Improved KRACK Attacks Against WPA2 Implementations

Mathy Vanhoef — @vanhoefm

OPCDE, Dubai, 7 April 2018

KU LEUVEN DistriNet

Overview

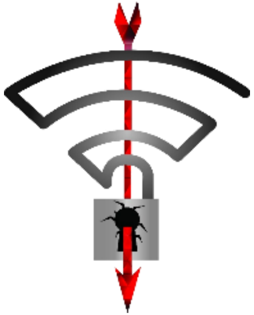
Key reinstalls in 4-way handshake

New KRACKs

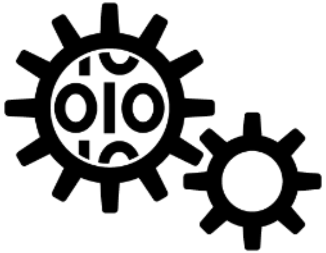
Practical impact

Lessons learned

Overview



Key reinstalls in 4-way handshake



New KRACKs

Practical impact

Lessons learned

The 4-way handshake

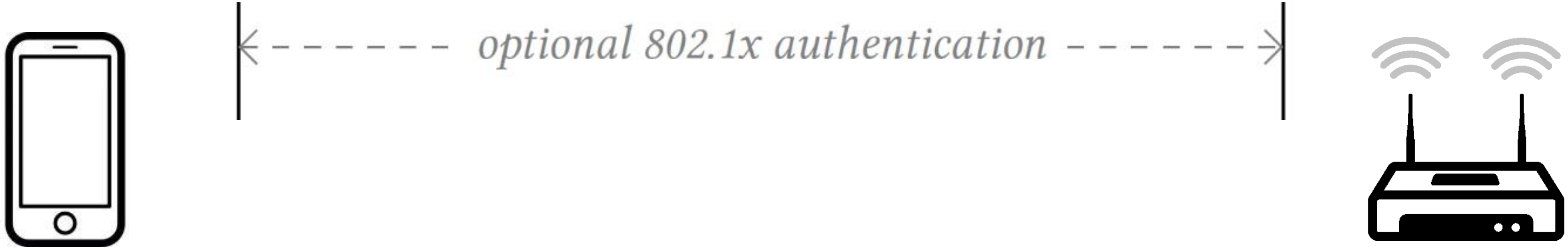
Used to connect to any protected Wi-Fi network

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

Appeared to be secure:

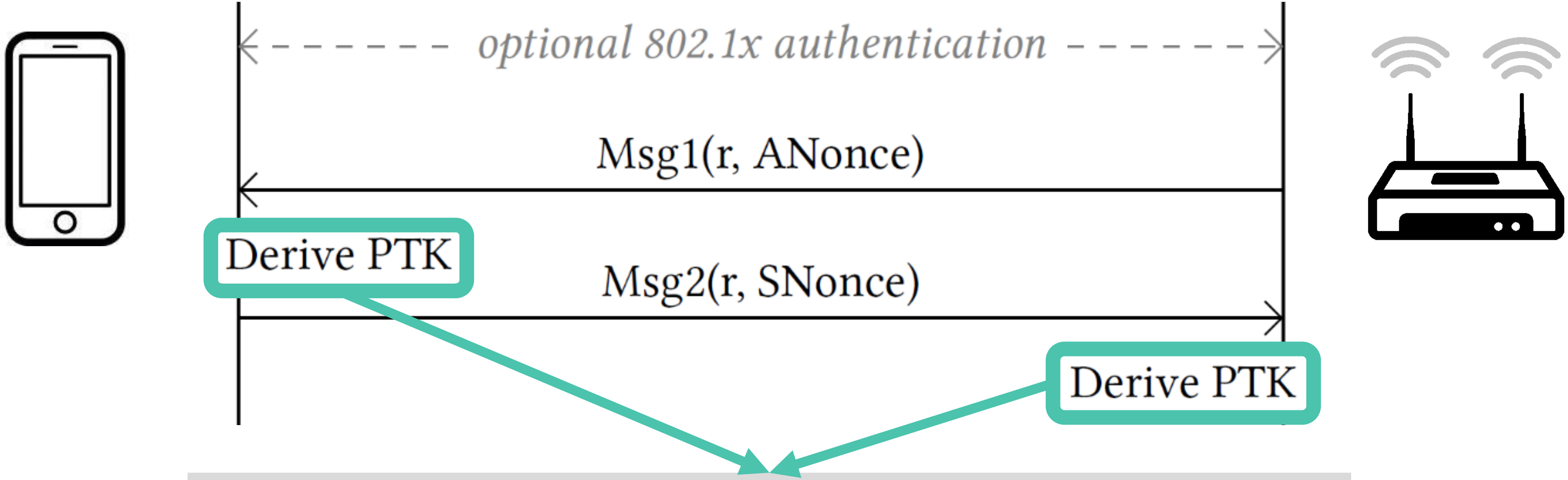
- No attacks in over a decade (apart from password guessing)
- Proven that negotiated key (PTK) is secret[1]
- And encryption protocol proven secure[5]

