WIRELESS SECURITY
Lecture 21

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

September 16, 2021

Source of some slides: **Missouri State University**, **University of Twente** and **University of Trento**

WHAT IS WiFi?

- WiFi stands for **Wi**reless **Fi**delity
- WiFi is a wireless technology that uses radio frequency to transmit data through the air
- It is also known as Wireless LAN (WLAN)
- It is based on IEEE 802.11
- IEEE established the 802.11 group in 1990
- Specifications ratified in 1997
- IEEE modified the standard in 1999 to include
  - 802.11b
  - 802.11a
  - 802.11g
- There are variants of 802.11 based on data rate, range and bandwidth

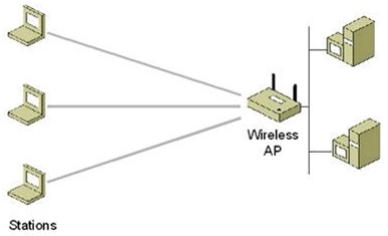
WLAN ADVANTAGES

- Freedom
  - You can work from any location that you can get a signal
- Setup cost
  - No cabling required
- Flexibility
  - Quick and easy to setup
- Scalable
  - Can be expanded with growth
- Mobile access
  - Can access the network on the move

WLAN DISADVANTAGES

- Speed
  - Slower than cable
- Range
  - Affected by various medium
  - Travels best through open space
  - Reduced by walls, glass and water
- Security
  - Greater exposure to risks
    - Eavesdropping
    - Unauthorised modification
    - Denial of Service (DoS)

WLAN COMPONENTS



- Wireless Station (STA)
  - A desktop, laptop PC, smartphone or other wireless device with a wireless 802.11 NIC (Network Interface Card)

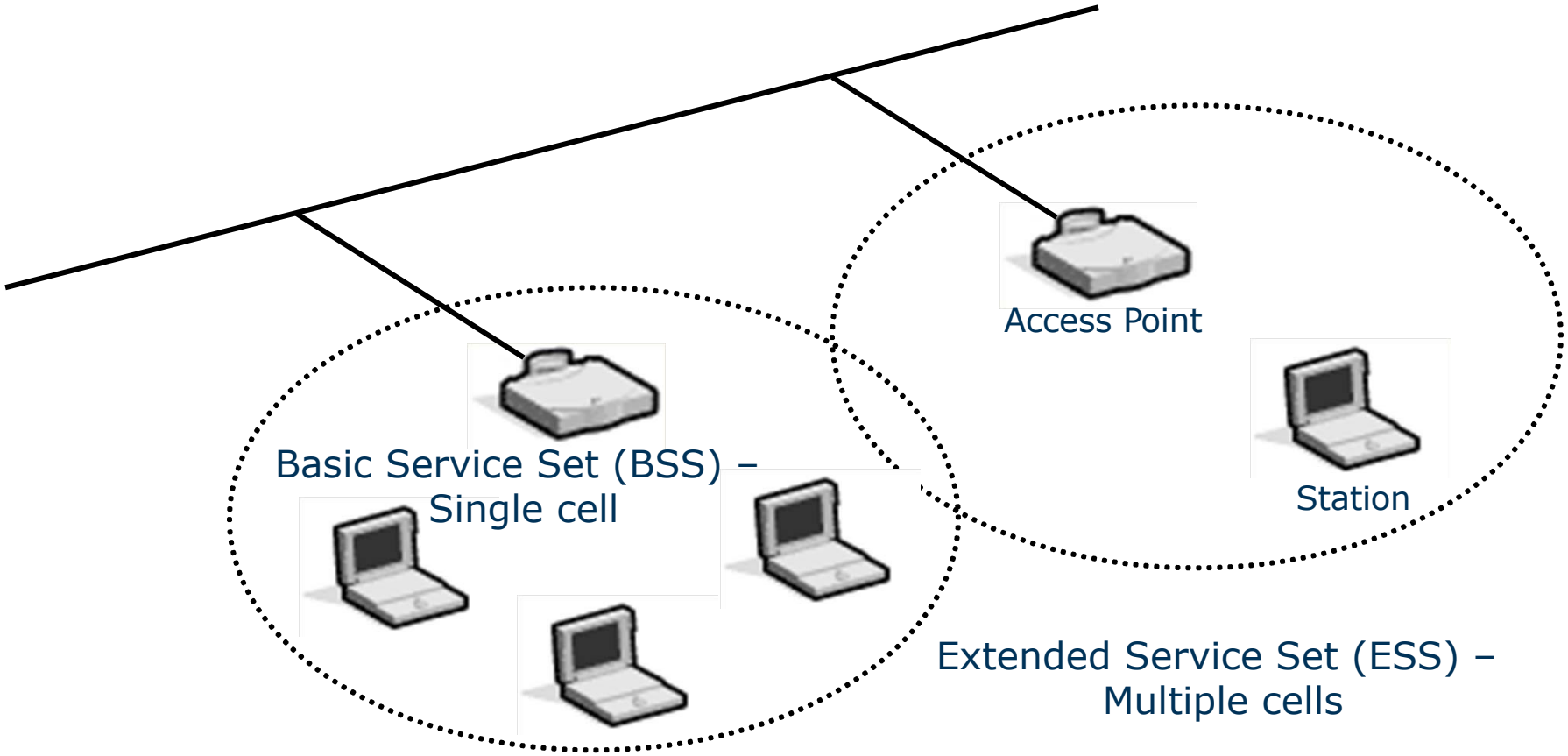
- Access Point (AP)
  - A bridge between wireless and wired networks
  - Composed of
    - Radio
    - Wired network interface (usually 802.3)
    - Bridging software
  - Aggregates access for multiple wireless stations to wired network

TWO WLAN MODES

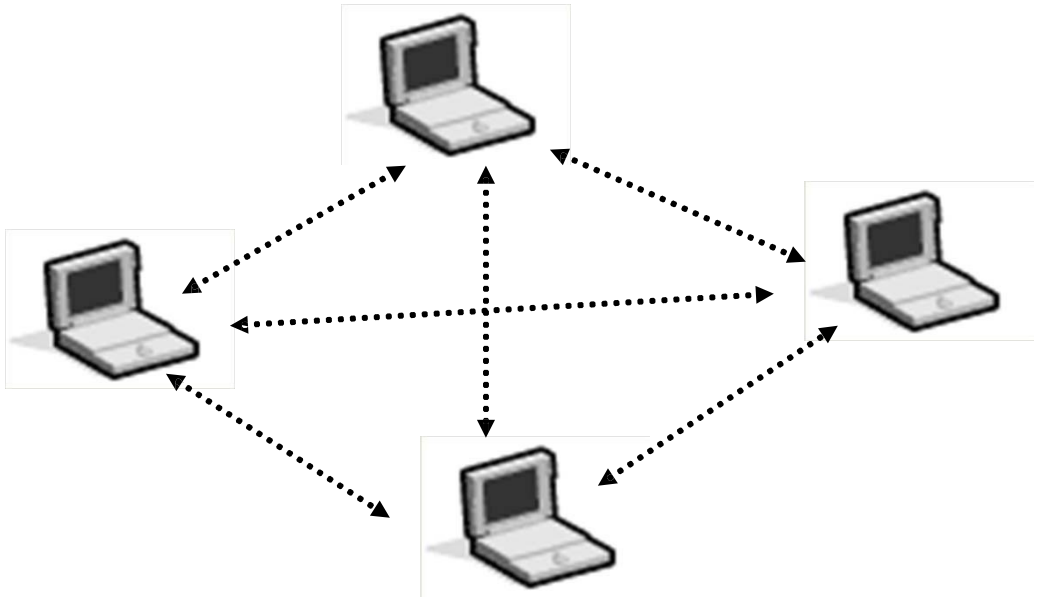
- Infrastructure mode
  - Basic Service Set (BSS)
    - One AP
  - Extended Service Set (ESS)
    - Two or more BSSes forming a single subnet
  - Most corporate LANs in this mode

- Ad-hoc mode
  - Independent BSS
  - Set of 802.11 wireless stations that communicate directly without AP
  - Useful for quick and easy wireless networks

INFRASTRUCTURE MODE



AD-HOC MODE



Independent Basic Service Set (IBSS)

CONNECTION AND SSID

- Before data can be transmitted, AP and STA must establish a connection
  - Scan for APs
  - Authentication and association
- A 32-octet Service Set Identifier (SSID) is a human readable identifier of the network

ACCESSING WLAN

- When STA enters range of one or more APs
  - STA probes for the channel
  - APs send beacons
  - AP beacon can include SSID
  - AP chosen on signal strength and observed error rates
- Periodically, all channels surveyed
  - To check for stronger or more reliable APs
  - If found, re-associates with new AP

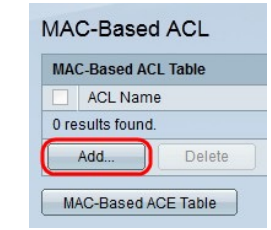
WLAN SECURITY MECHANISMS

- SSID based
  - Open mode
    - No security
  - Closed mode
    - No crypto
- MAC Access Control List (ACL)
- Wired Equivalent Privacy (WEP)
- WiFi Protected Access (WPA) and 802.11i
  - Actual standard for security in 802.11

SSID

- STA must specify SSID to AP when requesting association
- Multiple APs with same SSID form ESS
- Two modes
  - Open mode
    - APs broadcast their SSID
  - Closed mode
    - SSID is not broadcasted in beacons
    - Association requests from clients contains SSID in clear

MAC ACL



- Every network device has a unique Media Access Control (MAC) address
- MAC filtering only allows certain addresses access
  - Using Access Control List (ACL)
- Mostly for home use
- Issues
  - Masquerading
  - Tedious to implement on a large scale

WEP

- WEP is a protocol to protect link-level data during wireless transmission between STA and AP
- Original security solution offered by the IEEE 802.11 standard
- Security services
  - Authentication
  - Confidentiality
  - Integrity

WEP DETAIL

- A simple authentication protocol
- A pre-shared key K between all STAs and all APs
- Manual configuration of the pre-shared key K
- Uses RC4 encryption as cryptographic primitive with pre-shared keys and 24-bit initialisation vectors
- Uses CRC-32 for integrity protection

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!