CSC429 – Computer Security

LECTURE 13
WIRELESS SECURITY

Mohammed H. Almeshekah, PhD
meshekah@ksu.edu.sa

Wireless Security

WiFi Protected Access (WPA)

Improving 802.11 Security

- The IEEE 802.11 community has responded to the many security problems identified in WEP.
- Intermediate solution: Wi-Fi Protected Access (WPA).
- Longer-term solution: WPA2.

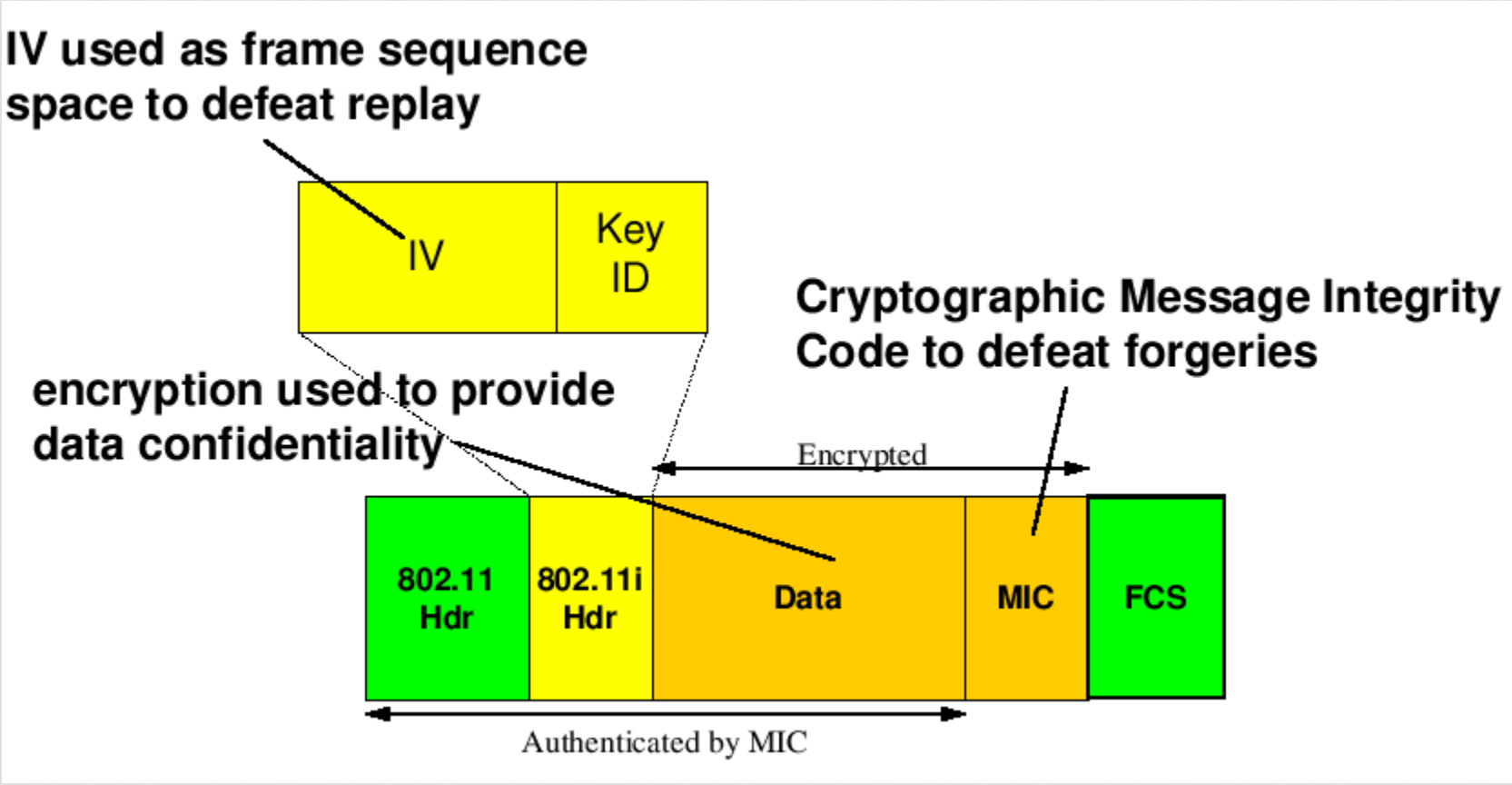
WPA

- Wi-Fi Protected Access (WPA)
  - An intermediate solution to address WEP's problems.
  - Existing hardware can still be used; only firmware upgrade needed.
- WPA introduced new authentication protocol, improved integrity protection measure and per-packet keys.
  - To provide stronger authentication than in WEP.
  - To prevent spoofing attacks:
    - An attack of "bit flipping" on WEP CRC.
  - To prevent FMS-style attacks.

WPA – TKIP

- WPA introduced TKIP: Temporal Key Integrity Protocol.
  - TKIP uses a 128-bit per packet encryption key.
    - Derived from: Pairwise Transient Key (PTK), MAC addresses, 48-bit TKIP sequence counter (TSC).
    - PTK itself is derived from PMK, MAC addresses and nonces exchanged during authentication protocol.
  - TKIP introduces a special-purpose 8-byte MAC algorithm called "Michael" to replace WEP's CRC.
    - A MAC algorithm with 64-bit keys derived from PTK.

WPA – TKIP


IV used as frame sequence space to defeat replay
IV
Key ID
Cryptographic Message Integrity Code to defeat forgeries
encryption used to provide data confidentiality
Encrypted
802.11 Hdr
802.11i Hdr
Data
MIC
FCS
Authenticated by MIC

WPA – Authentication Protocol

- WPA also introduced a new authentication protocol to replace the one used in WEP.
  - Protected negotiation of capabilities (WEP, WPA, WPA2, …)
  - Exchange of nonces and MACs on nonces to provide mutual authentication.

Practical WPA attacks

- Dictionary attack on pre-shared key mode
  - Attack first proposed by Robert Moskowitz.
  - Works if PMK has low entropy (e.g. derived from pass-phrase).
  - Implemented in CoWPAtty (Joshua Wright).
  - http://sourceforge.net/projects/cowpatty/
- Denial of service attack
  - If WPA equipment sees two packets with invalid MICs in 1 second, then:
    - All clients are disassociated.
    - All activity stopped for one minute.
    - So two malicious packets per minute is enough to stop a wireless network.

Wireless Security

WPA2

WPA2

- Supersedes WPA's interim solution to WEP issues but does require new hardware.

- Main features:
  - Use of 128-bit AES-CCMP (AES Counter Mode with Cipher Block Chaining Message Authentication Code) for confidentiality and integrity.
  - Pre-shared mode and 802.1X for key management (as in WPA).
    - And pre-shared mode has same dictionary attack issue as WPA.
  - Use of a similar handshake for distributing AES-CCMP keys.

WPA3

- In January 2018, WPA3 was announced as a replacement to WPA2.

- The new standard uses:
  - 128-bit encryption in WPA3-Personal mode *(WPA-PSK)*
  - 192-bit in WPA3-Enterprise (WPA-802.1X) and forward secrecy

Next Lecture

- Risk Management
- Reading for next lecture:
  - Anderson's book – section 25.5
  - NIST Special Publication 800-37 (general overview of the documents)