



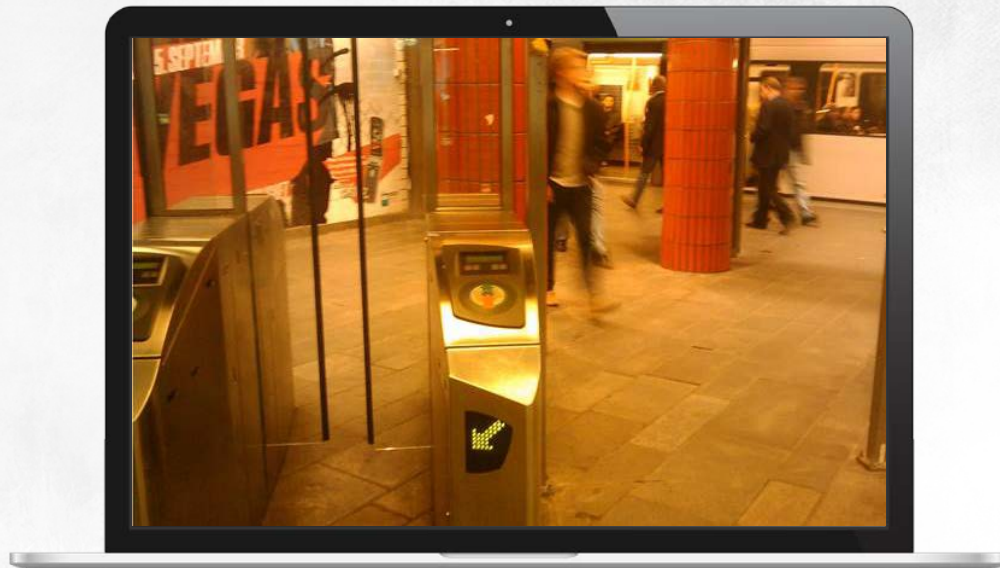
Standards And Security Solutions

Wi-fi networks

Introduction

Wireless networks were first introduced in 1991. The wireless networking is an invention that makes it possible to transfer data packets over standard network protocols: the only difference is that it uses radio waves rather than wires or optical fibres

Since this signal is broadcast and may be received by all hosts within the range of an access point, eavesdropping on wireless transmissions is not only easier to do but also virtually undiscoverable

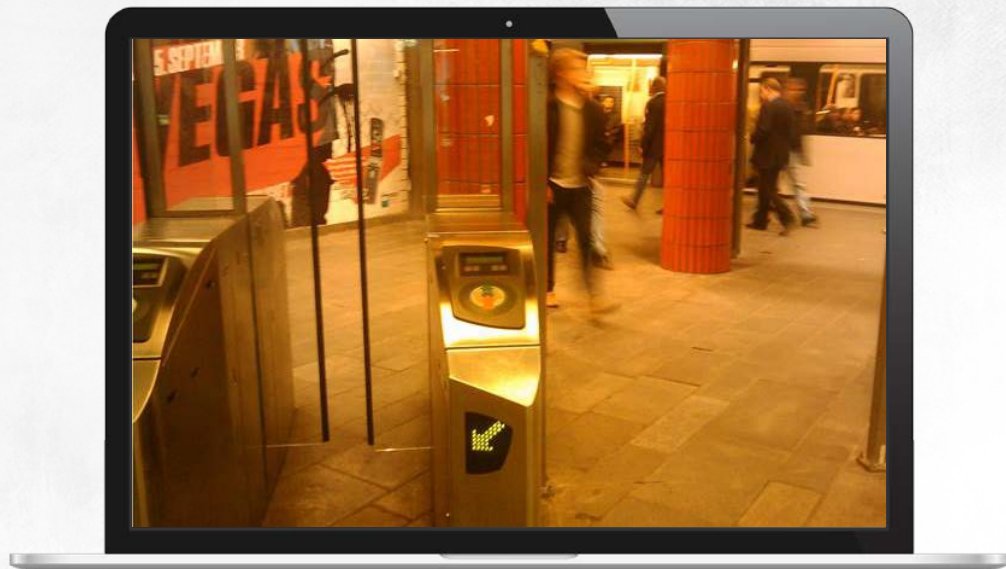


Wi-fi networks

Introduction

Each client has access to every transmission sent across the network in Wi-Fi LANs, including usernames and passwords passed on by other users and the URLs of websites they visit

If an attacker takes over an access point, this subjects data to the threat of both eavesdropping and uncontrolled modification of transmissions



Wi-fi networks

Standards

The 802.11 standard (Wi-Fi) is a set of IEEE specifications regarding wireless local area networks (WLANs) that defines the physical layer and access to TCP/IP stack data

