Department of Computer Science

FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

CSE 4820: Wireless and Mobile Security

8. WPA Security

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

Outline

WPS

WPA/WPA2 Brute Force

Recall: Review WEP

- Weak Encryption Protocol
  - Authentication
  - Access control
  - Replay prevention
  - Message modification detection
  - Message privacy
  - Key protection

Reaver Brute-force Attack

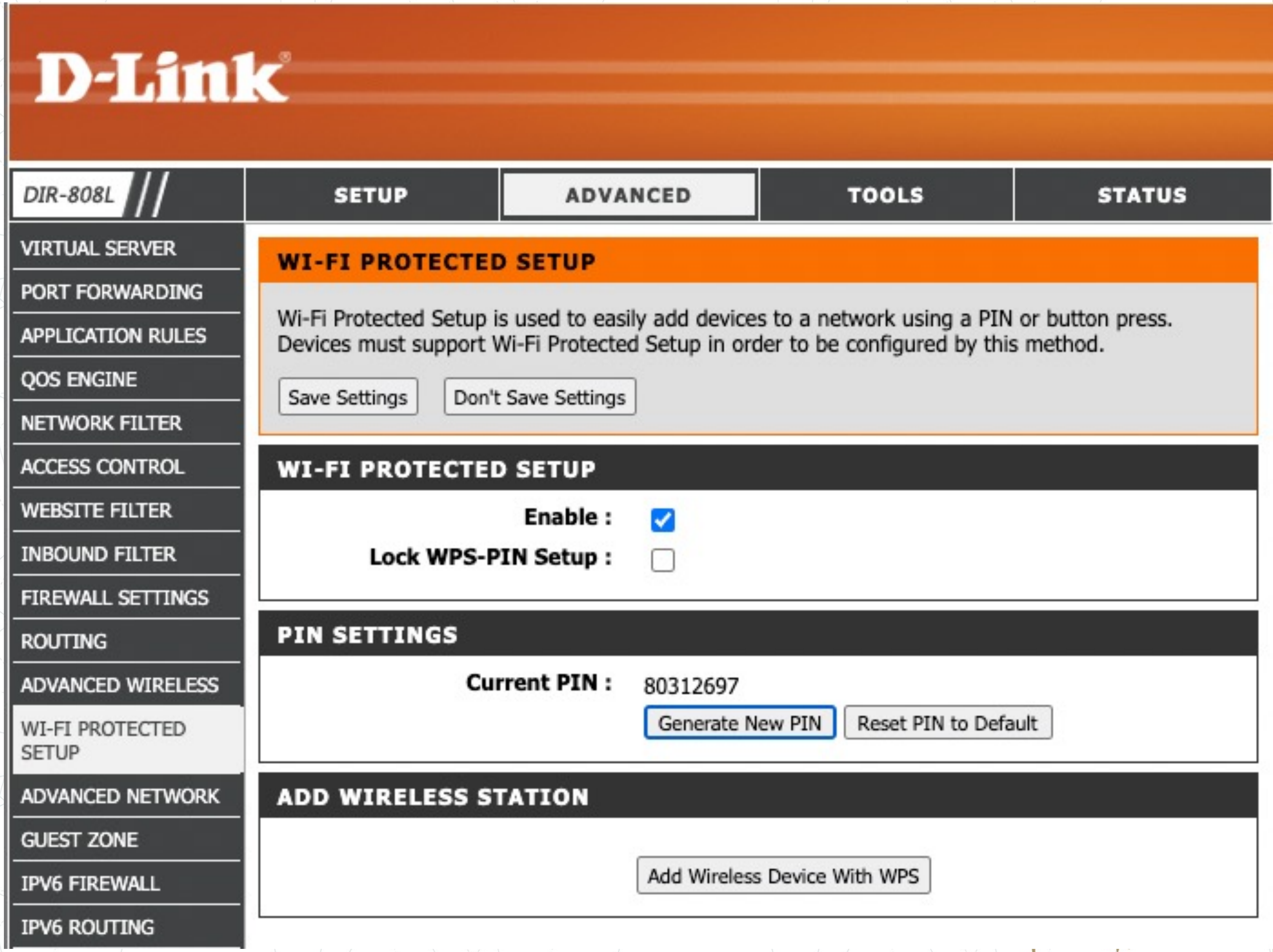
- Was a radical new weapon for Wi-Fi hacking when it was presented in 2011
  - Now obsolete against most routers
- One of the first practical attacks against WPA- and WPA2-encrypted networks, it totally ignored the type of encryption a network used, exploiting poor design choices in the WPS protocol
- Reaver allowed a hacker to sit within range of a network and brute-force the WPS PIN, spilling all the credentials for the router
  - Worse, the 8-digit-long PIN could be guessed in two separate halves, allowing for the attack to take significantly shorter than working against the full length of the PIN

