FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

2. WiFi (IEEE 802.11)

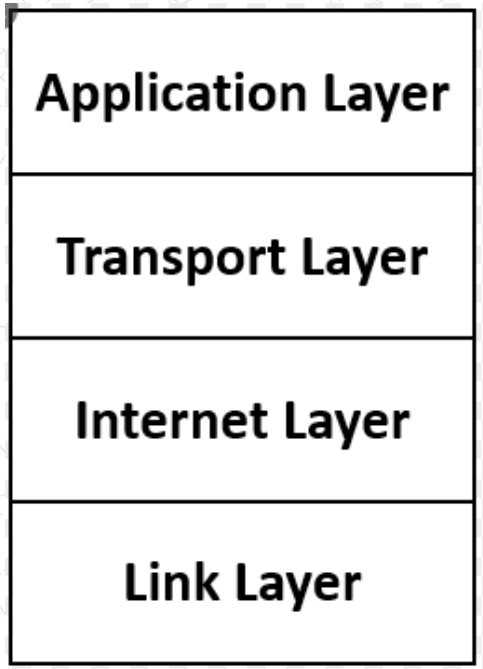
Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

Outline

- WiFi
- WiFi Security
  - WEP
  - WPA/WPA2/WPA3

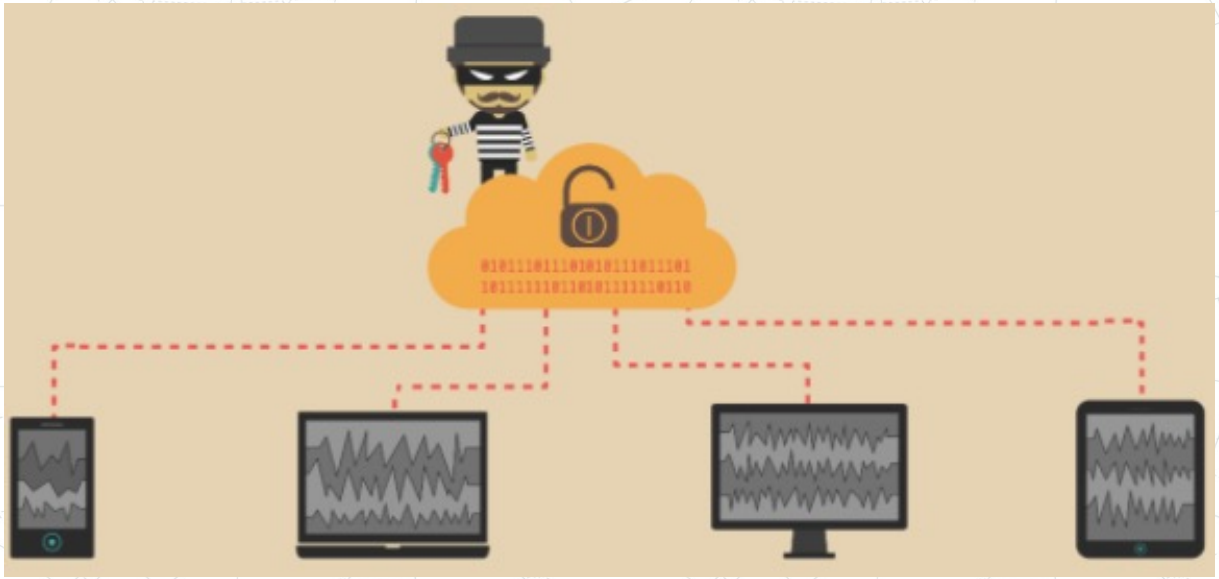
Recall: Network Protocols

- **Application Layers:** End-user applications
- **Transport Layer:** Data transfer from end to end
- **Internet (Network) Layer:** Routing of data from source to destination
- **Link (Physical) Layer:** Physical media carrying the data