Standard	Data rate	Frequency	Modulation	Comments
802.11	1 or 2 Mbit/s	2.4 GHz	FHSS, DSSS	First standard, defines physical and MAC layers
802.11a	6, 9, 12, 18, 24, 36, 48, or 54 Mbit/s	5.0 GHz	OFDM	Incompatible with other standards, usually used in ATM networks
802.11b	1, 2, 5.5 or 11 Mbit/s	2.4 GHz	DSSS, HR-DSSS	Popular in home networks
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48 or 54 Mbit/s	2.4 GHz	DSSS, HR-DSSS, OFDM	Backward compatible with 802.11b. Offers bigger throughput but covers a smaller distance
802.11n	100, 150, 300, 450 or 600 Mbit/s	2.4 or 5 GHz	OFDM	The MIMO technology enables sending and receiving signals through multiple output antennas

Developed in 1997, the 802.11 standard can also involve infrared transmissions covering a small distance with the data rate of 1 or 2 Mbit/s: this version is known as 802.11 IR

Wi-fi networks

How they work

To set up a connection with an access point, you need to determine a channel number (the frequency of your access point) and an SSID

The SSID (service set ID) is a string whose primary function is to provide a way of distinguishing between different Wi-Fi networks that use the same channels. They are not meant to provide client authentication: this is the reason access points broadcast their names by sending SSIDs in broadcast packets

While you can turn off SSID broadcasting, this will not improve the security of your WLAN in any way

Turning off SSID broadcasting may cause a client to try to connect with every access point in its proximity, which means it will send its authentication data to these APs

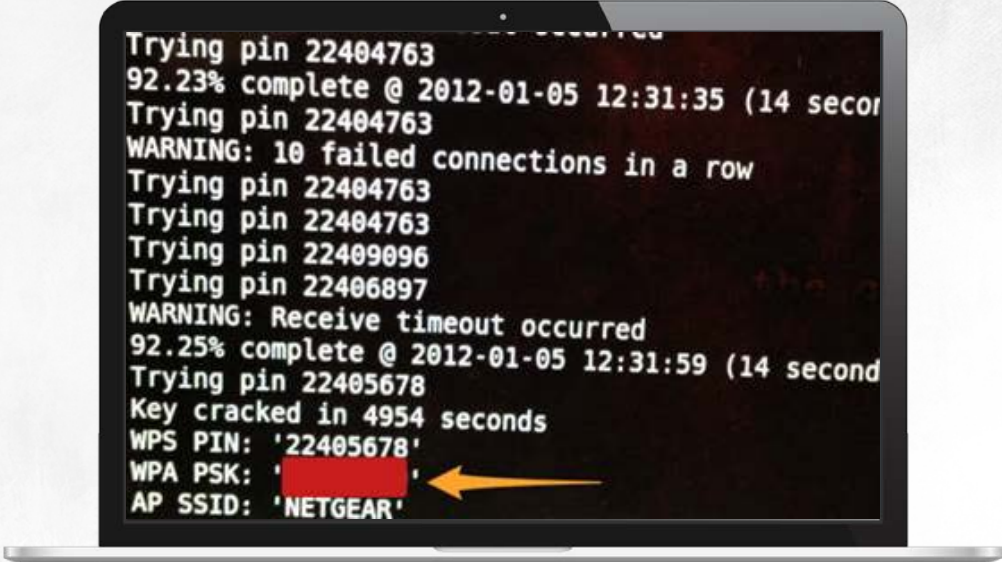
If a rogue access point obtains this data, it can facilitate an attack. An attacker will be able to connect to a WPA or WEP network: this means that **turning off SSID broadcasting can effectively lower the security of your WLAN**

Wi-fi networks

Wi-Fi Protected Setup

The WPS protocol was developed to automate access point configuration. Supported in all modern APs, this protocol can let you secure network access using the PIN External Register method

A host has to submit an 8-digit PIN (usually printed on a sticker on a device)



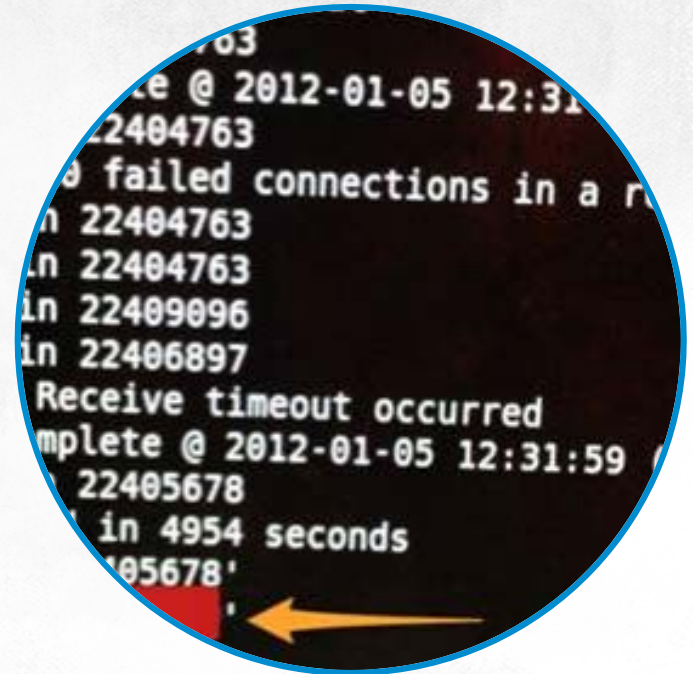
```
Trying pin 22404763
92.23% complete @ 2012-01-05 12:31:35 (14 seconds)
Trying pin 22404763
WARNING: 10 failed connections in a row
Trying pin 22404763
Trying pin 22404763
Trying pin 22409096
Trying pin 22406897
WARNING: Receive timeout occurred
92.25% complete @ 2012-01-05 12:31:59 (14 seconds)
Trying pin 22405678
Key cracked in 4954 seconds
WPS PIN: '22405678'
WPA PSK: '[REDACTED]'
AP SSID: 'NETGEAR'
```

Wi-fi networks

Wi-Fi Protected Setup

A vulnerability detected in 2011 allows an attacker to determine and submit this number:

- If a client submits the wrong PIN, the access point will send an EAP-NACK message that discloses whether or not the first half of the submitted PIN was correct
- The last digit in the PIN is its checksum
- This reduces the number of combinations to be tried to about 11 thousand. A brute-force attack on a WPS-protected AP needs to check only $10^4 + 10^3$ numbers
- Almost all APs do not detect and block these brute-forcing attempts
- If an attacker obtains the PIN, it means he will be able to connect to the WLAN and change the AP configuration



Other wireless technologies



- The first wireless technology for transferring data between devices, now obsolete, is CDPD
- GPRS transfers data with a speed up to 171.2 Kbit/s: the WAP protocols still use this solution
- Bluetooth uses the 2.45 GHz frequency band and has the maximum range of 10 metres, which effectively is the only security solution employed in these networks
- The RFID solution is mostly used to tag and identify objects. Because Radio Frequency Identification is on the rise, there is also an increasingly growing list of tools for scanning and duplicating RFID transponders
- Near Field Communication (NFC) provides data transfer between an initiator and target who are in close proximity (several inches). NFC networks may be active, but they are widely used in the passive mode



Security solutions

While you can manage and control access to switches and wires, medium access control for sending and receiving radio waves is impossible

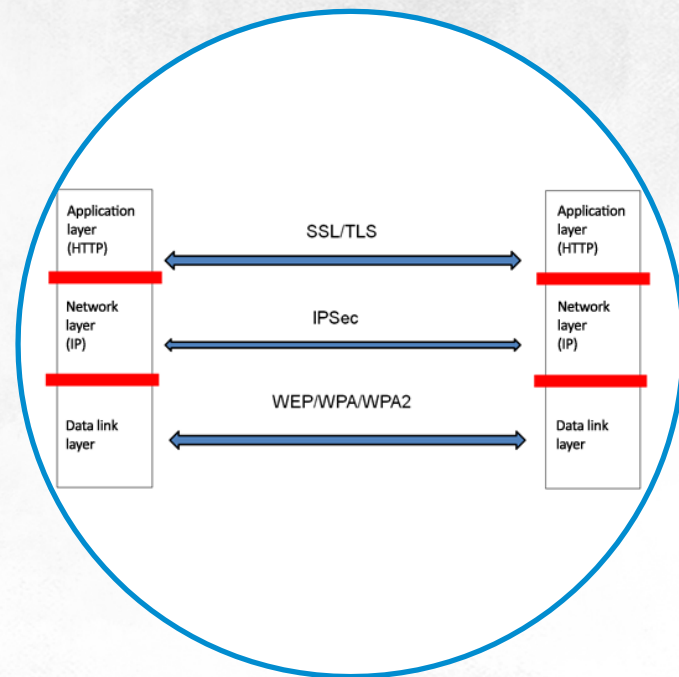
If attackers have an antenna that is big and sensitive enough, they will be able to receive an access point signal even from several kilometres



Security solutions

To reduce this threat, the WEP standard was adopted in 1999 (it was developed two years before)

Only two years later, after Peter Shipley's talk on WarDriving at DefCon more decisive steps were taken to secure wireless LANs better

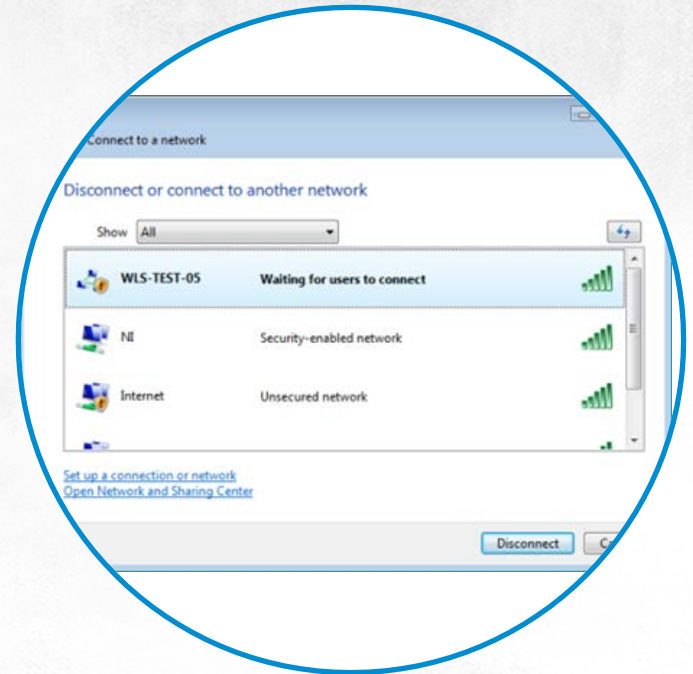


Security solutions

Ineffective solutions

Turning off SSID broadcasting will not hide your LAN or its ID: SSID is emitted in plaintext in broadcast packets like Probe requests, Probe responses, Association requests and Re-association requests

Using static IP addresses again does not improve security: everything an attacker needs to set up a connection can be found in UDP broadcast packets sent by an AP and its networked hosts

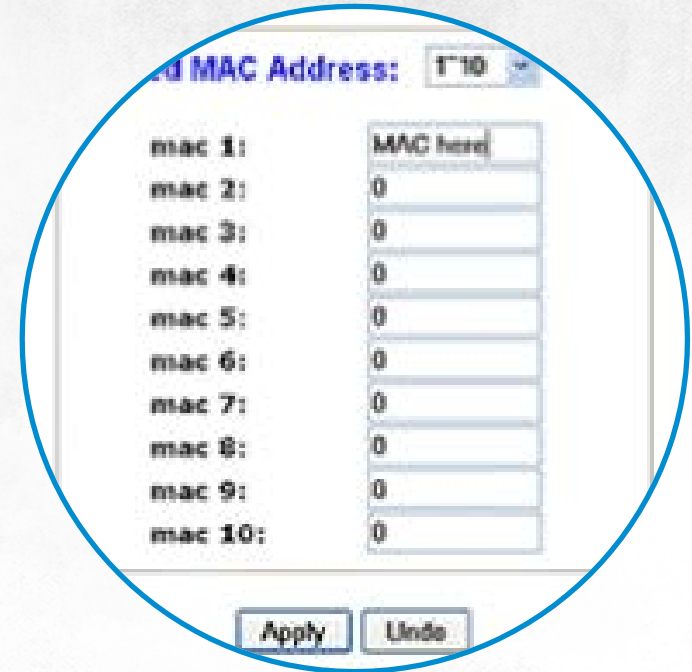


Security solutions

Ineffective solutions

MAC address control is simply filtering MAC addresses. Because they are sent in plaintext by hosts connected to an access point, the attacker only needs to intercept one correct address and change the MAC address in the Wi-Fi card he uses to this address

Hiding networks by changing channels or reducing AP broadcast strength will only cause trouble for legitimate users of a network. Attackers always have or can obtain bigger and more sensitive antennas



Authentication methods

Wireless networks can:

- Authenticate without verifying users' identity
- Verify users' identity based on a shared key
- Use the 802.1x standard and a RADIUS server to authenticate users

You can use any of the three authentication methods together with different encryption

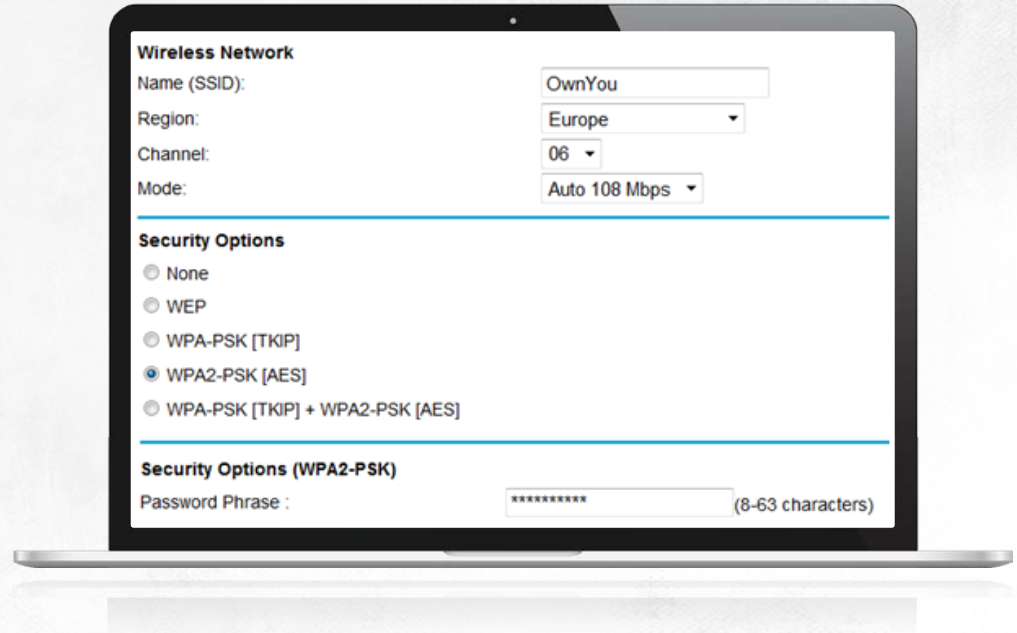
Open network systems (OSA) have been defined in the 802.11 standard. To establish a connection successfully, a user only needs to submit the correct SSID

The identity of users is verified against the MAC addresses of their NICs

If the data sent across a network is encrypted, a WEP key used for encryption is not checked by the AP, but the packets it will not be able to decrypt (the packets that have been encrypted using a wrong key) will be rejected

Authentication methods

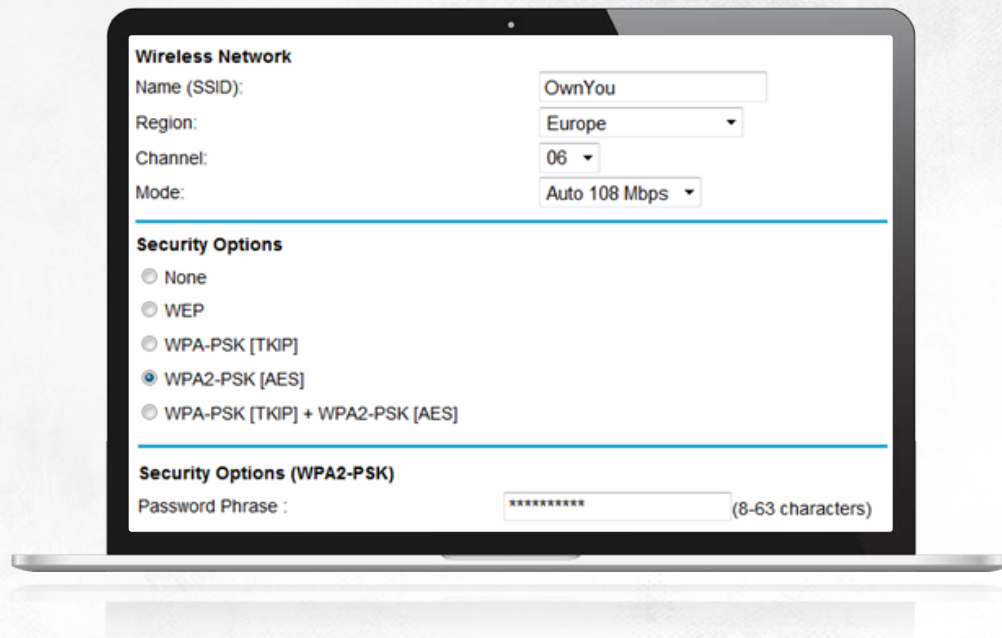
Shared key authentication (SKA) is a method of authenticating where the same key has to be stored in the access point and in all clients in a network



Authentication methods

This authentication is an exchange of a series of challenge and response messages:

- The client requests to be connected with a selected WLAN
- The AP generates a pseudorandom challenge and sends it to the client
- The client encrypts the challenge using the shared key and sends this response to the AP
- The AP decrypts the response using its key and compares the result against the challenge it sent earlier. If they match, the client is connected

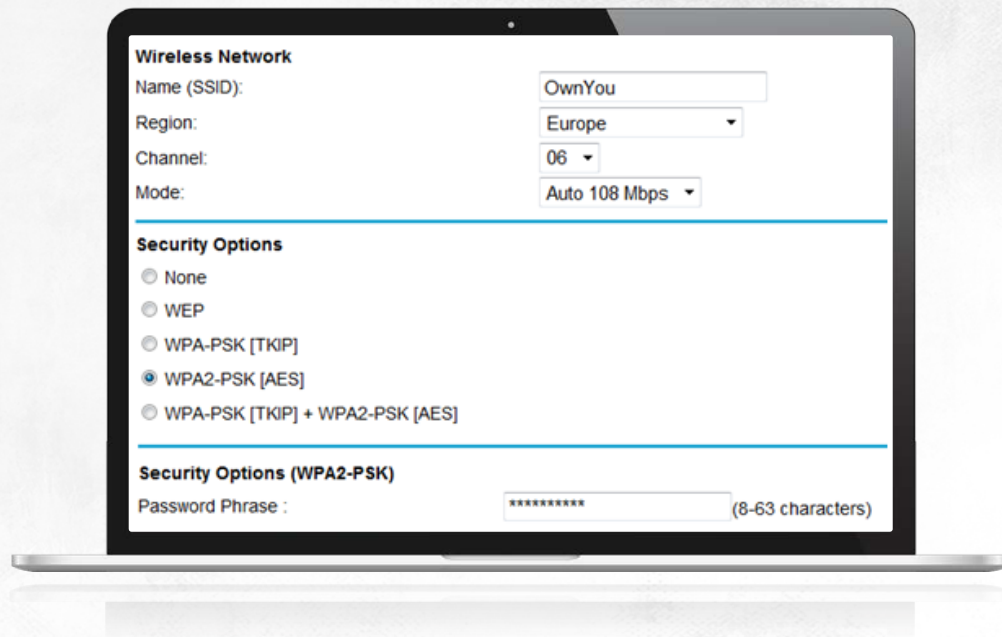


Authentication methods

An **attacker** can eavesdrop on the transmissions and sniff out credentials sent in plaintext

Using **SKA** means all clients in possession of the key have shared access to a network and may listen on the data transmitted by other users

The **necessity** to configure the key manually in each client



Authentication methods

The one fully secure solution for verifying the identity of wireless network users is the 801.1x standard

While using a RADIUS server for network access control in non-wireless networks is not very effective, it's a great solution for WLANs



Authentication methods

An **access point** assumes the role of a RADIUS client and sends (using the EAP protocol) user credentials to a RADIUS server

The **RADIUS server** verifies the identity of the users and can either allow or disallow the AP to connect the users

As a **result**, each user is authenticated against private data (a certificate issued for the user or credentials generated from the password), so keys do not have to be shared



Authentication methods

Even though implementing the 802.1x standard requires you to deploy a RADIUS server and a CA, this task can be made easier by using pre-defined wireless network user templates available in all Windows Server versions

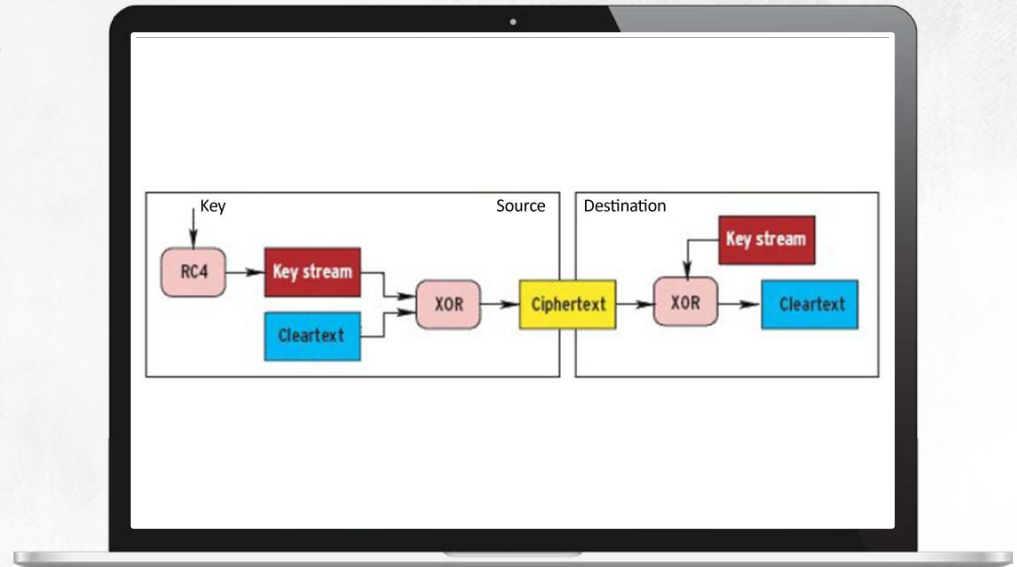


802.11 wep

The WEP standard was the first protection developed for securing the confidentiality of transmitted data in WLANs, and this solution is still in use

A WEP key is used also as an additional method for authenticating hosts: only the hosts that have a shared WEP key can connect to an access point

The WEP standard does not specify the MO of many security-relevant matters, including key sharing and key change mechanisms

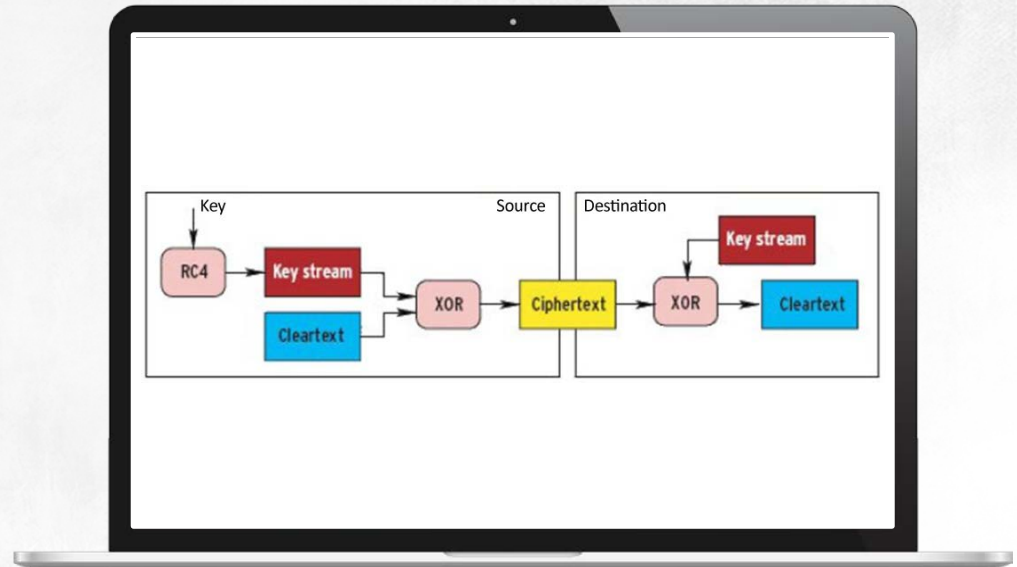


802.11 wep

The encryption used in the standard is equally lacking. Here's what it looks like:

- First the CRC checksum is calculated
- It is appended to a packet
- Next, the NIC generates a 25-bit initialisation vector (IV)
- The WEP key (K) and the IV are used to encrypt packet streams using the RC4 algorithm following this equation:
$$\text{ciphertext} = K, IV(P, c)$$

WEP provides for the use of keys that are 64-bit (WEP 64), 128-bit (WEP 128) or 256-bit (WEP 256, also known as WEP2)



802.11 WEP

Flaws

Too few initialisation vectors. The basic security principle for stream ciphers is never reusing a key. A 24-bit IV can take one of only 16,777,216 values. This means that intercepting as few as 5,000 packets gives an attacker a 50% chance of finding reused Ivs

No specified IV generation mechanism

Encrypting data, but not the headers. This means an attacker can both obtain the source and destination IP addresses of hosts, their MAC addresses and network SSIDs and can modify the destinations of the packets. This flaw makes networks vulnerable to a Man-in-the-Middle attack and can mean an attacker is able to redirect IP packets and run DOS attacks

802.11 WEP

Flaws

The way encrypted packet checksums are appended. Because data packets are XOR-ed with key stream bits, a ciphertext byte depends on the plaintext byte in the corresponding position. To try and determine the last message byte, you need to remove the last ciphertext byte and replace it with something else and then send the modified packet back to the network. If the byte has not been determined correctly, the access point will reject it as having the wrong checksum. Repeating this procedure for every byte in the message may decode the WEP packet and retrieve the stream key (the KoreK attack exploits this vulnerability)

Dependencies exist between the ciphertext and the initialisation vector (the PTW attack exploits this vulnerability)

802.11i wpa

Adopted by Wi-Fi Alliance in 2003

Designed as an interim solution that enhances the security of wireless devices that comply with the earlier WEP standard until their manufacturers develop and introduce devices that support WPA-2

Like WEP, it uses the RC4 algorithm to encrypt data. The differences are that:

- WPA uses a 128-bit key complemented with a longer, 48-bit IV
- WPA uses TKIP to automatically manage keys. The TKIP protocol enforces frequent changes of encryption keys, which, together with the increased length of the IV ($2^{48} = 281,474,976,710,656$) is a good protection against brute-force attacks

WPA can also authenticate clients against a shared 256-bit key (in the WPA-Personal mode) and authenticate clients using a RADIUS server

802.11i wpa

It is a vast improvement in protecting the integrity of packets: WEP simply calculated the packet checksum, which could allow attackers to easily modify packets without having to decrypt them before, while WPA uses the MIC hash

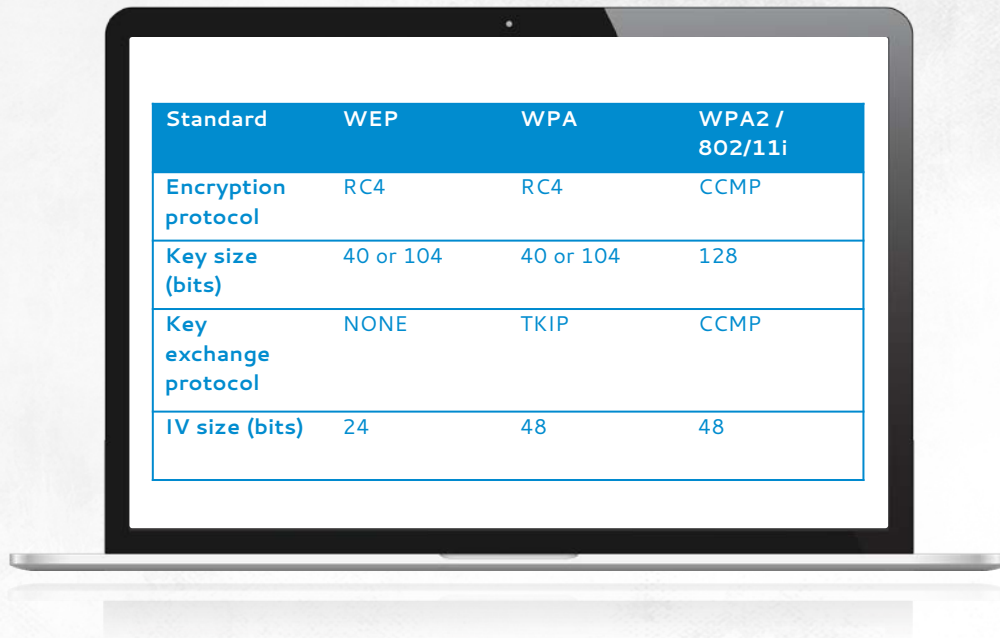
What makes WPA-Personal secure is the length of the shared key and making sure it is not a word to be found in any dictionary of any language: the most typical WPA attack is trying to determine the PSK based on intercepted client authentication messages (EAPOL packets)

Authentication methods

Like the first version of WPA, the IEEE 802.11i standard might be used in the PSK mode or together with a RADIUS server

For data encryption, it uses the AES-based CCMP algorithm with a 128-bit key and a 48-bit initialisation vector

Generally considered secure, this algorithm is also employed in automatic key management

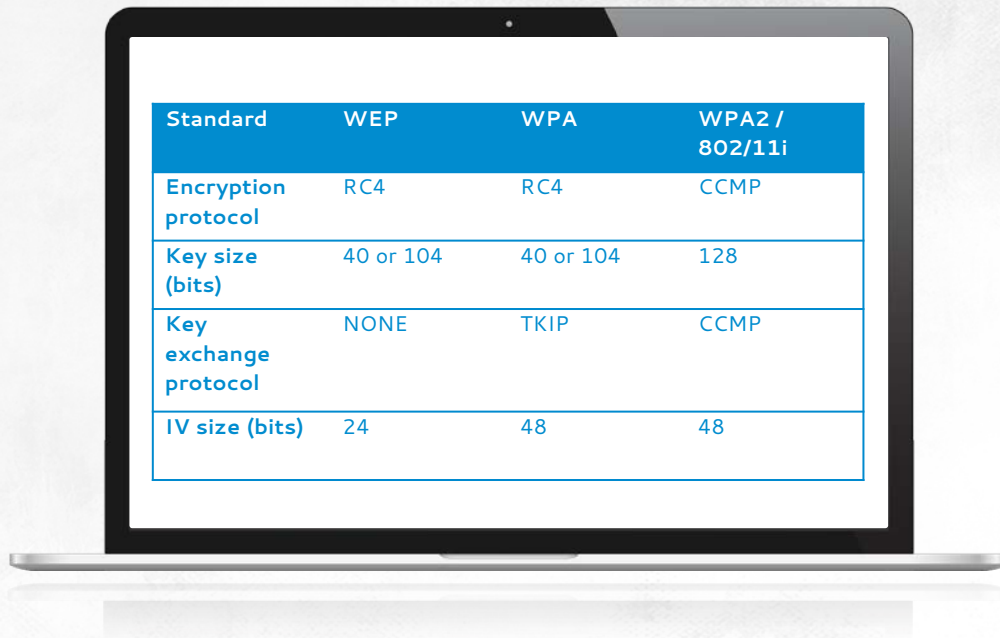


Standard	WEP	WPA	WPA2 / 802/11i
Encryption protocol	RC4	RC4	CCMP
Key size (bits)	40 or 104	40 or 104	128
Key exchange protocol	NONE	TKIP	CCMP
IV size (bits)	24	48	48

Authentication methods

The most prevalent attacks on WPA2 involve PSK cracking using intercepted client authentication messages, which means only Wi-Fi networks with weak passwords are vulnerable to them

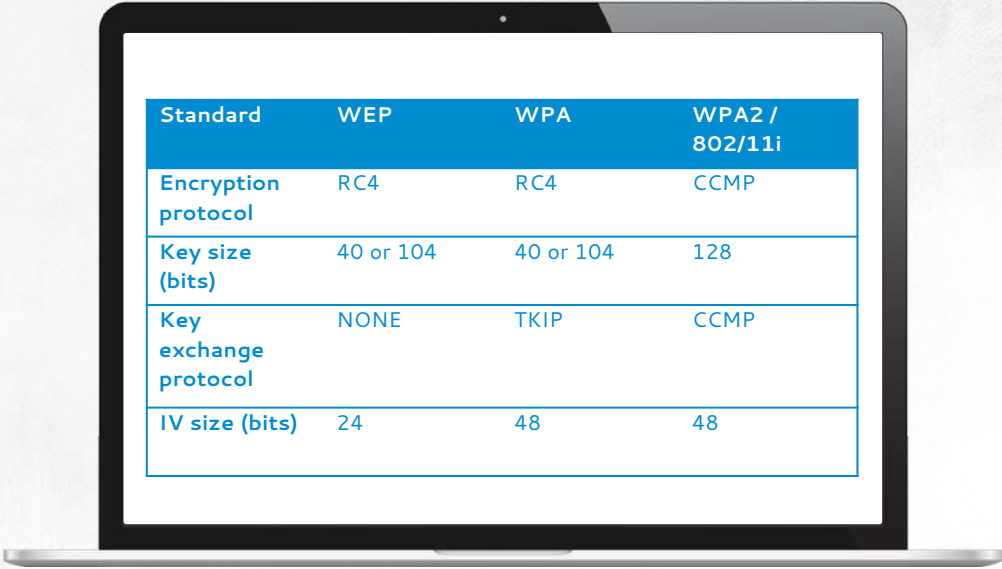
As for the requirements for passwords used to access a network in the PSK mode, they are the same as in WPA. A password may have from 8 to 63 characters (ASCII), but to make it adequately secure, it should contain no less than 30 random characters



Standard	WEP	WPA	WPA2 / 802.11i
Encryption protocol	RC4	RC4	CCMP
Key size (bits)	40 or 104	40 or 104	128
Key exchange protocol	NONE	TKIP	CCMP
IV size (bits)	24	48	48

Authentication methods

Additionally, the SSID should not be a word in any language



Standard	WEP	WPA	WPA2 / 802.11i
Encryption protocol	RC4	RC4	CCMP
Key size (bits)	40 or 104	40 or 104	128
Key exchange protocol	NONE	TKIP	CCMP
IV size (bits)	24	48	48

THANKS