WPS (Wi-Fi Protected Setup)

- It is a network security standard created by the WiFi Alliance in 2006 as an alternative to the regular way of adding devices to the network
    - Instead of requiring the user to insert the SSID (WiFi network name) passkey, it relies on various other methods, such as a PIN, NFC, or Push button to greatly simplify the device pairing process
- This means that the WPS's reason of existence is simplicity and user friendliness, but it was also a reaction to the independent development of similar solutions by the major manufacturers (the WPS remains non-proprietary and universal)
    - Was created out of necessity, but has been proven to be problematic on the long run

WPS Settings:

- Solution:
  - Disable the WPS
  - To time-out the pairing process in case a brute-force attack was detected



WI-FI PROTECTED SETUP

Wi-Fi Protected Setup is used to easily add devices to a network using a PIN or button press. Devices must support Wi-Fi Protected Setup in order to be configured by this method.

WI-FI PROTECTED SETUP

Enable : ☑

Lock WPS-PIN Setup : ☐

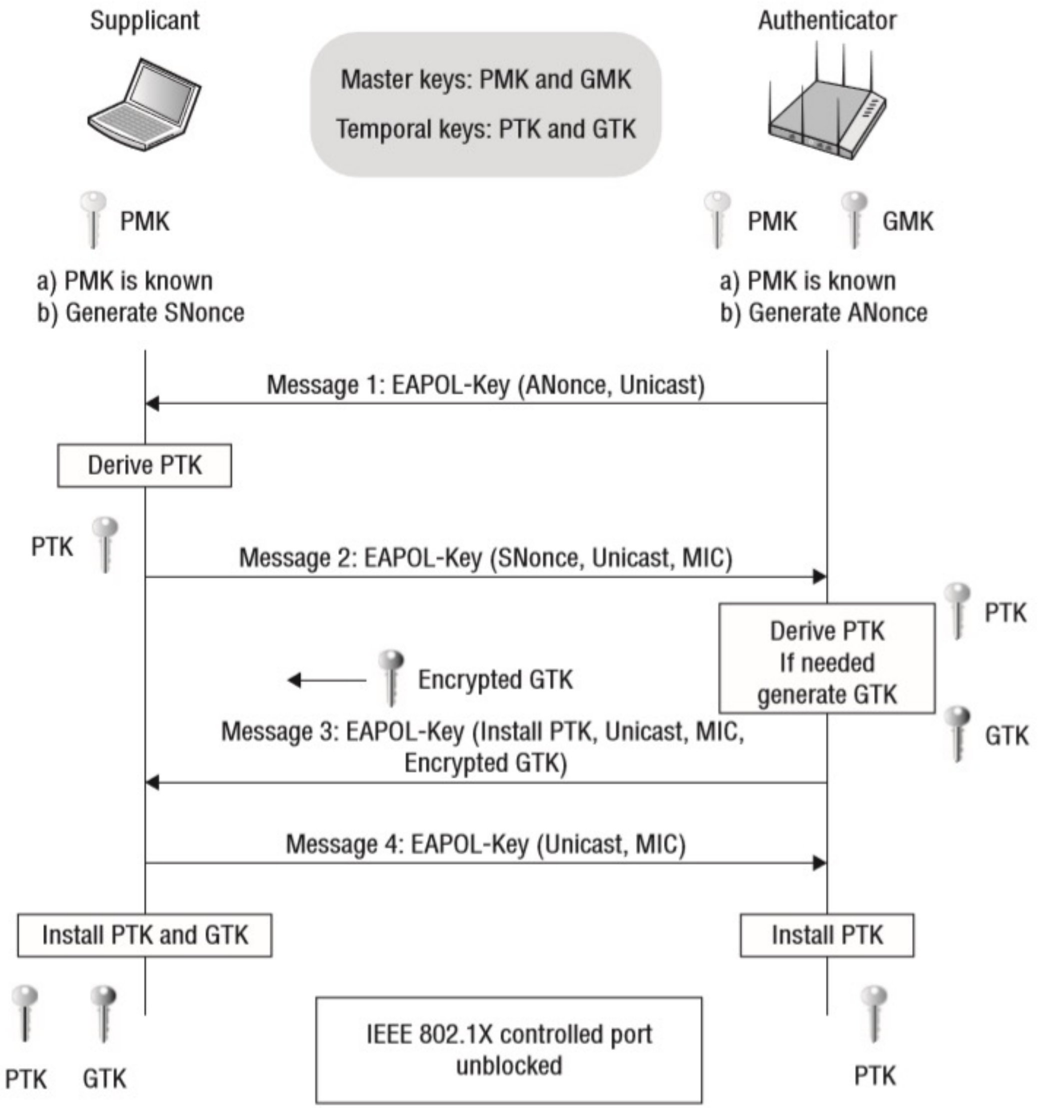
PIN SETTINGS

Current PIN : 80312697

ADD WIRELESS STATION

Recall: WPA Handshake

- 4-way handshake
- PTK is derived on run-time
- PMK is pre-installed


Supplicant
Authenticator
Master keys: PMK and GMK
Temporal keys: PTK and GTK
PMK
PMK
GMK
a) PMK is known
b) Generate SNonce
a) PMK is known
b) Generate ANonce
Message 1: EAPOL-Key (ANonce, Unicast)
Derive PTK
PTK
