Wireless Network Security

Wireless Basics

Uses Radio Frequency (RF) to communicate

- if same (or comparable) frequency is interfering, effect is *jamming*, also called *incidental interference*
- NICs have MAC addresses (48b, 6B)
- IEEE 802.11 max output is 200 mW
- Wireless Access Points (WAP)
- *Channel Width* - how much of the spectrum is tuned for this WAP
- WAPs traditionally radiate in all directions, and should be centrally located
- May require a *site survey* to make decisions on optimal WAP placement
- *Fat APs* are self-contained, while *Thin APs* are usually PoE and relay the same wireless signal

Major parts of a WAP:

- Antenna
- Transciever
- Bridging Software
- NIC

Security

> *"War Driving"* - the act of driving around, snooping for vulnerable access points

WEP Normally:

- 64b Key Length
- 24b IV

Can be enhanced with TKIP:

- 64b MIC (Message Integrity Check - HMAC) value
- 128b Key Length
- IV increased to 48b
- Passphrases are used to derive a shared master key
- session keys are derived from master key + MAC

WPA2

- AES-CCMP
  - AES-256 with 13 rounds
- WPA Personal is authenticated with PSK

EAP

- Four packet types: Request, Response, Success, Failure
- *Supplicant* sends identity information to *Authenticator*
- *Authenticator* is responsible for issuing EAP request packets

Captive Portal AP

802.1x Authentication

- Most secure is *certificate-based authentication*

BlueTooth

- Current version: 5
  - max-range: 800ft
- Vulnerable to *bluesnarfing* and *bluejacking*
  - snarfing - smell, jacking - uh…
- uses *short-range* radio
- *Personal Area Networks*
- make *piconets*
  - *active* and *parked* slaves
  - interconnected piconets form *scatternets*