Lecture 11: WiFi Security

Stephen Huang

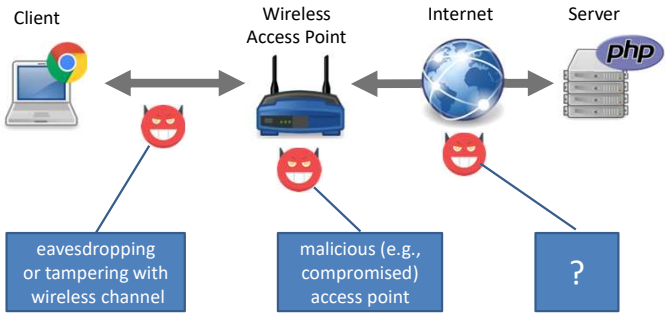
Content

1. Introduction to Security Protocol
2. IEEE 802.11 Standard
3. Wireless Security
4. WEP

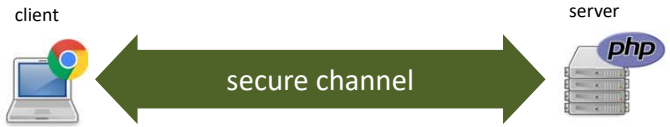
IEEE 802.11 specifies technical standard for implementing Wireless LAN (WLAN) computer communication.

1. Security Protocol

- Communication Threats in Practice



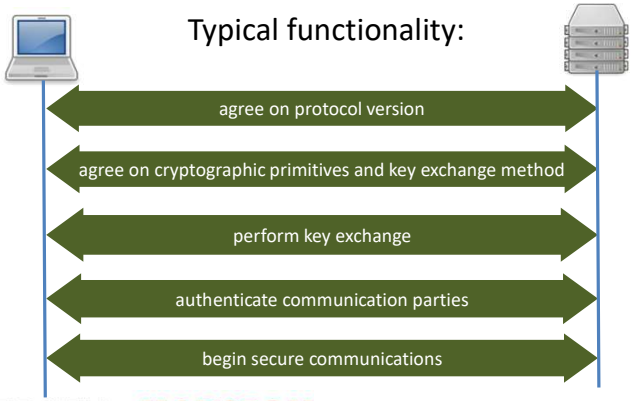
Security



How can devices, software products, etc. from different vendors, manufacturers, etc. communicate with each other?

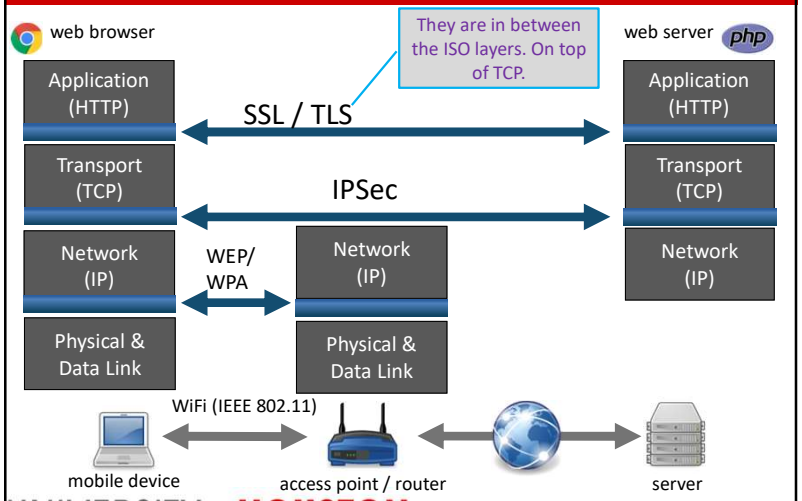
Security Protocols

- Standard security protocols specify messages, data structures, and the usage of cryptographic primitives to provide interoperability.



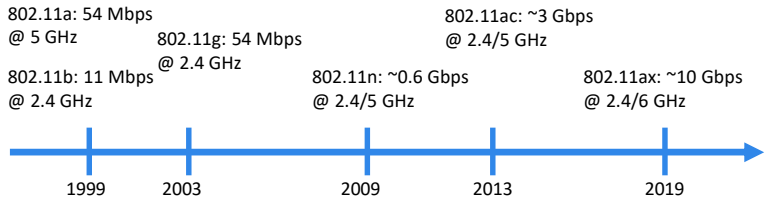
Communication in Practice

Protocol Stack in Practice



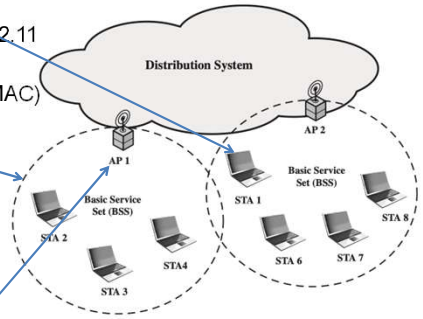
2. IEEE 802.11 Standard

- IEEE 802.11: set of standards for wireless local area networks (WLANs). It was accepted by ISO/OSI as standard.
- Wi-Fi Alliance
  - non-profit organization of companies, certifies devices for interoperability
  - WiFi = WLAN based on 802.11 standard



IEEE 802.11 Network Components

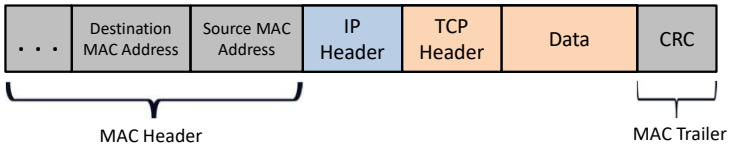
- Station (STA)
  - any device using IEEE 802.11
  - interface identified by a medium access control (MAC) address
- Basic Service Set
  - set of stations executing the same medium access control protocol
  - identified by a service set identifier (SSID)
- Access Point (AP)
  - has station functionality and provides access to the distribution system



MAC

- A media access control (MAC) address is a computer's unique identification number used by the network.
- MAC addresses are hardcoded into the Network Interface Card (NIC) when it's manufactured.
- The MAC is globally unique, so two devices can't have the same MAC address.
- MAC is represented in a hexadecimal format like this: `00:0a:45:2e:52:28`.
- Applications: MAC filtering (white-listing), MAC masking (black-listing).
- MAC Address Spoofing.
- MAC address randomization (iOS) can be used to prevent device tracking..

IEEE 802 Frame



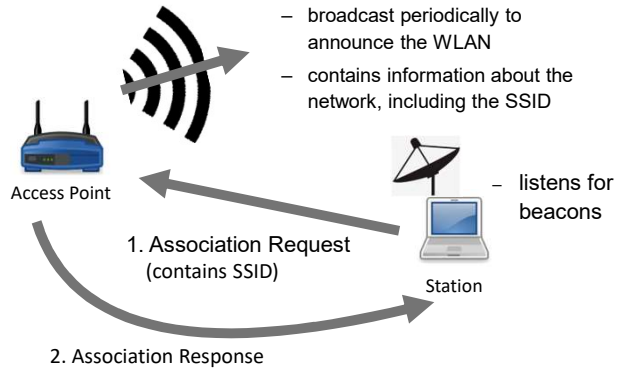
Medium Access Control (MAC) frame format:

- Destination MAC address: destination's physical address on the LAN.
- Source MAC address: source's physical address on the LAN.
- MAC Service Data Unit: data from higher laye.
- CRC: cyclic redundancy check field for transmission error detection.

IEEE 802.11 Beacons and Association

Beacon:

- broadcast periodically to announce the WLAN
- contains information about the network, including the SSID

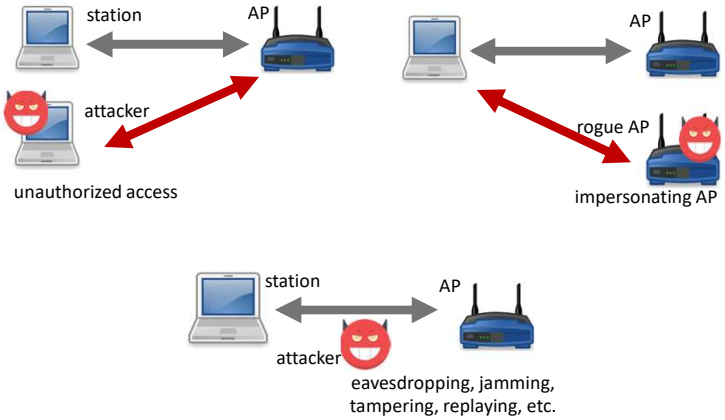


3. Wireless Security

Problem: no inherent physical protection

- Joining a network does not require physical access.
- Radio transmissions are broadcast → Anyone in range can eavesdrop.
- Injecting new messages or replaying old messages is possible.
- Jamming attacks against availability.
- Jamming and injecting messages can be combined into tampering attacks.

Security Challenges



Access Control: Hidden SSID

- SSID: Service Set Identifier, a network's name.
- The association request must contain the network's SSID. By default, the AP broadcasts it periodically in the beacon.
- AP may be configured to stop announcing the SSID. SSID may be used as a "password".
- However,
  - SSID must be hard to guess.
  - every authorized user must know the SSID.
  - SSID can be easily eavesdropped whenever an authorized station connects to the network. It does not provide any security.
  - Tools are available for eavesdropping.

https://www.aircrack-ng.org/

Access Control: MAC Address-Based Filtering

- AP may be configured to allow only devices with certain MAC addresses to connect.
  - MAC addresses of all authorized devices must be registered in advance.
- However,
  - MAC address is sent in plaintext in every packet
  - Many WLAN devices allow their MAC addresses to be changed. An attacker can easily impersonate an authorized user.
- *Example*: changing MAC address of macOS

```
$ sudo ifconfig en0 ether 6c:40:aa:11:22:33
```

IEEE 802.11 Security Standards

- WEP (Wired Equivalent Privacy)
  - introduced in 1997 as part of the original 802.11 standard
  - shown to be insecure in 2001
- WPA (WiFi Protected Access)
  - introduced in 2003, as a quick fix to WEP
  - subset of draft IEEE 802.11i
- WPA-2 (IEEE 802.11i)
  - standardized in 2004
- WPA-3
  - announced in 2018
  - very similar to WPA-2

4. WEP

- How not to design a security protocol…
- WEP: Wired Equivalent Privacy (IEEE 802.11)

Wired Equivalent Privacy (WEP)

- Goal: Making WiFi at least as secure as wired networks.
  - Not a very ambitious goal, but fell short of even this goal …
- Design overview
  - Security is based on a 40- or 104-bit **secret key**
    - WiFi "password" shared by all users
  - **Confidentiality**: RC4 stream cipher
    - The key is extended by a 24-bit IV, which is changed for each message → used as a nonce to prevent key reuse problems
  - **Integrity**: encrypted CRC32 (Cyclic Redundancy Check) checksum.
  - **Access control**: challenge-response between AP and station.

WEP Design Flaws

- Authentication
  - One-way authentication (only for the station to AP), AP can be impersonated.
- Integrity Protection
  - Based on error-detection code (CRC32) instead of cryptographic hash → forging authentication tags is trivial.
  - No message replay protection.
- Key usage
  - No session key: long-term key used for all purposes (authentication, encryption, integrity protection).
  - Short nonce (i.e., 24-bit IV) → danger of key reuse for stream cipher
    - busy network with 1000 packets per second reuses in less than 5 hours.

Fluhrer-Mantin-Shamir Attack (2001)

- The attacker knows the first three bytes of RC4 key (i.e., the 24-bit IV).
- Due to RC4 weaknesses, attacker can guess the 4th key byte (i.e., 1st secret byte) correctly with a probability of ≈ 0.58% using a single ciphertext-plaintext pair.
  - random guess should be correct only with probability = 1/256 ≈ 0.39%
- With enough ciphertext-plaintext pairs, an attacker can discover the 4th key byte (with probability ≈ 100%)
- Then, the attacker can discover the 5th, 6th, … bytes using the same approach (i.e., 2nd, 3rd, … secret bytes)
- In practice, WEP keys can be broken in a matter of minutes (or less) → WEP is not secure
  - easy to use tools for breaking WEP are available

Lessons Learned from WEP

- Aiming for mediocre security will likely result in no security.
- Follow design principles (or face the consequences)
  - do not use error-detection codes for message authentication.
  - use session keys for data encryption and authentication.
- …
- Do not use WEP!
- Problem: WEP needed to be replaced very quickly in 2001
  - existing devices (e.g., access points, wireless interface cards) had hardware support only for WEP (e.g., for RC4)
  - many networking devices had low computational performance

IEEE 802.11 Security Standards

- WEP (Wired Equivalent Privacy)
  - introduced in 1997 as part of the original 802.11 standard
  - shown to be insecure in 2001
- WPA (WiFi Protected Access)
  - introduced in 2003, as a quick fix to WEP
  - subset of draft IEEE 802.11i
- WPA-2 (IEEE 802.11i)
  - standardized in 2004

WiFi Protected Access (WPA)

Standard: 802.11i TKIP (Temporal Key Integrity Protocol)

- Design goals: fix the flaws of WEP and be compatible with legacy hardware
- Overview
  - key usage: the session key is established during a secure two-way authentication
  - confidentiality: RC4 encryption, but with 48-bit IV, which is mixed thoroughly with the session key and source MAC address
    - prevents key reuse and the Fluhrer-Mantin-Shamir attack
  - integrity: 64-bit message integrity codes computed using Michael, which is computationally very efficient but provides only ~20 bits of effective security
    - after the wrong code, the station is banned for a minute and needs to re-authenticate
- Deprecated in later revisions of the standard

Next Topic

- Protocol, WiFi Security
- WPA2 and IP Security
- Transportation Layer Security