Wireless Security

Wireless networking standards

- Wireless networking provides a means to connect network nodes without installing network cabling.
- There are numerous technologies for wireless networking, those in the 802.11 family of standards are the most widely implemented and least expensive.

The 802.11 standard

- The IEEE 802.11 standard specifies a wireless computer networking technology that operates in the 2.4 and 5GHz radio frequency (RF) bands.
- The IEEE 802.11 standards are defined at the Data Link layer of the Open Systems Interconnection (OSI) model.
- The current and future 802.11 standards are shown in the following table, and described in more detail in the accompanying document.

Standard	Description
802.11a	Ratified in 1999, 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM) signaling to transmit data. OFDM offers significant performance benefits compared with the more traditional spread-spectrum systems. OFDM is a modulation technique for transmitting large amounts of digital data over radio waves. Capacity per channel is 54 Mbps with real throughput at about 31 Mbps. It operates at a frequency of 5 GHz, which supports eight overlapping channels.
802.11b	Ratified in 1999, 802.11b is one of the most commonly used 802.1x technologies. Uses Direct Sequence Spread Spectrum (DSSS). Capacity per channel is 11 Mbps with real throughput at about 6 Mbps. It operates at a frequency of 2.4 GHz, which supports three non-overlapping channels.
802.11d	Ratified in 2001, 802.11d aims to produce versions of 802.11b that are compatible with other frequencies so it can be used in countries where the 2.4 GHz band isn't available.
802.11e	802.11e adds Quality of Service (QoS) capabilities to 802.11 networks. It uses a Time Division Multiple Access (TDMA) data signaling scheme and adds extra error correction.
802.11g	Ratified in 2003, 802.11g is a combination of 802.11a and 802.11b. It can use either Direct Sequence Spread Spectrum (DSSS) or Orthogonal Frequency Division Multiplexing (OFDM) to transmit data. Capacity per channel is 54 Mbps with real throughput at about 12 Mbps. It operates at a frequency of 2.4 GHz and is a popular 802.11 technology.
802.11h	Ratified in 2003, 802.11h attempts to improve on 802.11a by adding better control over radio channel selection and transmission power.
802.11i	Ratified in 2004, 802.11i deals with security and is based on the Advanced Encryption Standard (AES). The 802.11i standard has a feature called Robust Security Network (RSN), which defines two security methodologies. The first is for legacy-based hardware using RC4, and the second one is for new hardware based on AES.
802.11j	Ratified in 2004, 802.11j allows 802.11a and HiperLAN2 networks to coexist on the same airwaves. The 802.11j standard changed the 5GHz signaling capabilities to support Japanese regulatory requirements.
802.11n	802.11n is a 100+ Mbps standard. Many access points are available that are compatible with 802.11n and 802.11a and b.

WiMAX (IEEE 802.16 Air Interface Standard)

- WiMAX, Worldwide Interoperability of Microwave Access, provides wireless DSL and T1-level service.
- Emerging point-to-multipoint broadband wireless access standard that services wide area and metropolitan area networks, allowing wireless users with 802.16e devices to roam between wireless hotspots.
- WiMAX operates in the frequency ranges of 10–66 GHz for licensed communications, and 2–11 GHz for unlicensed communications, providing a bandwidth in excess of 70 Mbps, which is shared among the network's users. It has a theoretical maximum of 31 miles with no obstructions.

Device compatibility

- Although devices that support the 802.11a standard are generally incompatible with those that support 802.11b, some devices are equipped to support either 802.11a or 802.11b.
- The newest approved standard, 802.11n, allows 802.11b, 802.11g, and 802.11n devices to operate together on the same network.
- Many modern APs support multiple standards. For example, one AP might offer concurrent support for 802.11a, b, g, and n clients in addition to 100 Mbps wired network clients.

