WiFi Security & KRACK Attack

Ainy Afzal & Mohammed Alghazali

What is Wi-Fi?

- WiFi stands for Wireless Fidelity - same as saying WLAN which stands for "Wireless Local Area Network."
- Radio frequencies to send signals between devices, transmits and receives data in the Gigahertz range
- Initially developed as a way to replace ethernet cable

History of WiFi

- 1971- first public demonstration of a wireless packet data network
- 1973 - First network standard
- 1985 - IBM introduces Token Ring LAN, running at 4 Mbps.
- 1988 - Release of WaveLan
- 1990 - The IEEE 802.11 Working Group for Wireless LANs is founded, under the Chairmanship of Vic Hayes, the “Father of WiFi”.
- 1993 - conflict reduction in radio wave transmition
- 1997 - The first version of the 802.11 protocol is released, providing up to 2 Mbps link speeds.
- 1998 - Mobilestar hotspots introduced
- 1999 - The 802.11b standard is approved, allowing 11 Mbps link speeds on the 2.4Ghz frequency.

How does Wi-Fi work?

- Similar to two way radio communication
- IEEE 802.11 standard defines the protocols that enable communications with current Wi-Fi-enabled wireless devices
- Security features such as WPA2 (Wi-Fi Protected Access) and AES (Advanced Encryption Standard)

Security Concerns with Wireless Networks

- Lack of a physical barrier makes WiFi vulnerable to unlawful interception, eavesdropping, hacking and a range of other cyber security issues
- All wireless connected devices come with some risks
- Important to learn about the various types of attacks

Piggybacking

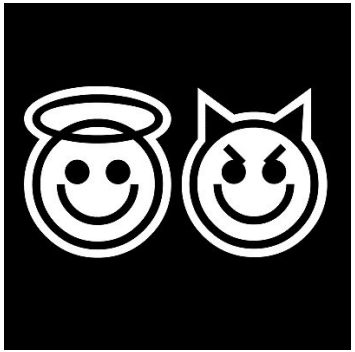
Not securing your wifi connection with a password, allowing unintended users to be able to monitor your activity and use your network

Wardriving

Hackers drive around with a powerful antennae looking for unsecured wireless networks

Evil Twin Attacks

- adversary gathers information about a public network access point, then sets up their system to impersonate it
- uses a broadcast signal stronger than the one generated by the legitimate access point
- unsuspecting users connect using the stronger signal



Unauthorized Computer Access

An unsecured public wireless network combined with unsecured file sharing could allow a malicious user to access any directories and files you have unintentionally made available for sharing

Wireless Sniffing

public access points are not secured and the traffic they carry is not encrypted. malicious actors could use sniffing tools to obtain sensitive information

Shoulder Surfing

In public areas malicious actors can simply glance over your shoulder as you type. By simply watching you, they can steal sensitive or personal information.

Denial of Service

Extreme brute force attack that overwhelms wireless network

Cracking Attacks

Ways to crack passwords to gain access

Brute Force or complex

Can use the Aircrack-ng and similar tools and a wireless card in monitor mode to perform the attack

WiFi Encryption

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

Four-way handshake

The four-way handshake is used to authenticate the client, negotiate a session key, and if WPA2 is used also transport the Group Temporal Key

Group key handshake

802.11i defines a Group Key Handshake that consists of a two-way handshake which is used to distribute a new group key

FT (Fast Transition) handshake

The FT key hierarchy is designed to allow clients to make fast BSS transitions between APs without requiring re authentication at every AP

WPA2 protocol

WPA2 is a security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. It implements the mandatory elements of IEEE 802.11i. In particular, it includes mandatory support for CCMP, an AES-based encryption mode, and it uses the 4-way handshake which is defined in 802.11i

Definitions

Supplicant: client or software connecting to the network

Access Point (AP): Networking hardware device that allows other Wi-Fi devices to connect to a wired network