Message 2: EAPOL-Key (SNonce, Unicast, MIC)
Derive PTK
If needed
generate GTK
PTK
GTK
Encrypted GTK
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)
Message 4: EAPOL-Key (Unicast, MIC)
Install PTK and GTK
Install PTK
PTK
GTK
IEEE 802.1X controlled port unblocked
PTK

WPA Brute Force

- To authenticate with a WPA/WPA2-Personal AP, a station must complete a four-way handshake, securely providing the PSK (Pre-shared Key) without disclosing it in plaintext
- To perform the handshake, both the AP and the station must generate a nonce (a number used only once) to share with one another
  - The AP and the station then both feed the nonce and the pre-shared key (PSK) into a pseudo-random function which generates a pairwise transient key (PTK)
  - The created PTK is unique to both the AP and the station and is used to encrypt communications between the devices, completing the authentication

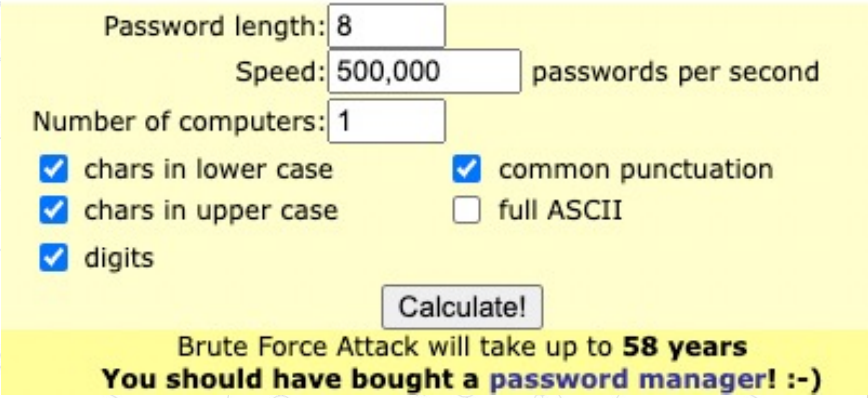
WPA Brute Force

- However, authentication to an AP is conducted through management frames; meaning, if an attacker can capture the four-way handshake, they will have access to all factors which generated the PTK
  - Isolating the wireless password as the missing variable
- To crack the password, loop this pseudo-random function (with the same nonce's) and a list of possible password as input for the pre-shared key
  - Starting with dictionary list (dictionary attack)
  - Once the transient key generated matches the one from the captured traffic, the password is correct

https://www.wikihow.com/Hack-WPA/WPA2-Wi-Fi-with-Kali-Linux

WPA Brute Force

- How much would it take to brute force all?
  - Quite long for regular devices
  - Unless it is in dictionary, your chances are slim



Password length: 8

Speed: 500,000 passwords per second

Number of computers: 1

☑ chars in lower case
☑ chars in upper case
☑ digits
☑ common punctuation
□ full ASCII

Brute Force Attack will take up to **58 years**

You should have bought a password manager! :-)

- Even better for attackers is to use “Rainbow Table”
  - Pre-computing hashing in a lookup table
  - As a The ESSID is used as a salt in the encryption process, this speeds up the cracking process for common or reused network names

http://lastbit.com/pswcalc.asp

WPA Brute Force

- No difference between cracking WPA or WPA2 networks
  - The authentication methodology is basically the same between them
  - Thus, the techniques you use are identical
- This can be done either actively or passively
  - "Actively" means you will accelerate the process by deauthenticating an existing wireless client
  - "Passively" means you simply wait for a wireless client to authenticate to the WPA/WPA2 network

Recovering WPA Keys from Clients

- If you have physical access to the device
  - Android, MacOS, Win, etc. all store the WiFi passwords in the file system
  - Mostly do not require root access
- Not really our concern though

