Network Security

Dr. Ihsan Ullah

Department of Computer Science & IT
University of Balochistan, Quetta
Pakistan

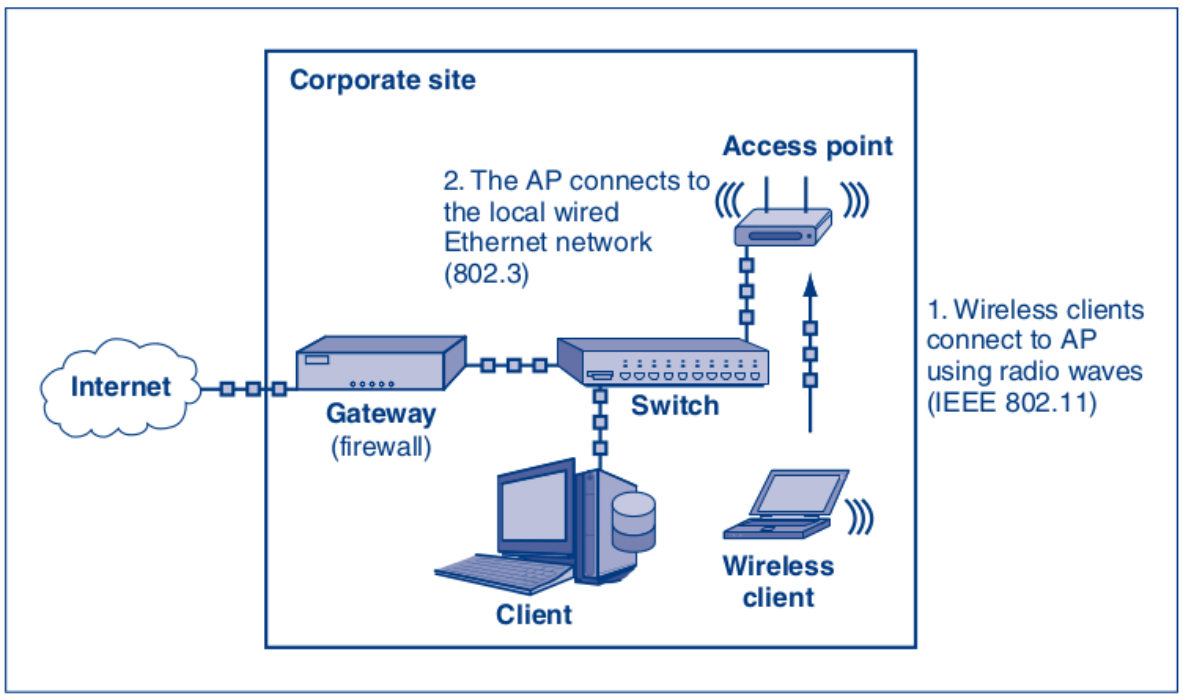
June 25, 2015

Wireless LAN security

- Wireless LANs (WLAN) have more security issues to consider than wired LANs
- Can be attacked by drive-by hackers who don't even have to enter the building to gain access to the LAN
- Attackers can sit across the street, or in an adjacent building, and easily access an internal network without raising suspicions
- Wireless networks are in widespread use because they are quicker, easier, and less expensive to set up and offer greater mobility, productivity, and functionality
- Security measures for these networks have not kept pace with their rapid growth

Wireless LAN security

- Users connect via radio waves to a wireless access point (AP) using the 802.11 standards
- The AP then connects to the local Ethernet (802.3) network with a wired connection
- The AP acts as a relay point between the two networks



Wireless LAN security

- Wireless attacks focus on the access point
- Wireless 802.11 networks typically have a range of 30 to 100 meters extending in all directions from the AP
- This allows the attacker to attack the AP, and the internal network, while staying outside the physical boundaries of the corporate site

Wireless attacks

1. Unauthorized network access
2. A man-in-the-middle attack using an evil twin
3. Wireless denial-of-service attacks

Wireless attacks

Unauthorized network access

- Unauthorized access is connecting to a network without permission
- Can be done by cracking the security protocols
- Rogue access points: unauthorized access points set up by individuals or departments in a network are a serious threat to wireless security

Wireless attacks

Possible harms by unauthorized network access

1. Harm to internal resources
2. Harm that appears to come from your network

Unauthorized network access

Internal harm

- Attackers have greater access to internal information, resources, and other network traffic
- They can covertly steal confidential information, read and record network traffic, alter network devices, or plant malware on targeted clients or servers
- They may also have access to network shares that were assumed to be protected behind the firewall

Unauthorized network access

External harm

- Since attacker is connected to the network, his traffic appears to be coming from the network
- Attacks and damages done will seem to be done by the organization owning the network
- An attacker could anonymously download, upload, and store illegal content via the wireless network
- Even worse, the network could be used as a launching pad for an external attack

Wireless attacks

Evil twin access points

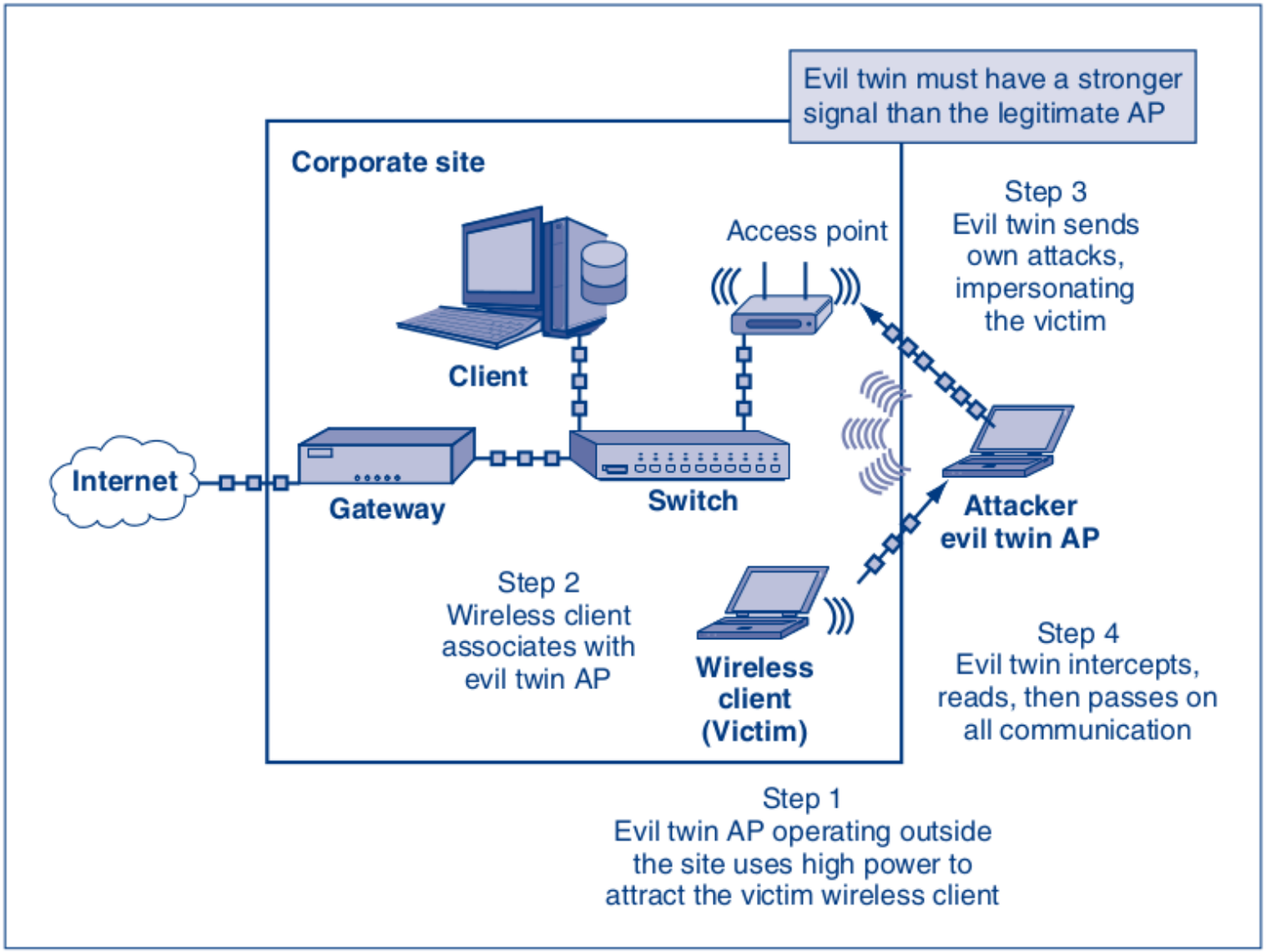
- Although wireless networks offer strong security, they are susceptible to man-in- the-middle attacks that intercept messages during and after security setup
- In wireless LANs, man-in-the-middle attacks use evil twin access points to alter the functionality of the network
- An evil twin access point is simply a PC that has software to allow it to masquerade as an access point.

Wireless attacks

Evil twin access points

- The attacker sets up an evil twin access point outside the company's premises
- The attacker sets transmission power high because clients often associate with the access point that has the strongest signal
- If the victim wireless client is such a client, it will associate with the evil twin access point instead of with its legitimate access point
- The evil twin will then associate with the legitimate access point within the corporate walls, pretending to be the supplicant user
- This effectively puts it between the wireless client and the legitimate access point

Wireless attacks: Evil twin access points



Wireless Denial of Service

To prevent hosts from accessing a wireless network

Main three methods

- Flood the frequency
- Flood the access point
- Send attack commands

Wireless Denial of Service

Flood the frequency

- Wireless 802.11 networks transmit on 2.4-GHz and/or 5-GHz frequency bands
- Attackers can alter wireless devices to flood these frequency bands with radio frequency interference (RFI)
- The interference, or noise, damages the 802.11 signal and makes the packets unreadable
- Attackers can use common household items such as baby monitors, cordless phones, and Bluetooth devices to interfere with an 802.11 network
- Commercial wireless jamming appliances that can flood not only 802.11 frequencies, but cellular phone frequencies too
- Network administrators can use wireless spectrum analyzers to identify DoS floods

Wireless Denial of Service

Flood the access point

- Attackers can overwhelm an access point with too much traffic
- All of the hosts on a WLAN share access to the AP
- If an attacker continually sends an inordinate number of packets to the AP, all other hosts would be effectively denied access
- The AP uses all of its resources sending and receiving the attacker's packets
- An equally effective flooding method would be to send a very large file multiple times

Wireless Denial of Service

Send attack commands

- Takes advantage of the protocols implemented in the 802.11 standard
- An attacker sends attack commands to clients, APs, or both
- Many of these attack commands are actually 802.11 management or control frames used to manage the connection of hosts and transmission of signals
- For example, an attacker could use packet injection to send spoofed deauthenticate messages to the AP
- The spoofed source addresses would correspond to each wireless client on the WLAN
- The deauthenticate message says that the sender wants to terminate the authenticated connection

Wireless Denial of Service

Send attack commands (2)

- The victim must reauthenticate with the AP before it can communicate
- A continuous stream of spoofed deauthenticate messages could keep clients from connecting to the AP
- The attacker can send deauthenticate messages to wireless clients too
- An attacker could flood wireless clients with request-to-send (RTS) or clear-to-send (CTS) frames
- RTS frames tell other wireless clients that you want to transmit for a given amount of time (transmission duration)

Wireless Denial of Service

Send attack commands (3)

- CTS frames tell other clients that you have received a RTS frame, and that they should not transmit until the designated time expires
- A flood of CTS frames with long transmission durations keeps other clients waiting
- A flood of RTS frames produces a flood of CTS frames
- Both produce an effective DoS attack on the wireless network
- All these messages are not authenticated