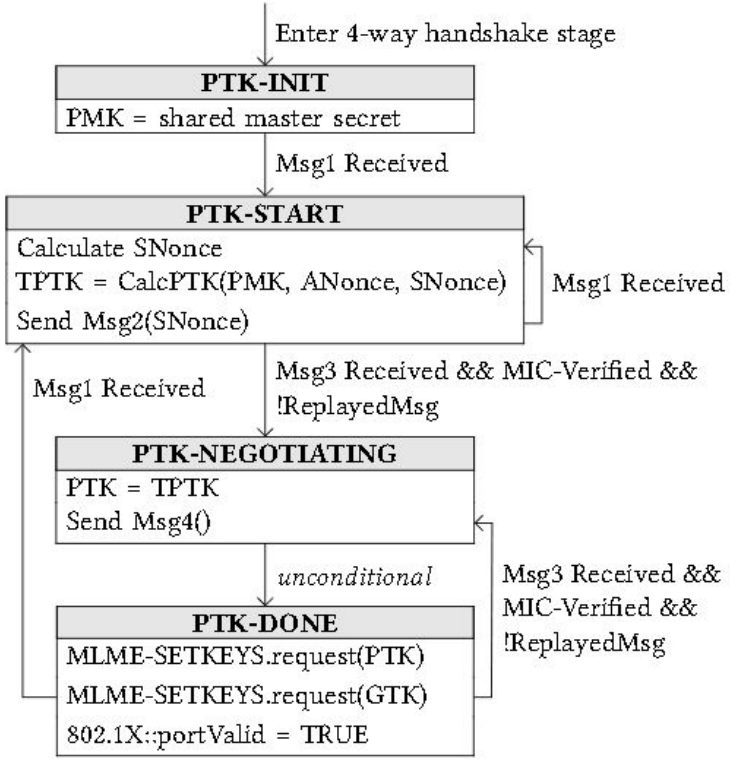
ANonce: random number generated by AP used to make PTK

SNonce: random number generated by Supplicant used to make PTK

MAC address: A unique identifier assigned to a network interface controller

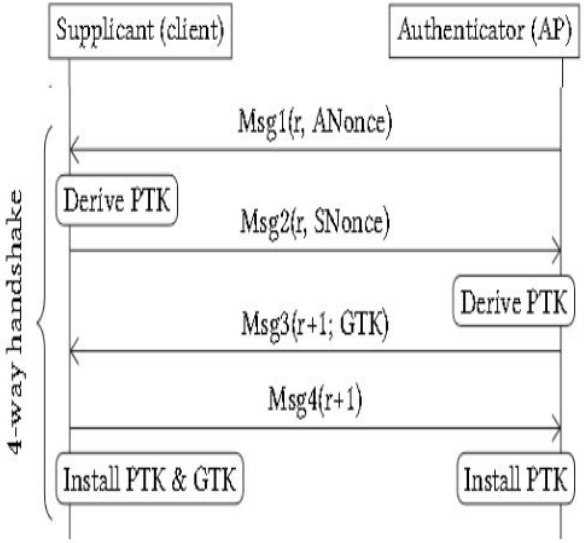
PTK: session key derived from shared key, supplicant mac address, AP mac address, SNonce, ANonce

