Lecture notes for wireless security

[Draw picture of node & internet cloud with last hop using wireless link]

Comparing wireless links to wired links

- Eavesdropping
  - ... on wired link requires physical access to wire
  - ... on wireless link only requires nearness
  - Wireless transmissions broadcast to all within range
- Access
  - ... to wired network requires physical access to network
  - ... to wireless network requires nearness
- Goal: make wireless links as secure / more secure than wired links

SSID non-broadcast

- Network identifier, e.g. GTwireless
- Attacker accessing wireless network must know SSID
- Normally broadcast
- If not broadcast, attacker can wait for a legit user to connect; beacon frame carries SSID in cleartext
- Prevents casual hacking

Of little use: MAC address filtering

- Allow only wireless adapters with whitelisted MAC addresses to connect
- Attacker can wait for legit user to connect; all frame headers carry user's MAC address in cleartext; attacker can change her address to that of user
- Prevents casual hacking

Primary encryption protocols

- WEP
- WPA
- WPA2

WEP (circa 1999) (Wired equivalent protocol)

- Confidentiality, integrity, authentication
- Encrypt network traffic
- [Draw frame: short 802.11 header, long data]
  - [Encapsulation: 802.11 header, IV, encrypted data, ICV(CRC)]
- Encryption uses RC4 algorithm
  - Weaknesses known in mid-1990s, WEP designed by non-cryptographers
- Key length: either 40 bits or 104 bits

WEP Problems

- One key... key reuse leads to easier cryptanalysis
- Short keys
- CRC is not a cryptographic integrity check
- IV space (24 bits) is too small, high probability of collision
  - Key sequences repeated every 16 million packets (2^24)
- No protection against replay of old data
- Use of crypto with known weaknesses
- ~ 100K packets (minutes) needed to crack 40-bit key

WPA (2002) (Wi-fi protected access)

- Subset of WPA2
- Uses TKIP (temporal key integrity protocol): wrapper around WEP
  - Expands IV space to 48 bits

WPA2 (2004)

- Full implementation of 802.11i standard
- Uses AES in counter mode
- Uses CBC-MAC for integrity

WPA/WPA2

1. Confirmation of association ability
2. Authentication: 802.1x or pre-shared key
3. 4-way handshake
4. Derivation of keys
5. Bulk encryption using TKIP (WPA) or AES (WPA2)

WPA Evaluation

- Home use: WPA-PSK (preshared key)
  - Attacks exist (google “wpa cracker”)
- Enterprise use: WPA + 802.1x, no attacks known

WPA2 Evaluation

- Home use: WPA2-PSK
  - Potentially insecure
- Enterprise use: WPA + 802.1x, very secure

Lots of tools available:

- Netstumbler, Kismet, Aircrack, Airodump

Why does GT use WEP?