Wireless Networks

Welcome to Wireless

• Radio waves
  – No need to be physically plugged into the network
  – Remote access

• Coverage
  – Personal Area Network (PAN)
  – Local Area Network (LAN)
  – Metropolitan Area Network (MAN)

• Security concerns
  – Radio signals leaking outside buildings
  – Unauthorized devices
  – Verification of users
  – Intercepting wireless communications
  – Man-in-the-middle attacks
Types of Wireless Networks

- **Infrastructure**
  - Client machines establish a radio connection to a special network device, called access point
  - Access points connected to a wired network, which provides a gateway to the internet
  - Most common type of wireless network

- **Peer-to-peer**
  - Multiple peer machines connect to each other
  - Typically used in ad-hoc networks and internet connection sharing

SSID

- **Multiple wireless networks can coexist**
  - Each network is identified by a 32-character service set ID (SSID)
  - Typical default SSID of access point is manufacturer’s name
  - SSIDs often broadcasted to enable discovery of the network by prospective clients

- **SSIDs are not signed, thus enabling a simple spoofing attack**
  - Place a rogue access point in a public location (e.g., cafe, airport)
  - Use the SSID of an ISP
  - Set up a login page similar to the one of the ISP
  - Wait for clients to connect to rogue access point and authenticate
  - Possibly forward session to ISP network
  - Facilitated by automatic connection defaults
Eavesdropping and Spoofing

- All wireless network traffic can be eavesdropped
- Wireless access point (AP) manages link layer of protocol stack
- IEEE 802.11 standard connection management:
  - Authentication and Association frames
  - Dissociation and Deauthentication frames
  - Re-association frames
- MAC-based authentication typically used to identify approved machines in corporate network
- MAC spoofing attacks possible, as in wired networks
  - Sessions kept active after brief disconnects
  - If ISP client does not explicitly end a session, MAC spoofing allows to take over that session

Captive Portal

- Protocol
  - DHCP provides IP address
  - Name server maps everything to authentication server
  - Firewall blocks all other traffic
  - Any URL is redirected to authentication page
  - After authentication, regular network services reinstated
  - Client identified by MAC address
  - Used by wireless ISPs
- Security issues
  - A MAC spoofing and session stealing attack may be performed if client does not actively disconnect
  - A tunneling attack can bypass captive portal if (DNS) traffic beyond firewall is not blocked before authentication
Wardriving and Warchalking

- Driving around looking for wireless local area networks
- Some use GPS devices to log locations, post online
- Software such as NetStumbler for Windows, KisMac for Macs and Kismet for Linux are easily available online
- Use antennas to increase range
- Legality is unclear when no information is transmitted, and no network services are used
- Warchalking involves leaving chalk marks (derived from hobo symbols) on the side walk marking wireless networks and associated information

Wired Equivalent Privacy

- Goals
  - Confidentiality: eavesdropping is prevented
  - Data integrity: packets cannot be tampered with
  - Access control: only properly encrypted packets are routed
- Design constraints
  - Inexpensive hardware implementation with 90's technology
  - Compliance with early U.S. export control regulations on encryption devices (40-bit keys)
- Implementation and limitations
  - Encrypts the body of each frame at the data-link level
  - Fit within IEEE 802.11 communication standard
WEP Protocol

• Setup
  – Access point and client share 40-bit key K
  – The key never changes during a WEP session

• Encryption
  – Compute CRC-32 checksum of message M (payload of frame)
  – Pick 24-bit initialization vector V
  – Using the RC4 stream cipher, generate key stream S(K,V)
  – Create ciphertext
    \[ C = (M \ || \ \text{crc}(M)) \oplus S(K,V) \]

• Client authentication
  – Access point sends unencrypted random challenge to client
  – Client responds with encrypted challenge

• Transmission
  – Send \( V \ || \ C \)

Message Modification Attack

• Message modification
  – Given an arbitrary string \( \Delta \), we want to replace message M with \( M' = M \oplus \Delta \)
  – Man-in-the-middle replaces ciphertext C with \( C' = C \oplus (\Delta \ || \ \text{crc}(M) \oplus \text{crc}(M')) \)

• Targeted text replacement
  – Possible if we know position of text in message
  – E.g., change date in email

• Reason of vulnerability
  – CRC checksum commutative with XOR
  – Insufficient encryption: stream cipher allows malleability
Reused Initialization Vectors

- Repeated IV implies reused key stream
  - Attacker obtains XOR of two messages
  - Attacker can get both messages and the key stream
  - Recovered key stream can be used by attacker to inject traffic
- Default IV
  - Several flawed implementations of IV generation
  - E.g., start at zero when device turned on and then repeatedly increment by one
- Random IV
  - Small length (24 bits) leads to repetition in a short amount of time even randomly generated
  - E.g., collision expected with high probability after \(2^{12} \approx 4,000\) transmissions

Authentication Spoofing

- Attacker wants to spoof a legitimate client
  - Does not know the secret key \(K\)
  - Can eavesdrop authentication messages
- Attack
  - Obtain challenge \(R\) and encrypted challenge \(C = (R \mid \text{crc}(R)) \oplus S(K,V)\)
  - Compute key stream \(S(K,V) = (R \mid \text{crc}(R)) \oplus C\)
  - Reuse key stream \(S(K,V)\) when challenged from access point
DEMO: WARDRIVING AND WEP CRACKING

3/10/2012 Wireless Networks 13

Wardriving Tools

• Netstumbler wifi scanner

• Antenna for db gain

• Wireless card with plug and monitor mode

• GPS (optional)
Wireless Networks

Wardriving Setup

- The access point and client are using WEP encryption
- The hacker is sniffing using wardriving tools

Slow Attack: WEP Sniffing

- To crack a 64-bit WEP key you can capture:
  - 50,000 to 200,000 packets containing Initialization Vectors (IVs)
  - Only about ¼ of the packets contain IVs
  - So you need 200,000 to 800,000 packets
- It can take a long time (typically several hours or even days) to capture that many packets
Initialization vector (IV)

- One for each packet, a 24-bit value
- Sent in the cleartext part of the message!
- Small space of initialization vectors guarantees reuse of the same key stream
- IV Collision:
  - Attack the XOR of the two plaintext messages
  - IV is often very predictable and introduces a lot of redundancy

Wi-Fi Protected Access (WPA)

- WEP became widely known as insecure
  - In 2005, FBI publically cracked a WEP key in only 3 minutes!
- Wi-Fi Protected Access (WPA) proposed in 2003
- Improves on WEP in several ways:
  - Larger secret key (128 bits) and initialization data (48 bits)
  - Supports various types of authentication besides a shared secret, such as username/password
  - Dynamically changes keys as session continues
  - Cryptographic method to check integrity
  - Frame counter to prevent replay attacks
WPA2

• WPA was an intermediate stepping-stone
  – Final version: IEEE 802.11i, aka WPA2
• Improvements over WPA are incremental rather than changes in philosophy:
  – Uses AES instead of RC4
  – Handles encryption, key management, and integrity
  – MAC provided by Counter Mode with Cipher Block Chaining (CCMP) used in conjunction with AES
• WPA2 needs recent hardware to operate properly, but this will get better over time

Alternatives and Add-Ons

• WEP, WPA, and WPA2 all protect your traffic only up to the access point
  – No security provided beyond access point
• Other methods can encrypt end-to-end:
  – SSL, SSH, VPN, PGP, and so on
• End-to-end encryption is often simpler than setting up network-level encryption
• Most of these solutions require per-application configuration