4-Way Handshake state machine

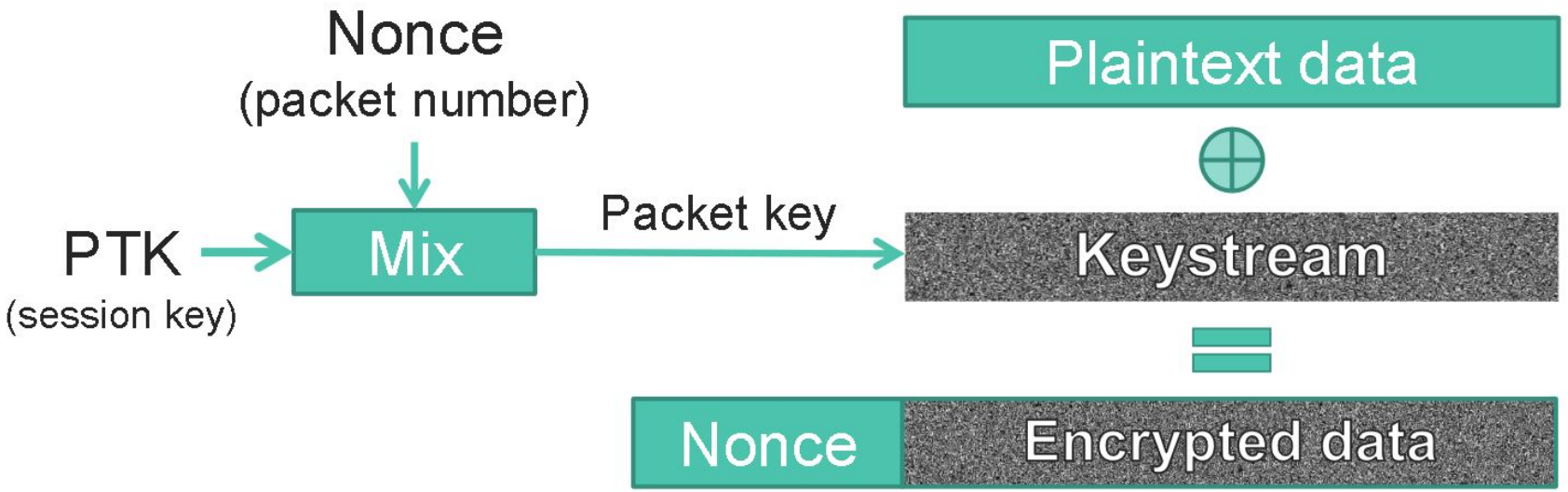


4 way handshake

- The supplicant and the AP have a pre shared secret
- The first message of the handshake, the AP sends a random number (ANonce) to the supplicant
- The supplicant replies with a random number (SNonce) and generates Pairwise Transient Key (PTK) which will be used to encrypt data frames
- Once the AP receives message 2 it will derive PTK then send message 3 to confirm both client and supplicant have the same PTK
- After receiving message 3 the client will install PTK for use and send message 4 to confirm it received message 3
- Finally after AP receives message 4 it will install the PTK for use