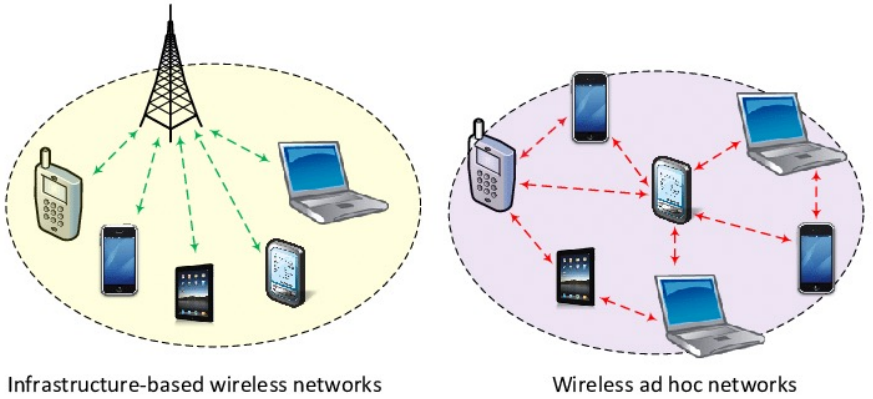


Recall: Some Common Attack Types

- Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks
- Man-in-the-middle (MitM) attack
- Phishing and spear phishing attacks
- Malware attack



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

802.11 Packet Types

- Data packets are used for carrying high-level data (e.g., IP packets)
- Management packets to control the network
  - Attackers are interested in these mostly
  - Beacon and De-authentication are examples of management
- Control packets are used to mediating access to shared medium
  - Examples: RTS (Request to Send) and CTS (Clear to Send)

802.11 Packets

- Three addresses: Source, destination and BSSID (basic service set ID)
  - Where the packets are going, who sent them and what AP to go through
- BSSID identifies the AP and its collected stations
  - Often same MAC address as the wireless interface on the AP

WiFi History

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

802.11 (legacy)

- The original version of the standard IEEE 802.11 was released in 1997 and clarified in 1999, but is now obsolete
  - It specified two net bit rates of 1 or 2 megabits per second (Mbit/s) and it specified three alternative physical layer technologies:
    - Diffuse infrared operating at 1 Mbit/s; frequency-hopping spread spectrum (FHSS) operating at 1 Mbit/s or 2 Mbit/s
    - Direct-sequence spread spectrum (DSSS) operating at 1 Mbit/s or 2 Mbit/s
  - The latter two radio technologies used microwave transmission over the Industrial Scientific Medical frequency band at 2.4 GHz

802.11b

- Has a maximum raw data rate of 11 Mbit/s, and uses the same media access method defined in the original standard
- 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard
- The dramatic increase in throughput of 802.11b (compared to the original standard) along with simultaneous substantial price reductions led to the rapid acceptance of 802.11b as the definitive wireless LAN technology
- Devices using 802.11b experience interference from other products operating in the 2.4 GHz band
  - E.g., microwave ovens, Bluetooth devices, cordless telephones, and some amateur radio equipment

802.11a

- Provides protocols that allow transmission and reception of data at rates of 1.5 to 54 Mbit/s
  - It has seen widespread worldwide implementation, particularly within the corporate workspace
- While the original amendment is no longer valid, the term *802.11a* is still used by wireless access point (cards and routers) manufacturers to describe interoperability of their systems at 5 GHz, 54 Mbit/s
- The 802.11a standard uses the same data link layer protocol and frame format as the original standard, but an OFDM (Orthogonal frequency-division multiplexing) based air interface (physical layer)

802.11a

- Since the 2.4 GHz band is heavily used to the point of being crowded, using the relatively unused 5 GHz band gives 802.11a a significant advantage
- However, this high carrier frequency also brings a disadvantage: the effective overall range of 802.11a is less than that of 802.11b/g
  - In theory, 802.11a signals are absorbed more readily by walls and other solid objects in their path due to their smaller wavelength, and, as a result, cannot penetrate as far as those of 802.11b
  - In practice, 802.11b typically has a higher range at low speeds (802.11b will reduce speed to 5.5 Mbit/s or even 1 Mbit/s at low signal strengths)
  - 802.11a also suffers from interference, but locally there may be fewer signals to interfere with, resulting in less interference and better throughput

802.11g

- Works in the 2.4 GHz band (like 802.11b) but uses the same OFDM based transmission scheme as 802.11a
  - It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput
- 802.11g hardware is fully backward compatible with 802.11b hardware, and therefore is encumbered with legacy issues that reduce throughput by ~21% when compared to 802.11a

802.11g

- It was rapidly adopted in the market starting in January 2003, well before ratification, due to the desire for higher data rates as well as to reductions in manufacturing costs
- Details of making b and g work well together occupied much of the lingering technical process; in an 802.11g network, however, activity of an 802.11b participant will reduce the data rate of the overall 802.11g network
- Like 802.11b, 802.11g devices suffer interference from other products operating in the 2.4 GHz band, for example wireless keyboards

802.11n

- 802.11n is an amendment that improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) antennas 802.11n operates on both the 2.4 GHz and the 5 GHz bands
  - Support for 5 GHz bands is optional
- It operates at a maximum net data rate from 54 Mbit/s to 600 Mbit/s

802.11ac

- IEEE 802.11ac-2013 is an amendment to IEEE 802.11, published in December 2013, that builds on 802.11n
- Changes compared to 802.11n include wider channels (80 or 160 MHz versus 40 MHz) in the 5 GHz band, more spatial streams (up to eight versus four), higher-order modulation (up to 256-QAM vs. 64-QAM), and the addition of Multi-user MIMO (MU-MIMO)
- Vendors have announced plans to release so-called "Wave 2" devices with support for 160 MHz channels, four spatial streams, and MU-MIMO in 2014 and 2015

802.11ax

- In 2017, the first draft of the 802.11ax standard is published, and manufacturers begin to make devices based on the draft specification
- 802.11ax adds OFDMA, 1024-QAM modulation, up to 8 spatial streams and bi-directional MU-MIMO, for data rates up to 1200 Mbps over a single spatial stream in a 160 MHz channel

Renaming WiFi

- 802.11b = Wi-Fi 1
- 802.11a = Wi-Fi 2
- 802.11g = Wi-Fi 3
- 802.11n = Wi-Fi 4
- 802.11ac = Wi-Fi 5
- 802.11ax = Wi-Fi 6

802.11 Security

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

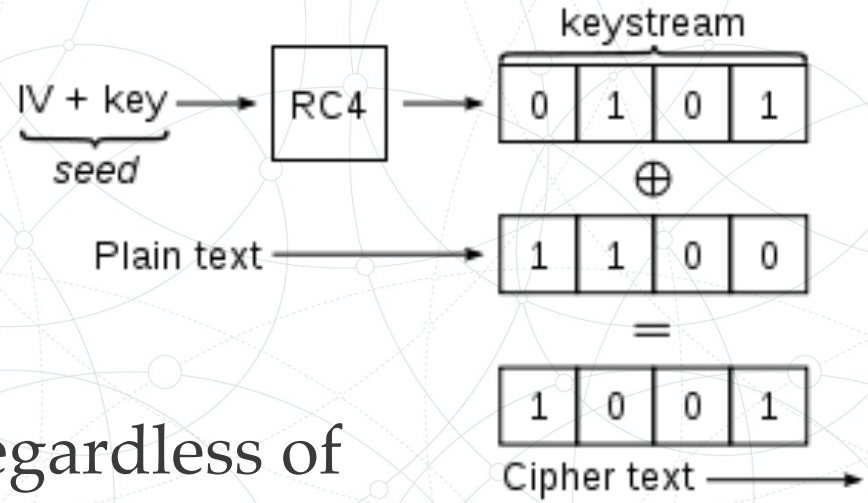
WEP

- Introduced in 1997, was the first attempt at wireless protection
- The aim was to add security to wireless networks by encrypting data
  - If wireless data were intercepted, it would be unrecognizable to the interceptors since it had been encrypted
  - However, systems that are authorized on the network would be able to recognize and decrypt the data
  - This is because devices on the network make use of the same encryption algorithm

WEP: **Encryption**

- WEP initially used a 64-bit key with the RC4 stream encryption algorithm to encrypt data transmitted wirelessly
- Later versions of the protocol added support for 128-bit keys and 256-bit keys for improved security
- WEP uses a 24-bit initialization vector, which resulted in effective key lengths of 40, 104 and 232 bits