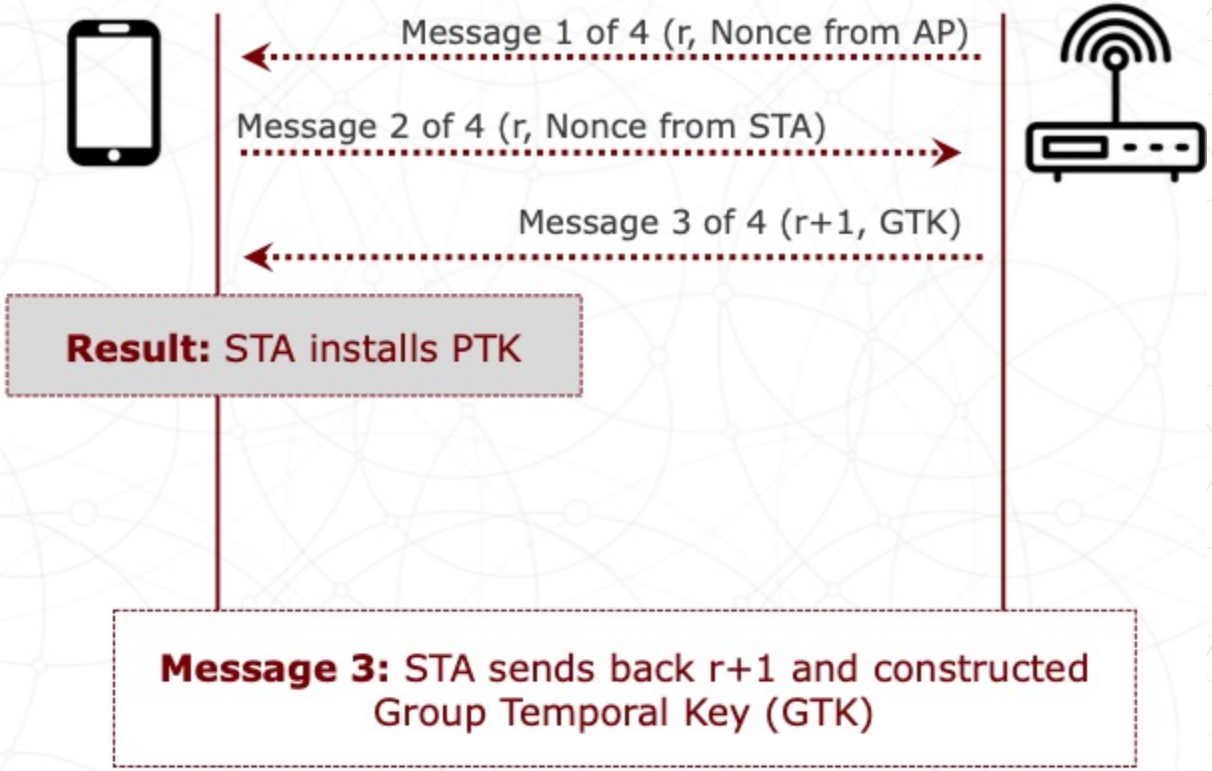
Decrypting the Traffic

- Every user has a unique PTK (pairwise transient key)
- Attacker obtains PMK but not PTK for each user
- Need to capture handshake for that specific user to get PTK
  - Force client to disconnect
  - Then watch/capture re-connection

KRACK (Key Reinstallation attack)

- High Level Idea: attack targets WPA2 four-way handshake protocol flaw specification that allows for third message to be sent repeatedly without changing encryption key
- Discovered in 2016;
  - 14 years after WPA2 was certified by WiFi Alliance
- Attack Discussed in: Vanhoef, Mathy, and Frank Piessens. "Key reinstallation attacks: Forcing nonce reuse in WPA2." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

KRACK (Key Reinstallation attack)



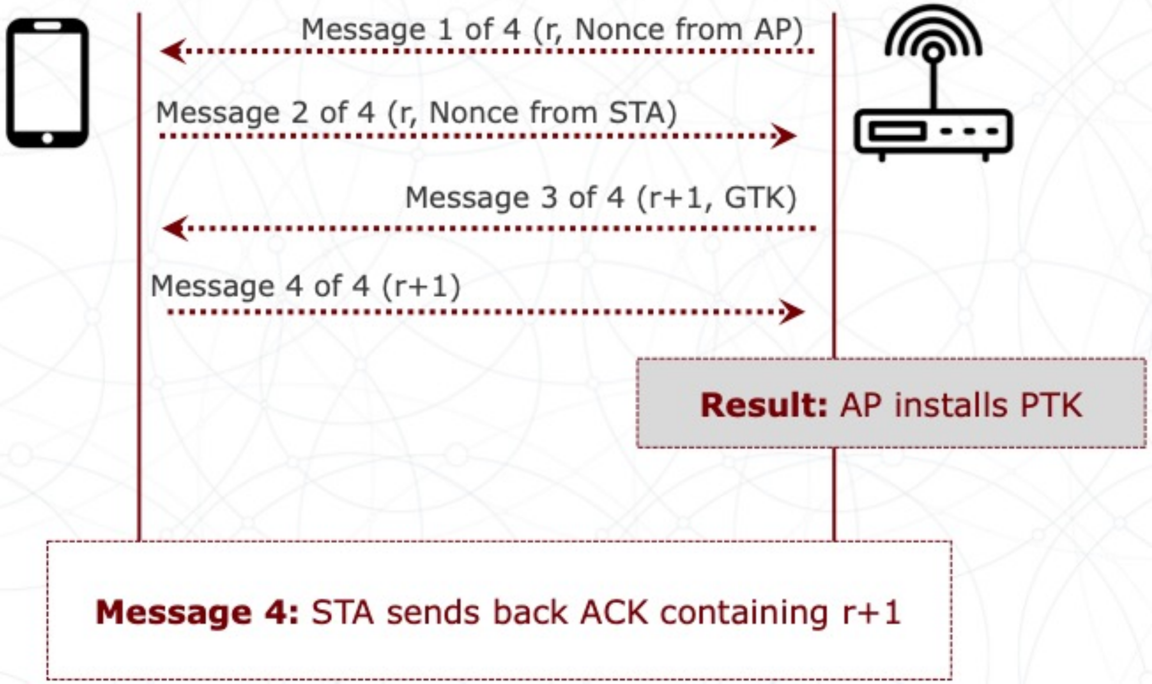
Message 1 of 4 (r, Nonce from AP)