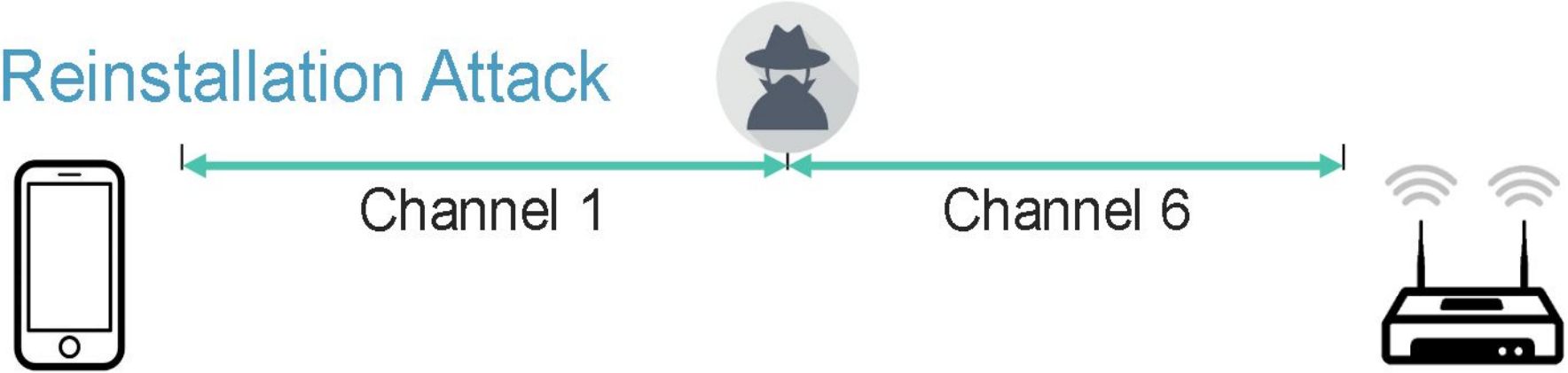
Stream Cyphers



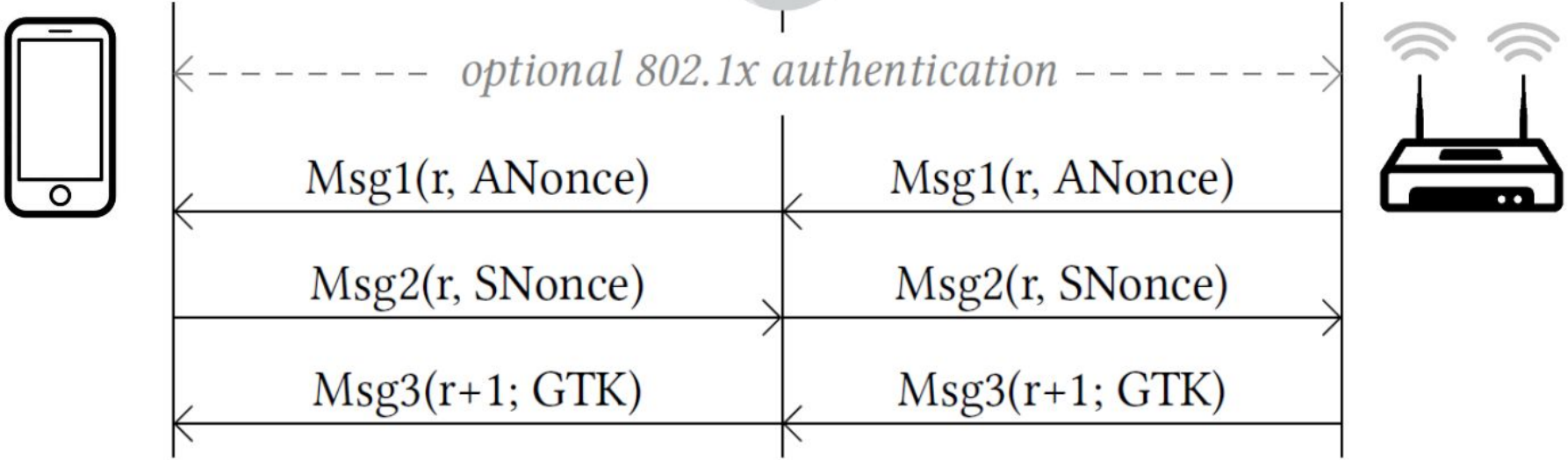
The Key Reinstallation Attack

- The supplicant installs the PTK after sending message 4
- If AP does not receive message 4 it will resend 3
- When Supplicant receives another message 3 it will reinstall the PTK and reset the nonce
- An attacker can block message 4 and resend message 3 to force nonce reuse
- Since nonce was reused the data confidentiality protocol becomes insecure and the attacker can replay, decrypt, or forge packets depending on which protocol is used.

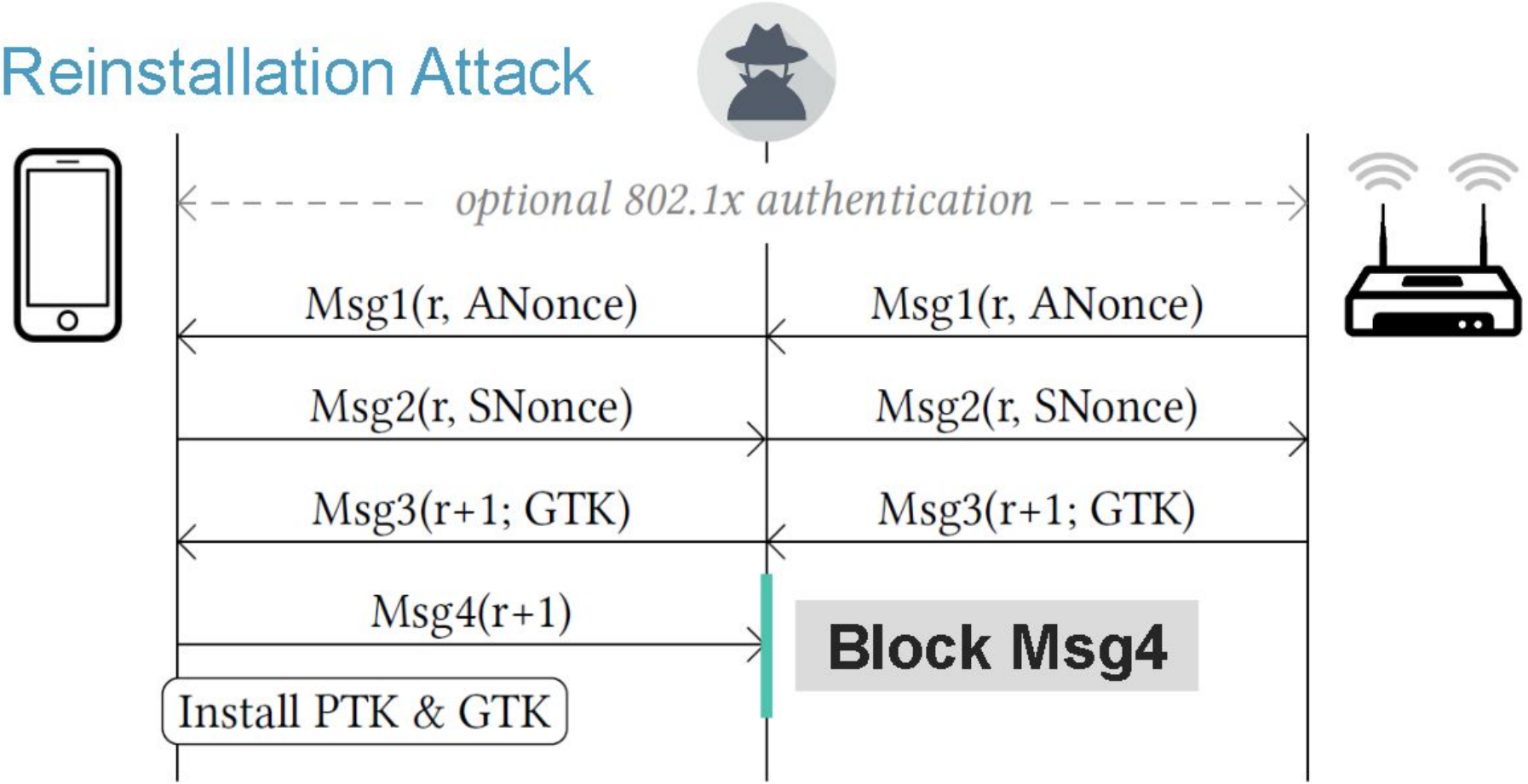
Reinstallation Attack



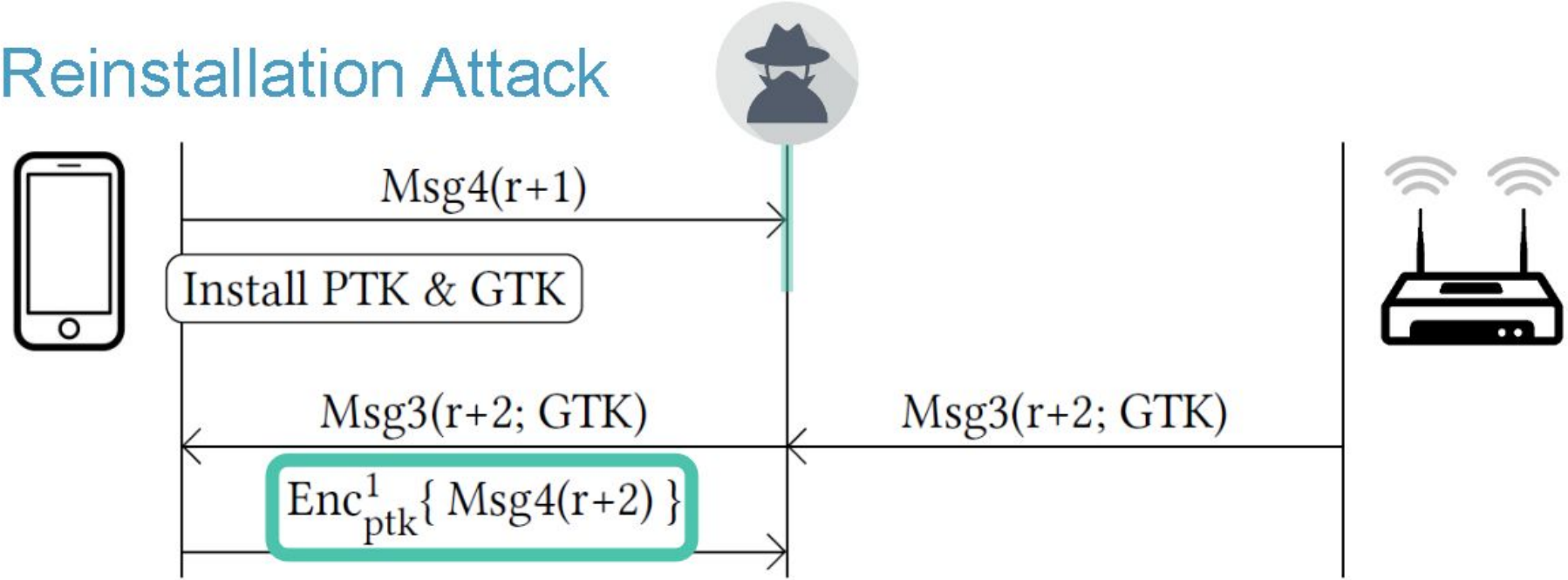
Reinstallation Attack



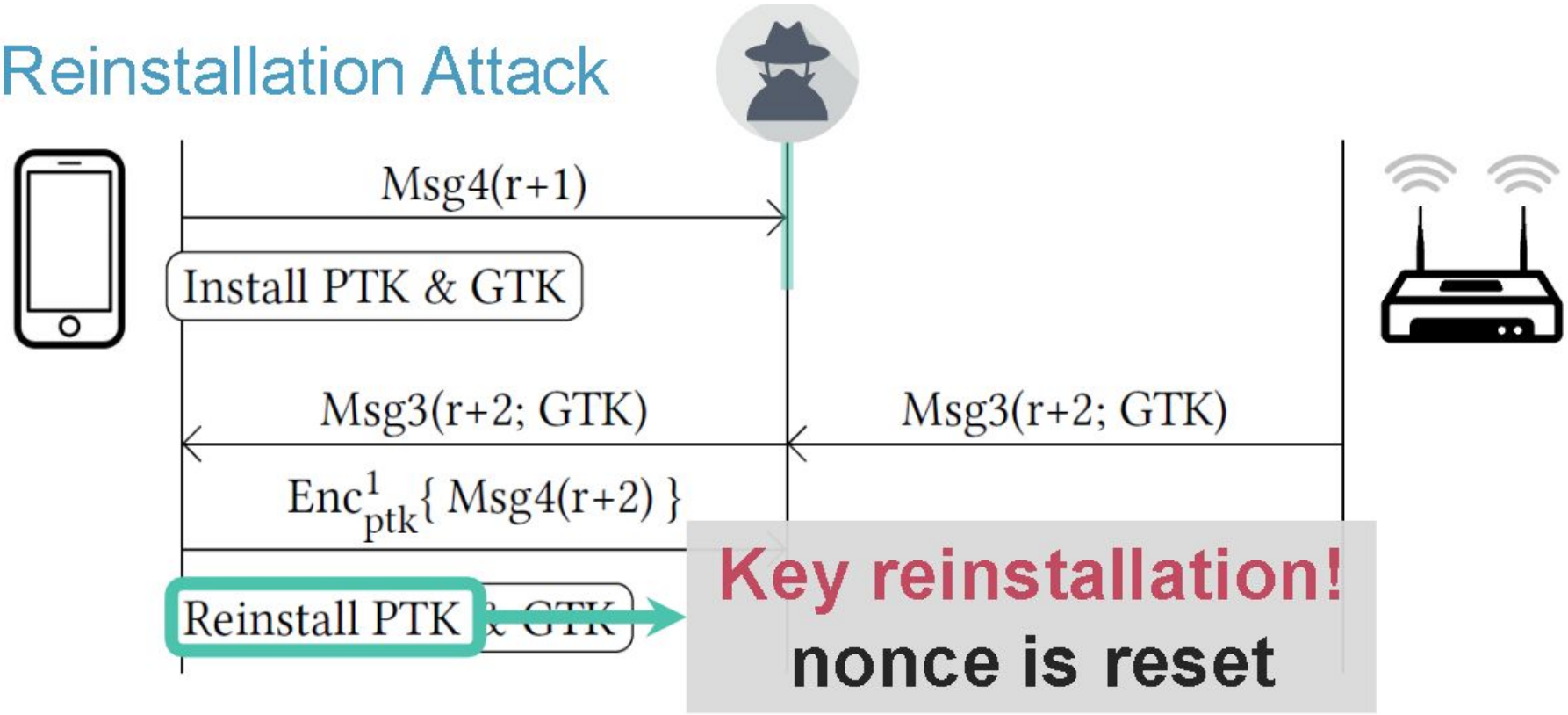
Reinstallation Attack



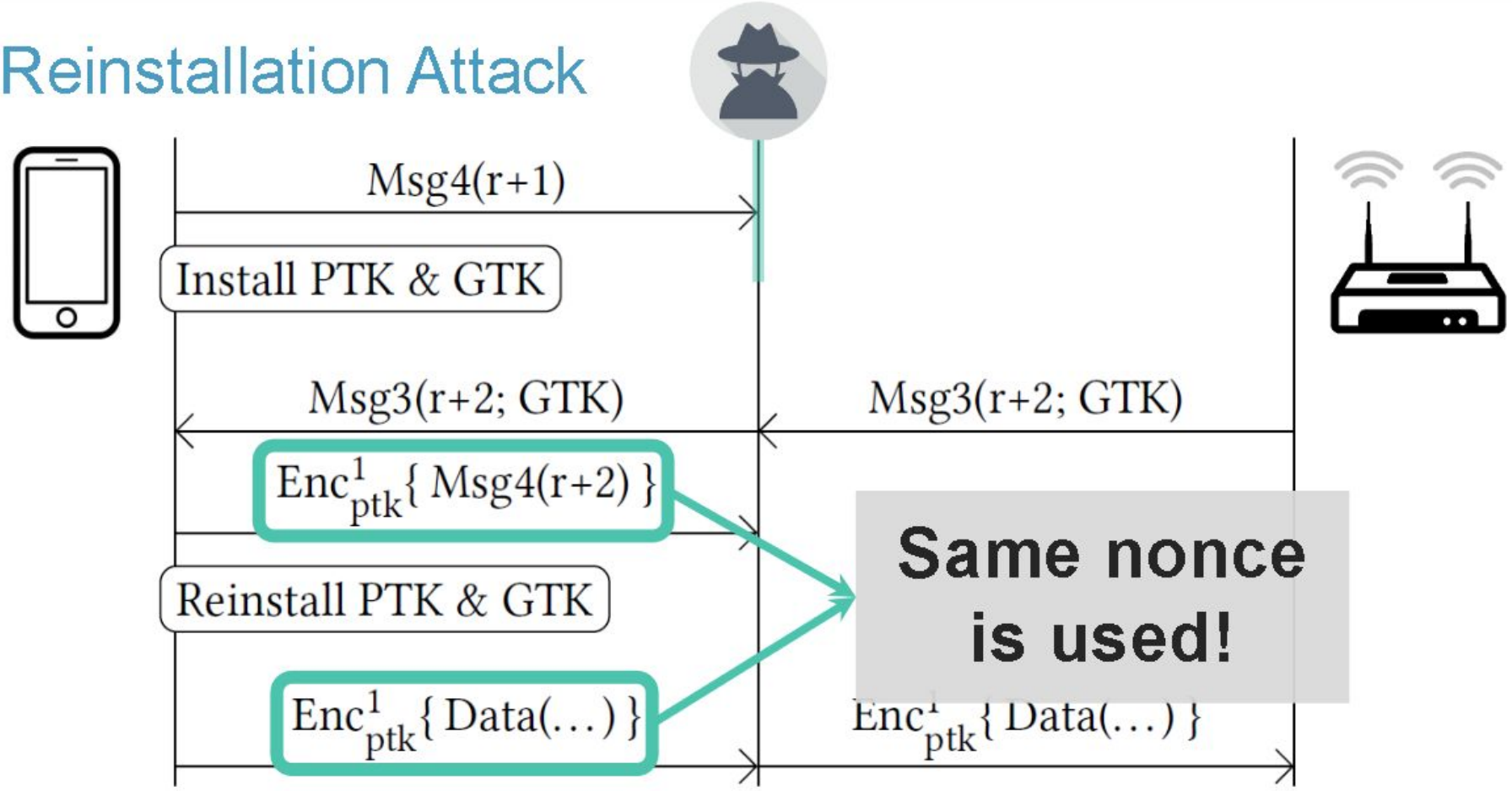
Reinstallation Attack



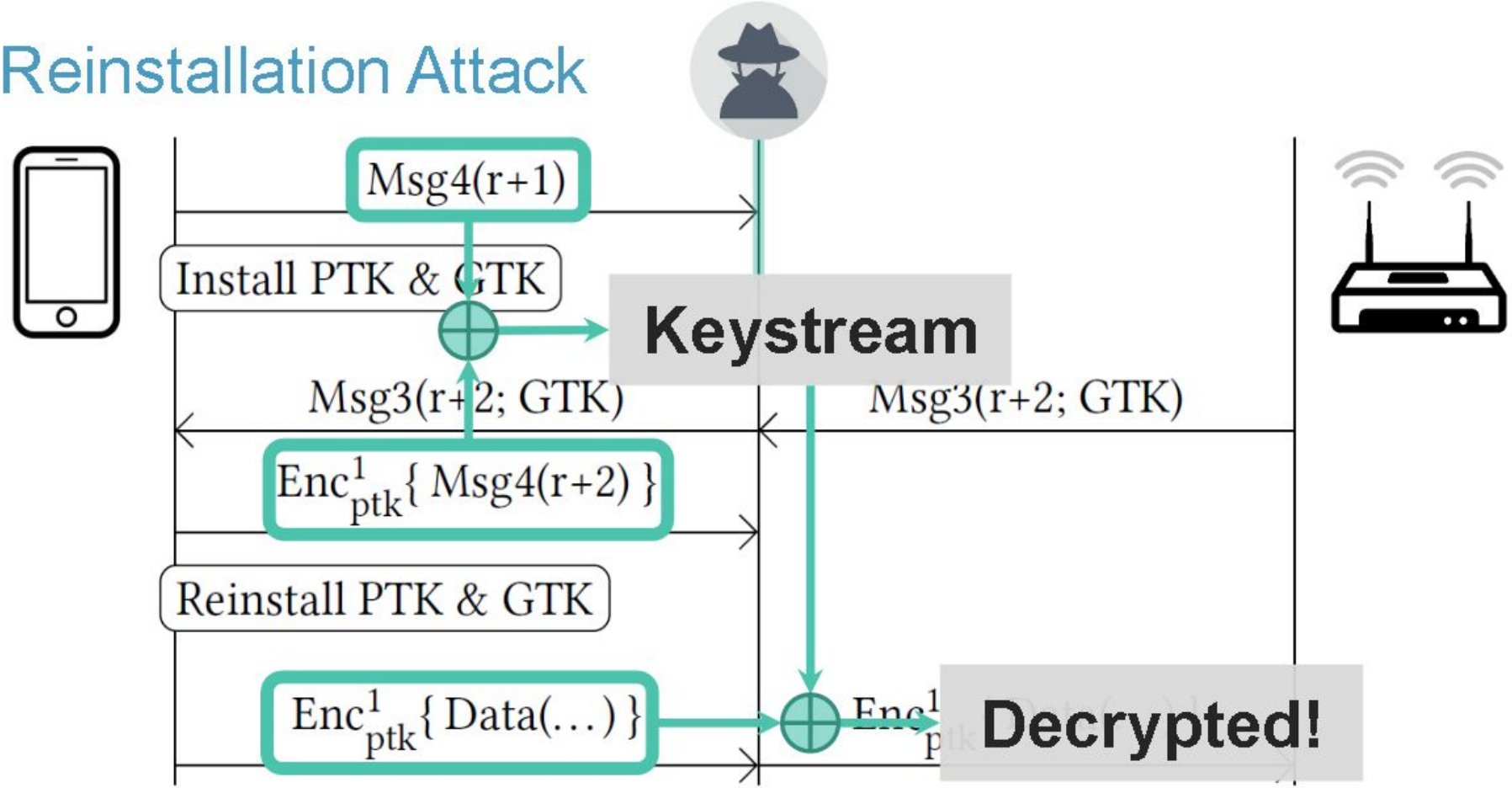
Reinstallation Attack



Reinstallation Attack



Reinstallation Attack



Demo

Practical Use of the Attack

- In practice there are some challenges to performing the attack
- Not all clients properly implement the state machine
- Windows and iOS do not accept retransmissions of message 3
- However attacks on other handshakes like the group key handshake still work

All-Zero encryption key

- This key reinstallation attack against the 4-way handshake uncovered special behavior in wpa_supplicant, which is a free software implementation of fully featured WPA2.
- Version 2.4 and 2.5 would install an all-zero encryption key when receiving retransmitted message 3
- This effect devices using linux and all Android 6.0 releases

Impact of Nonce Reuse

The impact of the nonce reuse depends on which data-confidentiality protocol is being used

	TKIP - WPA	CCMP - WPA2	GCMP - WPA3
Reuse of keystream	✔	✔	✔
Replay attacks	✔	✔	✔
Recover MIC key	✔		
Recover the authentication key			✔

Countermeasures

How can we prevent this attack?

1. The data-confidentiality protocol should check whether an already-in-use key is being installed
2. Make sure that a particular key is only installed once into the entity implementing the data-confidentiality protocol during a handshake execution

References

https://papers.mathyvanhoef.com/ccs2017.pdf - Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

https://papers.mathyvanhoef.com/nullcon2018-slides.pdf - KRACKingWPA2 by Forcing Nonce Reuse

https://getvoip.com/history-of-wifi/

https://www.grandmetric.com/2018/07/06/ended-wpa3-wi-fi-security-evolution/

https://www.scientificamerican.com/article/how-does-wi-fi-work/#:~:text=WiFi%20stands%20for%20Wireless%20Fidelity,to%20send%20signals%20between%20devices

https://cybersecurity.att.com/blogs/security-essentials/security-issues-of-wifi-how-it-works