WEP: **Encryption**



- This is a static key, which means all traffic, regardless of device, is encrypted using a single key
- A WEP key allows computers on a network to exchange encoded messages while hiding the messages' contents from intruders
- This key is what is used to connect to a wireless-security-enabled network

WEP: **Data integrity:**

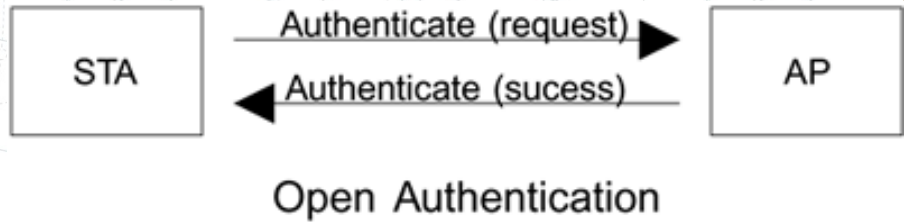
- WEP uses the CRC-32 checksum algorithm to check that transmitted data is unchanged at its destination
- The sender uses the CRC-32 cyclic redundancy check to generate a 32-bit hash value from a sequence of data
- The recipient uses the same check on receipt
- If the two values differ, the recipient can request a retransmission

WEP: **Authentication**

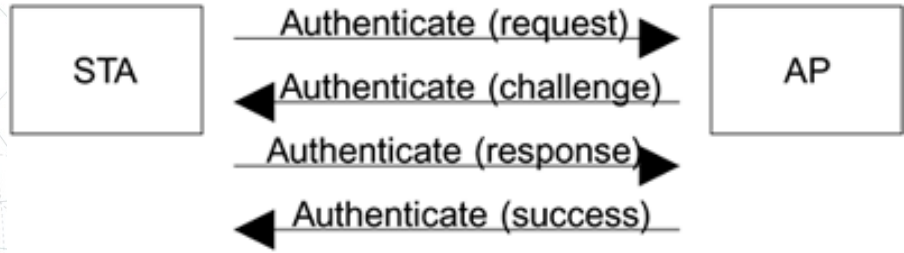
- WEP authenticates clients when they first connect to the wireless network access point:
  - **Open System Authentication;** Wi-Fi-connected systems can access any WEP network access point, as long as the connected system uses a service set identifier that matches the access point SSID.
  - **Shared Key Authentication;** Wi-Fi-connected systems use a four-step challenge-response algorithm to authenticate.

WEP: Authentication: Shared Key

- A four-step challenge-response handshake:
  - The client sends an authentication request to the AP
  - The AP replies with a clear-text challenge
  - The client encrypts the challenge-text using the configured WEP key and sends it back in 'authentication response'
  - The AP decrypts the response. If this matches the challenge text, the AP sends back a positive reply



Open Authentication



WEP Authentication

WPA

- The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard
- WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999
  - However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA

WPA

- The WPA protocol implements the Temporal Key Integrity Protocol (TKIP)
  - WEP used a 64-bit or 128-bit encryption key that must be manually entered on wireless access points and devices and does not change
- TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP

WPA

- WPA also includes a Message Integrity Check, which is designed to prevent an attacker from altering and resending data packets
  - This replaces the cyclic redundancy check (CRC) that was used by the WEP standard
- CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled
  - Well-tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards

WPA

- WPA uses a message integrity check algorithm called *TKIP* to verify the integrity of the packets
  - TKIP is much stronger than a CRC, but not as strong as the algorithm used in WPA2
- However, despite these improvements, elements of WPA came to be exploited – which led to WPA2

WPA: Pre-shared Key

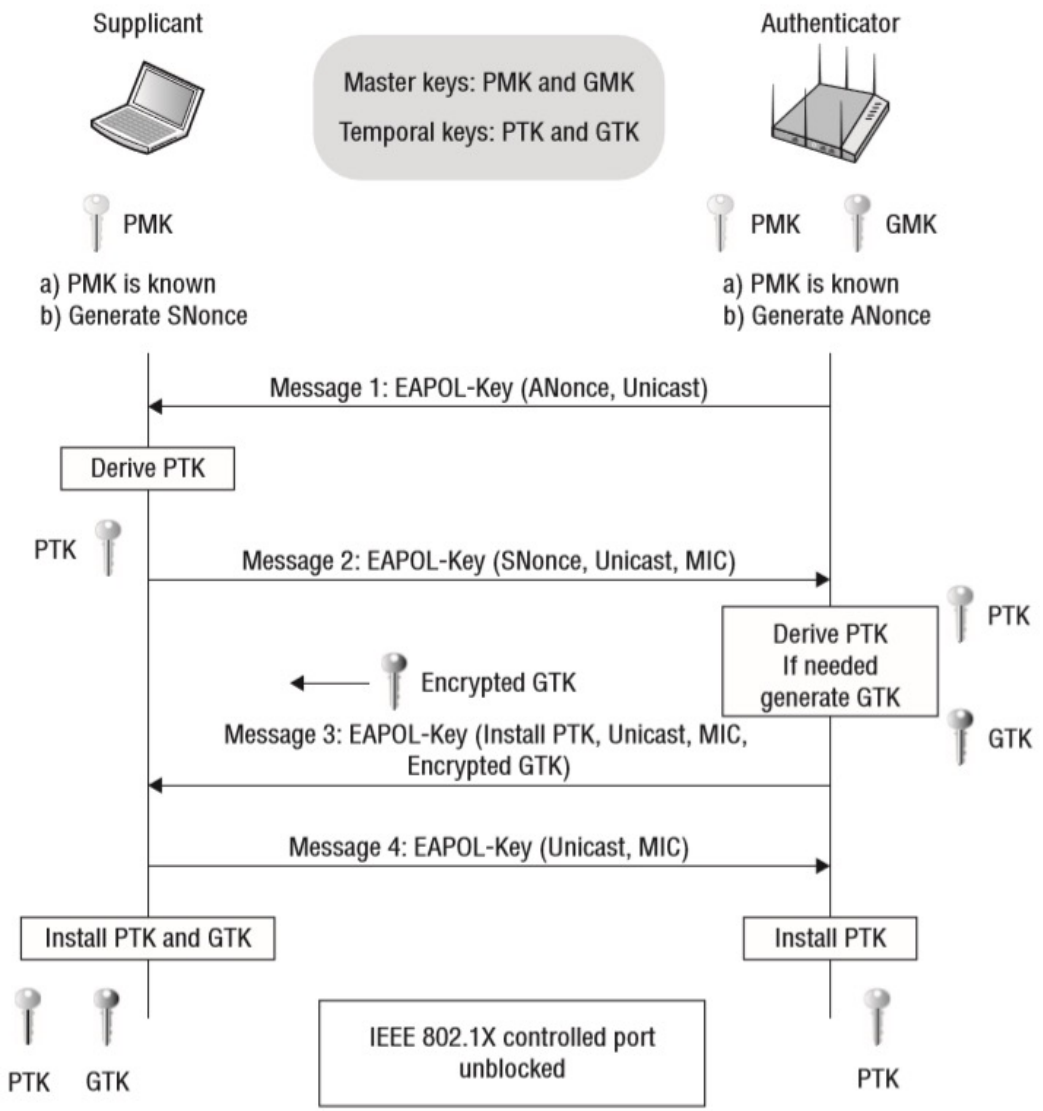
- Similar to WEP
  - Requires connecting party to provide a key to access to network
- Pre-shared key is between 8-63 ASCII long
- Encryption relies on pairwise master key (PMK)
  - That is computed from the pre-shared key and SSID

WPA: Pre-shared Key

- Once client has PMK, it will negotiate with AP for PTK (pairwise transient key)
  - These keys are created dynamically every time client connects
  - Function of PMK, random numbers, and MAC addresses
    - To ensure they are unique and non-repeating

WPA: Pre-shared Key

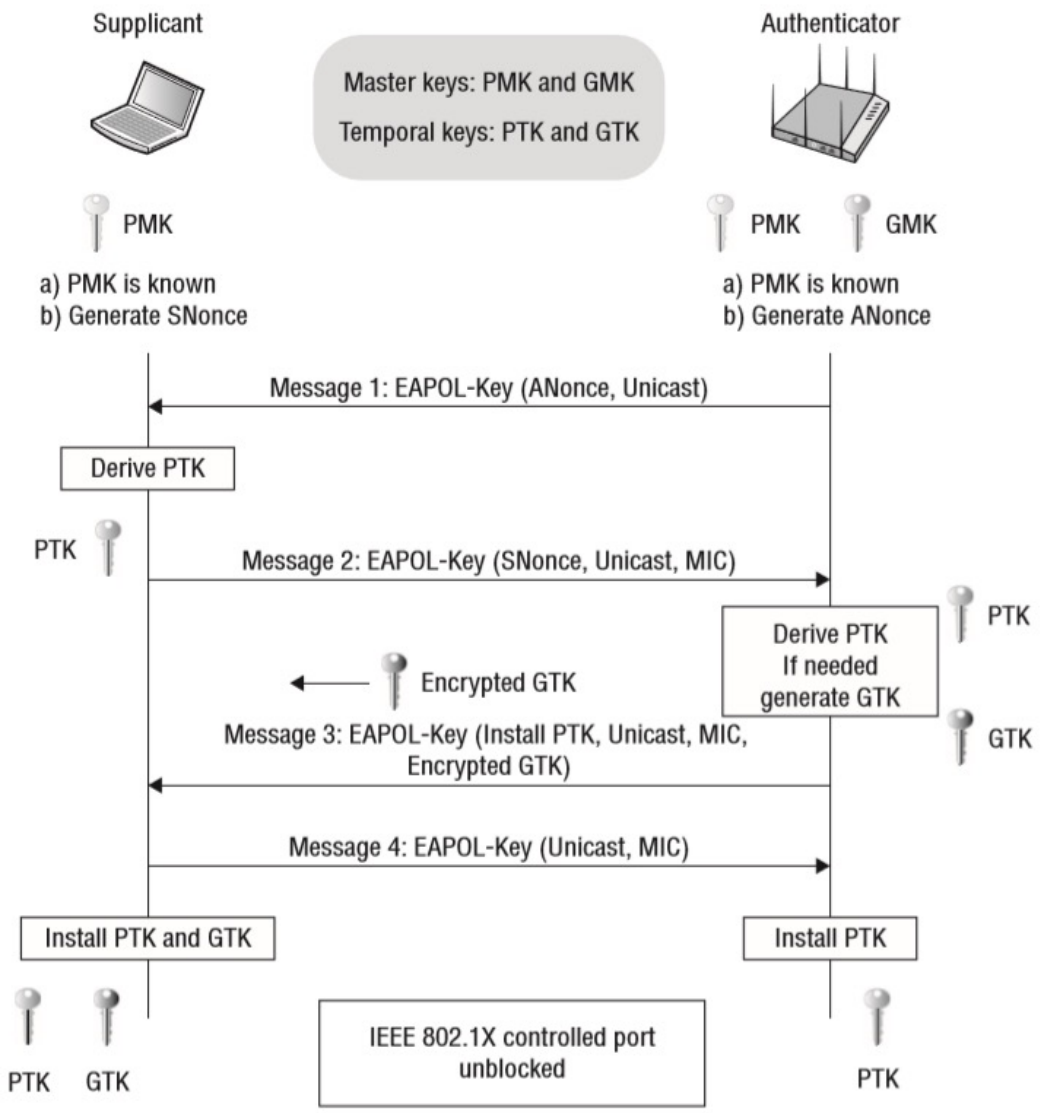
- **Message1:** AP sends EAPOL message with Anonce (random number) to the device to generate PTK
  - Client device knows AP's MAC because its connected to it
  - It has PMK, Snonce and its own MAC address
  - Once it receives Anonce from AP, it has all the inputs to create the PTK