Wireless LAN connection components

- To establish a wireless LAN, you need wireless network cards in the computers and a wireless router or wireless access point (WAP) device on the network. (The 802.11 standard defines an *access point* as a device that functions as a transparent bridge between the wireless clients and the wired network.)
- The router or access point broadcasts radio signals, and the wireless network cards pick up the broadcasts.

Wireless NICs

- LAN network adapters of all current types (e.g. PCI, PC Card, and USB) come in wireless versions.
- Wireless capability is built into most laptops as standard equipment and can easily be added to laptops via wireless PC Cards or USB NICs.
- Desktops can also be easily outfitted with wireless capabilities by adding PCI Cards or USB wireless NICs.
- If wireless access is available, these cards can communicate with a wireless access point.

Wireless NICs

PCI NIC

PC Card NIC

USB NIC

Wireless access points

- A wireless access point connects a WLAN to a wired Ethernet network. The access point (AP) contains the following: at least one interface for connecting to the wired network (this interface is typically called the "WAN port"); transmitting equipment for connecting with the wireless clients; and IEEE 802.1D bridging software to act as a bridge between wireless and wired Data Link layers.
- Access points often integrate other networking functions. Many APs include Ethernet networking ports for connecting wired devices and thus function as switches.
- Many APs also include routing capabilities, and such devices most often also include firewall functions.

Wireless access points

Cisco Aironet Access Point

Linksys Wireless-G 2.4 GHz router/wireless access point

Security threats to wireless networks

- Wireless devices present a whole new set of threats that we need to be aware of.
- Obvious risks concerning wireless networks are theft and rogue devices.
- Mobile phones, pagers, PDAs, tablets, and wireless NICs are small enough that they can easily be lost or stolen.
- Because they are easy to conceal and contain valuable information about a company, they have become favourite targets of intruders.
- Wireless LANs can be subject to session hijacking and man-in-the-middle attacks. Additional risks remain because anyone can purchase an access point and set it up.

Security threats to wireless networks

- Wireless access points generally have no security configured out of the box.
- They broadcast their presence.
- Free availability of 802.11 network audit tools, such as AirSnort and NetStumbler, means breaking into wireless networks configured with weak security is quite easy.
- These tools can be used to check wireless security by identifying unauthorised clients or access points and verifying encryption usage.
- To eliminate 802.11 shortcomings the Institute of Electronic and Electric Engineers (IEEE) and the Wi-Fi Alliance proposed standards for significantly improved user authentication and media access control mechanisms.

Additional risks:

- 802.11 transmissions generate detectable radio-frequency traffic in all directions. Persons wanting to intercept the data transmitted over the network might use many solutions to increase the distance over which detection is possible, including the use of metal tubes such as Pringles cans or large tomato-juice cans.
- Without the use of an encryption standard of some type, data is passed in clear text form. Even though technologies such as Wired Equivalent Privacy (WEP) encrypt the data, they still lack good security. A determined listener can easily obtain enough traffic data to calculate the encryption key in use.

Additional risks:

- The authentication mechanism is one-way, so it's easy for an intruder to wait until authentication is completed and then generate a signal to the client to trick it into thinking it has been disconnected from the access point. Meanwhile, the intruder, pretending to be the original client, begins to send data traffic to the server.
- The client connection request is a one-way open broadcast. This gives an intruder the opportunity to act as an access point to the client, and act as a client to the real network access point. An intruder can watch all data transactions between the client and access point, and then sniff, read, modify, insert, or delete packets at will.
- Wireless networks are vulnerable to war driving which involves using other people's open wireless access points.

WLAN security components

There are four components to security on a wireless network:

- Access control
- Encryption
- Authentication
- Isolation

For each security method implemented on the AP, the clients must also be configured to match.

