

ITRAINONLINE

WIRELESS SECURITY HANDOUT

Developed by: Alberto Escudero Pascual, IT +46

Table of Contents

| | |
|--|----|
| 1. About this document..... | 1 |
| 1.1 Copyright information..... | 2 |
| 1.2 Prerequisites..... | 2 |
| 1.3 Degree of Difficulty..... | 2 |
| 2. Introduction..... | 2 |
| 3. Defining wireless security..... | 2 |
| 4. What is information security?..... | 2 |
| 4.1 Confidentiality..... | 3 |
| 4.2 Authentication..... | 3 |
| 4.3 Integrity..... | 3 |
| 4.4 Availability..... | 3 |
| 4.5 Non-repudiation (accountability)..... | 3 |
| 5. Information security and WLAN..... | 4 |
| 6. Implementing security attributes..... | 4 |
| 6.1 General comments about link level encryption..... | 5 |
| 7. Wireless (LAN) confidentiality..... | 5 |
| 7.1 To WEP or not to WEP..... | 5 |
| 7.2 WEP dies, WPA and WPA2 are born..... | 6 |
| 8. Wireless (LAN) Authentication..... | 7 |
| 8.1 To stop the broadcast of SSID as a security measure..... | 7 |
| 8.2 To use MAC address filtering as a security measure..... | 8 |
| 8.3 Wireless captive portals..... | 8 |
| 9. Wireless (LAN) data integrity..... | 9 |
| 9.1 Security notice about WPA..... | 9 |
| 10. Wireless (LAN) availability..... | 10 |
| 11. Wireless (LAN) non-repudiation (accountability)..... | 10 |
| 12. Wireless (LAN) security threats..... | 10 |
| 13. Conclusions..... | 11 |

1. About this document

These materials are part of the ItrainOnline Multimedia Training Kit (MMTK). The MMTK provides an integrated set of multimedia training materials and resources to support community media, community multimedia centres, telecentres, and other initiatives using information and communications technologies (ICTs) to empower communities and support development work.

1.1 Copyright information

This unit is made available under the Creative Commons Attribution-ShareAlike 2.5 License. To find out how you may use these materials please read the copyright statement included with this unit or see <http://creativecommons.org/licenses/by-sa/2.5/>.

1.2 Prerequisites

It is recommended to read the unit “Advanced Networking” before this unit.

1.3 Degree of Difficulty

The degree of difficulty of this unit is Advanced.

2. Introduction

This handout starts by giving a brief introduction to the OSI reference model and key security concepts before introducing wireless security in the context of IEEE 802.11 or WLAN.

Security in the context of Information Security is targeted and, five general security attributes (Confidentiality, Authentication, Integrity, Non-Repudiation and Availability) are described and later evaluated in the context of IEEE 802.11 (WLAN). The unit finishes by presenting some important security threats that need to be considered in any wireless design.

The unit focuses on giving an image of wireless security within the broad context of information security. It aims to give an understanding of where “security” can be built into each layer of the OSI/Internet protocol stack. Furthermore, it considers the key security elements that need to be addressed when performing wireless design planning.

3. Defining wireless security

The definition of security is in large measure context specific; the word security embraces a wide range of fields inside and outside the computing arena. We can talk about security when describing road safety measures or describing a new computing platform that is secure against virus software. Several disciplines have been developed to address each specific security aspect.

With that in mind, we have tried to frame the term “wireless security” in a recognized security category that will help us to review security in WLAN. This unit describes wireless security in the context of Information Security. When we talk about wireless security we are talking about “Information Security in WLAN¹ wireless networks”.

4. What is information security?

To understand the meaning of Information Security it is necessary to understand how the term has evolved over time.

¹ Here referred to as the working group of IEEE 802.11

Until the late 70's, this area of security was referred as Communication Security. Communication Security or COMSEC was defined by the 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."

Four areas were included as parts of the COMSEC security activities: Cryptosecurity, Transmission Security, Emission Security and Physical Security. COMSEC security included two security attributes related to this unit: Confidentiality and Authentication.

4.1 Confidentiality

Assurance that information is not disclosed to unauthorized persons, processes, or devices (Protection from unauthorized disclosure).

4.2 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).

In the 80's with the growth of (personal) computers another security era started: Computer Security (COMPUSEC). COMPUSEC was defined by 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"

COMPUSEC introduced two more security attributes related to this unit: Integrity and Availability.

4.3 Integrity

The quality of an Information System (IS) reflects 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.

4.4 Availability

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

Finally in the 90's, the two security eras COMSEC and COMPUSEC were merged together to form Information Systems Security (INFOSEC). INFOSEC included the four attributes: Confidentiality, Authentication, Integrity and Availability from COMSEC and COMPUSEC but also a new attribute was added: non-repudiation.

4.5 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.

5. Information security and WLAN

The NSTISSI defines Information Systems Security (INFOSEC) 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.



Wireless security is presented from the point of view of “Information Systems Security” or INFOSEC.

It is very common in literature related to WLAN security to describe security features without providing a proper security framework. By listing security “features” the reader tends to remember acronyms but forgets what each “feature” exactly is intended for. To avoid that, we will not “list” all the security attributes presented in WLAN but rather present each of the five security attributes of INFOSEC and **then** discuss how WLAN implements each and one of them.

This approach will help the reader to have a methodological approach when designing secure wireless networks.

The five security attributes that will be discussed are: Confidentiality, Authentication, Integrity, Non-Repudiation and Availability.¹

6. Implementing security attributes

The OSI (*Open Systems Interconnection*) Reference Model, created by ISO (International Standards Organization), is an abstract description for computer network (communication) protocol design. The model splits different communication functions in seven different layers that can work independent of each other.

As described in detail in the unit “Advanced Networking”, the OSI protocol design follows the principles of a “*stack*”. Having a *layered* or *stack* protocol model implies that each layer only uses the functionality of the layer below and only provides functionality to layers above.

This layered approach has direct implications on how we can implement security attributes.



Wireless standards normally refer to layer 1 and layer 2 of the OSI protocol *stack*, keeping the IP packet unaltered. The “IP packets” are transported over **wireless specific** physical and data link protocols.

For example, if we consider “confidentiality of the data traffic” between two access points, we can achieve similar results (secrecy of the payload) by three different means:

- The application layer (by means of TLS/SSL)
- IP layer (by means of IPSEC) and,
- Link layer (by means of wireless encryption)

Remember that when we talk about wireless security, we are only examining the security mechanisms that are present in layer 1 and layer 2, i.e. wireless (link level) encryption. Other security mechanisms present in layer 3 and above are part of network or application security.

¹ For a more formal approach to Security read: The Common Criteria for Information Technology Security Evaluation, typically abbreviated as just “Common Criteria” or “CC.” The CC provides both Functional and Assurance requirements for security products and systems.

6.1 General comments about link level encryption

Link level encryption is the process to *secure data* at the link level when data is transmitted between two nodes attached to the same physical link (they can also be in two different physical links by means of a repeater e.g. satellite). With link level encryption, any other protocol or application data running over the physical link are protected from eavesdroppers.

Encryption requires a certain key or secret shared between the communication parties and an agreed encryption algorithm. When the sender and the 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.

The link level encryption is normally used when higher level protocol encryption is not present.



Link level encryption in IEEE 802.11

The best known link level encryption algorithm for IEEE 802.11 is the so called Wired Equivalent Privacy (WEP). WEP has been proven to be insecure and other alternatives, such as Wi-Fi Protected Access (WPA), have been proposed and standardised. The new standard IEEE 802.11i will include an enhancement of WPA, named WPA2.

Link encryption **does not provide end-to-end security** outside of the physical link and should always be considered as just an *extra security* measure in your network design.

Link encryption requires more hardware resources in access points and security design of key distribution and management.

7. Wireless (LAN) confidentiality

7.1 To WEP or not to WEP

We define wireless confidentiality as the assurance that information transmitted between access points and clients is not disclosed to unauthorized persons. Wireless confidentiality needs to ensure that either the communication between a set of access points in a wireless distribution system (WDS) or between an access point (AP) and a station/client (STA) remains protected.

Wireless confidentiality has been traditionally associated with the term “Wired Equivalent Privacy” or WEP. WEP was part of the original IEEE 802.11 standard of 1999.

WEP's goal was to provide wireless networks a “comparable level of confidentiality” to traditional wired networks. The need for a protocol like WEP was obvious: wireless networks use radio waves and hence are open to eavesdropping.

The lifetime of WEP was very short; a bad and not very transparent design led to several successful attacks to the implementation. A few months after WEP was released, the protocol was broken and obsolete. Although the key-length was initially limited in size due to export restrictions, the protocol was proven weak independent of the length of the key size.

It was not only the security design flaws that made WEP obsolete, it was also the lack of a key management system in the protocol itself. WEP did not include any key management at all. The way that WEP keys were distributed was as simple as setting/typing manually a key in each wireless device (a secret shared by many is not a secret!).

WEP was followed by some proprietary enhancements that were also inadequate e.g. WEP+ from Lucent and WEP2 from Cisco.



WEP and its enhancements (WEP+, WEP2) are currently obsolete. WEP is based on the “RC4 stream cypher” which implementations in IEEE 802.11 has been proven insecure.

There are multiple available attacks and implemented software to break WEP (Airsnot, wepcrack, kismac, aircrack etc). Some of the attacks are based on the numerical limitation of the Initialization Vectors of a RC4 stream cypher or the presence of the so called “weak IV” in a datagram.

Those interested in the history of WEP security should check the Additional Resources component of this unit.

7.2 WEP dies, WPA and WPA2 are born

After the death of WEP, Wi-Fi Protected Access (WPA) was proposed in 2003 and later certified as part of the IEEE 802.11i standard with the name of WPA2 (2004).

WPA and WPA2 is designed to work with or without a key management server. If the key management server is not used, all the stations share a “pre-shared key” (PSK). This PSK mode is known as WPA or WPA2-Personal.

When a key management server is used, WPA2 is known as WPA2-Enterprise. In WPA-Enterprise, a IEEE 802.1X server is used for the distribution of the keys.

One major improvement in WPA2 over the old WEP is the possibility of exchanging keys dynamically by means of Temporal Key Integrity Protocol (TKIP).



WPA2 Wi-Fi Protected Access

WPA2 is the certified version of WPA and a part of the Standard IEEE 802.11i. Two main changes are included in WPA2 vs WPA:

1. The replacement of the Michael algorithm by a message authentication code known as the Counter-Mode/CBC-Mac Protocol (CCMP) that is considered cryptographically secure.
2. The replacement of the stream cypher RC4 by the Advanced Encryption Standard (AES) also known as Rijndael.

Data confidentiality recommendations

If wireless confidentiality is needed by means of encryption in the link level: WPA2-Enterprise mode is the best of the options.

In case of using a simpler solution as WPA-2-Personal, special care needs to be taken when choosing passwords (pre-shared key).

WEP and all variants as WEP+, WEP2 should be discarded.

8. Wireless (LAN) Authentication

In the context of wireless LAN, authentication is the measure designed to establish the validity of a transmission between access points and/or wireless stations (STA). In simple words, Wireless authentication means “the right to send data to and via the access point”

In order to understand “Authentication” in wireless networks is necessary to understand what happens in the beginning of the communication session between an access point and/or a wireless station. The beginning of the communication starts by a process called “association”.

Two main “association” mechanisms were introduced when IEEE 802.11b was designed:

- Open Authentication and
- Shared Key Authentication

Open Authentication implies NO security and everyone can start talking to the access point. In Shared Key Authentication, a secret (password) is shared between the access point and the client station/access point. A challenge response mechanism allows the access point to verify that the client knows the shared secret and grant it access.



WEP and Authentication in Layer-2

The Shared Key Authentication implemented in WEP is also obsolete. Several plain-cypher text attacks can easily be performed against WEP-based authentication. Due to the fact that the “encryption” key and “authentication” key are the same shared secret, once one is compromised so is also the other.

Wireless Authentication recommendations

Wireless Authentication by means of Layer 2 requires the use of WPA2-Enterprise mode.

Authentication in wireless networks, as the ones implemented by Wireless Internet Service Providers, is normally implemented in higher network layers (IP layer) by means of captive portals (log into a website).

It is important to understand that by moving the authentication to a “captive portal” we have NO simple means to stop the flow of traffic that bridges (crosses) our access points.

8.1 To stop the broadcast of SSID as a security measure

Lucent Technologies developed in 2000, a variation of the Open authentication scheme called “Closed Network”. Closed networks differ from standard IEEE 802.11b networks in that the Access Points do NOT periodically broadcast SSID beacon frames.

Turning off the broadcast of SSID implies that the wireless clients need to know in advance which SSID to use to “associate” with an (or distribution of) access point. This new feature has been implemented by many vendors as a “security” enhancement. The truth is, while turning off SSID broadcasting will prevent normal wireless clients from learning the SSID from a beacon, it will not prevent other software to find the SSID name 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 the association frame.



Turning Off the SSID broadcast

Turning off the broadcast of SSID will NOT stop an “interested” person to find the SSID of your network. Configuring your wireless network as “Close” will just add an extra hurdle to an average intruder. Turning off the SSID broadcast setting should be considered as an “extra precaution” but NOT as a security protection.

8.2 To use MAC address filtering as a security measure

It has become common in many wireless ISPs (WISP) to use the MAC address of the wireless interface as a mechanism to limit/provide access to a wireless network. The assumption behind it is that MAC addresses are “hard-coded” and can not be modified by normal users. The reality is very different and MAC addresses in most (wireless) network interfaces can easily be modified.



Using MAC addresses for authentication

An authentication mechanism based ONLY on MAC addresses is insecure.

8.3 Wireless captive portals

The discussion of “wireless captive portals” deserves a whole unit by itself but they deserve a brief introduction in this unit due to their relevance in wireless security.

Although there are many different implementations of wireless captive portals, the majority of them are based on the same type of concept. In a network where authentication is implemented by using “captive portals”, the clients are allowed to associate with an access point (no wireless authentication) and obtain an IP by DHCP (no authentication to obtain IP address). Once the client has obtained an IP address, all HTTP requests are captured and the client is forced to a “log-in” web page.

The captive portals are responsible of verifying the validity of the user password and modifying the status of a firewall. Firewall rules are normally based on the values of the client's MAC and DHCP IP address.

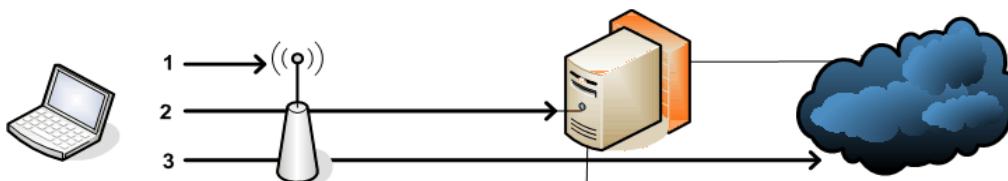


Image 1: A captive portal with authentication in three steps.

In the picture, we can see the “captive portal” authentication in three steps. The first step (1) requires the client to associate to the wireless network. no wireless authentication in terms of WEP/WPA is required and SSID is normally announced. In the second step (2), the client will obtain an IP address by means of DHCP. IP traffic is bridged in the access point without any authentication. In the final step (3), the client's HTTP connections are redirected to the captive portal server. The client logs-in to the server (normally by using HTTPS + user + password). Finally the captive server modifies/creates a firewall rule that allows the client to reach the internet.

There are several security problems regarding this type of implementation. For more information check the proposed exercises.

9. Wireless (LAN) data integrity

We define wireless data integrity as the capability of a wireless protocol to determine if the payload has been altered by unauthorised users.

In 1999, WEP was also intended to provide payload integrity but unfortunately the integrity mechanism or cyclic redundancy check (CRC) used in WEP was also insecure. The flawed design of WEP allows alteration of the payload and updating the message CRC without knowing the WEP key. Traffic could be modified without being noticed.

WPA and WPA2 solved the problem of data integrity of WEP by including a more secure message authentication code and the inclusion of a frame counter, which prevents the so called “replay attacks”. In a “reply attack” the

attacker records the conversation between a wireless client and an access point to gain unauthorised access. By replaying an “old” conversation the attacker does not need to know the WEP shared secret or key.



Data Integrity: WEP vs WPA2

Data integrity by means of WEP is obsolete.

Data integrity recommendations

WPA or WPA2 should be implemented to achieve wireless data integrity by means of encryption in the link level.

9.1 Security notice about WPA

WPA was designed as an “intermediate” step towards WPA2 (standard IEEE 802.11i). WPA includes only a subset of features of IEEE 802.11i and focuses on being backward compatible with WEP IEEE 802.11b adapters.

WPA targeted the flaws found in WEP. WPA increased the size of the keys, the number of keys in use and added a new secure message authentication code. The Michael algorithm was chosen as it was the strongest that would still work with most of the older network cards. The Michael algorithm is still a subject to attack and that is why WPA-based networks implement a shut down mechanism for 30 seconds whenever an attack is detected.

| | | <i>WPA</i> | <i>WPA2</i> |
|-----------------|----------------|------------------------------|-----------------|
| Enterprise Mode | Authentication | IEEE 802.1X/EAP ¹ | IEEE 802.1X/EAP |
| | Encryption | TKIP ² /MIC | AES-CCMP |
| Personal Mode | Authentication | PSK | PSK |
| | Encryption | TKIP/MIC | AES-CCMP |

Table 1: Authentication and encryption in WPA and WPA2 (Enterprise and Personal mode).

¹ EAP stands for Extensible Authentication Protocol, it is a security protocol invoked by an IEEE 802.1X enabled Network Access Server (NAS) device such as an IEEE 802.11 a/b/g Wireless Access Point.

² TKIP stand for the Temporal Key Integrity Protocol.

10. Wireless (LAN) availability

We define wireless (LAN) availability as the capability of the technology to ensure reliable access to data and information services for authorized users.

The first thing that you should consider is that it is not simple to stop someone to interfere with your wireless radio signal. WLAN operates in a set of predefined radio channels that anyone can use to send radio signals. Preventing unauthorized users to interfere with your network is almost impossible. The only thing that you can do is to monitor carefully your links to identify possible sources of "interference". (See Monitoring and Management MMTK unit).



Denial of Service

WLAN networks are vulnerable to Denial of Service (DoS) by radio interference. Consider the scenario where some other network operator decides to configure their radio devices in the same radio channel that your network. Furthermore imagine that the same SSID is also advertised.

To avoid this kind of intentional or unintentional attacks, consider scheduling periodical radio frequency scans.

To avoid interfering with other networks, do not overpower your links.

There are multiple reasons why a wireless link can perform bad or become unavailable. The presence of hidden nodes can seriously affect the performance of the IEEE 802.11 protocol family. Viruses, peer-to-peer software, spam etc. can also flood your network and limit the amount of bandwidth available for authorized connections to legitimate services.

As discussed in the "Authentication" section of this unit, it is difficult to prevent illegitimate users from communicating with your access point or your captive portal. Wireless (LAN) availability requires the establishment of good network monitoring practices.

11. Wireless (LAN) non-repudiation (accountability)

The family of standards IEEE 802.11 does not deal with traffic data "accountability". The wireless protocols "per se" 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.

12. Wireless (LAN) security threats

The following table presents the ten most relevant security threats in wireless networks and provides a set of recommendations for each and one of them.

| | | | |
|----|------------------------------------|---|--|
| 1 | Confidentiality | Risk of eavesdropping, unauthorised users can gain access to data traffic in your wireless backbone | Use link level encryption in your wireless links (WPA2). Recommend to your users the use of "encryption" in higher level protocols (HTTPS, Secure SMTP) |
| 2 | Confidentiality | Risk of traffic hijacking, unauthorised users can implement a man-in-the-middle attacks | Recommendation 1 + Monitor the SNR, SSID and AP MAC address of your connection. |
| 3 | Authentication | Risk of unauthorised access to your wireless network | Implement IEEE 802.1X (WPA2) Do not rely in MAC-only authentication scheme Do not broadcast your SSID |
| 4 | Authentication | Risk of unauthorised access to your network and Internet | Implement IEEE 802.1X Implement a Captive Portal |
| 5 | Integrity | Risk of traffic modification on wireless transit | Recommend to your users the use of "encryption" in higher level protocols (HTTPS, Secure SMTP) Use link level encryption in your wireless links (WPA2). |
| 6 | Availability | Risk of wireless interference Radio Denial of Service (Jamming) | Monitor radio spectrum periodically Do not over power your links |
| 7 | Availability | Risk of unavailable bandwidth due to radio retransmissions | Check for hidden nodes and sources of interference Monitor radio AP for link level retransmissions |
| 8 | Availability | Risk of unavailable bandwidth due to malicious software | Monitor IP traffic, specially ICMP and UDP traffic Include Intrusion Detection Systems if needed |
| 9 | Authentication Accountability | Risk of unauthorised access to your Intranet | Implement Wireless Network outside of your firewall Implement a Virtual Private Network and allow only connections via the VPN concentrator |
| 10 | (Network Access) Accountability | Risk of unauthorised use of wireless and network resources | Implemented IEEE 802.1X Implement Captive Portal based on Digital Signatures |

Table 2: The ten most relevant security threats in wireless networks with recommendations of preventive measures.

13. Conclusions

This unit presents wireless security from the point of view of "Information Systems Security" or INFOSEC.

Five security attributes - Confidentiality, Authentication, Integrity, Non-Repudiation and Availability - have been presented in the context of wireless LAN.

Since wireless standards such as IEEE 802.11 only refer to layer 1 and 2 of the OSI protocol stack, some security attributes by means of higher level protocols can also be implemented.

A good wireless network designer should consider where to implement each security attribute. For example, encryption for confidentiality can be implemented in the link layer or in the IP/application layer, SSID can be broadcast or not, authentication can be implemented using IEEE 802.1X, a Captive Portal or simple and static MAC filtering etc.

Any security implementation will always be “scenario and application” dependent.

The five main issues you should remember from this unit can be summarized as:

1. Pure “wireless” security only includes security mechanisms that are present in layer 1 and layer 2
2. Link level encryption (WEP, WPA, WPA2) is a common security measurement but does not ensure end-to-end confidentiality. If link level security is needed avoid WEP and use IEEE 802.11i (WPA2)
3. Turning off SSID broadcasting and using MAC filtering are not secure authentication methods. A higher level authentication method, such as captive portal, is needed.
4. A network can become inoperative as a result of evil DoS attacks or malicious software but also due to unconscious hidden nodes and interference problems. Only by monitoring the traffic on your network, you can find out the real cause of your problem.
5. There is no “standard security solution” that fits all wireless networks. It is needed to have clear security requirements, as solutions depend on each scenario.