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

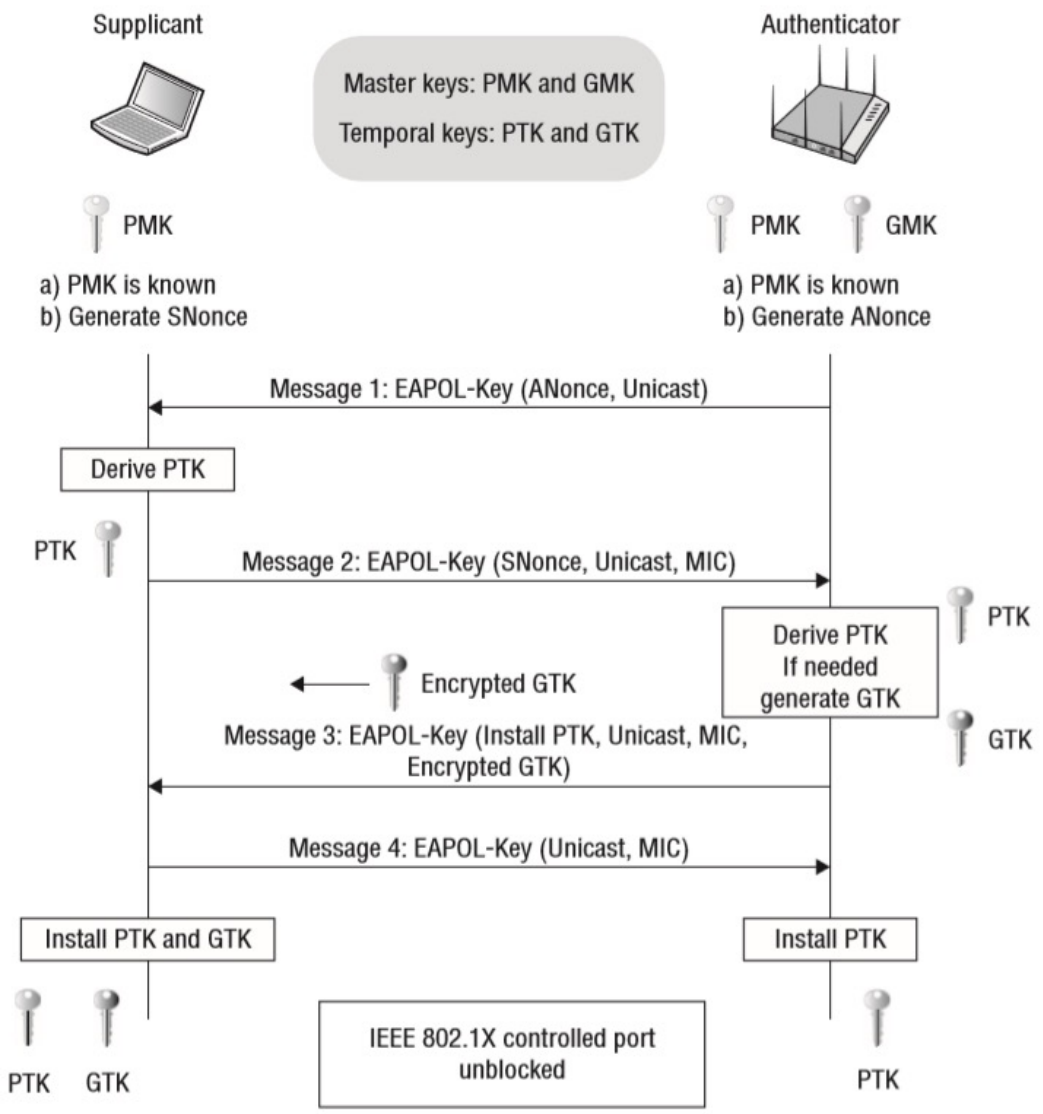
WPA: Pre-shared Key

- **Message2:** Once the device has created its PTK it sends out SNonce which is needed by the access point to generate PTK as well
  - The device sends EAPOL to AP message2 with MIC (message integrity check) to make sure when the access point can verify whether this message corrupted or modified
  - Once SNonce received by the AP it can generate PTK as well for unicast traffic encryption



WPA: Pre-shared Key

- **Message3:** EAPOL message3 is sent from AP to client device containing GTK
  - AP creates GTK without the involvement of the client from GMK
- **Message4:** Fourth and last EPOL message will be sent from the client to AP just to confirm that Keys have been installed



WPA: Pre-shared Key

- **4-way handshake Result: Control port unlocked**
  - Once the 4-way handshake is completed successfully virtual control port which blocks all the traffic will be open and now encrypted traffic can flow
  - Now all unicast traffic will be encrypted with PTK and all multicast traffic will be encrypted via GTK which created in the 4-way handshake process

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger