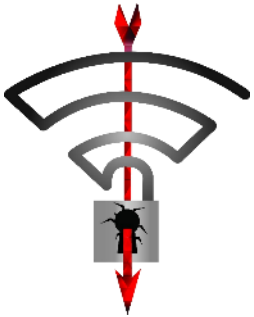
How WPA2 got KRACKed using Key Reinstallation Attacks

Mathy Vanhoef — @vanhoefm

ITF Belgium, 24 May 2018

KU LEUVEN DistriNet

Overview



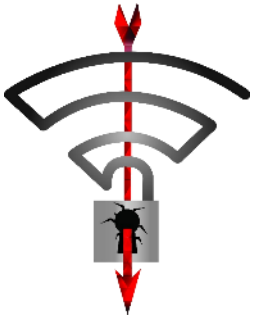
Key reinstalls in
4-way handshake

Misconceptions

Practical impact

Lessons learned

Overview



Key reinstalls in 4-way handshake

Misconceptions

Practical impact

Lessons learned

The 4-way handshake

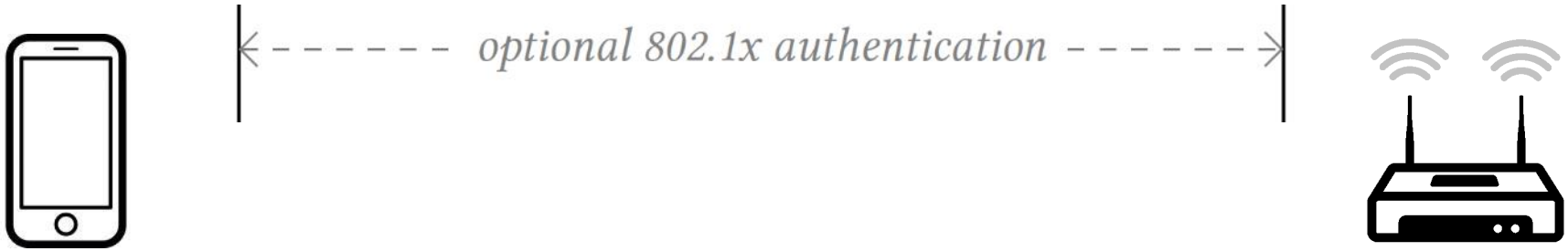
Used to connect to any protected Wi-Fi network

- Provides mutual authentication
- Negotiates fresh PTK: pairwise transient key

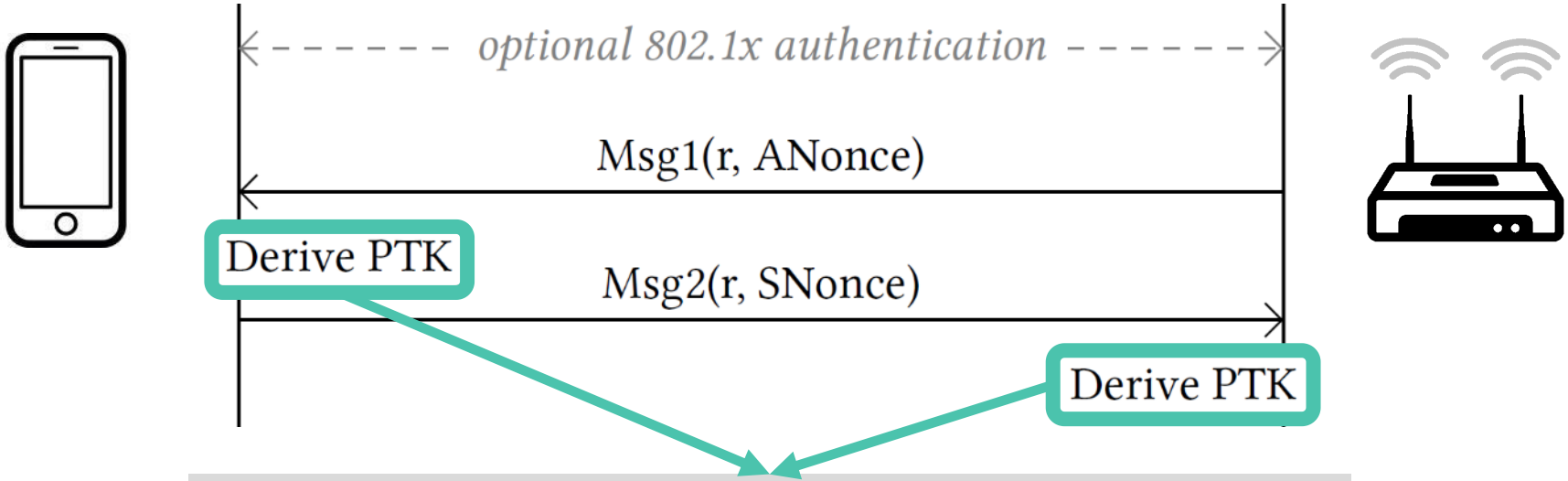
Appeared to be secure:

- No attacks in over a decade (apart from password guessing)
- Proven that negotiated key (PTK) is secret[1]
- And encryption protocol proven secure[7]

4-way handshake (simplified)

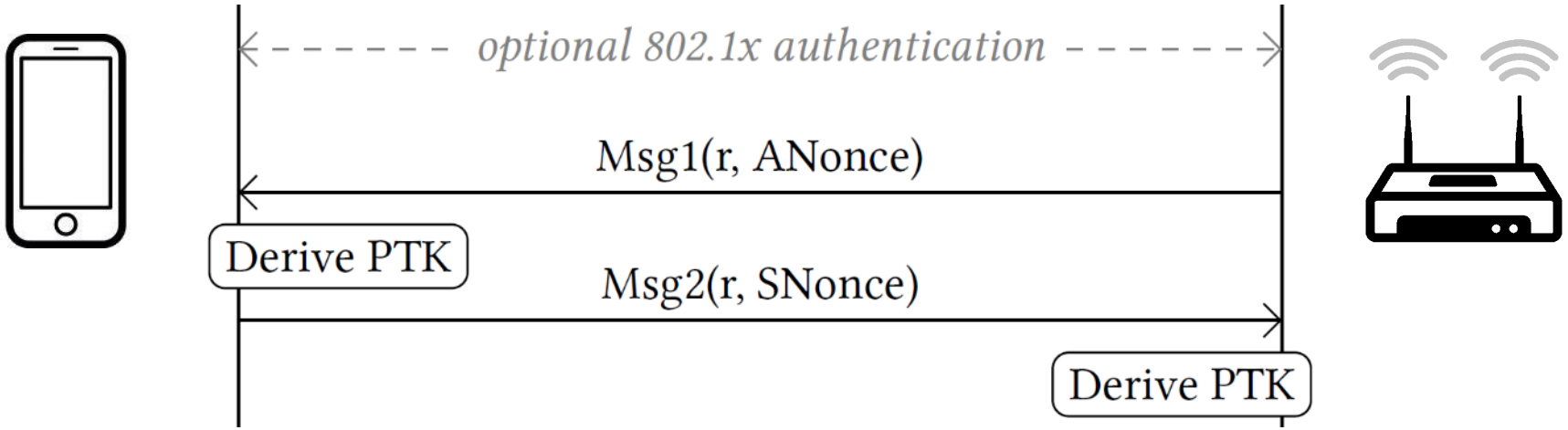


4-way handshake (simplified)

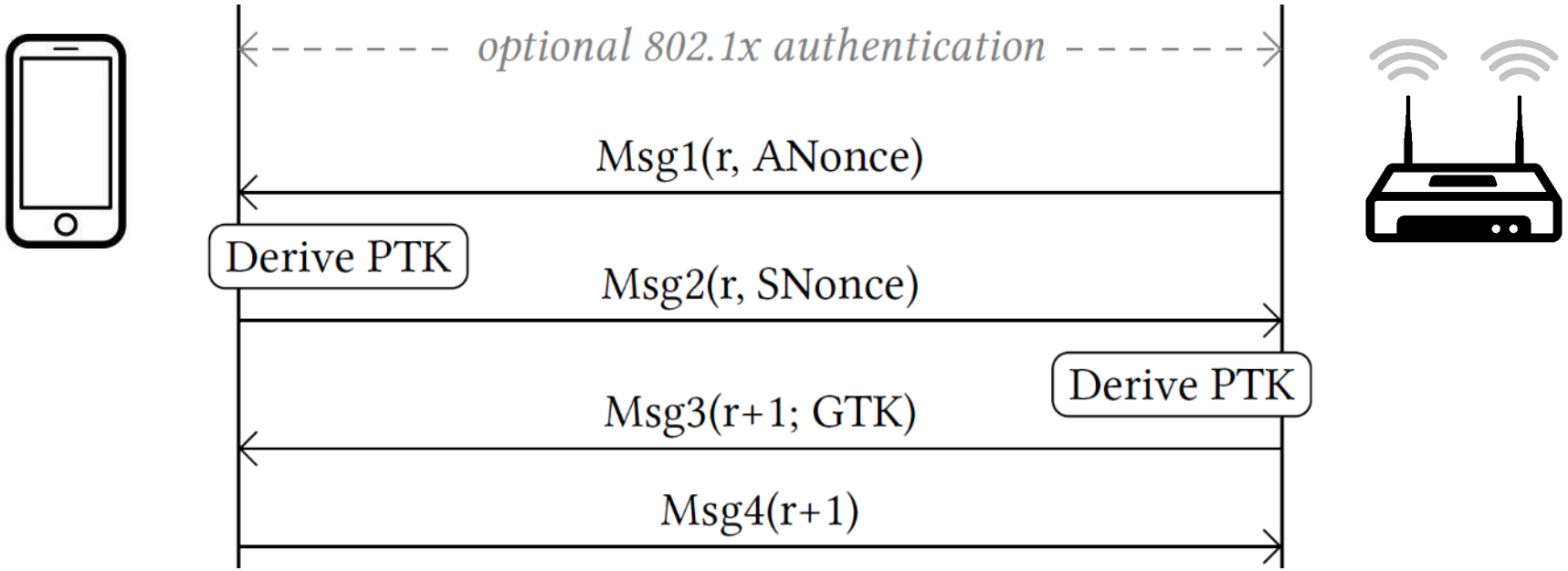


PTK = Combine(shared secret, ANonce, SNonce)

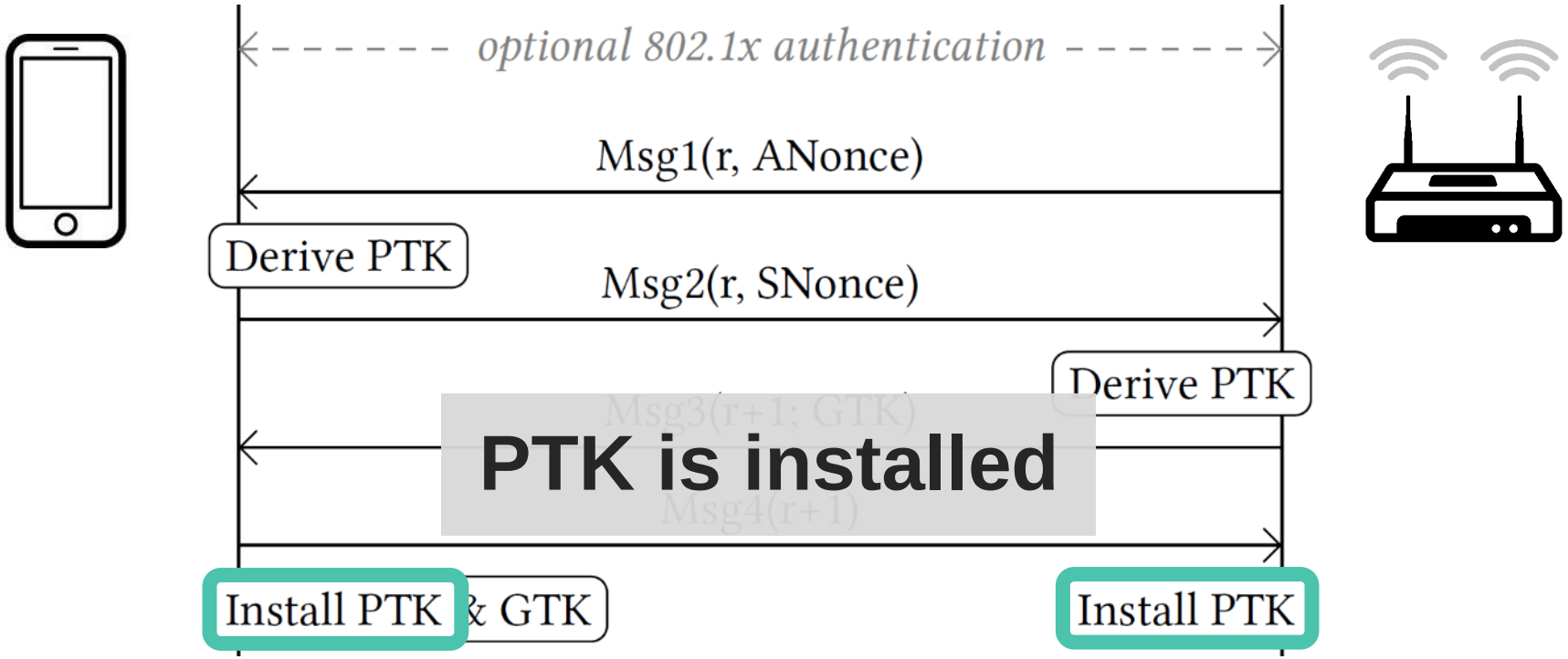
4-way handshake (simplified)



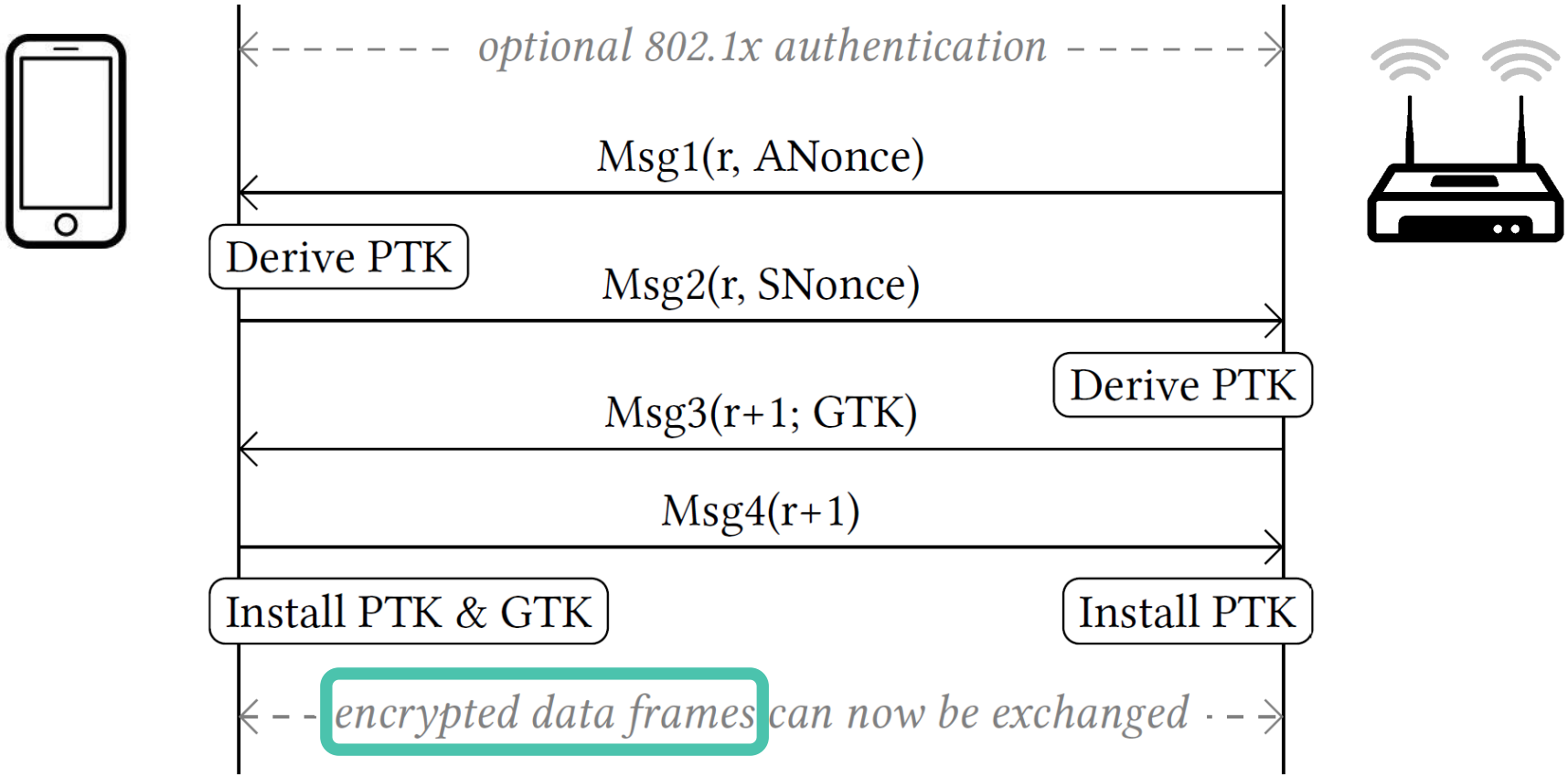
4-way handshake (simplified)



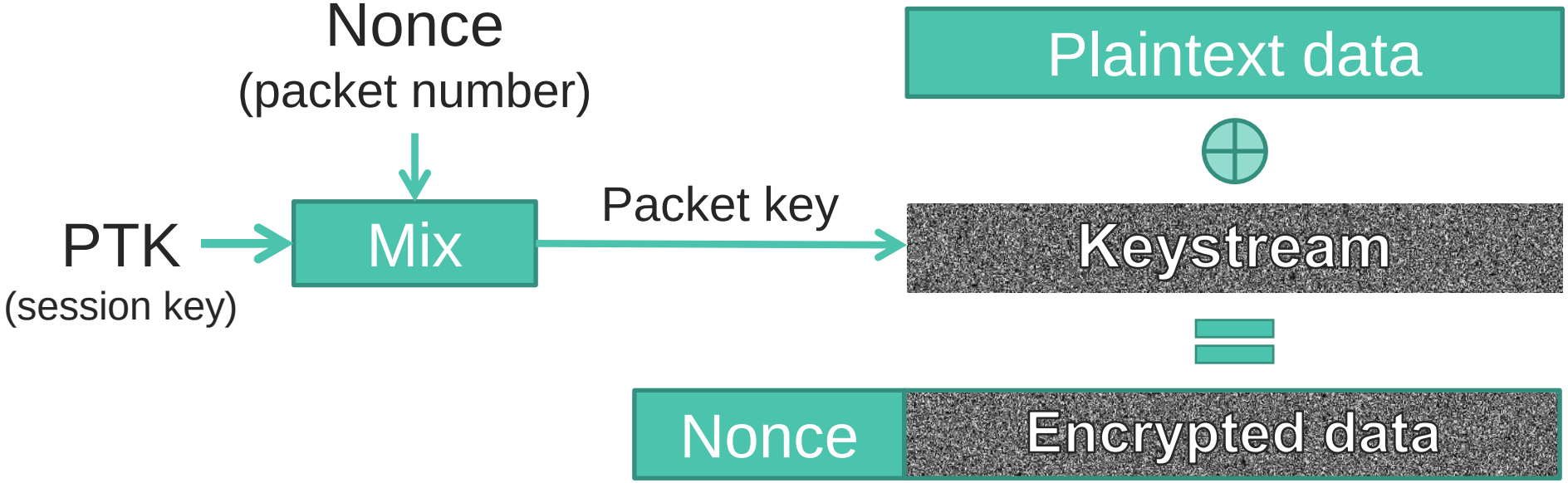
4-way handshake (simplified)



4-way handshake (simplified)

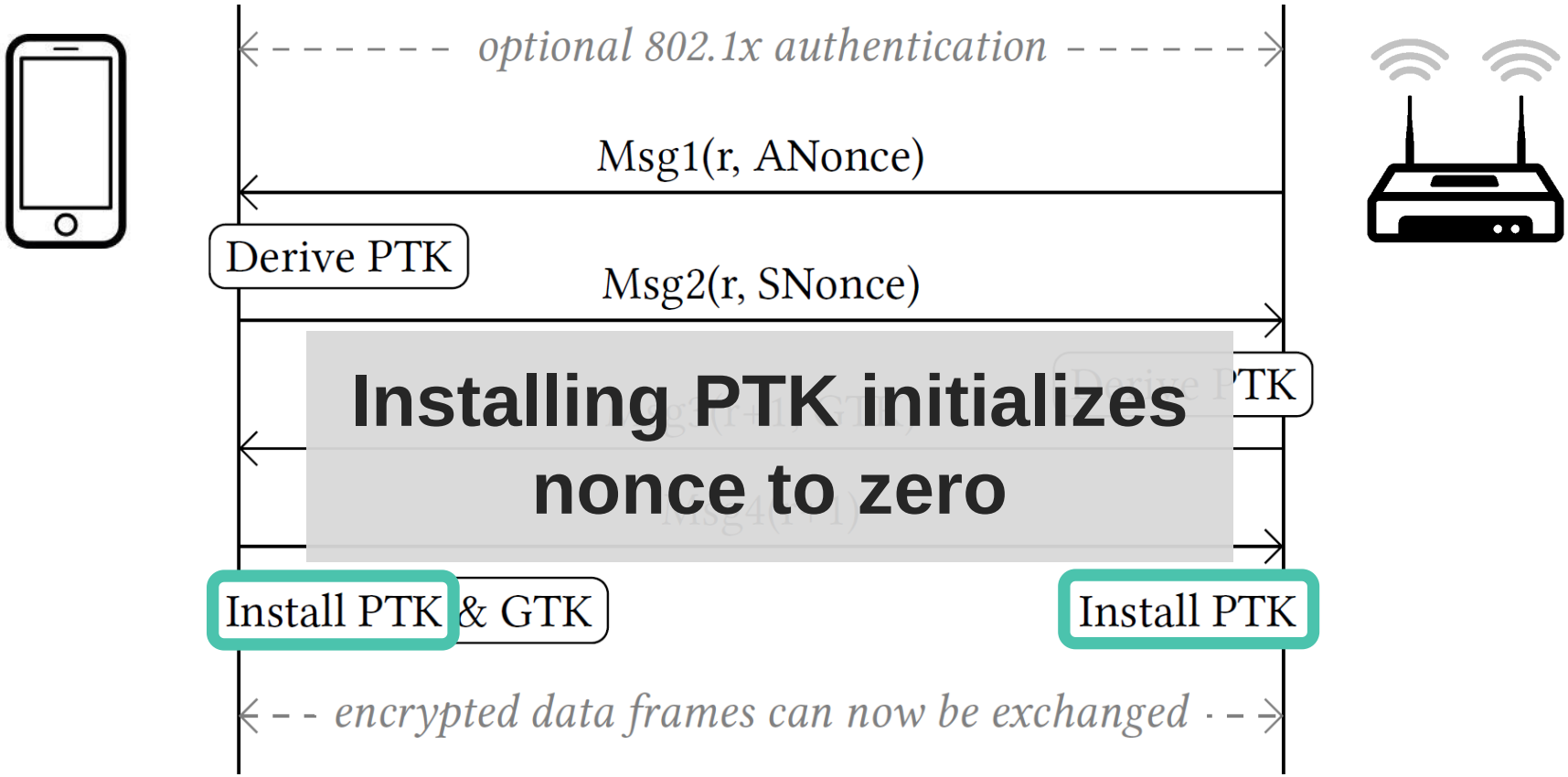


Frame encryption (simplified)



→ Nonce reuse implies keystream reuse (in all WPA2 ciphers)

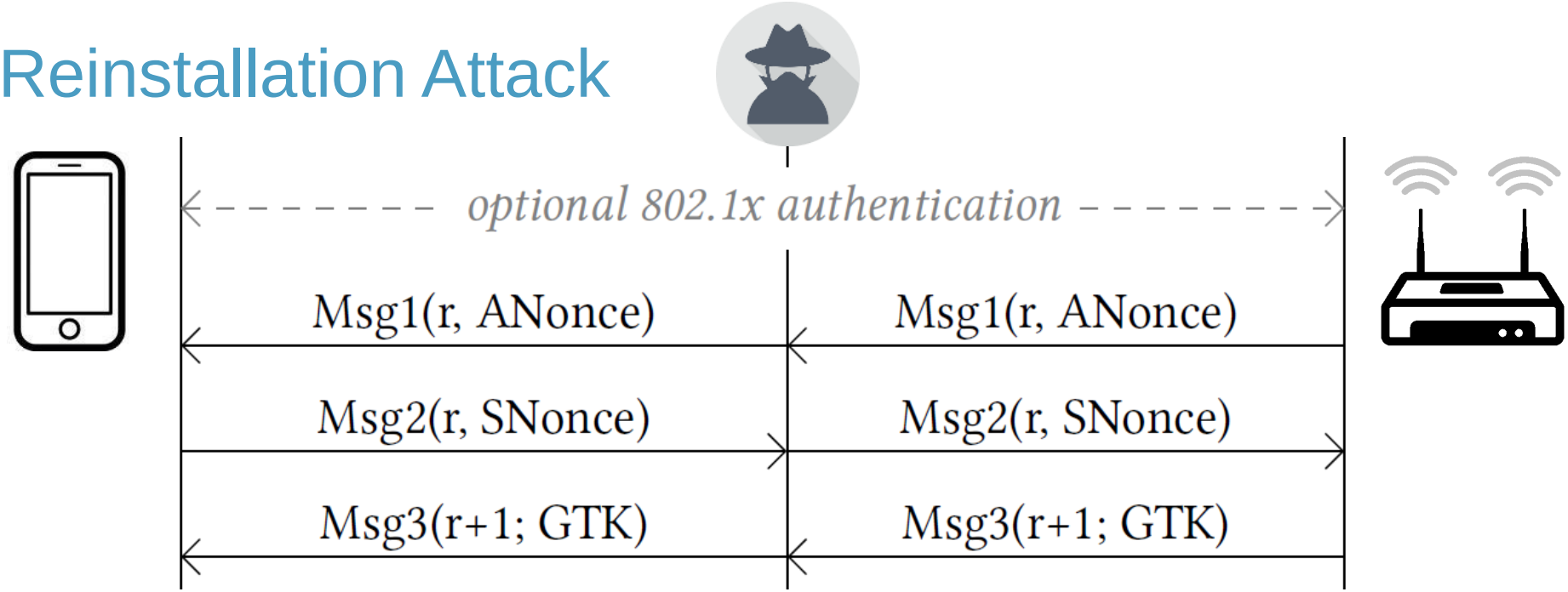
4-way handshake (simplified)



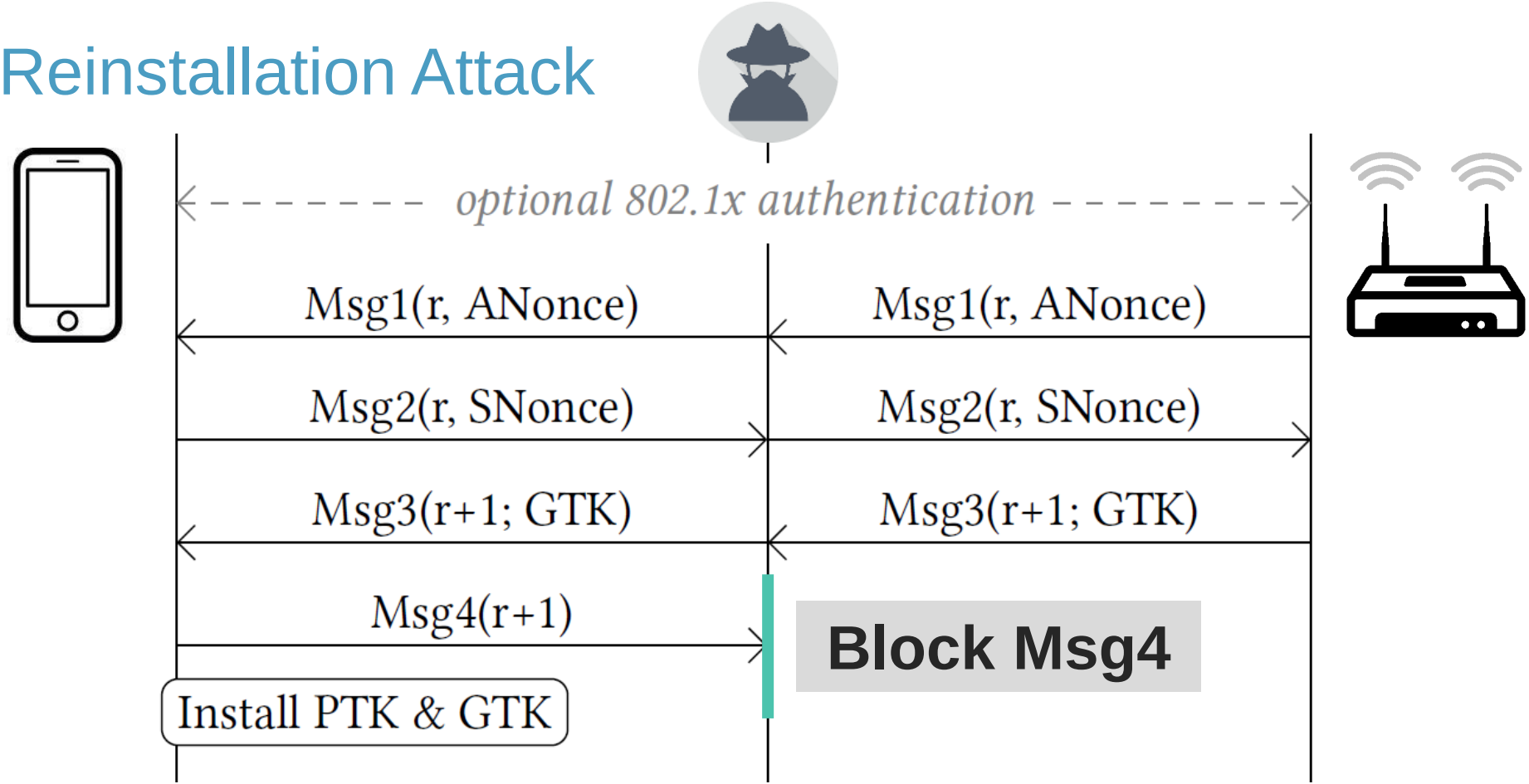
Reinstallation Attack

Reinstallation Attack

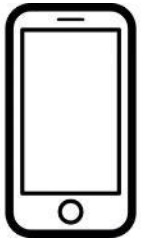
Reinstallation Attack

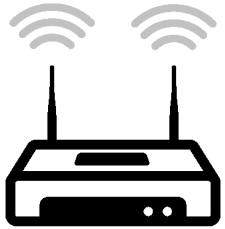


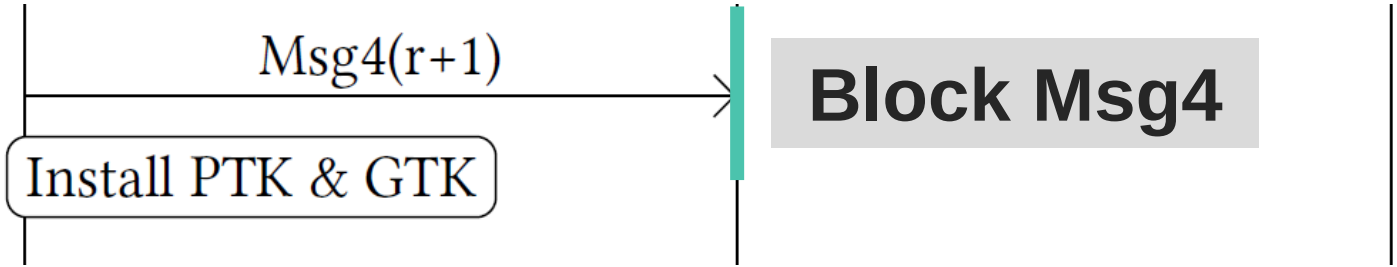
Reinstallation Attack



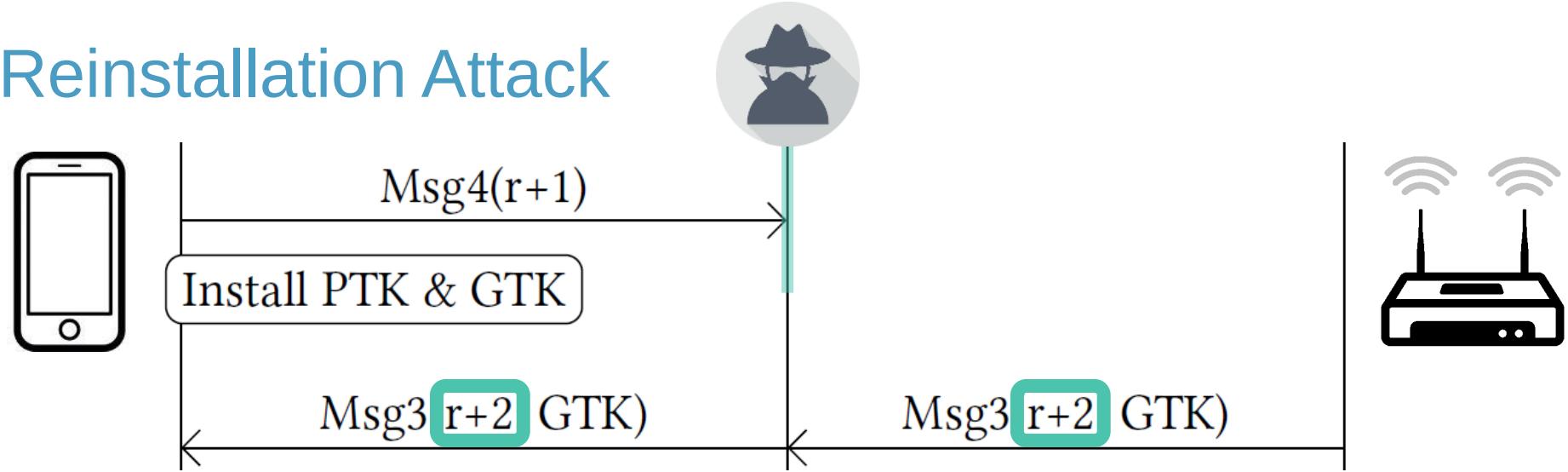
Reinstallation Attack





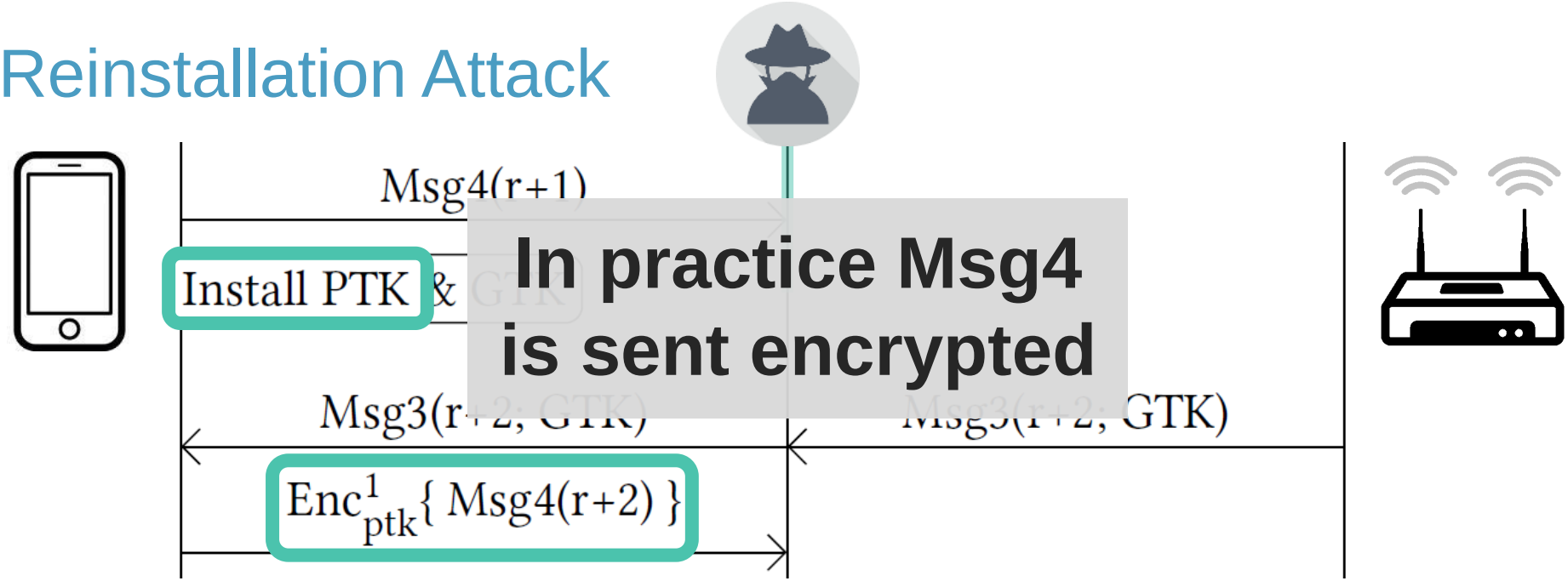


Reinstallation Attack



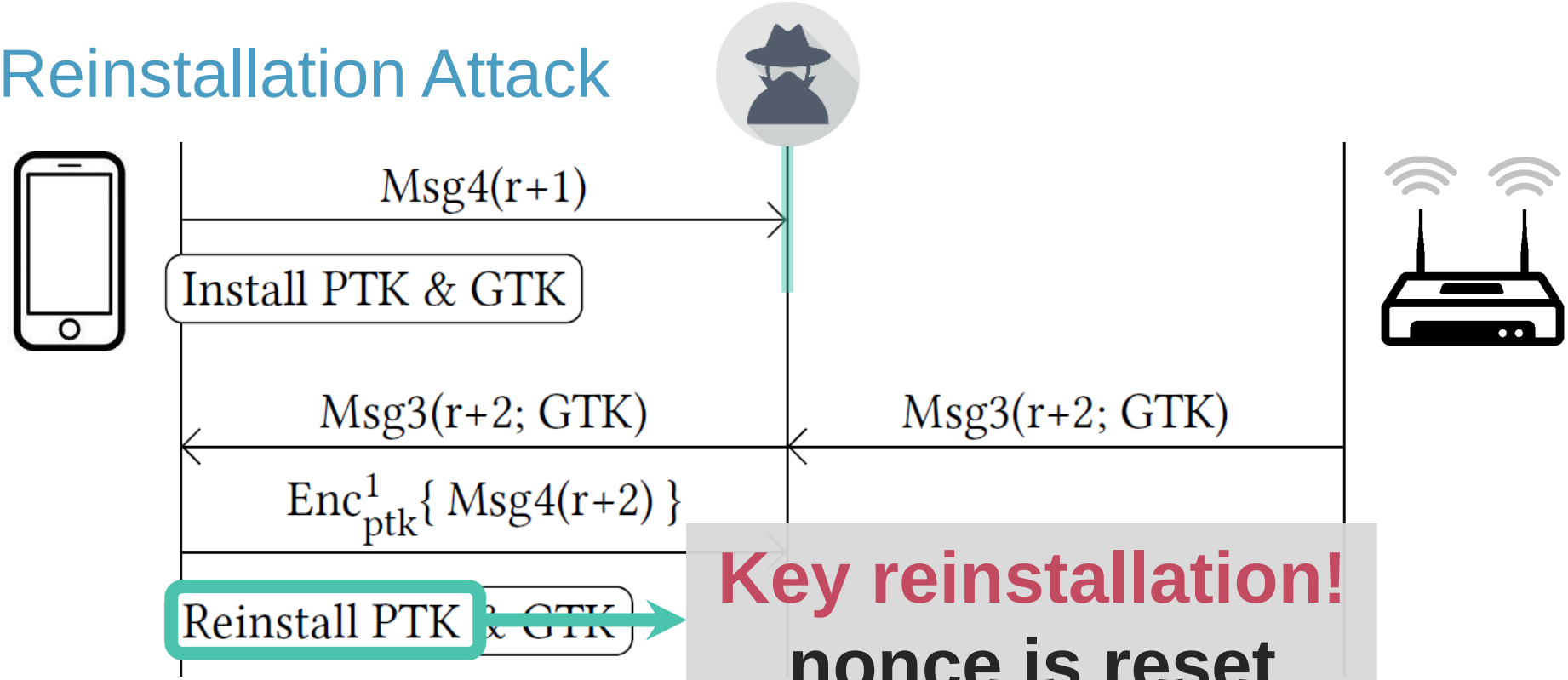
New replay counter

Reinstallation Attack

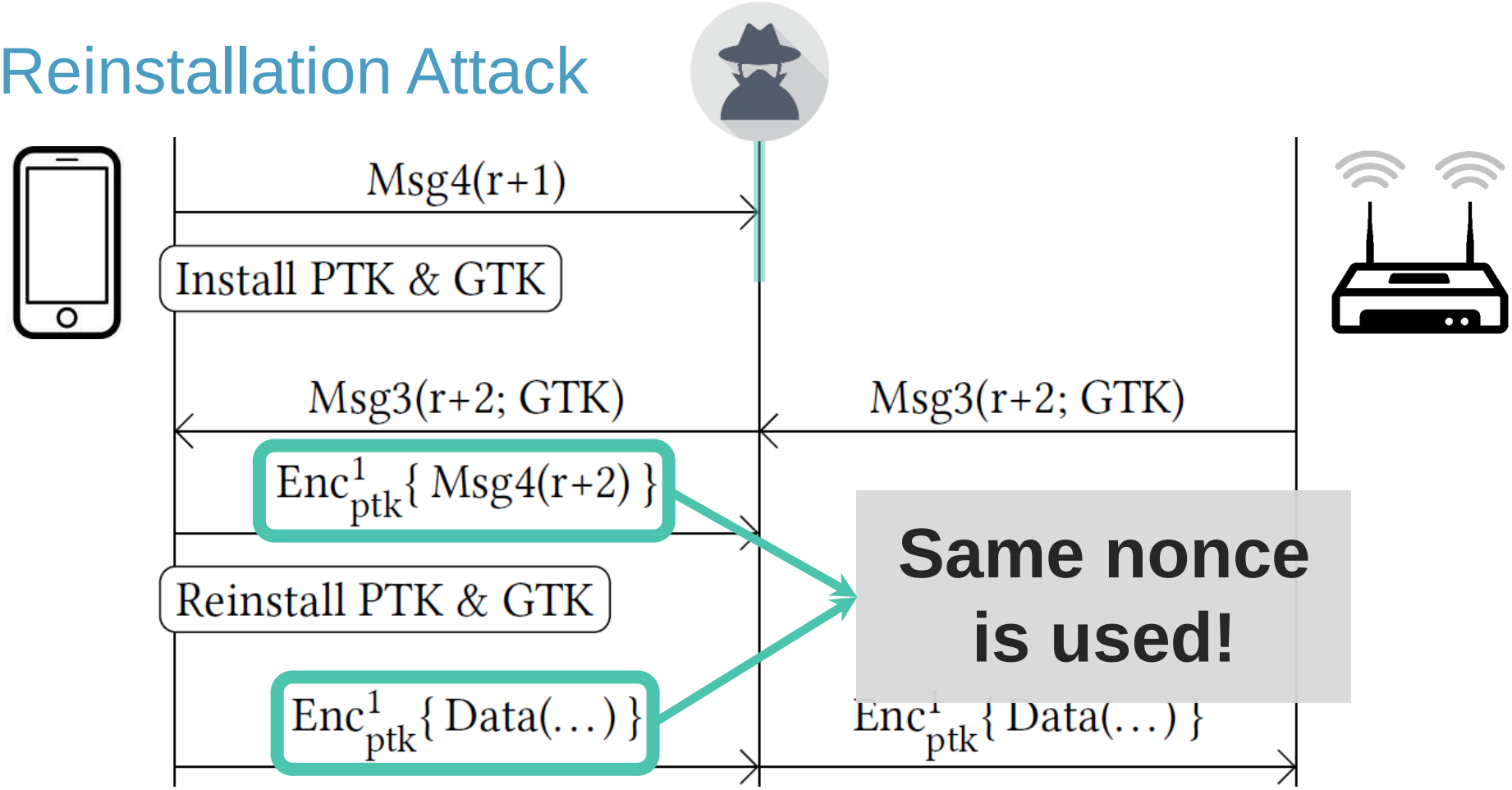


In practice Msg4 is sent encrypted

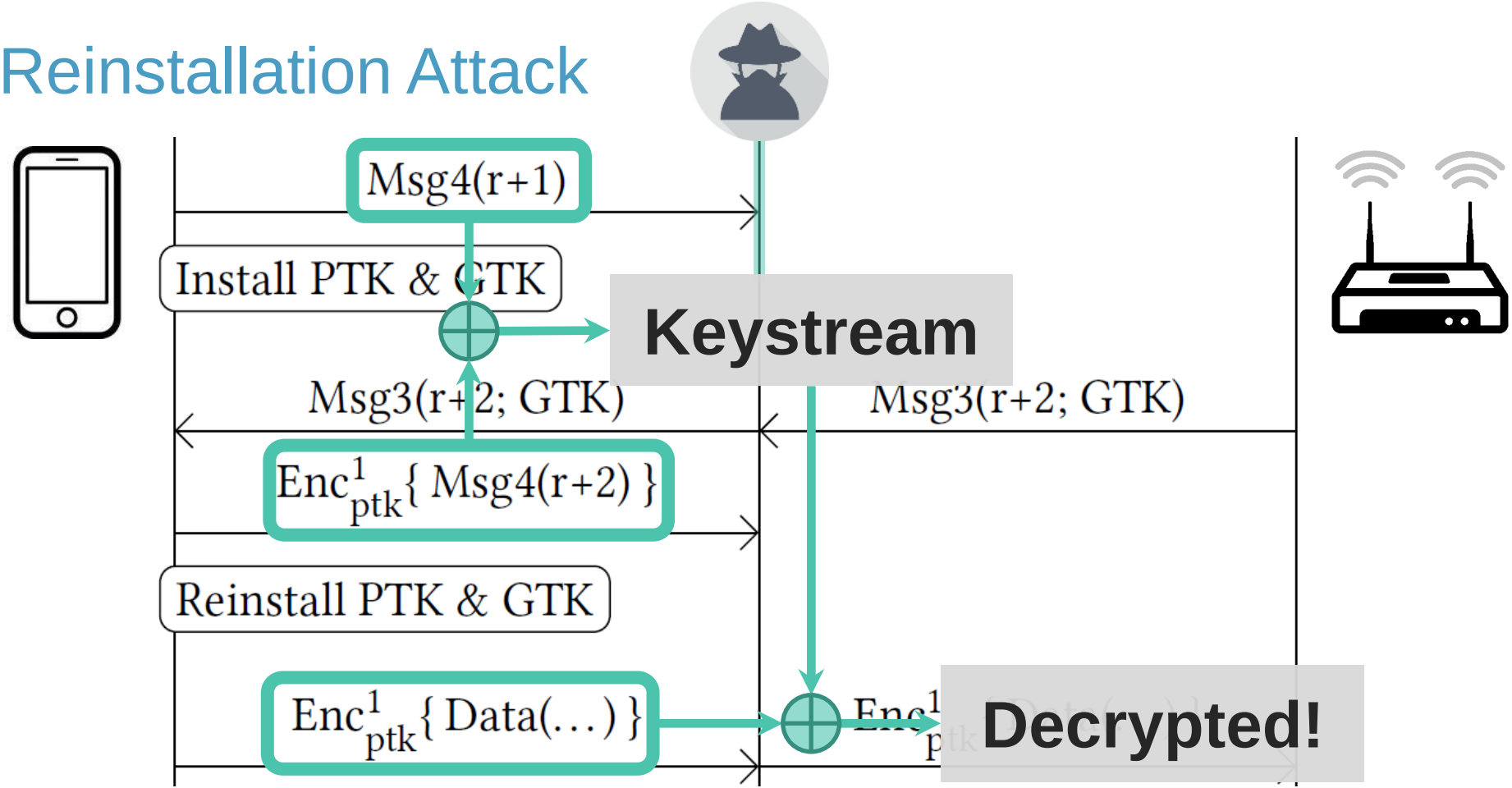
Reinstallation Attack



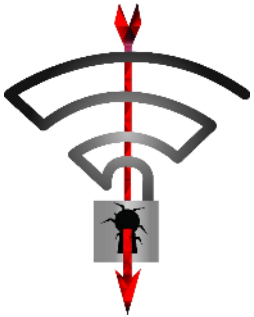
Reinstallation Attack



Reinstallation Attack



Overview



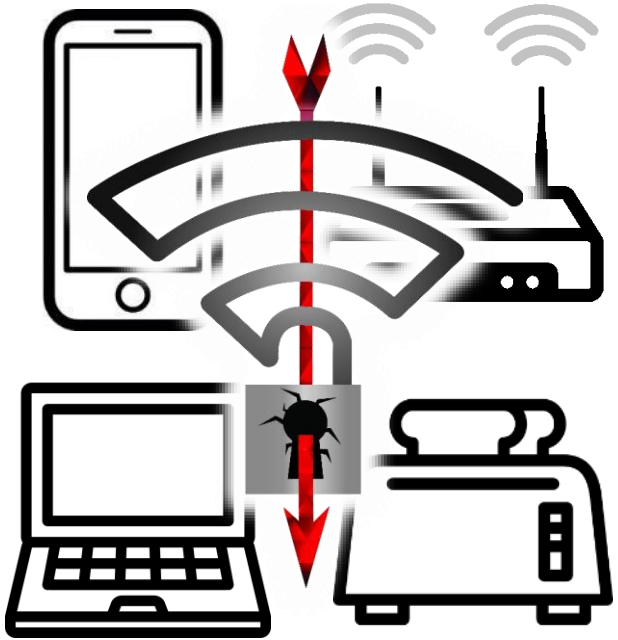
Key reinstalls in
4-way handshake

Misconceptions

Practical impact

Lessons learned

General impact



Transmit nonce reset

Decrypt frames sent by victim

Receive replay counter reset

Replay frames towards victim

Cipher suite specific

AES-CCMP: No practical frame forging attacks

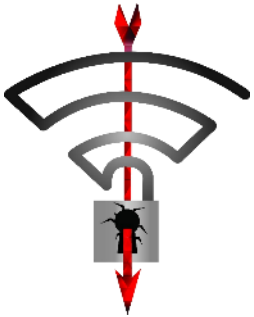
WPA-TKIP:

- Can recover authentication key
- **Forge/inject** frames sent by the device under attack

GCMP (WiGig):

- Can recover authentication key
- **Forge/inject** frames in **both directions**

Overview



Key reinstalls in
4-way handshake

Misconceptions

Practical impact

Lessons learned

Misconceptions

Updating only the client or AP is sufficient

› Both vulnerable clients & vulnerable APs must apply patches

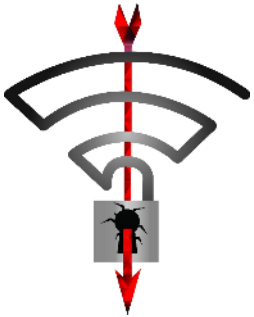
Need to be close to network and victim

› Can use special antenna from afar

Corporate networks (802.1x) aren’t affected

› Also use 4-way handshake & are affected

Overview



Key reinstalls in
4-way handshake

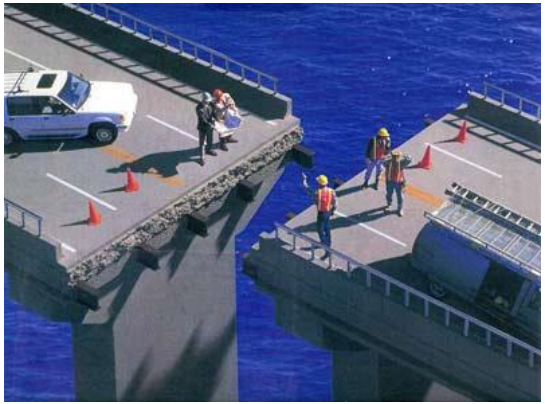
Misconceptions

Practical impact

Lessons learned

Limitations of formal proofs

- 4-way handshake proven secure
- Encryption protocol proven secure



The combination was not proven secure!

Conclusion

- Flaw is in WPA2 standard
- Proven correct but is insecure!
- Attack has practical impact
- Update all clients & check APs

Thank you!

Questions?

krackattacks.com

Implementation specific

iOS 10 and Windows: 4-way handshake not affected

- **Cannot decrypt or replay traffic**
- But iOS 11 is vulnerable!

wpa_supplicant 2.4+

- Wi-Fi client used on Linux and Android 6.0+
- On retransmitted msg3 will **install all-zero key**