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
- *Air Snort* - software for listening to packets, in "promiscuous mode"
- *Wireless LAN Controller* - Doohickey for figuring out how to control APs FIXME
  - uses Controller APs (thin APs)
- *Wireless AP Probes* - observe wireless traffic
  - Wireless device probes, dedicated probes, AP probes

Major parts of a WAP:

- Antenna
- Transciever
- Bridging Software
- NIC

Security

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

Wired Equivalent Privacy (WEP)

- Uses RC4
- can take only a few hours to crack, 4/5 million packets (due to weak IVs)

Normally:

- 64b Key Length (802.11 a and g extended to 152b)
- 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
- new key for every **packet**

Wi-Fi Protected Access (WPA)

WEP + TKIP

- lack of forward secrecy protection - if attacker knows WPA key, they can listen to *all* connections
- *Open-System Authentication* - session key based on SSID, issued to client

WPA2 - 802.11i

- Uses 802.1X for authentication
- AES-CCMP for encryption (Counter Mode with Cipher Block Chaining - Message Authentication Code Protocol)
  - AES-256 with 13 rounds
  - provides message integrity in AES
  - requires new hardware

PSK (Pre-Shared Key) vs Enterprise

- WPA Personal is authenticated with PSK, passphrase up to 63 characters, converted to 256b key
  - should be at least 20 chars
- WPA Enterprise uses 802.1X and RADIUS server
  - can integrate NAC

Captive Portal

- Uses HTTP to handle authentication (public hotspots)

Authentication Protocols

Extensible Authentication Protocol (EAP)

- Heritage from PPP
- Framework to secure the authentication process
- Four packet types: Request, Response, Success, Failure
- *Supplicant* sends identity information to *Authenticator*
- *Authenticator* is responsible for issuing EAP request packets
- Supports many authentication methods - tokens, smart cards, certs, one-time-passwords, public keys
- Wi-Fi Protected Setup (WPS)
  - 8-digit PIN - not secure
  - Push-button - secure

EAP-FAST (Flexible Authentication via Secure Tunneling)

- 2010, Cisco, replacement for LEAP (also Cisco)
- Passes a Protected Access Credential (PAC) to establish TLS, through which client creds are verified
- Uses both *passwords* and *tokens*, with TLS

EAP-TLS

- 2010, IETF
- one of the most secure
- Uses client-side certs

EAP-TTLS (EAP-Tunneled TLS)

- 2010
- Like EAP-TLS, but tunnels the client's authentication
- Allows secure use of legacy auth like
  - Password Authentication Protocol (PAP)
  - Challenge-Handshake Authentication Protocol (CHAP)
  - MS-CHAP, MS-CHAPv2
- Doesn't necessarily require client-side certs

802.1X Authentication

- Most secure is *certificate-based authentication*
- "port-based" authentication service
- When used over wireless, either 802.11i or EAP is used

RADIUS

- "Federated" logins

BlueTooth

- Current version: 5
  - max-range: 800ft
- Version 4: 24Mbps
- "Classic, High Speed, Low Energy" modes
- 2.4 GHz
- 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*

ANT

- Similar to bluetooth
- 2.4 GHz
- low chance of interference, great for clusters of devices