP Address
Server Name/IP Address	137.30.122.195	0.0.0.0
Destination Port	1812	1812
Shared Secret	******	******
Confirm Shared Secret	******	******
Response Time (seconds)	3	3
Maximum Retransmissions (1-4)	3	3

Figure 27: RADIUS configuration

6.3. FreeRADIUS configuration

First, the RADIUS server needs to know the location of the access point. Then to protect the communication channel (encryption and signed packets) between the access point and the RADIUS server, a static key is used. It is often referred to as a "*shared secret*".

Figure 28 below is a portion of the *clients.conf* file. Our access point is configured there:

```
TEST OF RADIUS SERVER WITH THE ACCESS POINT ORINOCO AP-600

client 137.30.123.253 {

     secret  = michel
     shortname    = MichelAP
     nastype = other
}
```

Figure 28: Portion of *clients.conf* file

The location of the access point in the network is specified (137.30.123.253) and the shared secret between this access point and the RADIUS server is also mentioned (michel). A short name is used as an alias for the IP address. Another attribute (nastype) tells the RADIUS server what NAS-specific method to use to query the NAS in case of simultaneous use.

The other important configuration file is the *users* file. It contains authentication security and configuration information for each user. Basically, when the RADIUS server gets the username and the password of the user connecting to the network, the RADIUS server parses the *users* file and tries to match an entry. The password of the user can be statically entered in this file or if the keyword "system" is used, the RADIUS server will check the system password file instead.

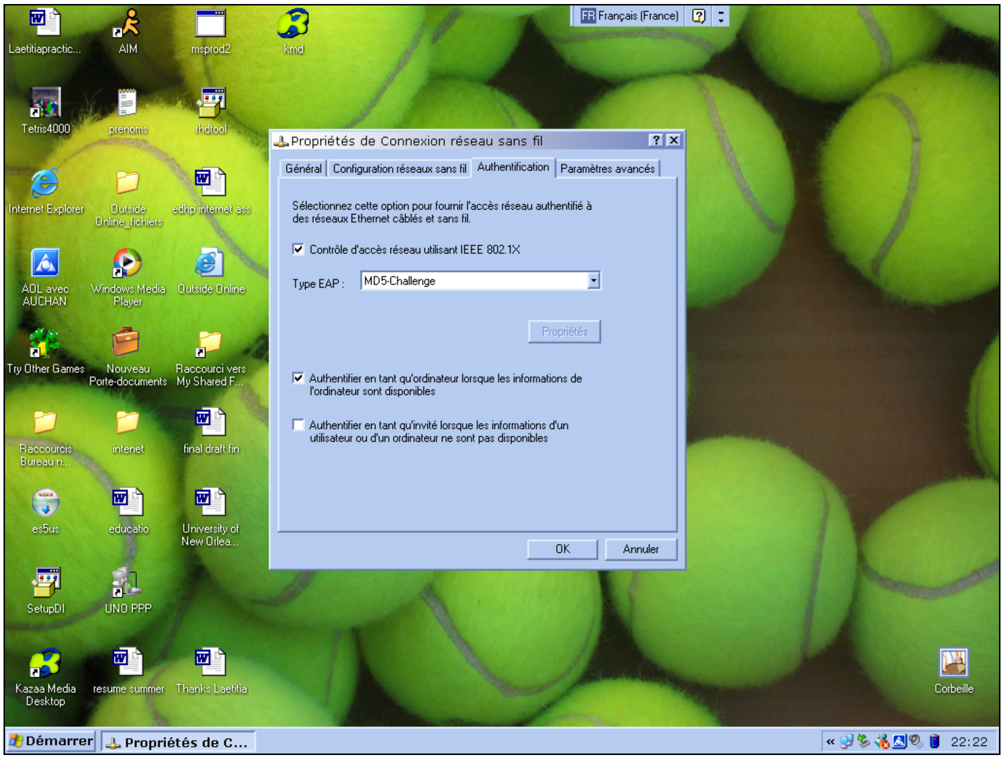
The portion of the *users* file below (figure 29) shows different possibilities of user configurations. It contains three entries (lameuser, michel and Peter Doe) and a default entry (DEFAULT). Any other username than lameuser, michel or Peter Doe will match the default entry. The default entry specifies the system as authentication type. So, for example, if the username is John, the RADIUS server will parse the password file system and will verify the password entered by John. In the case of Peter Doe, the authentication type is EAP. The RADIUS server will check the default EAP authentication method chosen in the *radiusd.conf* configuration file and apply that EAP method.

```
lameuser      Auth-Type := Reject
                     Reply-Message = "Your account has been disabled."

michel        Auth-Type := System
                     Reply-Message = "Hello, %u",
                     Fall-Through = No

"Peter Doe"  Auth-Type := EAP, User-Password == "hello"
                     Reply-Message = "Hello, %u"


DEFAULT   Auth-Type = System
                     Fall-Through = 1
```

Figure 29: Portion of *users* file

7. Tests and results

7.1. Client (Windows XP) configuration



Propriétés de Connexion réseau sans fil

Général | Configuration réseaux sans fil | Authentification | Paramètres avancés

Sélectionnez cette option pour fournir l'accès réseau authentifié à des réseaux Ethernet câblés et sans fil.

☑ Contrôle d'accès réseau utilisant IEEE 802.1X

Type EAP : MD5-Challenge

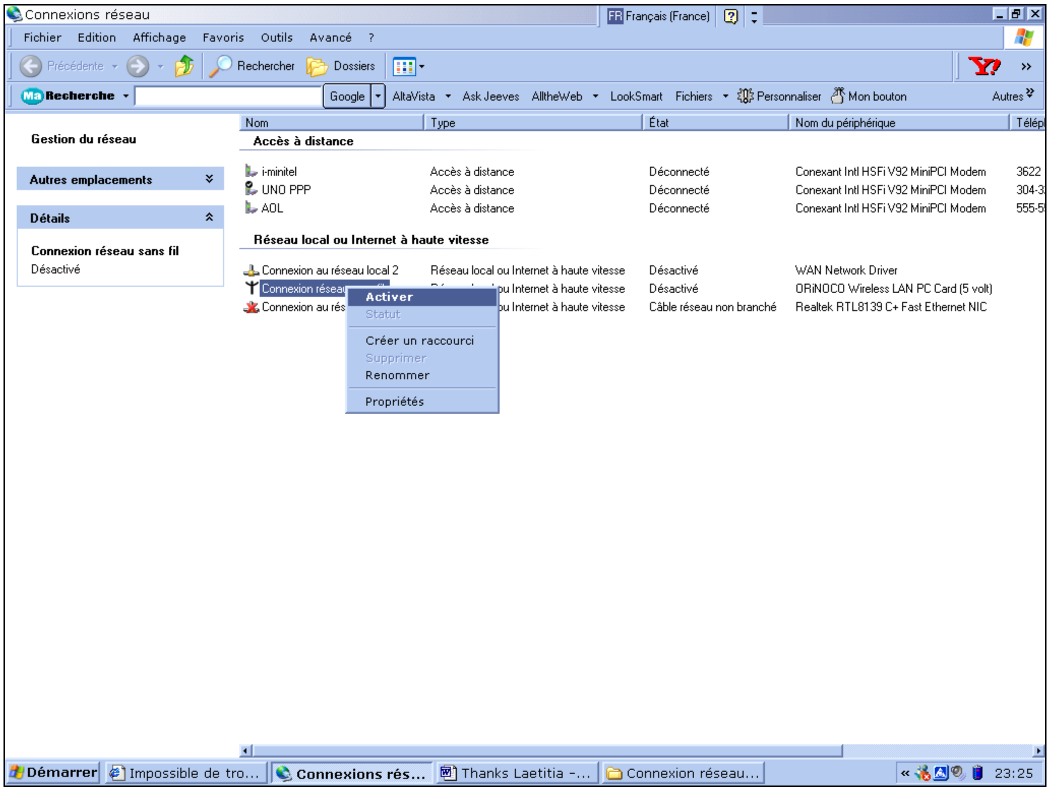
Propriétés

☑ Authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles

☐ Authentifier en tant qu'invité lorsque les informations d'un utilisateur ou d'un ordinateur ne sont pas disponibles

OK | Annuler

Figure 30: Choice of the EAP type (EAP-MD5)



Gestion du réseau

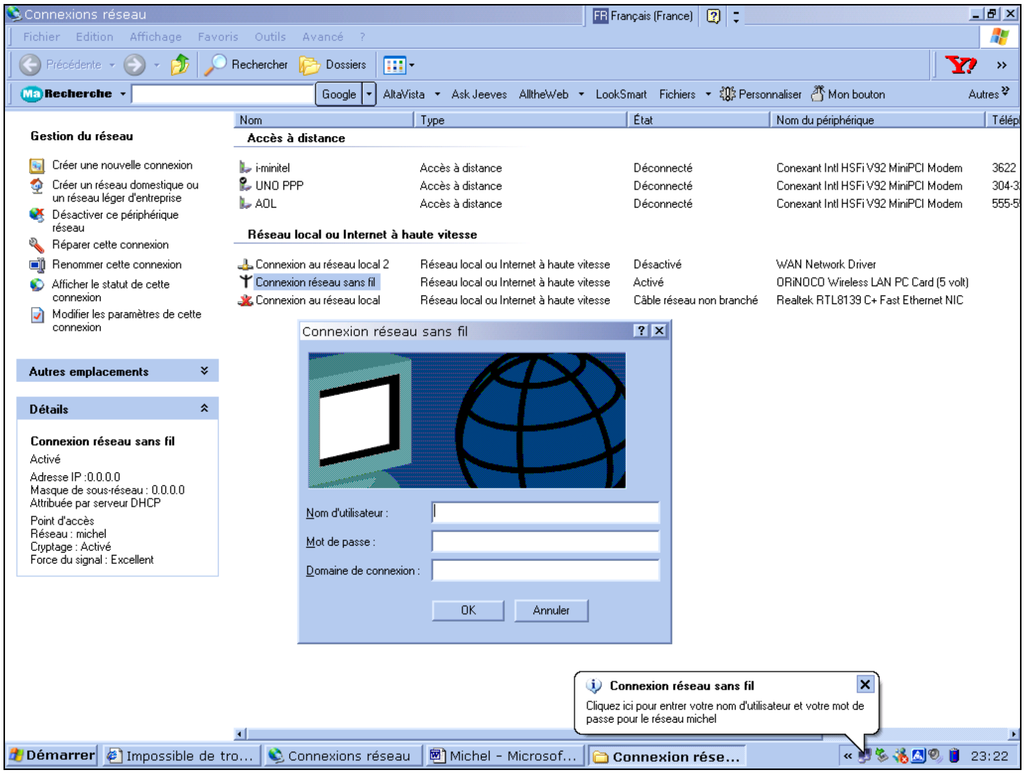
Autres emplacements

Détails

Connexion réseau sans fil
Désactivé

Nom	Type	État	Nom du périphérique	Télép
Accès à distance				
i-minitel	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	3622
UNO PPP	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	304-3
AOL	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	555-5
Réseau local ou Internet à haute vitesse				
Connexion au réseau local 2	Réseau local ou Internet à haute vitesse	Désactivé	WAN Network Driver	
Connexion résea	ou Internet à haute vitesse	Désactivé	ORiNOCO Wireless LAN PC Card (5 volt)	
Connexion au rés	ou Internet à haute vitesse	Câble réseau non branché	Realtek RTL8139 C+ Fast Ethernet NIC	

Figure 31: We enable the wireless card



Gestion du réseau

- Créer une nouvelle connexion
- Créer un réseau domestique ou un réseau léger d'entreprise
- Désactiver ce périphérique réseau
- Réparer cette connexion
- Renommer cette connexion
- Afficher le statut de cette connexion
- Modifier les paramètres de cette connexion

Autres emplacements

Détails

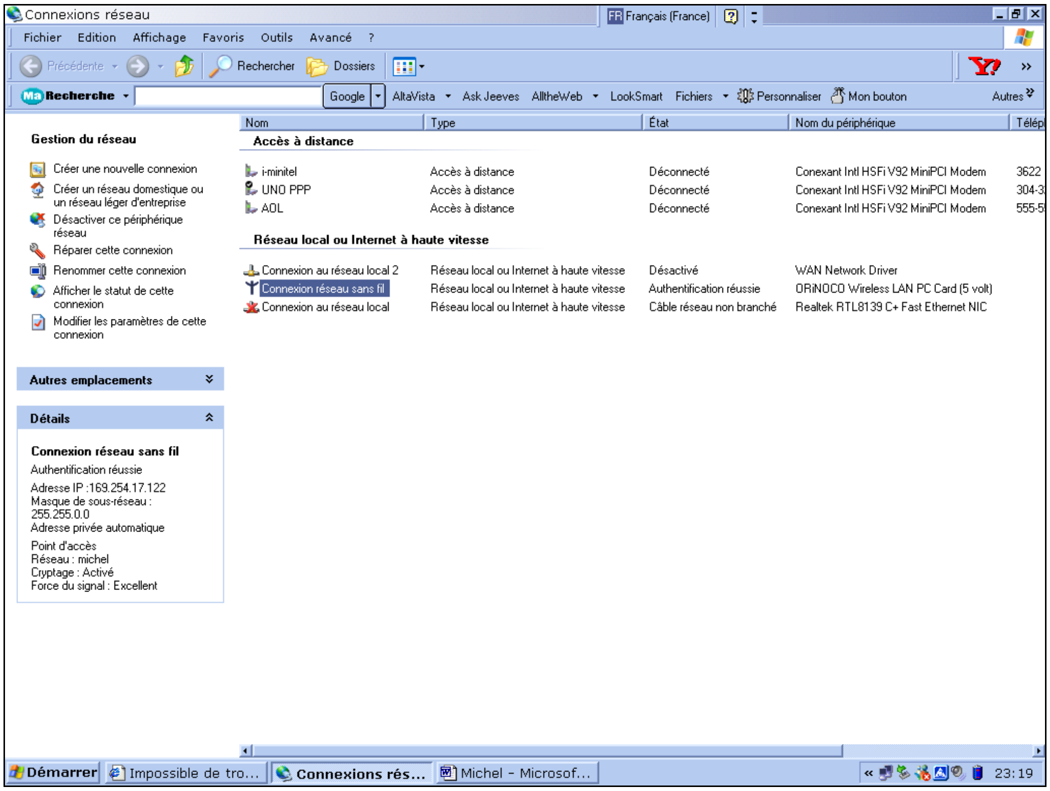
Connexion réseau sans fil
Activé
Adresse IP : 0.0.0.0
Masque de sous-réseau : 0.0.0.0
Attribuée par serveur DHCP
Point d'accès
Réseau : michel
Cryptage : Activé
Force du signal : Excellent

Nom	Type	État	Nom du périphérique	Télép
Accès à distance				
i-minitel	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	3622
UNO PPP	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	304-3
AOL	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	555-5
Réseau local ou Internet à haute vitesse				
Connexion au réseau local 2	Réseau local ou Internet à haute vitesse	Désactivé	WAN Network Driver	
Connexion réseau sans fil	Réseau local ou Internet à haute vitesse	Activé	ORiNOCO Wireless LAN PC Card (5 volt)	
Connexion au réseau local	Réseau local ou Internet à haute vitesse	Câble réseau non branché	Realtek RTL8139 C+ Fast Ethernet NIC	

Nom d'utilisateur :
Mot de passe :
Domaine de connexion :