Message 2 of 4 (r, Nonce from STA)

Message 3 of 4 (r+1, GTK)

Result: STA installs PTK

Message 3: STA sends back r+1 and constructed Group Temporal Key (GTK)



Message 1 of 4 (r, Nonce from AP)

Message 2 of 4 (r, Nonce from STA)

Message 3 of 4 (r+1, GTK)

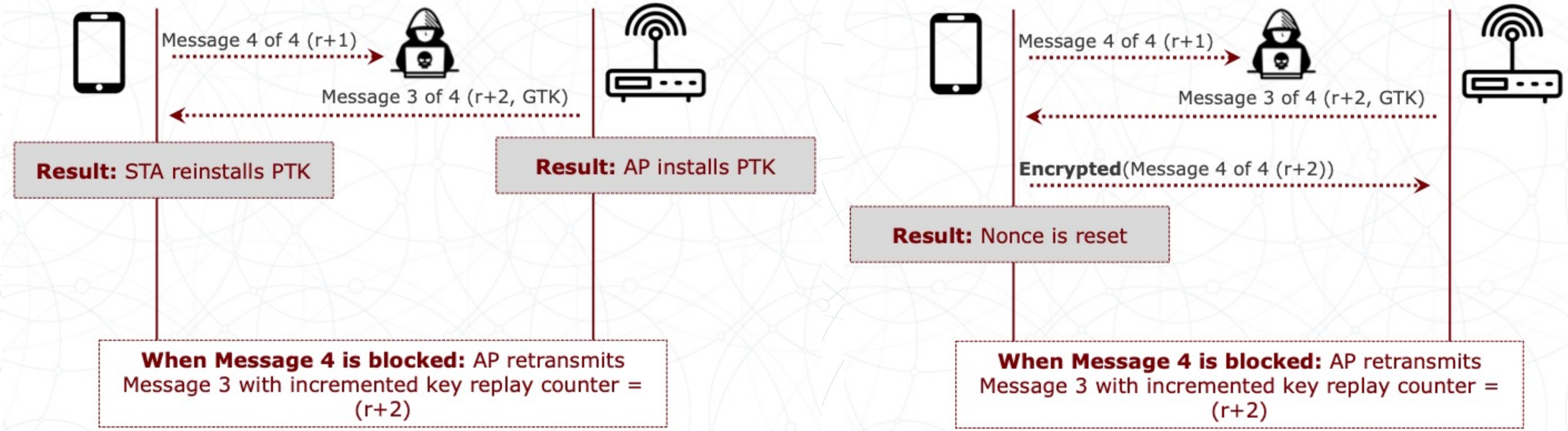
Message 4 of 4 (r+1)

Result: AP installs PTK

Message 4: STA sends back ACK containing r+1

KRACK (Key Reinstallation attack)

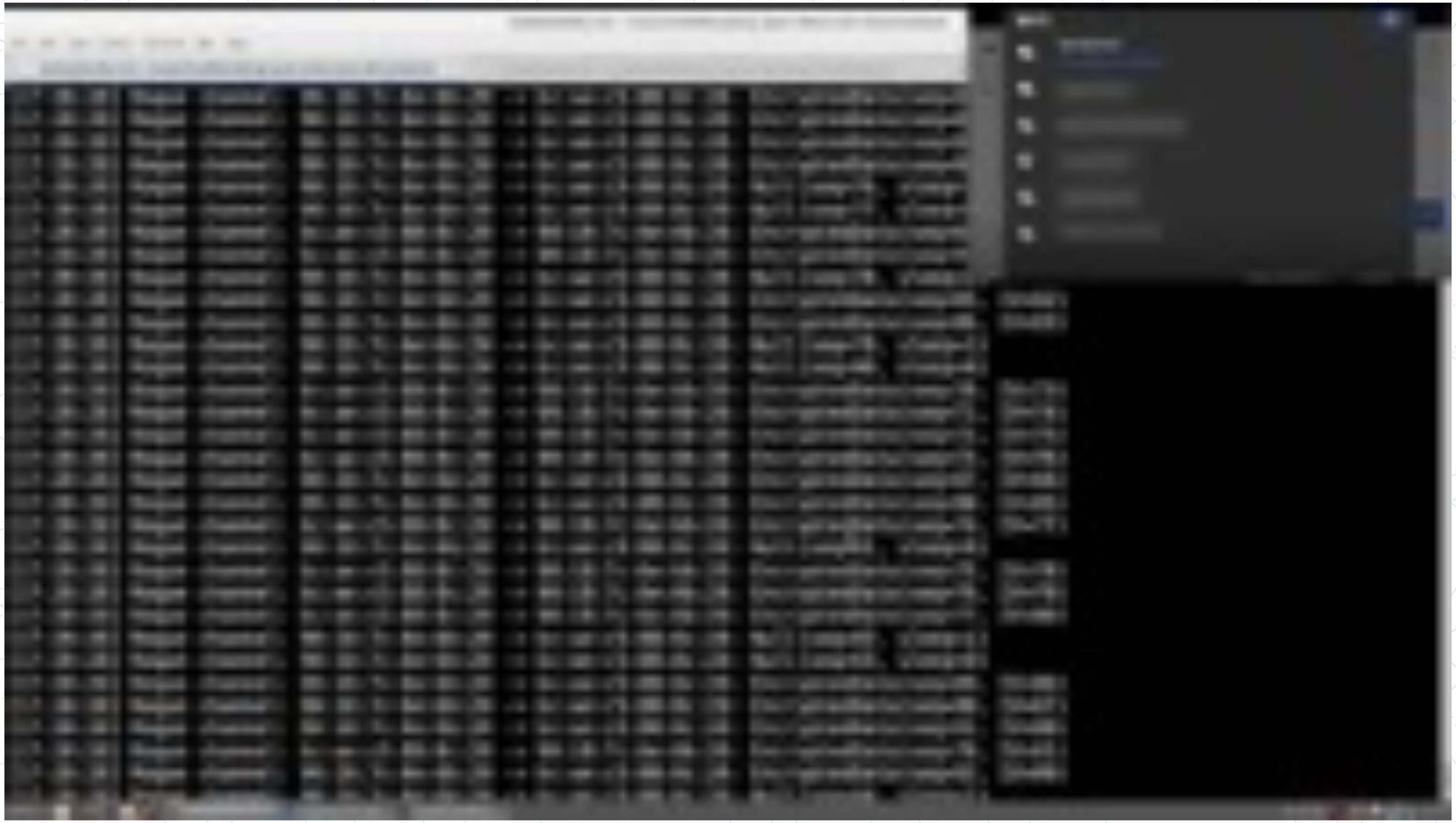
- Attacker blocks message 4
  - Re-transmit message 3 with increasing ‘r’


Message 4 of 4 (r+1)
Message 3 of 4 (r+2, GTK)
Result: STA reinstalls PTK
Result: AP installs PTK
When Message 4 is blocked: AP retransmits Message 3 with incremented key replay counter = (r+2)
Message 4 of 4 (r+1)
Message 3 of 4 (r+2, GTK)
Encrypted(Message 4 of 4 (r+2))
Result: Nonce is reset
When Message 4 is blocked: AP retransmits Message 3 with incremented key replay counter = (r+2)

KRACK: Example Scenario

- KRACK allow an adversary to decrypt a TCP packet, learn the sequence number, and hijack the TCP stream to inject arbitrary data
  - Without knowing the password of WiFi
- This enables one of the most common attacks over Wi-Fi networks: injecting malicious data into an unencrypted HTTP connection

KRACK: Explained



https://www.youtube.com/watch?v=Oh4WURZoR98&t=1s

FLORIDA TECH
FLORIDA'S **STEM** UNIVERSITY™

Thank you.
Questions?

Dr. Abdullah Aydeger