

Wireless Security

Developed by: Alberto Escudero Pascual, IT +46

Goals

- To be able to situate wireless security within the broad context of information security.
- To understand where “security” can be built into each layer of the OSI/Internet protocol stack
- To be able to identify the key security elements that need to be considered when performing wireless design planning.

Table of Contents

- Part I
 - Wireless Security/Information Systems Security
 - OSI model and link level encryption
- Part II
 - Five security attributes in the context of WLAN
- Part III
 - Ten threats for security in WLAN

Defining Wireless Security

- Security is a wide and general concept
- What "Security" are we talking about?
- We need to start by defining the right "Security Context" to study WLAN Security
- We will present Wireless Security in the context of Information Security.

What is Information Security? (COMSEC)

- Late 70's, referred to as "Communication Security"
- COMSEC was defined by "U.S. National Security Telecommunications and Information Systems Security Instruction" (NSTISSI) as:

"Measurement and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications."

What is Information Security? (COMSEC)

- COMSEC security included two security attributes related to this unit:
 - **Confidentiality**
 - **Authentication**

Confidentiality

“Assurance that information is not disclosed to unauthorized persons, processes, or devices.”

Protection from unauthorized disclosure

Authentication

“Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information”

Verification of originator

What is Information Security? (COMPUSEC)

- Growth of PC's in the 80's lead to a new security era
- COMPUSEC was defined by the NSTISSI as:

“Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated”

What is Information Security? (COMPUSEC)

- COMPUSEC introduced two more security attributes related to this unit:
 - **Integrity**
 - **Availability**

Integrity

“Quality of an Information System (IS) reflecting the local correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.”

The data can not be modified without notice

Availability

“Timely, reliable access to data and information services for authorized users.”

The access is “reliable”

What is Information Security? (INFOSEC)

- In the 90's, COMSEC and COMPUSEC merged to form Information Systems Security (INFOSEC)
- INFOSEC included the four attributes:
Confidentiality, Authentication, Integrity and Availability from COMSEC and COMPUSEC

What is Information Security? (INFOSEC)

- INFOSEC included also a new attribute:
 - **Non-Repudiation**

Non-Repudiation (Accountability)

“Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data.”

INFOSEC in WLAN

INFOSEC is defined by the U.S. NSTISSI as:

*”The **protection** of information systems against **unauthorized access** to or **modification** of information, whether in storage, processing or transit, and against the **denial of service** to authorized users or the provision of service to unauthorized users, including those measures necessary to **detect**, document, and counter such threats.”*

The Methodology

What: Wireless Security will be presented from the point of view of INFOSEC

Why: To give a methodological approach for designing security of a wireless network

How: All five security attributes of INFOSEC are presented and we discuss how WLAN (can) implements each of them

Two reminders

- Before moving into the five security attributes, two reminders from the Advanced Internetworking Unit
 - OSI model and WLAN standards
 - Link level encryption

The OSI Model and Wireless Security (reminder)

- Wireless standards refers to layer 1 and 2 of the OSI protocol stack
- Security in WLAN tends to be identified as setting properly "Wireless Link Level Encryption"
- Security mechanisms in layer 3 and above do not belong to "wireless security" and should be considered as part of a "Network or Application Security Unit"

Link Level Encryption

- **Definition:** The process to secure data at link level when data is transmitted between two nodes attached to the same physical link.
- **Requirements:** A (secret/key) shared between the communication parties and an agreed encryption algorithm.

Link Level Encryption

- When sender and receiver are not present in the same media, the data needs to be decrypted and re-encrypted in each of the nodes along the way to the receiver. LL Encryption only works HOP-BY-HOP.
- The link level encryption is normally used when higher level protocol encryption is not present or in high assurance applications.

Link Level Encryption in IEEE 802.11

- WEP has been the most known link level encryption algorithm for IEEE 802.11 (1999-2004)
- WEP has been proven to be insecure.
- Other alternatives have been develop in the last five years and standardised as the Wi-Fi Protected Access (WPA2).
- The new standard IEEE 802.11i will include an enhancement of WPA, named WPA-2.

Link Level Encryption in IEEE 802.11

- Link encryption **does not provide end-to-end security** outside of the physical link
- Link Encryption should always be consider as just an *extra security* measure
- Link encryption requires more hardware resources in the access points and the security design of key distribution and management.