Access control

- Various techniques can be used to control which clients can use an AP. The simplest, and least effective, method is to simply turn off SSID (service set identifier) broadcasts. Doing this hides the presence of the AP. Clients can then be configured to connect to the appropriate AP by manually entering its SSID. However, the SSID is also included in routine client-to-AP traffic. Thus, it's easy for appropriately configured devices to detect SSIDs that aren't explicitly broadcast.
- A stronger method of access control is to enable MAC filtering on your AP. On most APs, you can enter a list of permitted MACs, or blocked MACs, to limit connections.
- As with the SSID, valid MAC addresses are transmitted across the wireless network. A malicious user could detect a valid MAC address and then configure his computer to impersonate that MAC address and gain access to the AP.

Encryption

- Communications between your AP and clients can be encrypted. Various techniques exist, with some being more secure than others. To make a connection, clients must use the same encryption scheme and possess the appropriate encryption key. After the connection is made, a static or dynamically changing key provides ongoing encryption.
- In theory, encryption blocks unapproved connections to your AP. Additionally, as long as the encryption scheme is sufficiently strong, data streams are kept private from eavesdroppers. However, not all wireless encryption systems are sufficiently robust to actually provide these protections.

Authentication

- Through RADIUS (Remote Authentication Dial-In User Service) or other systems, you can enable client authentication over your wireless network. Using a system essentially like the username and password you use when you log on, an AP can authenticate the identity of wireless networking clients.
- Authentication provides much stronger access control protection than does SSID hiding or MAC and IP address filtering. Encryption with authentication should also be used. Without it, eavesdroppers could access the data that legitimate clients transmit when those clients have connected to the AP. Authentication typically requires the use of additional software or hardware devices, such as a RADIUS server.

Isolation

Isolation is a means of segregating network traffic. There are two types: wireless client isolation and network isolation.

- With wireless client isolation, also called AP isolation, wireless clients are put onto individual VLANs (virtual LANs) so that they cannot access each other. This method is commonly used in public wireless networks to prevent one user from accessing another user's computer. E.g. in a library or coffee shop, another user might attempt to access your shared folders or mount brute-force attacks on your PC over the Wi-Fi (802.11 wireless) hotspot network.
- Network isolation can also be provided. For example, to permit wireless clients to access the Internet and corporate mail server, which is on the wired network, but to prevent wireless clients from accessing other wired nodes, such as file servers. Some APs offer network isolation through custom routing configurations. Isolation can also be implemented through general network design and firewall configuration.

Transmission encryption

- Enable transmission encryption on wireless routers unless there is a very good reason not to. Transmission encryption limits the clients that can connect to an AP and protects data from eavesdropping during transmission.
- Products certified as Wi-Fi compatible by the Wi-Fi Alliance must support at least the WPA Personal level of encryption. As of this writing, products don't have to support the 802.11i standard, but this requirement will soon take effect.
- The following table describes transmission encryption methods.

Encryption method	Description
WEP	Wired Equivalent Privacy was built into the 802.11 standards for wireless connectivity that govern how data can be encrypted while in transit on the wireless network. WEP uses a 64-bit or 128-bit symmetric encryption cipher. For WEP to work, a key is configured on both the WAP and the client. This key is used to encrypt the data transmitted between the WAP and the client. There are no standards for how the WEP key is to be placed on the clients and the WAP. Most implementations require you to type in the key manually on each client and the WAP. Although WEP provides an easy way to prevent casual hackers from viewing the traffic transmitted on your wireless LAN, it is the least secure encryption technique. WEP has known design flaws that make it relatively easy to crack. However, it is the only viable option for 802.11b and other older wireless clients.
WPA Personal and WPA2 Personal	Wi-Fi Protected Access (WPA) was developed to overcome the weaknesses in WEP. It uses the RC4 symmetric cipher with a 128-bit key. WPA Personal uses a pre-shared key (PSK), which simply means that you must enter the same passphrase on both the AP and the clients. The actual encryption key is built from this passphrase and various other data, such as the sending node's MAC address. With the Temporal Key Integrity Protocol (TKIP) option, the full encryption key changes for each packet. WPA authorizes and identifies users based on a secret key that changes automatically at regular intervals. WPA uses TKIP to change the temporal key every 10,000 packets. This ensures much greater security than does the standard WEP.
WPA2	WPA2 builds on WPA by adding more features from the 802.11i standard. Notably, WPA2 uses the Advanced Encryption Standard (AES) cipher for stronger encryption (equivalent to IEEE 802.11i). WPA2 uses the version of AES called AES-Counter Mode with Cipher Block Chaining Message Authentication Protocol, or AES-Counter Mode CBC-MAC Protocol, better known CCMP. This protocol uses AES in "counter mode" to provide even stronger security by making it more difficult for potential eavesdroppers to spot data patterns, and the message authentication provides a high level of message integrity.
WPA Enterprise, WPA2 Enterprise	These methods authenticate enterprise wireless clients by using a RADIUS or TACACS server and the user's username and password or digital certificate, rather than using a pre-shared key. WPA- and WPA2 Enterprise work in conjunction with an 802.1X authentication server (RADIUS or TACACS). Communications between the client and AP are encrypted using the individual's key.

Encryption method	Description
RADIUS	Remote Access Dial-in User Service (RADIUS) uses a specialized server for authentication and uses WEP for data encryption, as illustrated in Exhibit 10-3. The authentication server can include keys as part of the accept message that's sent back to the WAP. In addition, clients can usually request a key change. This feature ensures that keys are changed regularly to limit the ability of hackers to view information on the wireless network.
802.11i	This standard defines security mechanisms for wireless networks (equivalent to WPA2). CCMP is the preferred encryption protocol.
EAP, LEAP, and PEAP	EAP (Extensible Authentication Protocol) provides an authentication framework for a wireless client and a wireless access point and authenticating server, such as a RADIUS server, to negotiate a connection. The framework defines different ways to authenticate a connection. These ways, called EAP methods, include: • EAP-TLS, which uses TLS as the mechanism by which the client and AP authenticate each other; • EAP-Tunneled TLS (EAP-TTLS), which uses a secure tunnel to authenticate the client; and • EAP-Flexible Authentication via Secure Tunneling (EAP-FAST), which uses a TLS tunnel to exchange user credentials. LEAP (Lightweight EAP) is Cisco's proprietary version of EAP, which is not natively supported in Windows. Its major flaw is the lack of strong protection for user credentials. Cisco now recommends the use of EAP-FAST, PEAP, or EAP-TLS. PEAP (Protected EAP) was developed jointly by Cisco, Microsoft, and RSA Security. It encapsulates EAP in a TLS tunnel for stronger protection.

Securely configuring a wireless access point

- When setting up an AP, a service set identifier (SSID) is assigned, which is essentially a name for the wireless network.
- The default name is usually the name of the router or WAP manufacturer. Change this name as part of the device configuration to make the WLAN more secure. Changing the name isn't really a method of securing the network, however, because the SSID is sent in plain text over the network and can be found by anyone with the ability to read network packets. It's possible, and likely, that multiple wireless networks will be accessible from a given location. In such cases, clients use the SSID to distinguish between WLANs and connect to a particular network.
- An access point typically broadcasts the SSID. In this way, clients can discover the presence of a nearby access point. Such broadcasts identify the security mechanisms in place to enable clients to auto-configure their connections.

Securing an access point

- Out of the box, a wireless access point isn't secure. To aid security:
- Set the most secure transmission encryption method compatible with your clients — WEP, WPA Personal, WPA2, WPA Enterprise, RADIUS, and 802.11i.
- Update the access point's firmware version .
  - You can also find third-party vendor sites and download open-source replacement firmware. Download both the software and the installation (sometimes referred to as "flash") instructions.

Securing an access point

- Change default administrator accounts and passwords for the access point — Many devices don't have a default password set on the Administrator account.
  - Tools such as AirSnort identify the manufacturer based on the MAC address, so if you change only the SSID, an informed hacker can still easily gain access. Also, changing the name of the widely available administrator accounts presents an added barrier to anyone trying to connect to the access point.
- Change the default SSIDs — don't use anything that reflects the company's main names, divisions, products, or address. Doing so would make the organisation an easier target. If an SSID name is enticing enough, it might attract trouble.
- Disable SSID broadcasts — SSID broadcasting is enabled by default.

Securing an access point

- Separate the wireless network from the wired network — Consider using an additional level of authentication, such as RADIUS, before permitting an association with your access points. The wireless clients can be separated so the connections not only use RADIUS authentication but are also logged.
- Put the wireless network in an Internet-access-only zone or a demilitarised zone (DMZ) — Place wireless access points in a DMZ, and have wireless users tunnel into your network through a VPN (virtual private network).

Securing an access point

- Disable DHCP within the WLAN to keep tighter control over users — Assign static IP addresses to your wireless clients. Doing this creates more administrative overhead to manage, but makes it harder to access your network.
- Enable MAC address filtering on access points to limit unauthorised wireless NICs — Many access points allow you to control access based on the MAC address of the NIC attempting to associate with it.
- If the MAC address of the wireless client's NIC isn't in the access point's table, access is denied. Although there are ways to spoof a MAC address, doing so takes an additional level of sophistication.
- Enable 802.1X — This is the recommended method of authentication and encryption for enhanced security on computers running versions of Windows later than Windows XP.
  - 802.1X offers a solution for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys.
  - The 802.1X standard ties EAP to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication.

Securing an access point

- A network administrator should periodically survey the site, using a tool such as NetStumbler or AirSnort, to see if any rogue access points are installed on the network.
- In addition, the administrator can take a notebook equipped with a wireless sniffer and an external antenna outside the office building to see what information inside the building can be accessed by someone parked in the parking lot or across the street.

Wireless client security

- The operating system that a client is running determines how you configure its connection to a wireless network.
- Windows 7, Windows Vista, and Windows XP use the Wireless Zero Configuration and Wireless Auto Configuration technologies to make the connection process easier for end-users.

Windows 7, Windows Vista, and Windows XP wireless clients

- Wireless Auto Configuration dynamically selects the wireless network to which a connection attempt is made, based on configured preferences or default settings.
- Computers running Windows 7, Windows Vista, and Windows XP support Wireless Zero Configuration, which enables computers to automatically connect to available wireless networks.
- By default, Windows 7, Windows Vista, and Windows XP client computers can choose from available wireless networks and connect automatically without user action.
- Wireless Zero Configuration automatically configures such items as TCP/IP settings and DNS server addresses.

Default settings in Wireless Zero Configuration include:

- "Infrastructure before ad hoc mode, and computer authentication before user authentication."
- *Infrastructure mode* uses an access point to connect the wireless network to the wired network. It typically requires authentication in which the computer identifies itself to the authenticating server before the user credentials are sent. *Ad hoc mode* allows all wireless devices within range to discover and communicate with one another without a central access point.
- "WEP authentication attempts to perform an IEEE 802.11 shared key authentication if the network adapter has been preconfigured with a WEP shared key; otherwise, the network adapter reverts to the open system authentication."
- Although the IEEE 802.1X security enhancements are available in Windows 7, Windows Vista, and Windows XP, the network adapters and access points must also be compatible with this standard for deployment.
- You can change the default settings to allow guest access, which isn't enabled by default.
  - You shouldn't turn on guest access on a laptop using Wireless Zero Configuration. An unauthorized user could establish an *ad hoc* connection to the laptop and gain access to confidential information on it.

RADIUS servers

- When you implement an authenticating server, such as RADIUS, the wireless client must submit its credentials to the authenticating server before wireless network access is established. When the client computer is in range of the wireless AP, it tries to connect to the WLAN that is active on the wireless AP.
- If the wireless AP is configured to allow only secured or 802.1X-authenticated connections, it issues a challenge to the client. The wireless AP then sets up a restricted channel that allows the client to communicate with only the RADIUS server.
- The RADIUS server accepts a connection from only two sources: a trusted wireless AP; or a WAP that has been configured as a RADIUS client on the Microsoft Internet Authentication Service (IAS) server and that provides the shared secret key for that RADIUS client.
- The RADIUS server validates the client credentials against the directory. If the client is successfully authenticated, the RADIUS server decides whether to authorise the client to use the WLAN. If the client is granted access, the RADIUS server transmits the client's master key to the wireless AP. The client and the wireless AP now share common key information they can use to encrypt and decrypt the WLAN traffic passing between them. How clients are configured to participate in this process depends on the operating system.

Wireless network vulnerabilities

- Through careful technology selection and configuration, you can prevent unwanted access to an access point and block client-to-client access over a wireless network. Also consider vulnerabilities in your APs. As with other networking devices, access points include these common vulnerabilities:
  - Physical access
  - Firmware vulnerabilities
  - Default administrator accounts
- Just as you should prevent physical access to switches, routers, and servers, you should prevent physical access to APs. Use lockable enclosures for APs, or mount them in physically secure locations, such as a locked room. Unlike wired devices, you must take care to consider how these physical safeguards will affect the wireless signal propagation.

Wireless network vulnerabilities

- Check regularly for firmware upgrades. After careful testing, implement upgrades as they become available. Consider third-party router firmware, such as the open-source DD-WRT firmware.
- Change the passwords on all administration interfaces on APs. Typically, APs provide Web-based administration interfaces. Make sure to change the password on such interfaces because the default passwords for most APs are widely published on the Internet.
- Additionally, make sure to change the passwords for Telnet, SSH (secure shell), and SNMP interfaces. APs often support such interfaces, but their documentation and built-in administration tools provide little information on their availability. Third-party AP firmware typically offers easier access for managing these interfaces.

Wireless network vulnerabilities

Additional risks associated with wireless networks include the following:

- The authentication mechanism is one-way, so it is easy for an intruder to wait until authentication is completed and then generate a signal to the client that tricks the client into thinking it has been disconnected from the access point. Meanwhile, the intruder begins to send data traffic to the server, while pretending to be the original client.
- The client connection request is a one-way open broadcast. This gives an intruder the opportunity to act as an access point to the client, and act as a client to the real network access point. This allows an intruder to watch all data transactions between the client and access point, then modify, insert, or delete packets at will.

Wi-Fi scanners

- Generally wireless access points have no security configured when set up right out of the box, so by default, they broadcast their presence.
- Unsecured access points in an otherwise secure network are sometimes called "rogue access points" and represent a large vulnerability.
- Standalone Wi-Fi scanners are available, which detect the presence of wireless signals within range.
- We can also use software such as Airsnort or NetStumbler on a laptop to scan for WLANs.

Wi-Fi scanners

- War driving is the practice of scanning for open wireless access points in a region.
- Several websites provide detailed information about unsecured networks. These sites provide locations, sometimes on city maps, for the convenience of others looking for open access links to the Internet. War driving used to capture data from networks, and also as a way of getting free Internet/bandwidth.

Wi-Fi scanners

- After discovering a wireless network, attackers can launch an interference attack, which steals bandwidth and can result in a denial-of-service (DoS) attack by limiting the bandwidth available on your wireless network.
- Mitigate against interference attack by securing APs to prevent unauthorised access.
- Another kind of eavesdropping attack is called IV attack or CBC IV attack. It exploits a feature of TLS 1.0 in which the initialisation vector (IV) used for cipher block chaining encryption can be compromised to break the encryption. This vulnerability was removed from TLS 1.1 and later.
- Evil-twin attack, in which an attacker sets up a bogus access point, to eavesdrop on wireless communication, at a public hotspot or a home or business network. Although the AP uses an SSID that appears legitimate, it is in fact an AP set up by a third party. Users then give away usernames and passwords, thinking they're logging onto a valid AP.