4-way handshake (simplified)



optional 802.1x authentication

4-way handshake (simplified)



optional 802.1x authentication

Msg1(r, ANonce)

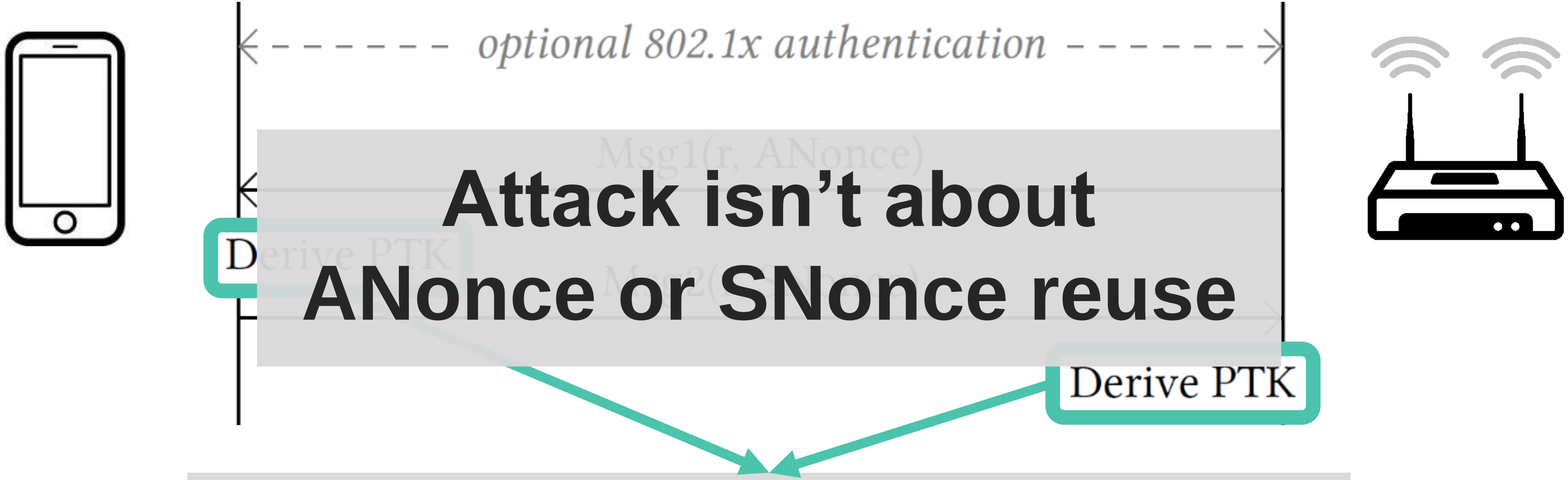
Derive PTK

Msg2(r, SNonce)

Derive PTK

PTK = Combine(shared secret, ANonce, SNonce)

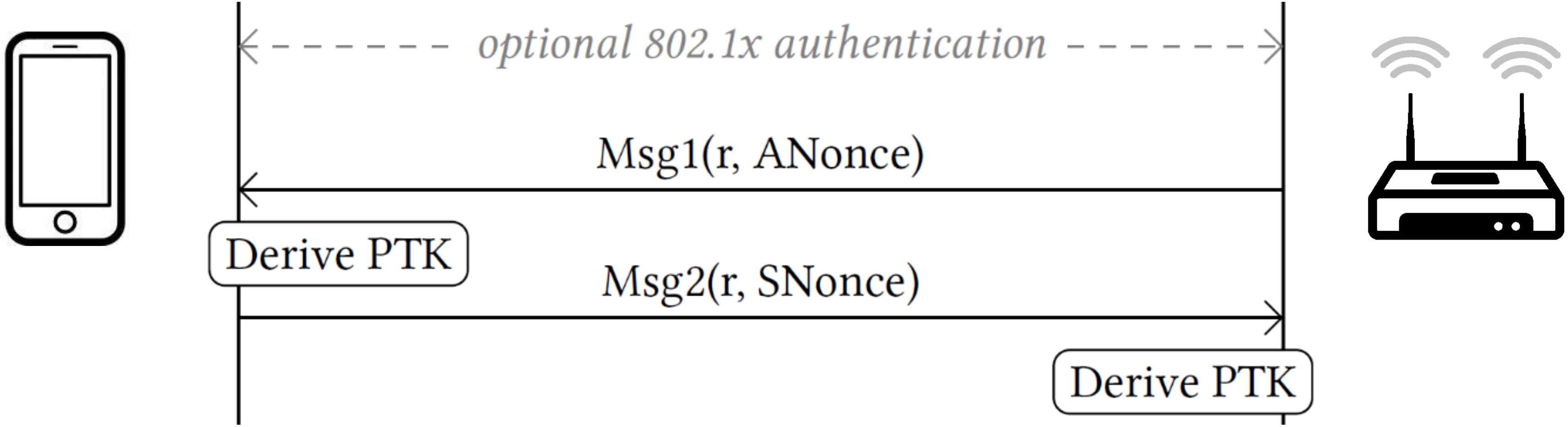
4-way handshake (simplified)



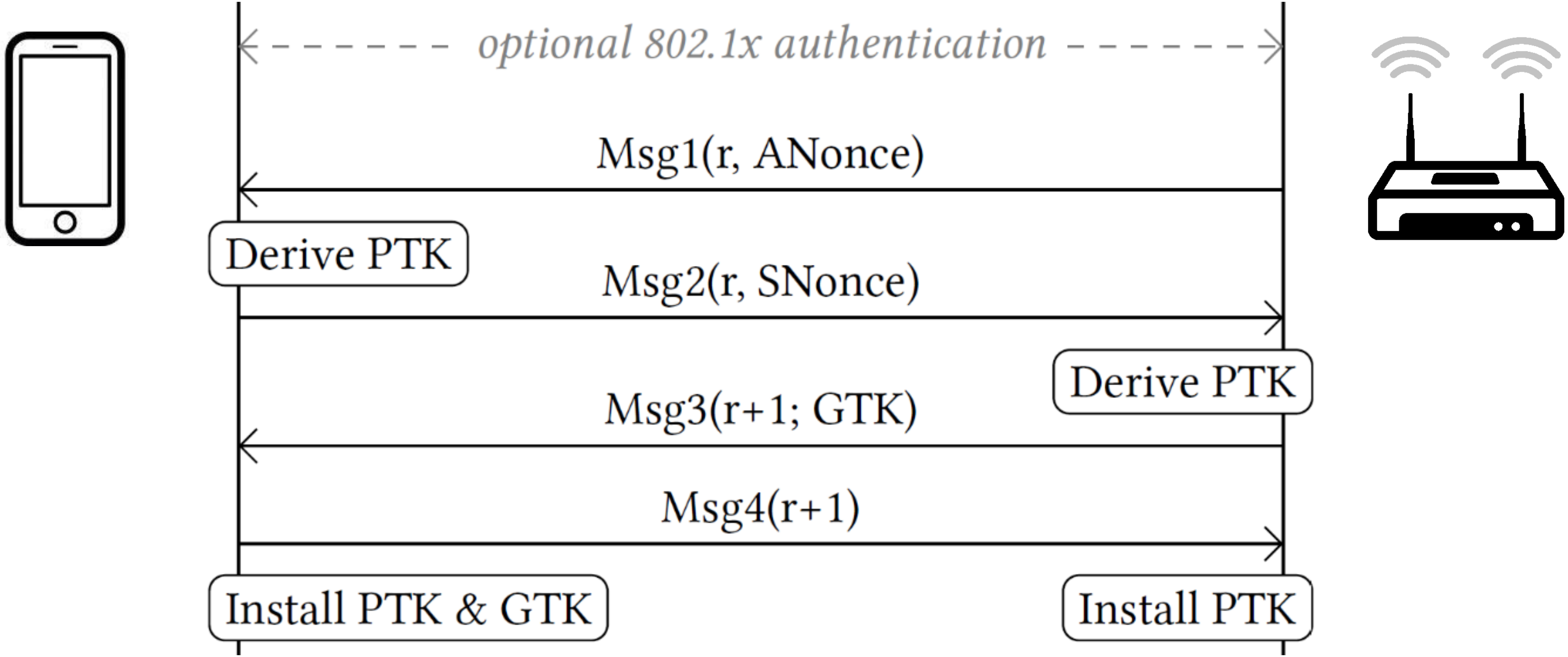
Attack isn’t about ANonce or SNonce reuse

PTK = Combine(shared secret, ANonce, SNonce)

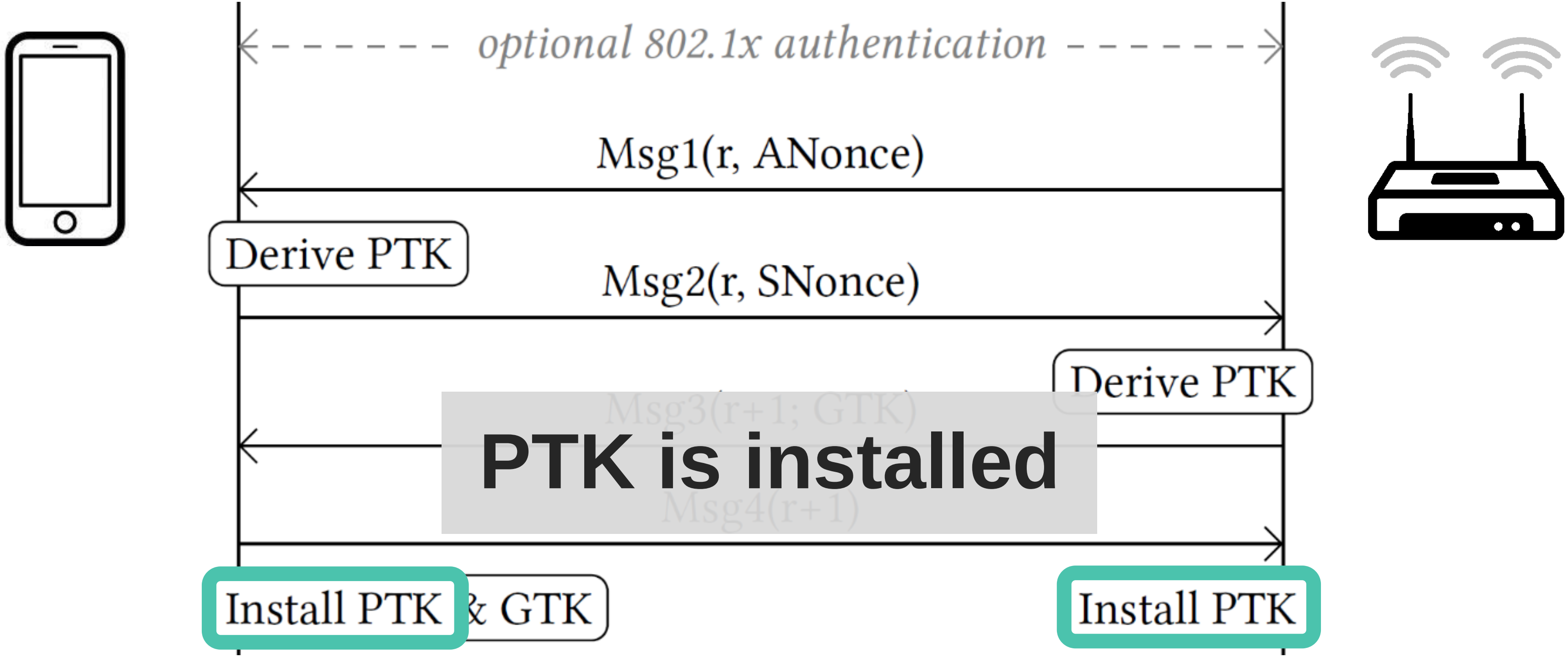
4-way handshake (simplified)



4-way handshake (simplified)

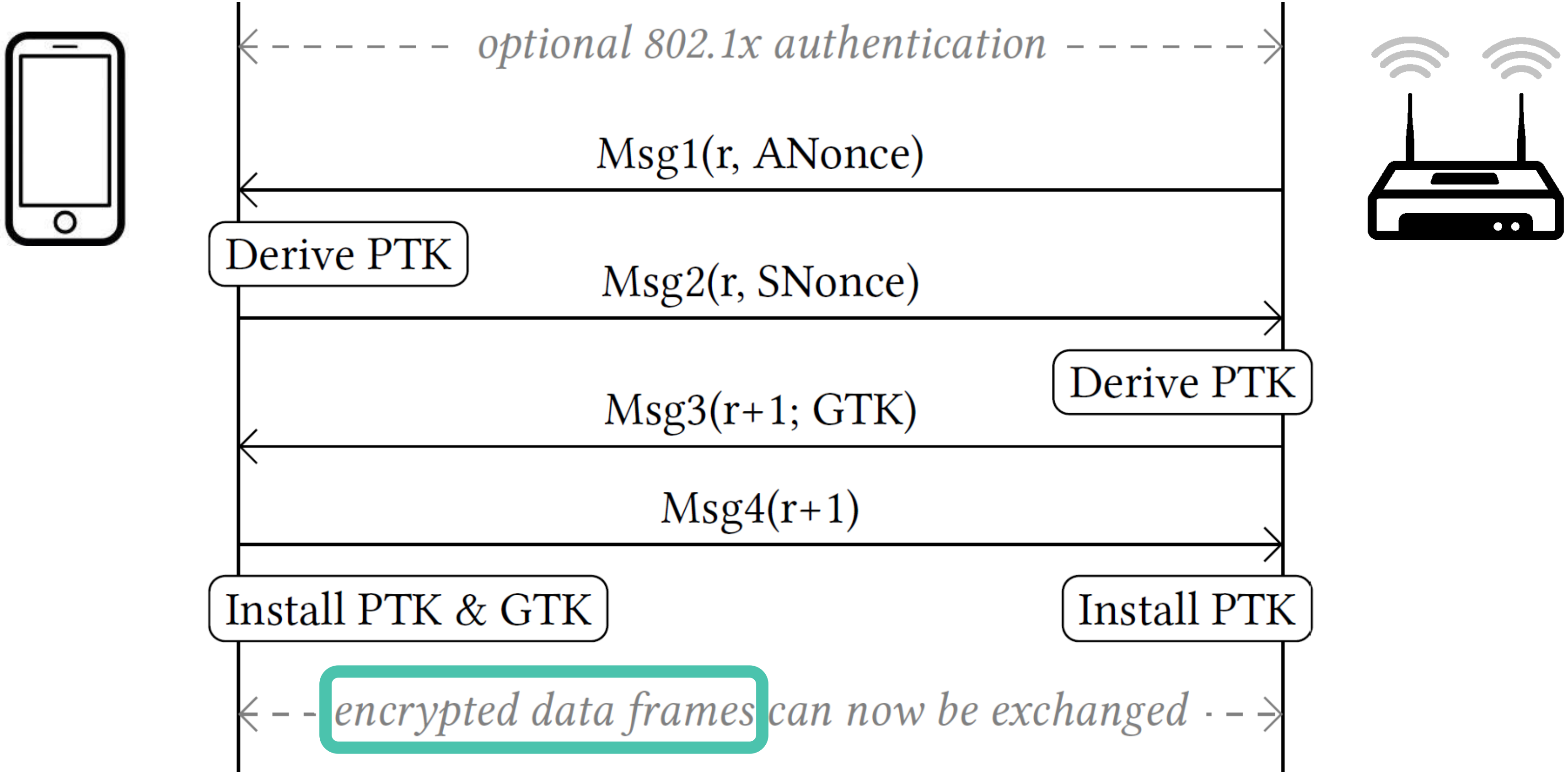


4-way handshake (simplified)



PTK is installed

4-way handshake (simplified)



optional 802.1x authentication

Msg1(r, ANonce)

Derive PTK

Msg2(r, SNonce)

Derive PTK

Msg3(r+1; GTK)

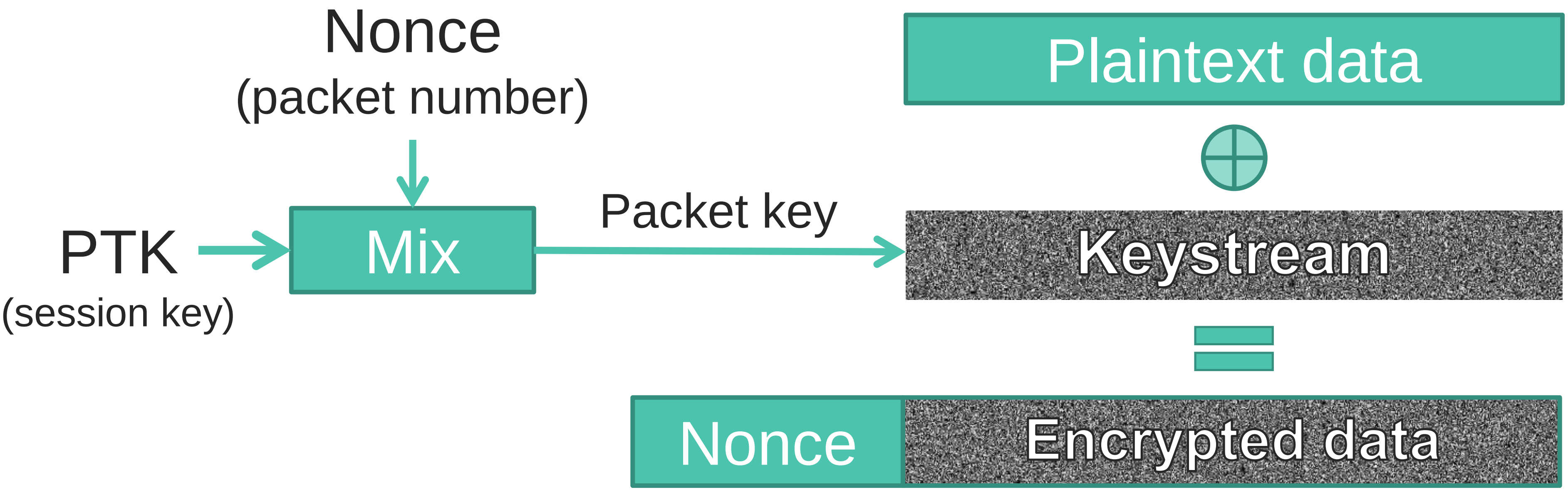
Msg4(r+1)

Install PTK & GTK

Install PTK

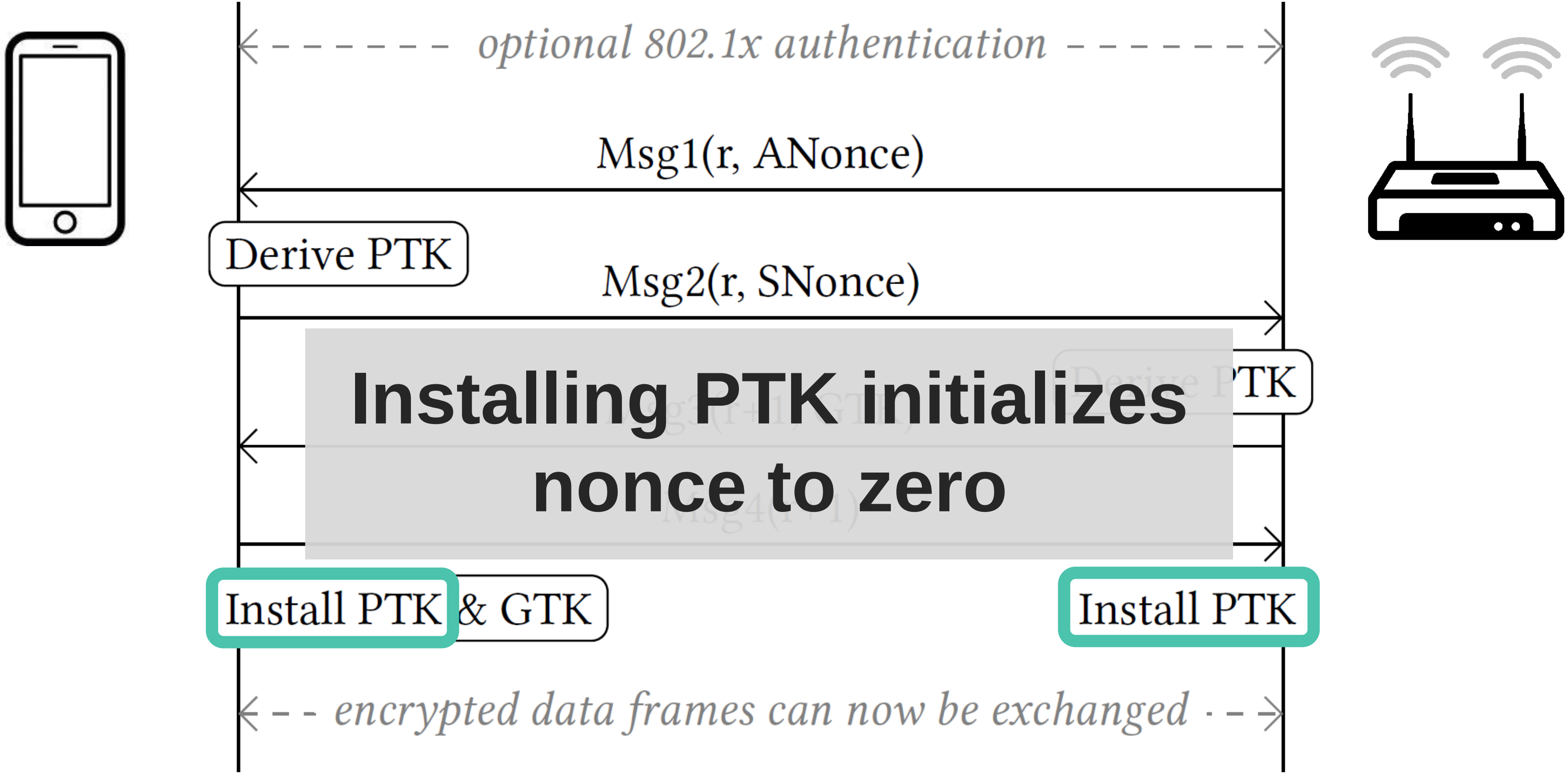
encrypted data frames can now be exchanged

Frame encryption (simplified)



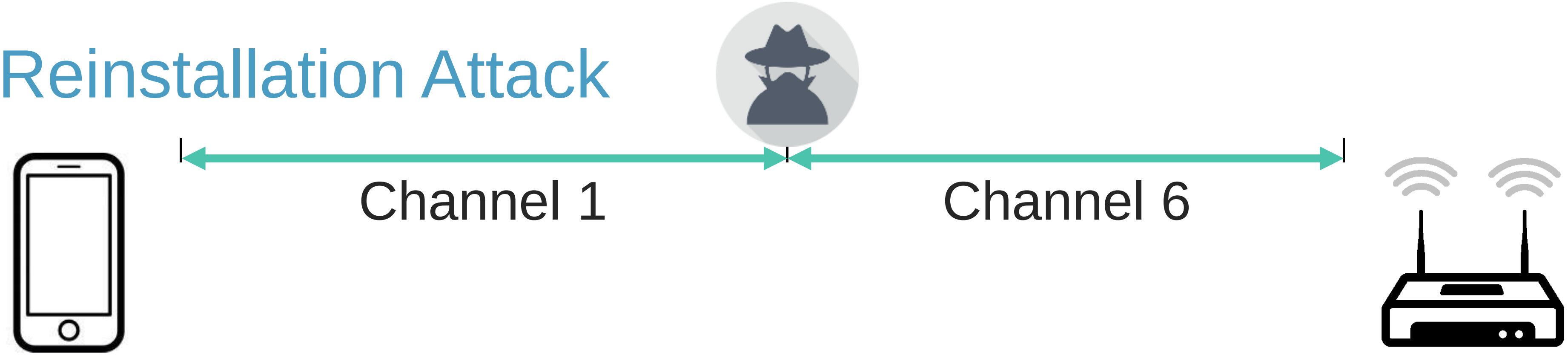
→ Nonce reuse implies keystream reuse (in all WPA2 ciphers)

4-way handshake (simplified)

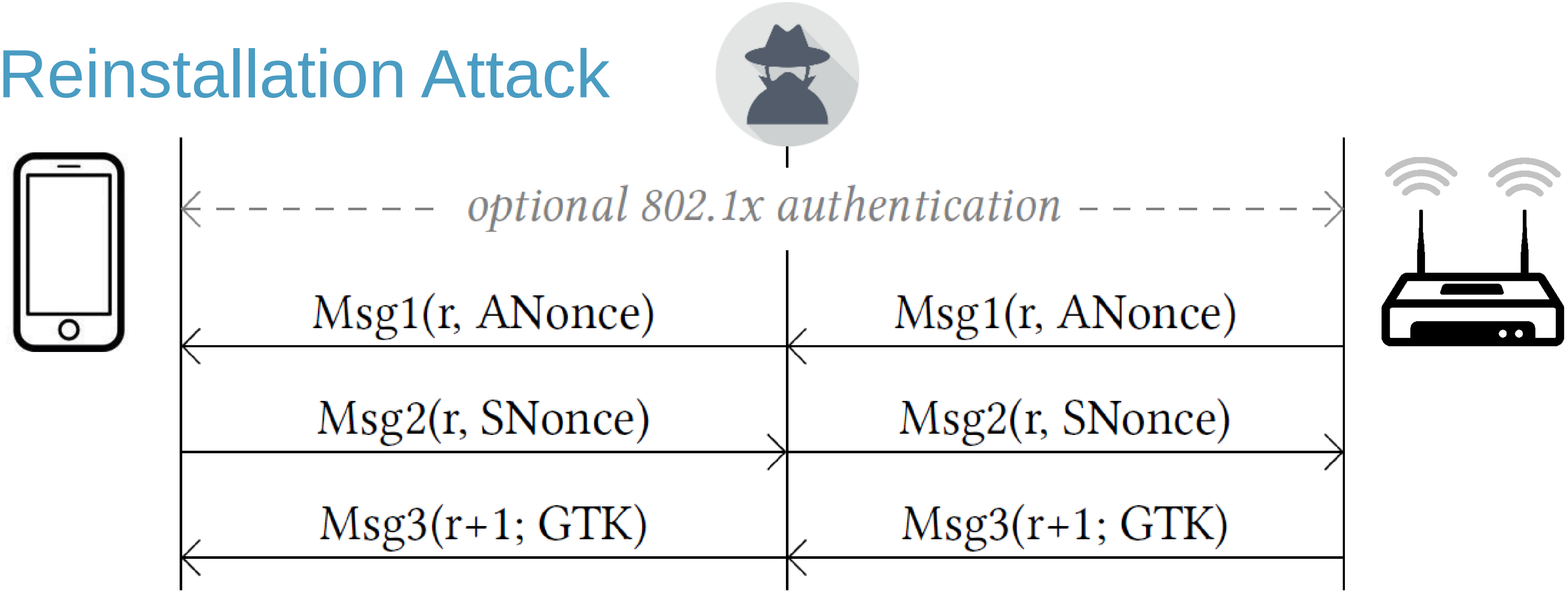


Installing PTK initializes nonce to zero

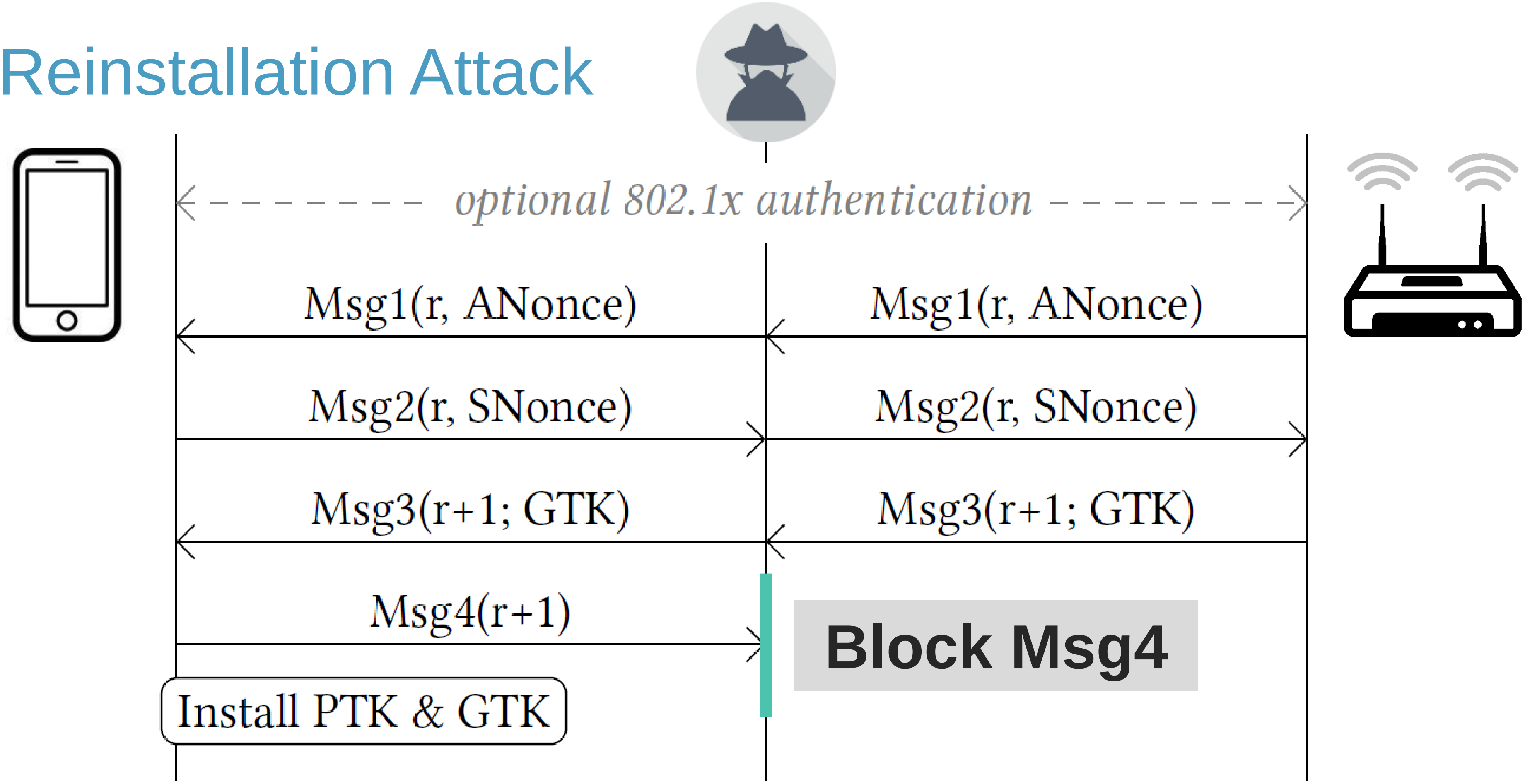
Reinstallation Attack