Connexion réseau sans fil
Cliquez ici pour entrer votre nom d'utilisateur et votre mot de passe pour le réseau michel

Figure 32: The wireless network is found. They prompted for a username and password



Nom	Type	État	Nom du périphérique	Télép
Accès à distance				
i-minitel	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	3622
UNO PPP	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	304-3
AOL	Accès à distance	Déconnecté	Conexant Intl HSFi V92 MiniPCI Modem	555-5
Réseau local ou Internet à haute vitesse				
Connexion au réseau local 2	Réseau local ou Internet à haute vitesse	Désactivé	WAN Network Driver	
Connexion réseau sans fil	Réseau local ou Internet à haute vitesse	Authentification réussie	ORiNOCO Wireless LAN PC Card (5 volt)	
Connexion au réseau local	Réseau local ou Internet à haute vitesse	Câble réseau non branché	Realtek RTL8139 C+ Fast Ethernet NIC	

Connexion réseau sans fil
Authentification réussie
Adresse IP :169.254.17.122
Masque de sous-réseau : 255.255.0.0
Adresse privée automatique
Point d'accès
Réseau : michel
Cryptage : Activé
Force du signal : Excellent

Figure 33: The credentials are sent to the RADIUS server via the access point. If they are corrects, then the authentication is successful (*Authentification reussie* in the figure).

When the station finds the wireless network, a pop-up window (if the client is windows XP) asks for a username and a password (figure 32). The credentials are then sent to the RADIUS server via the access point. If the credentials are right, the authenticator will authorize the access to the station (figure 33). Otherwise, the network access will be blocked.

7.2. Tests

I didn't get any majors problems to install the FreeRADIUS software. The configuration files of FreeRADIUS are described in the previous section. It is straightforward though there is no GUI to configure those files. To check if the server is well installed and listens to requests, freeRADIUS has a tool named *radclient* which is a radius client program. It sends arbitrary radius packets to a RADIUS server, and then shows the reply. So, it can be used to monitor if the server is up or to test changes made in the configuration of the RADIUS server. Once this local test was successful, I started configuring the access point and the RADIUS server so that they can communicate securely (by sharing a secret key)

Cf. section 6.2 and figure 28 in section 6.3. The final step is to configure the wireless client.

The client configuration depends on the operating system used. The first tests that I made were with a station running windows XP. My Windows XP version supports EAP-MD5 and EAP-TLS. I did the tests with EAP-MD5 since it does not require any certificates management. The tests were satisfying. However, since the SP1 version of XP, the EAP-MD5 method is no longer available for wireless networks. So, we need to use server certificates if we want to use EAP-TLS under windows XP. Regarding the problem since the XP sp1 version, there are a lot of complains from users who do not understand how Microsoft can remove this type of authentication since EAP-MD5 is defined in the RFC! There are two reasons: the "official" one is that obviously EAP-MD5 is not as secure as other methods that make use of certificates. The other reason is that Microsoft wants to promote its own authentication protocol and forces us to use PEAP. I chose EAP-MD5 instead of a more secure method –based on certificates- for two reasons; first, the down side to certificates is the cost of administration. It requires the authenticator to have a public key certificate signed by an authority that is recognized by the user's devices. This requires the network administrator either to purchase server certificates from a commercial certificate authority or to have the cumbersome task to generate them. Plus, each new user would need to install them. Despite the management problem, certificates would have been a good choice if our requirements were to strengthen the confidentiality. However, this is not the case. We just want better user identification. That's why EAP-MD5 fits well.

Regarding the new versions of windows XP that do not have EAP-MD5 method, there should be a patch. If not, there are client software in the market that supports EAP-MD5 (e.g. AEGIS client).

7.3. Advantages and recommendations

Those results meet the security requirements: we now have *user identification* without binding the identity of the user to a MAC address. We can assign dynamic IP addresses.

To improve the access control of our wireless network, I recommend using 802.1x protocol along with the RADIUS server - *FreeRADIUS*. This is a free software and it works very well.

Conclusion

In this paper, we presented the particular requirements of wireless networks from a security standpoint. We have seen that a security protocol is needed to get a wireless network as secure as an unprotected wired network. This was the primary goal of WEP. However, WEP fails to provide this security requirement. Sometimes, the algorithms chosen were not strong enough (CRC), or the implementation of the algorithms was not appropriate (this is the case of RC4). The main problem in WEP was undoubtedly the lack of automatic key management. This flaw lead to several known attacks described in chapter 3. Understanding the inefficiency of WEP along with the growing of wireless market, the wireless community decided to move forward and propose a new security standard for wireless networks. In the chapter 4, we went through those new algorithms developed by Task Group I. Some of them are targeted for the actual hardware (TKIP) where as others are designed for new hardware like CCMP. Those two algorithms enforce data integrity and confidentiality. However, the authentication part is enforced by 802.1x protocol. This protocol is based on EAP and thus provides a choice for the authentication method. This flexibility is very attractive since the authentication requirements can be very different from a company to another. EAP methods go from very basic ones (passwords) to very complex ones, based on certificates and public-key cryptography. 802.1x provides a dynamic key distribution, which solves the main flaw in WEP and the RADIUS server provides a centralized authentication.

We see that many different security mechanisms exist, they operate at different layers and they have a different cost. So, it is important to assess the security needed in order to make the right choice.

Sources

[1] Bruce Schneier – Applied Cryptography, Second edition – Chapter 9.

[2] Jesse Walker – 802.11 Security Series, Part I: The Wired Equivalent Privacy

[3] Jesse Walker – 802.11 Security Series, Part II: The Temporal Key Integrity Protocol

[4] Jesse Walker – 802.11i Overview Part I – Intel

[5] Roy Werber – WEP weaknesses – Hebrew University of Jerusalem

[6] On the Security of CTR + CBC-MAC – Jakob Jonsson

[7] Dennis Eaton - WLAN Security – Interstil

[8] Matthew S. Gast - 802.11 Wireless Networks, The Definitive Guide – O'Reilly

[9] CCMP AES – Vocal Technologies, Ltd

[10] Niels Ferguson, Mac Fergus – Michael: an improved MIC for 802.11 WEP – Jan, 17 2002

[11] Joel M Snyder - What is 802.1x? - Network World Global Test Alliance, Network World Fusion, 05/06/02

[12] Nikita Borisov, Ian Goldberg, David Wagner – Intercepting Mobile Communications: The insecurity of 802.11

[13] Robert Moskowitz - Weakness in Passphrase Choice in WPA Interface - ICSA Labs, a division of TruSecure Corp.

[14] Laurent Butty, Frank Veysset - Wi-Fi security: What's next? – France Telecom R&D, september 2003

[15] Bernard Adoba - Draft-aboba-pppext-key-problem-06.txt – EAPWG - IETF 56 – San Francisco, CA

[16] Bernard Adoba, Dan Simon - Draft-aboba-pppext-key-problem-05.txt – December 21st 2002

[17] Bernard Adoba, Dan Simon - Draft-aboba-pppext-key-problem-07.txt – August 9th 2003

[18] Cisilion – Advantages of wireless networking - http://www.cisilion.com/wireless_advantages.htm

[19] Mike M. Khayat - Wireless Local Area Network (WLAN) Advantages vs. Disadvantages March 12, 2002 - http://faculty.ed.umuc.edu/~meinkej/inss690/khayat.pdf

[20] Jenne Wong, Ray Hunt – Security Architectures in Wireless LANs, Computer Science department, University of Canterbury, New Zealand

[21] Guy Pujolle – Security and mobility management in the embedded Internet - University of Paris 6

Vita

Michel Getraide was born in Paris, France in August 9th, 1979. He graduated from the Universite de Marne La Vallee where he got a *Licence* in 2001 and a *Maitrise* in 2002 in Computer Science.