Five security attributes in WLAN

- Confidentiality
- Authentication
- Integrity
- Availability
- Non-repudation (Accountability)

1. Wireless (LAN) Confidentiality

- Defined as the assurance that information transmitted between access points and clients is not disclosed to unauthorized persons.
- Needs to ensure that either
 - 1) the communication between a set of access points in a wireless distribution system (WDS) is protected OR
 - 2) the communication between an access point (AP) and a station/client (STA) remains protected

WEP

- Part of the original IEEE 802.11b standard of 1999
- Aimed to provide a “*comparable level of confidentiality*” to a wired network
- WEP was broken and obsolete shortly after its release
- WEP was proven weak independently of the length of the key size
- The lack of any key management in the protocol itself did WEP even weaker (keys are distributed manually).
- Quickly, new alternatives popped up as WEP+ from Lucent and WEP2 from Cisco

WEP

- WEP and their enhancements (WEP+, WEP2) are currently obsolete
- WEP is based on the “RC4 stream cypher”
- Multiple available software to break WEP (Airsnort, wepcrack, kismac, aircrack etc).
- Interested in the history of WEP security?
 - check the “Additional Resources”

WPA and WPA2 are born

- Wi-Fi Protected Access (WPA) was proposed in 2003 while IEEE 802.11i was discussed.
- WPA focused on enable old-hardware to be easily updated. In 2004, WPA was enhanced to include AES and certified as part of the IEEE 802.11i standard with the name WPA2 (2004).
- WPA2 is designed to work with and without a key management server.

WPA and WPA2 are born

- If no key management server is used, all stations share a “pre-shared key” (PSK)
- PSK mode is known as WAP-Personal or WAP2 Personal

When a key management server is used, WPA2 is known as WPA(2)-Enterprise

- One major improvement in WPA2: the possibility of exchanging keys dynamically

2. Wireless (LAN) Authentication

- The measure designed to establish the validity of a transmission between Access Points and/or Wireless Stations (STA)

**The right to send *bridge/route* data
via the Access Point**

Association Mechanisms

- Open Authentication
 - NO security, everyone can start talking to the access point
- Shared Key Authentication
 - A secret is shared between access point and the client
 - A challenge response allows the access point to verify the shared secret and grant access

WEP and Authentication in Layer-2

- Shared Key Authentication in WEP is obsolete
- Plain-cypher text attacks can be easily performed
- “Encryption” key and “Authentication” key are the same shared secret
- Once one is compromised so is the other

WEP and Authentication in Layer-2

Recommendations:

- Use WAP2-Enterprise mode
- Authentication in major wireless networks (WISP) is normally implemented in higher network layers (IP layer) by means of captive portals
- By using a "captive portal" we have NO simple means to stop the flow of traffic that bridges (crosses) our access points.

Stop Broadcasting SSID

- A variation of "Open authentication" is called "Closed Network".
- "Closed networks" do NOT broadcast periodically SSID beacon frames (IEEE 802.11 link level management frames)
- Turning off the broadcast of SSID implies that the wireless clients need to know the SSID in advance

Stop Broadcasting SSID

A “security” protection?

- Will not prevent other software to find the SSID by “eavesdrop” the association frames of another station
- Finding the SSID of a “Close Network” is as simple as waiting for “someone” to get associated to the wireless network and extract the SSID string from an association frame
- Should be consider as an “extra precaution” but NOT as a real security protection.

MAC address filtering as security measure

Many WISPs use MAC address filtering to limit/provide access to a wireless networks assuming that MAC addresses are “hard-coded” and can not be easily modified

- MAC addresses in most (wireless) networks interfaces can easily be modified!
- An authentication mechanism based ONLY on MAC addresses is insecure.

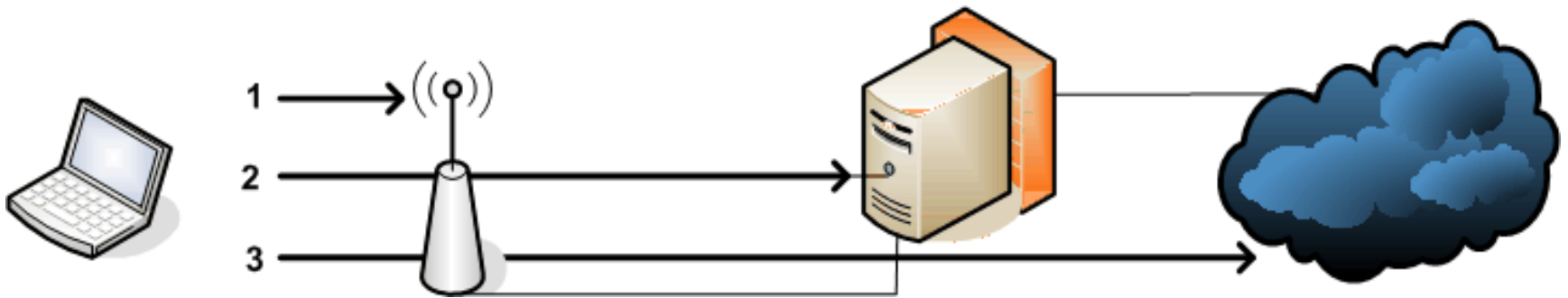
Wireless Captive Portals

- Moving Authentication out of the Wireless: Captive Portal
- There exists many implementations of Wireless Captive Portals
- The majority are based on the same type of concept: HTTP redirection and Dynamic Firewalling

Wireless Captive Portals

- 1) Clients are allowed to associate with an AP and obtain an IP by means of DHCP
- 2) Once the client has an IP, all HTTP requests are captured and the client is forced to a “log-in” web page.
- 3) The captive portal verifies the validity of the user/password and changes the status of a firewall (normally in the same machine)
- 4) Firewalls rules are normally based on the values of the client's MAC and DHCP IP address.

Wireless Captive Portal authentication in three steps



3. Wireless (LAN) Data Integrity

- The capability of a wireless protocol to determine if the payload has been altered by unauthorized users
- WEP was intended to provide payload integrity
- The integrity mechanism (CRC) used in WEP is also insecure. No surprises!
- The payload can be altered and the CRC message updated without knowing the WEP key

Wireless (LAN) Data Integrity

Result: Traffic can be modified without being noticed

WPA and WPA2: included a more secure message authentication code (MAC – cryptographic checksum) and the inclusion of a frame counter, which prevents “replay attacks”

Wireless (LAN) Data Integrity

WEP vs WPA2

- Data Integrity by means of WEP is obsolete
- WPA or WPA2 should be implemented to achieve Wireless Data Integrity by means of encryption in the link level

4. Wireless (LAN) Availability

“The capability of the technology to ensure reliable access to data and information services for authorized users.”

Interference in wireless radio channel

- WLAN operates in predefined radio channels open for anyone to use
- Preventing unauthorized users to interfere with your network is almost impossible
- **Advice:** Monitor carefully your links to identify possible sources of “interference”

Denial of Service (DoS)

- WLAN networks are vulnerable to DoS by radio interference, anyone can start using:
 - the same or adjacent radio channel
 - the same SSSID
- DoS can be intentional and/or unintentional
- Consider scheduling periodical radio frequency scans
- Do not overpower your links

Other threats to availability

- Presence of hidden nodes (heavy retransmission)
- Viruses (heavy scanning)
- Peer-to-peer software (heavy data transfer)
- Spam (heavy incoming/outgoing mail)

5. Wireless (LAN)

Non-repudiation (Accountability)

- The WLAN protocols do not have a mechanism to assure the sender of data is provided with **proof** of delivery and the recipient is provided with proof of the sender's identity.
- Accountability needs to be implemented in higher protocol layers.

Ten WLAN Security Threats

1	Confidentiality	Eavesdropping	<ul style="list-style-type: none">- WPA2- “Encryption” in higher level protocols
2	Confidentiality	Traffic hijacking, man-in-the-middle attack	<ul style="list-style-type: none">- Use (1)- Monitoring SNR, SSID and AP MAC addresses
3	Authentication	Unauthorised access to your wireless network	<ul style="list-style-type: none">- WPA2- Do not rely in MAC-only authentication- Do not broadcast your SSID

10 WLAN Security Threats

4	Authentication	Unauthorised access to your network and Internet	<ul style="list-style-type: none">- IEEE 802.1X- Captive Portal
5	Integrity	Traffic modification on wireless transit	<ul style="list-style-type: none">- “Encryption” in higher level protocols- WPA2
6	Availability	Wireless interference, Radio DoS	<ul style="list-style-type: none">- Monitor radio spectrum- Do not over power links
7	Availability	Unavailable bandwidth due to radio retransmissions	<ul style="list-style-type: none">- Check for hidden nodes and sources of interference- Check for link level retransmissions

10 WLAN Security Threats

8	Availability	Unavailable bandwidth due to malicious software	<ul style="list-style-type: none">- Monitor IP traffic, (ICMP and UDP)- Implement Intrusion Detection
9	Authentication Accountability	Unauthorised access to your Intranet	<ul style="list-style-type: none">- Wireless Network outside of firewall- Implement VPN- Allow connections only via the VPN
10	(Network Access) Accountability	Unauthorised use of wireless and network resources	<ul style="list-style-type: none">- IEEE 802.1X- Captive Portal based on Digital Signatures

Conclusions

1. Security attributes as described in INFOSEC can be implemented in different layers of the OSI model
2. If link level security is needed avoid WEP and use IEEE 802.11i (WPA2)
3. Have clear security requirements, as solutions depend on each scenario