CSC 574
Computer and Network Security

Wireless Security

Alexandros Kapravelos
kapravelos@ncsu.edu

(Derived from slides by Giovanni Vigna)

Wireless Networks

- Wireless networks allow to exchange network packets over a radio link
- Protocols are defined in the 802.11 standard series
- 802.11 supports bit rates up to 2 Mbps
- 802.11b-g provides bit rates up to 11 Mbps (2.4 GHz band)
- 802.11a provide bit rates up to 54 Mbps (5 GHz band)
- 802.11n uses both 2.4GHz and 5GHz bands for a bit rate of 600 Mb/s
- 802.11ad provides bit rates up to 6.75 Gb/s (60 GHz band)

802.11 Data Link Layer

- Logical Link Control (LLC) layer shared with other 802 lans (48-bit addresses)
- Different Media Access Control (MAC)
  - Wired Ethernet uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
  - Near/far problem radio transmission does not allow a station to listen for collisions
    - Stronger signals make weaker signals become noise
  - WLAN: Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

CSMA/CA

- Station A waits for “no activity”
- Station A waits for a random amount of time
- Station A starts sending
- Station B sends an ACK
- If station A does not receive a valid ACK
  - It assumes that the packet was lost or the ACK was lost
  - The packet is retransmitted after a random amount of time
- Robustness features
  - Ready To Send/Clear To Send (RTC/CTS)
  - CRC checksums

Modes of Operation

- Infrastructure mode
  - Wireless access point (AP) connected to wired network
  - Mobile stations with wireless cards
- Ad hoc mode
  - Mobile stations with wireless cards
  - Traffic not directed to in-range hosts must be routed by a mobile station

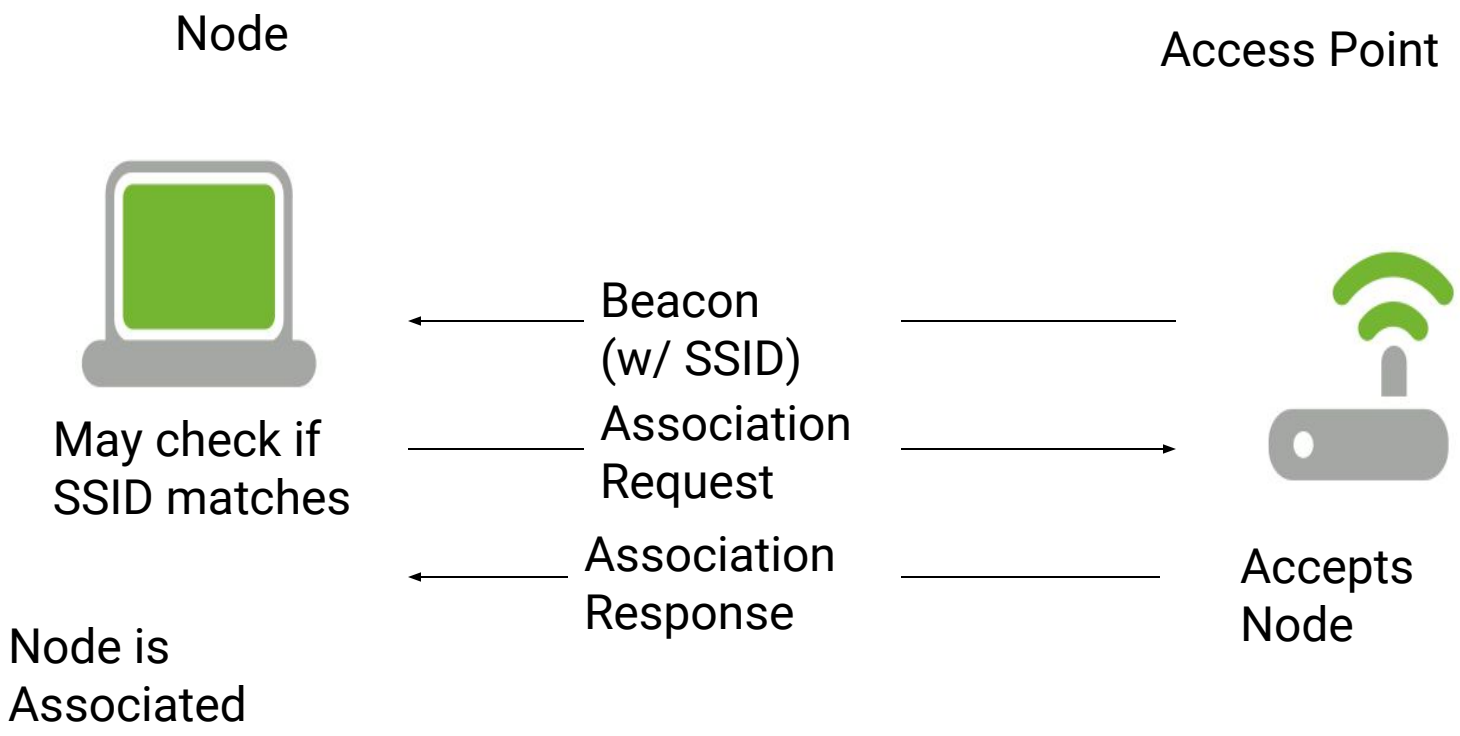
Type of Frames

- Management frames
  - Authentication frames
    - Open networks require a simple request-response
    - Networks protected by shared-key authentication require a number of steps in order to authenticate the client
  - Deauthentication frames
  - Association request/response frames
  - Disassociation frames
  - Beacon frames
  - Probe request/response frames
- Control frames
  - RTS/CTS frames
  - ACK frames
- Data frames

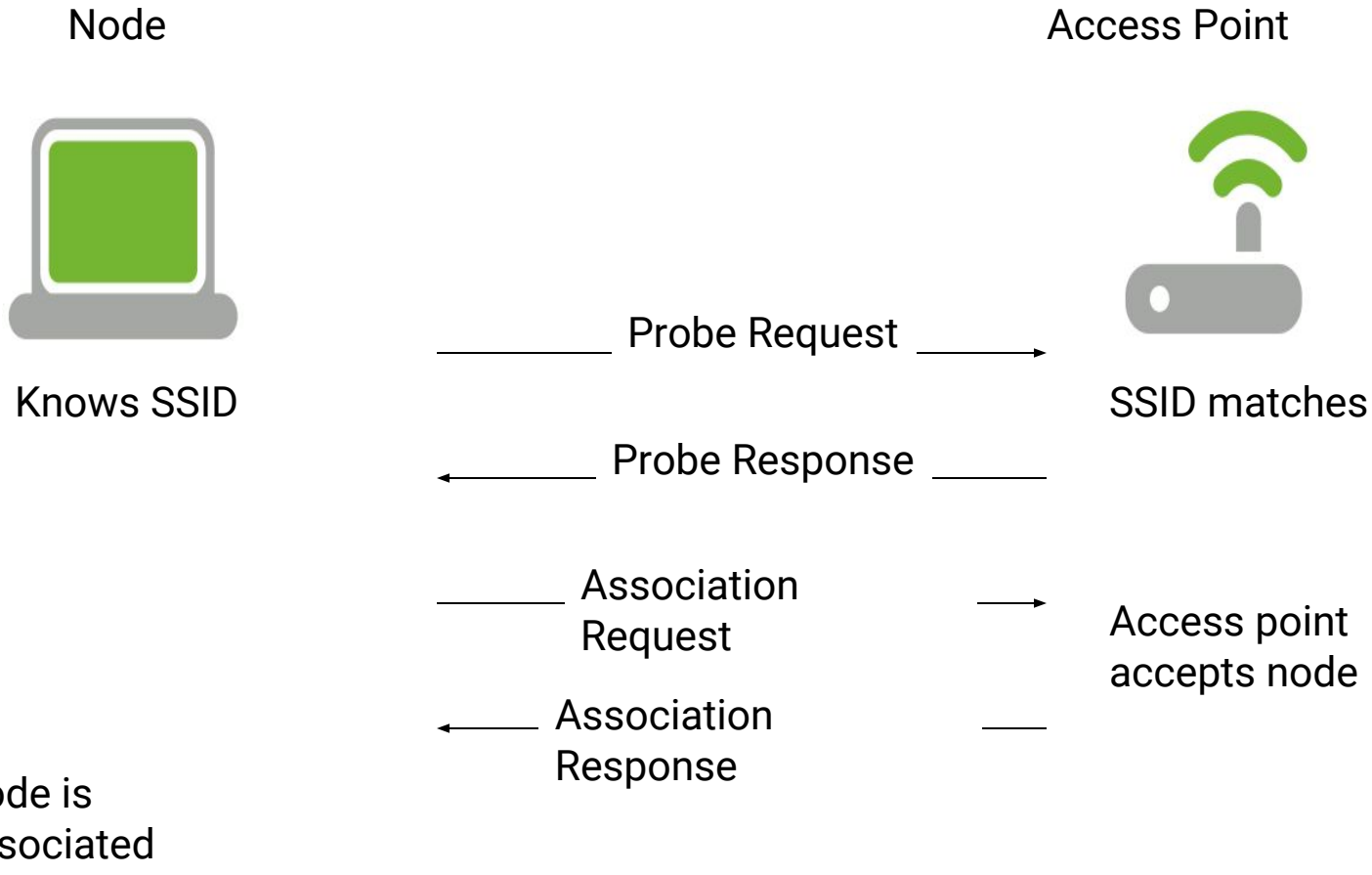
Association

- Clients (also called “stations”) associate with an access point (AP)
- Access points are identified by a service set identifier (SSID)
- When a mobile station enters the transmission range of one or more APs it will connect to the station with the strongest signal (and lowest observed error rate)
- Periodically it will scan the network for better APs
- MAC Access Control Lists can be used to regulate which stations can associate with an AP

Discovery - Open Network



Discovery - Closed Network



Wired Equivalent Privacy

- Wired Equivalent Privacy (WEP) is a series of mechanisms to provide security
- Encryption with shared-key can be used to encrypt traffic
  - RC4 with 40-bit or 104-bit static key, 24-bit IV in the clear
- This protocol was broken

WPA

- Wi-Fi Protected Access (WPA) was introduced to solve the security problems associated with WEP
  - Implements a subset of the 802.11i standard
  - Relies on TKIP (Temporal Key Integrity Protocol) which uses a per-packet key
    - Secret key and initialization vector for RC4 are composed in a complex way and not simply juxtaposed
    - Keys are routinely changed
    - A sequence number is added to prevent replay attacks
    - Introduces a message integrity check that is better than WEP's CRC
- WPA supports authentication mechanisms, such as 802.1X - EAP/Radius
- WPA does not rely on additional hardware and therefore can be used on hardware that supports WEP

WPA2

- A number of vulnerabilities have been found in WPA
  - See for example: M. Vanhoef and F. Piessens “Practical Verification of WPA-TKIP Vulnerabilities” in Proceedings of ASIACCS, 2013
- WPA/TKIP was deprecated by IEEE in 2009
- WPA2 is the evolution of WPA implements the full 802.11i standard
- Requires new hardware
- Uses AES instead of TKIP
- Supports both pre-shared key (PSK) and extended authorization (802.1X - EAP/RADIUS)

802.1x

- 802.1x provides “per-port authentication”
- The “supplicant” (mobile station) requests a connection to a “network port” on the “authenticator” (access point)
- The authenticator connects to an “authentication server” to verify the credentials of the user (e.g., using RADIUS)

Attacks Against Wireless Networks

- Wireless traffic sniffing
- Wireless network detection
  - Closed networks
- Injection attacks
  - Denial of service
  - Man in the middle
- WEP attacks
  - Stream reuse attacks
  - WEP traffic generation
  - Brute force attacks
  - FMS attack

Wireless Traffic Sniffing

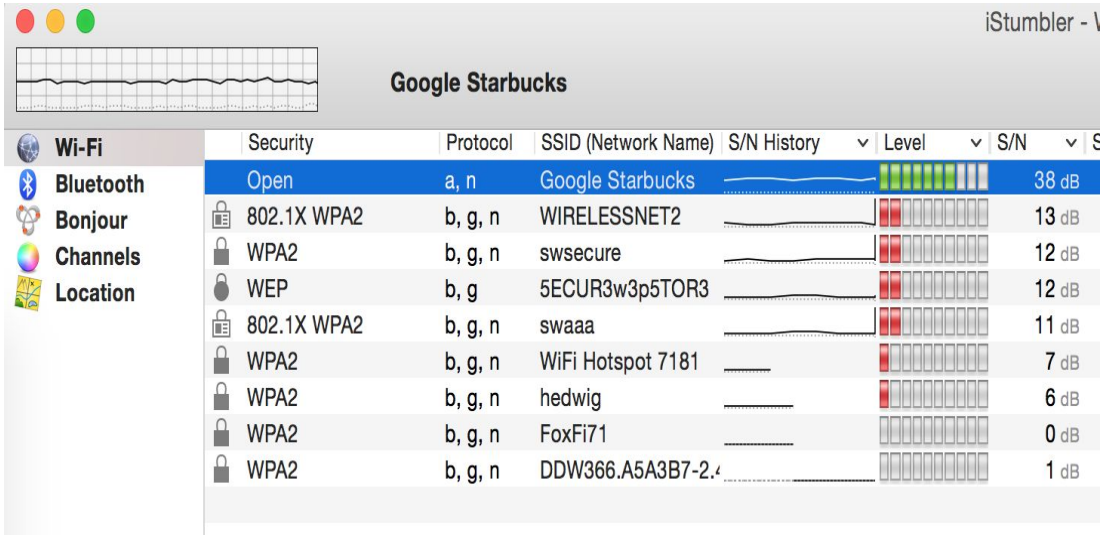
- Traffic in an open wireless network is particularly vulnerable to eavesdropping
  - No physical access is necessary (the “Parking lot attack”)
- Even when using encryption, source and destination MAC addresses are accessible
  - May be used to bypass MAC access control lists at another AP, configured differently (e.g., no encryption)
  - May be used to perform traffic flow analysis

Monitor vs. Promiscuous

- In promiscuous mode the 802.11 headers are removed and only the packets transmitted by the AP with whom the client is associated are passed on by the driver
- In order to observe all traffic (including management frames) the network card must be able to be in monitor mode (RFMON)
  - When in monitor mode, the card cannot send traffic

Wireless Network Detection

- Monitor Mode Protocol Analysis
  - Card set to monitor mode
  - Sniffs beacons and probes
  - Allows one to detect closed APs
  - Allows one to detect wireless nodes



Detecting Closed Networks

- Analyze probe responses from APs that are replies to probe requests from valid nodes
  - Probe requests are sent out roughly every 10 minutes
- Probe requests can be forced using a disassociation attack
  - Attacker sends spoofed disassociation frame pretending to be the AP
  - The disassociated station tries to connect again and sends a probe message (containing the SSID)

Denial of Service

- Wireless networks are particularly vulnerable to denial-of-service attacks
- One can send a disassociation request to nodes on a wireless network and continue to send disassociation messages whenever they re-associate
- One can use radio interference to make the wireless network unusable

Man-in-the-Middle Attacks

- There are two main ways to perform a man-in-the-middle attacks:
  - By performing ARP spoofing once associated with an AP
  - By deauthorizing a victim host
    - Attacker becomes an AP with the same SSID on a different channel
    - Attacker de-authorize victim
    - Victim reconnects to fake AP
    - Attacker relays frames back and forth

WEP Encryption

- A shared secret key K (40 or 104 bits) and a public IV (24 bits) are used to generate a stream of pseudo-random bits using RC4
- The message includes a CRC code computed on the plain text part of the message
- The stream is XORed with the message
- The message and the IV are sent to the receiver
  - A different IV is used every time
- At the receiving end, the IV is used to generate the same bit stream, which is then XORed with the encrypted message

WEP Attacks

- Brute Force
  - Brute forcing a 40-bit key is feasible
- Key stream reuse
  - If a key stream is reused, it is possible to obtain the XOR of two plaintext messages
    - (M1 ^ Si) ^ (M2 ^ Si) = M1 ^ M2 ^ Si ^ Si = M1 ^ M2
  - If one of the messages is known, it is possible to derive the other or the key stream for the IV,K used
    - The Shared Key Authentication mechanism worked by providing a plaintext challenge that the client had to encrypt to prove that he knew the password
    - This allowed one to collect that particular cipher stream
- Weak integrity check
  - Because the CRC is computed on the plaintext it is possible to modify the ciphertext without breaking the CRC

FMS Attack

- Fluher, Mantin, and Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”
  - Due to a flaw in the way the RC4 algorithm turns the “secret key” (4-256 bits) into a key stream, weak keys can be produced
    - A weak key is one that produce a (more) predictable set of bytes in the initial rounds of the stream generation
  - Collecting enough traffic allows one to recover the original RC4 key
- Stubblefield, Ioannidis, and Rubin, “Using the Fluher, Mantin, and Shamir Attack to break WEP”
  - First implementation of the attack
  - Demonstrates that key can actually be recovered using 4,000,000 to 6,000,000 packets
- Attack made available in a number of tools

Improvements to the FMS Attack

- In 2004 KoreK found that encrypted packets could be chopped and re-injected to discover the key faster
  - Required 500,000 to 2,000,000 packets
- In 2005, Andreas Klein discovered that there were more vulnerabilities in the way RC4 is used in WEP
  - A group of researcher at Darmstadt improved Klein's attack (this was called the TPW attack)
- In 2006, Andrea Bittau found ways to use link-level fragmentation to inject traffic without having to obtain the secret password

Traffic Generation To Help WEP Cracking

- The Caffe Latte approach was introduced to force the generation of traffic
  - Pretends to be a WEP-enabled AP with the SSID of a previously-joined AP
  - Records encrypted gratuitous ARP packets sent by client at connection
  - Modifies the ENCRYPTED packet so that it becomes an ARP request
  - Re-injects the packet and create the traffic
- Allows one to recover a 108-bit key in around six minutes

WEP Attack Countermeasures

- Closed Mode
- MAC Filtering
- Use Weak IV Filtering Hardware
- Keys Rotation

Closed Mode

- Strengths
  - Doesn’t send out any beacon frames (more difficult to detect)
  - Requires connecting nodes to supply the correct SSID in order to associate
- Weaknesses
  - AP can still be detected through sniffing probe requests and responses

MAC Filtering

- Strengths
  - Allows one to control which MAC addresses can associate with an access point
- Weaknesses
  - MAC addresses can be easily spoofed
  - One can easily determine which MAC addresses are allowed by monitoring activity on the network
  - Attackers can still monitor communications
  - One can easily brute force MAC addresses

Weak IV Filtering Hardware

- Strengths
  - It requires much more time for an attacker to crack the WEP key
- Weaknesses
  - An attacker can still crack the WEP key given enough time

Change Keys Frequently

- Strengths
  - Makes it more difficult for attackers to crack WEP
  - Even if an attacker cracks a key, they will only have access for a limited amount of time
- Weaknesses
  - With traffic generation, an attacker can crack a key in a reasonable amount of time
  - Attackers can still decrypt collected traffic using cracked keys

WPA2 Attack

- WPA2 does not have known serious vulnerability
- It is still open to a password guessing attack
- The attacker de-authenticate a connected user
- The user re-authenticate using a four-step handshake containing the encrypted password
- The four handshake is recorded and used offline to try a number of passwords (dictionaries, random permutation, etc.)

4-way Exchange

- Both Client and AP know a Password Master Key (PMK), derived by the PSK (Pre-Shared Key)

1. The AP sends to the client an Anonce
2. Client derives the Pairwise Transient Key (PTK) from Anonce, Snonce, and PMK and sends the Snonce protected by a Message Integrity Code (MIC) calculated using the PTK
3. AP also calculates the PTK and verifies the MIC. Then the AP sends the Group Transient Key (GTK) encrypted with the a subkey of the PTK
4. The Client receives the GTK and sends an acknowledgment

Wardriving

- Term that denotes the practice of driving around looking for open access points
- Pun on “wardialing”, which is the practice of trying a large number of telephone number looking for modems/terminal servers (see “Wargames” -- the movie)
- Equipment
  - Laptop with wireless card (and possibly external antenna)
  - GPS device to provide geographical information

Detecting Wardrivers

- Wardrivers can be detected by recognizing specific wardriving tool signatures
  - Kismet has a module to detect NetStumbler probes
- Wardrivers can be detected by identifying a suspiciously high number of probes
- Passive detection cannot be detected
- The position of wardrivers can be determined using triangulation techniques on the strength of the signal