FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

3. WPA2/WPA3

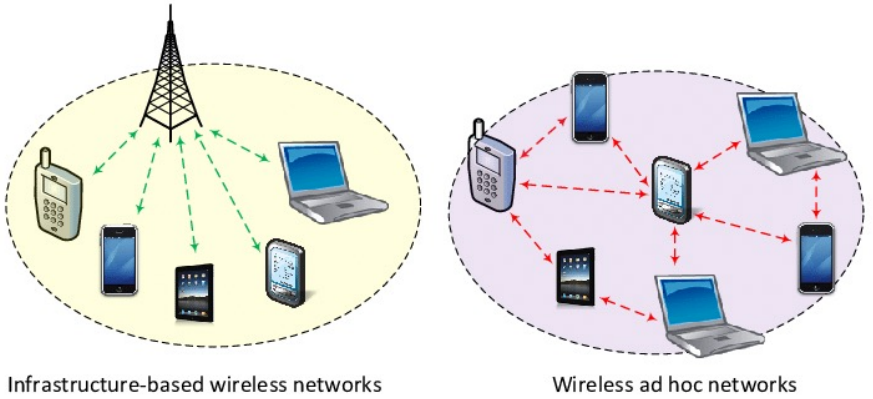
Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

WiFi Security

- WEP
- WPA/WPA2/WPA3

Recall: 802.11



- IEEE defines the 802.11 -> link layer wireless protocol
- Provides wireless access to wired networks with Access Points (AP)
  - Can be used without an AP which is referred as ad-hoc or IBSS (Independent Basic Service Set) mode
- Three packet categories:
  - Data, management, and control

Recall: WiFi History

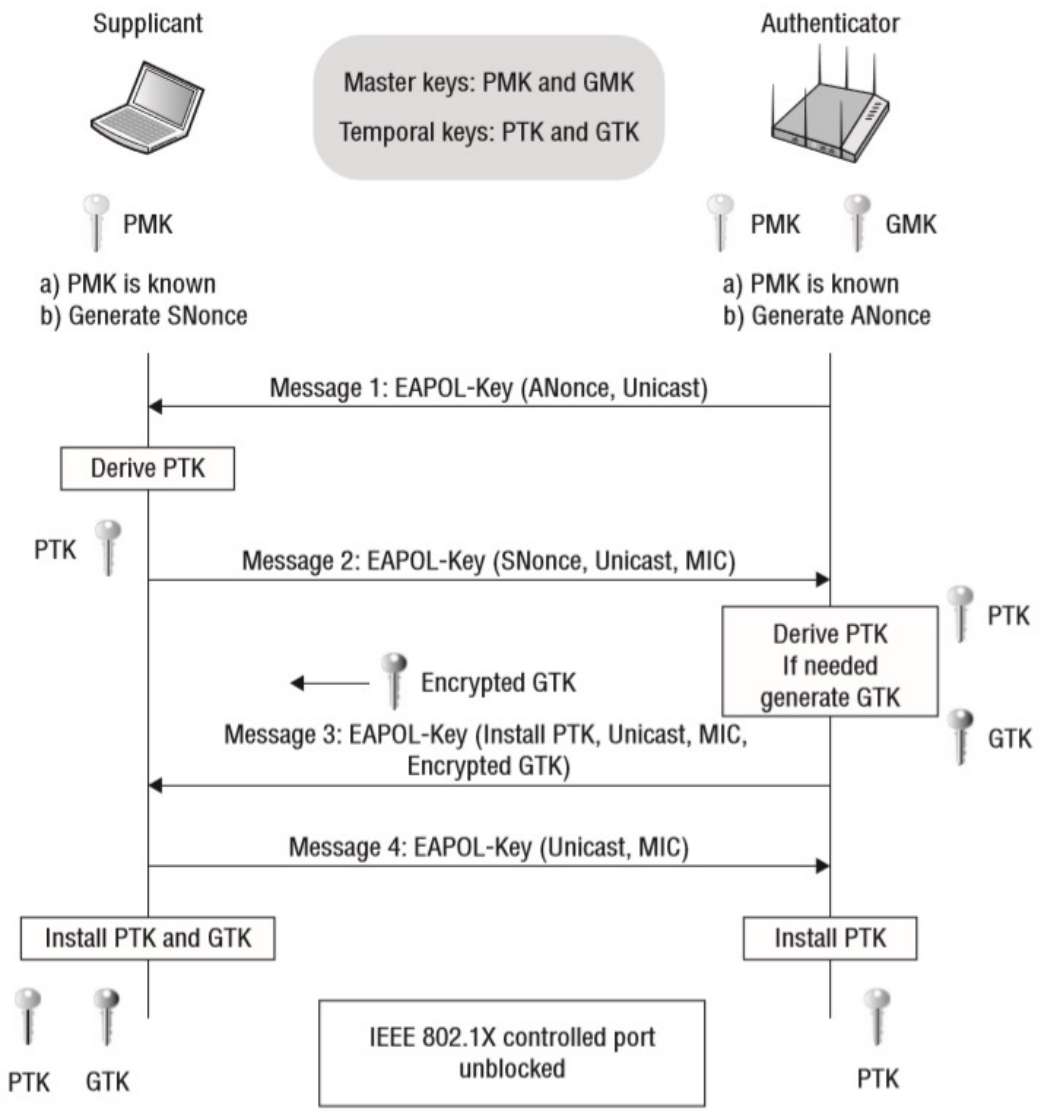
- 802.11 -> 1997
- 802.11a/b -> 2000
- 802.11g -> 2003
- 802.11n -> 2009
- 802.11ac -> 2013
- 802.11ax -> 2017

Recall: 802.11 Security

- Wired Equivalency Protocol (WEP)
- Wi-Fi Protected Access (WPA)

Recall: WPA: Pre-shared Key

- **Message1:** AP sends EAPOL message with Anonce (random number) to the device to generate PTK
  - Client device knows AP's MAC because its connected to it
  - It has PMK, Snonce and its own MAC address
  - Once it receives Anonce from AP, it has all the inputs to create the PTK



PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

WPA2

- WPA still uses the RC4 encryption algorithm, and retained other weaknesses from WEP
- WPA2 was introduced in 2004 and was an upgraded version of WPA
- WPA2 is based on the robust security network (RSN) mechanism and operates on two modes:
  - **Personal mode or Pre-shared Key (WPA2-PSK) –** which relies on a shared passcode for access and is usually used in home environments
  - **Enterprise mode (WPA2-EAP) –** as the name suggests, this is more suited to organizational or business use

WPA2

- Both modes use the CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol)
- The CCMP protocol is based on the Advanced Encryption Standard (AES) algorithm, which provides message authenticity and integrity verification
- CCMP is stronger and more reliable than WPA's original TKIP, making it more difficult for attackers to spot patterns

WPA2

- However, WPA2 still has drawbacks
  - For example, it is vulnerable to key reinstallation attacks (KRACK)
  - KRACK exploits a weakness in WPA2, which allows attackers to pose as a clone network and force the victim to connect to a malicious network instead
- This enables the hacker to decrypt a small piece of data that may be aggregated to crack the encryption key
- Yet, WPA2 is still considered sufficiently secure and more secure than WEP or WPA

WPA3

- WPA3 is the third iteration of the Wi-Fi Protected Access protocol
- The Wi-Fi Alliance introduced WPA3 in 2018
- WPA3 devices became widely available in 2019 and are backwards compatible with devices that use the WPA2 protocol
- WPA3 introduced new features for both personal and enterprise use

WPA3: Features

- **Individualized data encryption**: When logging on to a public network, WPA3 signs up a new device through a process other than a shared password
- WPA3 uses a Wi-Fi Device Provisioning Protocol (DPP) system that allows users to use Near Field Communication (NFC) tags or QR codes to allow devices on the network
- In addition, WPA3 security uses 256 encryption rather than the previously used 128-bit encryption

WPA3: Features

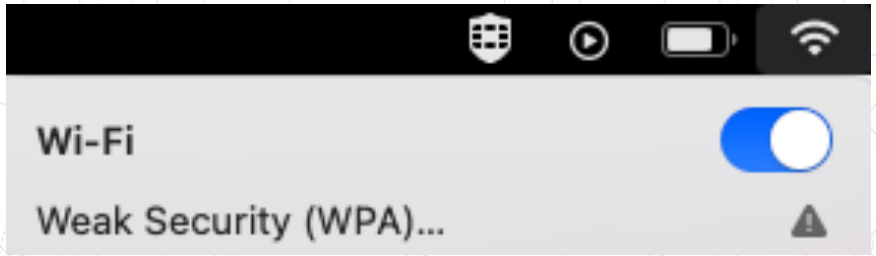
- **Simultaneous Authentication of Equals protocol**:
  - This is used to create a secure handshake, where a network device will connect to a wireless access point, and both devices communicate to verify authentication and connection
  - Even if a user's password is weak, WPA3 provides a more secure handshake using Wi-Fi DPP

WPA3: Features

- **Stronger brute force attack protection**:
  - WPA3 protects against offline password guesses by allowing a user only one guess, forcing the user to interact with the Wi-Fi device directly, meaning they would have to be physically present every time they want to guess the password
  - WPA2 lacks built-in encryption and privacy in public open networks, making brute for attacks a significant threat

What do you use?

- For MacOS; just check the wireless symbol on top:



FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger