Security in IEEE 802.11 Networks

Mário Nunes, Rui Silva, António Grilo

March 2013
1 – Introduction to the Security Services
2 – Basic security mechanisms in IEEE 802.11
   2.1 – Hidden SSID (Service Set Identifier) do AP
   2.2 – MAC address restriction at the Access Point
3 – WEP (IEEE 802.11)
4 - IEEE802.11i
   4.1 TKIP
   4.2 CCMP
5 - IEEE 802.1X
6 – Complementary security solutions
   6.1 – Layer3: Virtual Private Network (VPN)
   6.2 – Layer4: IP Address Control and Firewall
   6.3 – Layer 7: Proxy/Gateway
1- Introduction to the Security Services

1. Confidentiality
2. Data Integrity
3. Authentication
4. Non-repudiation
5. Service Availability
6. Access Control
1. Introduction to the Security Services

1. Confidentiality

Sender → Transformation → Receiver

Attacker's Domain

Coded !
1. Introduction to the Security Services

2. Data Integrity

- Transformation
- Insertion
- Integrity Check
- Error!
1. Introduction to the Security Services

3. Authentication
To verify the sender’s identity
1. Introduction to the Security Services

3.1. Digital Certificate issued by Certificate Authority (typical contents):

Serial Number: Used to uniquely identify the certificate.

Subject: The person, or entity identified.

Signature Algorithm: The algorithm used to create the signature.

Signature: The actual signature to verify that it came from the issuer.

Issuer: The entity that verified the information and issued the certificate.

Valid-From: The date the certificate is first valid from.

Valid-To: The expiration date.

Key-Usage: Purpose of the public key (e.g. encypherment, signature, certificate signing...).

Public Key: The public key.

Thumbprint Algorithm: The algorithm used to hash the public key certificate.

Thumbprint: The hash itself, used as an abbreviated form of the public key certificate.
1. Introduction to the Security Services

4. Non-Repudiation

- Sending Receipt
- Reception Receipt
- Sender’s Domain
1. Introduction to the Security Services

5. Service Availability
(corresponding attack: “denial of service”)
1. Introduction to the Security Services

6. Access Control
2 – Basic IEEE 802.11 Mechanisms

2.1 – Hidden SSID (*Service Set Identifier*) by the AP

To avoid the periodic broadcast of the Access Point (AP) identity in order to prevent its interception and misuse by an attacker.

2.2 – Restriction of authorized MAC addresses by the *Access Point*

To specify the MAC addresses that are allowed to use the network and associate with the AP.
2.1 – Hidden SSID

B – Beacon, periodically sent by the APs, without SSID
2.1 – Hidden SSID
2.1 – Hidden SSID

A user who knows the SSID, sends a Probe Request

The attacker waits for the Probe Response

Probe Response includes the SSID!
2.2 – MAC Address restriction by the AP

- The MAC addresses are transmitted in plain text and thus can be captured by the attacker.
- Most Wi-Fi cards allow the user to dynamically re-configure the MAC address.

<table>
<thead>
<tr>
<th>Protocol Version (2bits)</th>
<th>Type (2bits)</th>
<th>SubType (4bits)</th>
<th>To DS (1bit)</th>
<th>From DS (1bit)</th>
<th>More Frag. (1bit)</th>
<th>Retry (1bit)</th>
<th>Pwr. Mgmt (1bit)</th>
<th>More Data (1bit)</th>
<th>WEP (1bit)</th>
<th>Order (1bit)</th>
</tr>
</thead>
</table>

**Type:**
- 00 – Management
- 01 – Control
- 10 – Data
- 11 – Reserved

**SubType:**
- Probe
- Beacon
- Association Re/, Des/
- Authentication Des/
- RTS, CTS,
- ACK, CF, CF+ACK
- Power-Save Poll

**Generic MAC IEEE 802.11 Frame Format**

- AP Valid MAC ADDRESS Captured
3 - Wired Equivalent Privacy (WEP)

**Characteristics:**
- Included in IEEE 802.11
- Symmetric Key protocol
- Key distribution is not addressed by the standard
- Uses the RC4 cipher – “Ron Cipher 4” created in 1987 and publicly broken in the Internet in 1994

**Supported Services:**
- **Authentication:**
  1º) Open System Authentication: in means “no Authentication”
  2º) Shared Key Authentication: Performs authentication (*Pseudo*) based on a shared secret key
- **Data Integrity:**
  Adds a CRC to the message, sending it encrypted.
- **Confidentiality:**
  Encrypts the data based on a secret key shared by the communicating parites and the RC4 algorithm.
3 - Wired Equivalent Privacy (WEP)

Authentication

Shared Key

The challenge text is an arbitrary number of 128 bits
“Shared Key” Authentication Attacks [1/3]

1 – Collection of <challenge; response> pairs followed by an authentication attempt.

Data Base

- <c1; r1>
- . . .
- <cn; rm>

Attacker’s Domain

Captured challenge?

- YES
- NO! - Alert !!!

Authentication (request)
Authentication (challenge)
Authentication (response)
Authentication (success)
3 - Wired Equivalent Privacy (WEP)

“Shared Key” Authentication Attacks [2/3]

2 – Collection of <challenge; response> pairs followed by Cryptanalysis
3 - Wired Equivalent Privacy (WEP)

“Shared Key” Authentication Attacks

3 – Collection of IVs and creation of KeyStream library

Note: The Initialization Vector (IV) is a 24 bit string that is sent in plain text and constitutes the first 24 bits of the cipher key.
3 - Wired Equivalent Privacy (WEP)

**RC4 Algorithm**

- Secret Key
- Operation in Two Phases:
  1\(^a\) KSA – *Key Setup Algorithm*
  System Initialization
  2\(^a\) PRNG – *Pseudo-Random Number Generator*
  Byte Encryption in Stream Mode
3 - Wired Equivalent Privacy (WEP)

**RC4 Algorithm – KSA**

1ª Parte: Inicialização do array SBox

2ª Parte: Inicialização do array KBox

3ª Parte: Cálculo de Valores do SBox

```
i = j = 0;

// 1ª Parte
For i = 0 to 255
Sbox[i] = i;

// 2ª e 3ª Partes
For i = 0 to 255
Begin
j = j + Sbox[i] + Sbox[j]
Troca (Sbox[i], Sbox[j])
End
```
3 - Wired Equivalent Privacy (WEP)

RC4 Algorithm – PRNG and Cipher

A sequência de Números Aleatórios Gerados (KeyStream) é sempre a mesma para uma dada Chave

\[
\begin{bmatrix}
0 & 1 & 2 & 3 & \ldots & 39 & 40 & \ldots & 162 & 243 & 254 & 255 \\
40 & 162 & 243 & 254 & 3 & 0 & \ldots & 1 & 243 & 254 & 255 & 39 \\
\end{bmatrix}
\]

\[
i = (i + 1) \mod 256
\]
\[
j = (j + Sbox[i]) \mod 256
\]
\[
k = (Sbox[i] + Sbox[j]) \mod 256
\]
\[
R = Sbox[k]
\]

// Antes do Ciclo
i = j = 0;

// Ponto 1
i = (i + 1) \mod 256;

// Ponto 2
j = (j + Sbox[i]) \mod 256;

// Ponto 3
Troca (Sbox[i], Sbox[j]);

// Ponto 4
k = (Sbox[i] + Sbox[j]) \mod 256;
R = Sbox[k];
3 - Wired Equivalent Privacy (WEP)

**RC4 Algorithm – Weakness**

XOR Function Properties:

\[ a \text{ XOR } b = c \quad c \text{ XOR } a = b \quad c \text{ XOR } b = a \]

\(<\text{Original Message}>\) XOR \(<\text{KeyStream}>\) = \(<\text{Ciphertext}>\)

\(<\text{Original Message}>\) XOR \(<\text{Ciphertext}>\) = \(<\text{KeyStream}>\)

\(<\text{Ciphertext}>\) XOR \(<\text{KeyStream}>\) = \(<\text{Original Message}>\)

Since the KeyStream is always the same for the same Key, if we the attacker knows the KeyStream it is not necessary to know the Key in order to calculate the Original Message, based on the Ciphertext.

The IVs are used to make the KeyStream variable for the same secret key. E.g. 40-bit secret key + 24-bit IV = 64-bit key
3 - Wired Equivalent Privacy (WEP)

**Integrity Check**

ICV – *Integrity Check Value*

4 Bytes de CRC que vão anexados à mensagem e Cifrados

---

**Attack on the ICV:**

Due to CRC-32’s linear properties, it is easy to modify the frame and fix the encrypted CRC-32 accordingly.
3 - Wired Equivalent Privacy (WEP)

**Confidentiality**

IV – *Initialization Vector* (24 bits)

Tenta controlar o problema do XOR

O IV varia em todas as Mensagens

Existem $2^{24} = 16\,777\,216$ IVs possíveis

Vai constituir os primeiros 3 octetos da chave de cifra
Confidentiality Attack (Eavesdropping)

1º) To collect <IV, KeyStream> pairs


2º) To explore certain characteristics resulting from the concatenation of the IVs with the Secret Key, which originate “Keys” with predictable properties in RC4

3 - Wired Equivalent Privacy (WEP)

Confidentiality Attacks: Collection of IVs

Method 1:

Taking advantage of the Shared Key Authentication messages

Data Base

<IV 1; KeyStream 1>

...<IV n; KeyStream n>

Authentication (request)

Authentication (challenge)

Authentication (response)

Authentication (success)

AP

Attacker's Domain

802.11b at 11Mbps

Maximum frame length is 2346 bytes – 18768 bits

→ 586 frames per second

→ 586/4 authentication procedures per second

→ It takes 114500 seconds (circa 32 hours) to repeat the IVs ($2^{24}=16777216$)
3 - Wired Equivalent Privacy (WEP)

**Confidentiality Attacks: Collection of IVs**

Method 2:

To send know messages from the fixed network to the WLAN and retrieving the Ciphertext at the WLAN. By obtaining the Plaintext and the corresponding Ciphertext, it is possible:

1) To collect <IV, KeyStream> pairs.
2) To obtain the Key based on Cryptanalysis.

This method is potentially faster, but requires the attacker’s domain to encompass the fixed network (e.g., internal attacker).
3 - Wired Equivalent Privacy (WEP)

Problems of WEP key distribution:

- Key is manually set in the driver.
- The key cannot be protected from local users.
- When a user leaves the organization, technically you must change the key information on all stations.
  - What if a station is stolen?
- For a large organization, there is a need to publish the key which is a security problem.
3 - Wired Equivalent Privacy (WEP)

Problems of WEP key distribution (cont.):

- Weakness in the Key Scheduling Algorithm:
  "http://www.crypto.com/papers/others/rc4_ksaproc.pdf"
- A weakness of RC4 in generating the keystream.
- Hacker attack: using weak IV to attack a particular byte of the secret portion of the RC4 key.
- The time to attack is a linear algorithm to the key length.
- This is a complete break for WEP.
3 - Wired Equivalent Privacy (WEP)

- **WEPCrack**— breaks 802.11 keys

- **AirSnort**— breaks 802.11 keys
  - Needs only 5-10 million packets

- **NetStumbler**— access point reconnaissance
  - [http://www.netstumbler.com](http://www.netstumbler.com)
4 –IEEE 802.11i Robust Secure Network

4.1 – Temporal Key Interchange Protocol – TKIP
   (WPA - Wi-Fi Protected Access)
   – Employs RC4 as the Cipher basis
   – Supports the improvement of existing WEP products (the user is allowed to configure either WEP or TKIP)
   – Temporary security solution for Wi-Fi

4.2 - Counter Mode-CBC MAC Protocol – CCMP
   – Employs AES as the Cipher basis
   – Incompatible with WEP
   – Final security solution implemented in 802.11i WLANs

4.3 – Wi-Fi and the introduction of IEEE 802.11i
   – WPA (Wi-Fi Protected Access)
   – WPA2
4.1 Temporal Key Integrity Protocol (TKIP)

Problems to Solve

Problems detected in WEP
1 – Short IV and its Fast Reuse
2 – Direct attachment of the IV to the Secret Key – FMS Attack
3 – Does not use a trustable Integrity Check
4 – Use of a Unique Key; There are no Session Keys
5 – Does not avoid Message-Replay attacks

Solutions implemented in TKIP
1 – Extends the IV Dimension to avoid its reuse and the IV generation is based on a counter – TSC
2 – Generation of a New Session Key for each MPDU
3 – Uses a Trustable Integrity Check to avoid message-replay attack
4 – Uses a scheme to exchange and distribute Broadcast Keys
4.2 Counter Mode-CBC MAC Protocol (CCMP)

Implementation challenge:

WEP based systems architecture:
IV Generation and Sequence Number System of TKIP

- WEP is vulnerable to Message-Replay Attack
- The TKIP Solution includes:
  - Sequence Numbering of each MPDU
  - MPDUs with lower Sequence Numbers are discarded
  - The possibility of implementing a Sliding-Window mechanism
    - Sliding-Windows for 16 MPDUs – replay-window
    - The Sliding-Window records the last well received 16 MPDUs
    - According to the TCS of the received MPDUs, they are classified as:
      ACCEPT / REJECT / WINDOW
4.1 Temporal Key Integrity Protocol (TKIP)

TKIP MPDU Format:

1. TSC5 – More Weighty
2. TSC 0 – Less Weighty
3. When TSC1/TSC0 roll over, TSC2/3/4/5 are incremented as a whole
4. The “Extended IV” field is not encrypted
5. **WEPSeed** = (TSC1 | 0x20) & 0x7f  *(Avoids WEAK Keys)*
Message Integrity Check (MIC) Generation for each MSDU – Michael Mechanism

“Integrity Check” = “Just with CRC” ? ? ?
4.1 Temporal Key Integrity Protocol (TKIP)

New Key Generation for each MPDU
4.2 Counter Mode-CBC MAC Protocol (CCMP)

Counter Mode-CBC MAC Protocol – CCMP:
– Uses AES as the Cipher basis
– Adopted for use in 802.11i WLANs

Advanced Encryption Standard (AES) is a symmetric-key encryption standard adopted by the U.S. government in 2002.

The standard comprises three block ciphers, AES-128, AES-192 and AES-256, adopted from a larger collection originally published as Rijndael. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively.
4.3. Wi-Fi e IEEE 802.11i

Wi-Fi Alliance Strategy for the introduction of 802.11i

1) Interim standard WPA (Wi-Fi Protected Access)
   - TKIP or AES
   - 802.1X
   - For immediate implementation
   - Changes the SW at the APs and NICs

2) WPA2
   - Fully implements 802.11i
5. IEEE 802.1X

- Logical level solution for all IEEE 802 networks (both cabled and wireless).
- Based on the access control to logical entities (ports).
- The AP “opens” the network port if the Authentication Server (AS) validates the supplicants’s authentication data.
- In the beginning, the AP only opens the AS communication port.

EAP - Extensible Authentication Protocol
5. IEEE 802.1X

Suppliant — AP Authenticator — LAN/VLAN — Authentication Server (RADIUS)

(1) Remaining resources

(2) Remaining resources
5. IEEE 802.1X

Extensible Authentication Protocol (EAP)

- EAP is an IETF standard (RFC 2284) and adopted by IEEE as the basis for 802.1X. It is called the port based network access control. (also known as post-based authentication protocol)

- EAP supports both wired and wireless authentication.

<table>
<thead>
<tr>
<th>MD5</th>
<th>TLS</th>
<th>TTLS</th>
<th>LEAP</th>
<th>PEAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP</td>
<td>802.3</td>
<td>802.11</td>
<td>802.5</td>
<td></td>
</tr>
</tbody>
</table>

EAP

TLS: Transport Layer Security  TTLS: Tunnel TLS
LEAP: Lightweight EAP  PEAP: Protected EAP
5. IEEE 802.1X

EAP Authentication Methods:

- MD5 (Message Digest 5) - Username/Password. This is similar to MS_CHAP.
- TLS (Transport Layer Security) - PKI (certificates), strong authentication
- TTLS (Tunnel TLS) - Username/Password
- LEAP - Cisco proprietary lightweight EAP. It is to be phased out in favor of PEAP.
- PEAP - Protected EAP. Supported on Windows XP.
5. IEEE 802.1X

Supplicant → AP Authenticator

EAP over LAN

EAP over RADIUS

Authentication Server (RADIUS)

EAP Start

Ask client for identity

Provide identity

Pass request to RADIUS

Perform sequence defined by authentication method e.g. EAP-TLS, LEAP, etc

Pass session key to AP

Deliver broadcast key encrypted with session key

--- EAP Start ---

Identity request →

Identity response →

EAP Request →

EAP Response →

EAP success →

EAPoW key

--- EAP response ---

Access request →

Access challenge ←

Access response →

Access success ←

Note: Applicable to TKIP or any other system that uses session keys
5. IEEE 802.1X

New Product: Wireless Switch:

It is not cost effective to implement 802.1X on all Access points. It is also a management issue.
5. IEEE 802.1X

- **EAP Request**
- **EAP Response**
- **EAP success**
- **MAC Dissociate**
- **MAC Associate**
- **Dados**

(1) The client is authenticated at the AP
(2) The attacker captures the client’s MAC address and sends it Dissociate command, using the AP’s MAC address as sender address (it simulates the AP)
  - The client jumps to the Unassociate state, but is still authenticated.
(3) The attacker sends an Associate frame with the client’s MAC address and is now authenticated (it simulates the client).

Nota: It is assumed that the attacker knows the Cipher Key
5. IEEE 802.1X

• EAP was initially conceived in association with PPP and adapted to 802.1X
• The AP only allows the EAP traffic into the DS

• EAP was not conceived for wireless networks
  - The communication between clients and the AP during the EAP procedures should be encrypted
  - There may not be mutual authentication
6. Complementary Security Solutions

6.1 – Layer3: Virtual Private Network (VPN)
6.2 – Layer4: IP Address Control and Firewall
6.3 – Layer 7: Proxy
6.1 - Layer3: VPN

What is a VPN

Secure (encrypted) communication channel between two points (called tunnel)

What is Tunneling

Putting a packet inside another packet

Advantages of VPN

– Provides secure channel: authentication, privacy and integrity
– Easy to setup because it uses the same infrastructure
– Easy to deploy
6.1 - Layer3: VPN

VPN: Creation of a Tunnel between the wireless users and the organization’s VPN.

Layer 2/3 tunnel over a layer 3 protocol

<table>
<thead>
<tr>
<th>Data (encrypted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Tunnel</td>
</tr>
</tbody>
</table>

| IP | IP |
|------------------|
| Wireless LAN     | LAN |
6.1 - Layer3: VPN

- Local VPN (company, campus)
- Public location VPN
6.1 - Layer3: VPN

Disadvantages of VPN

• Overhead: encryption, encapsulation
• Single failure (Gateway) in the path disconnects the entire network
• Hard to troubleshoot because headers are encrypted
• IDS (Intrusion Detection System) is less effective because traffic is encrypted
• Integration difficulties with NAT (Ipsec Authentication Header only)
• Not scalable (Gateway must encrypt/decrypt all packets from all users…)
6.1 - Layer 3: VPN

Types of VPNs

– Layer 2:
  • PPTP (Point-to-Point Tunneling Protocol)
  • L2TP (Layer 2 Tunneling Protocol)

– Layer 3:
  • IPSec
1. Standard WLAN and DHCP procedure for a temporary IP to the wireless station.
2. The temporary IP address is used for authentication only. All other traffic is blocked by the router.
3. After user authentication, the station is given an official IP address which can go through the router.
4. May also register the MAC address to reduce the risk of hacker attack.
6.3 – Layer7: Proxy Gateway

1. Standard WLAN and DHCP procedure for an IP address to the wireless station.
2. User types any URL and the request is routed to the security server web page.
   - All other traffic is blocked.
3. After entering account info or credit card, the user is authenticated.
4. The gateway authorizes the traffic from the authenticated station.