Reinstallation Attack

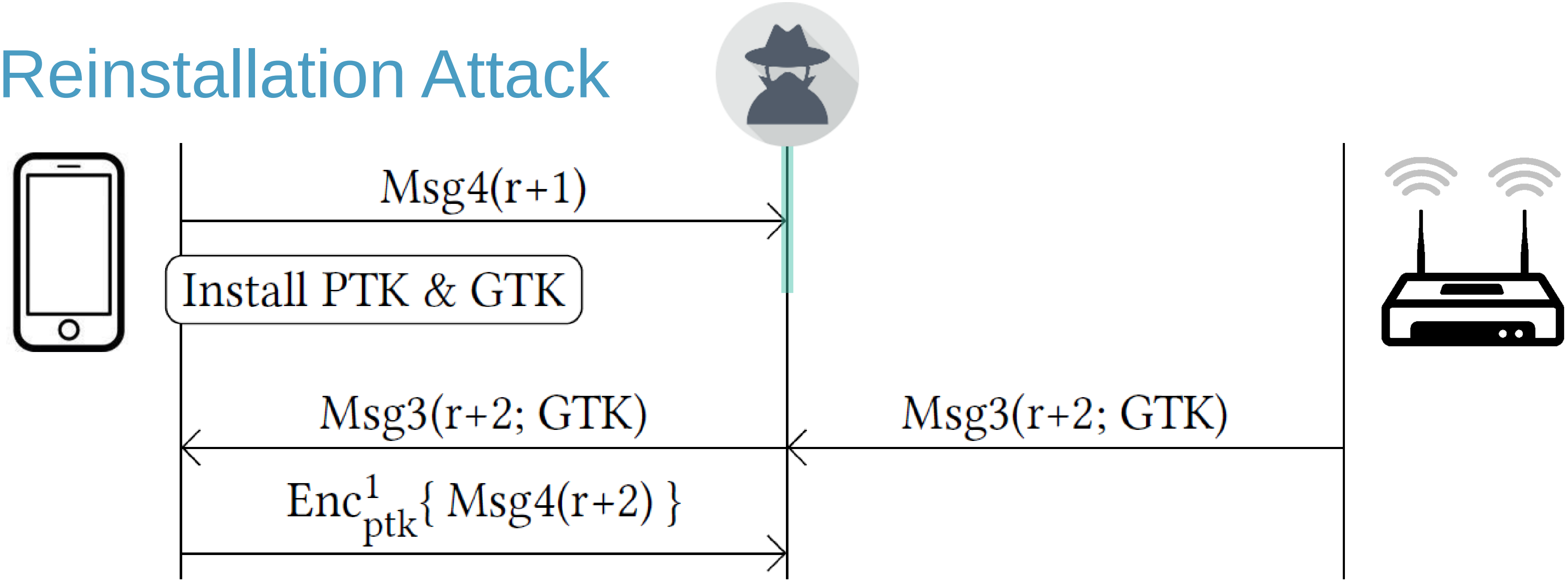


Reinstallation Attack



Block Msg4

Reinstallation Attack



Msg4(r+1)

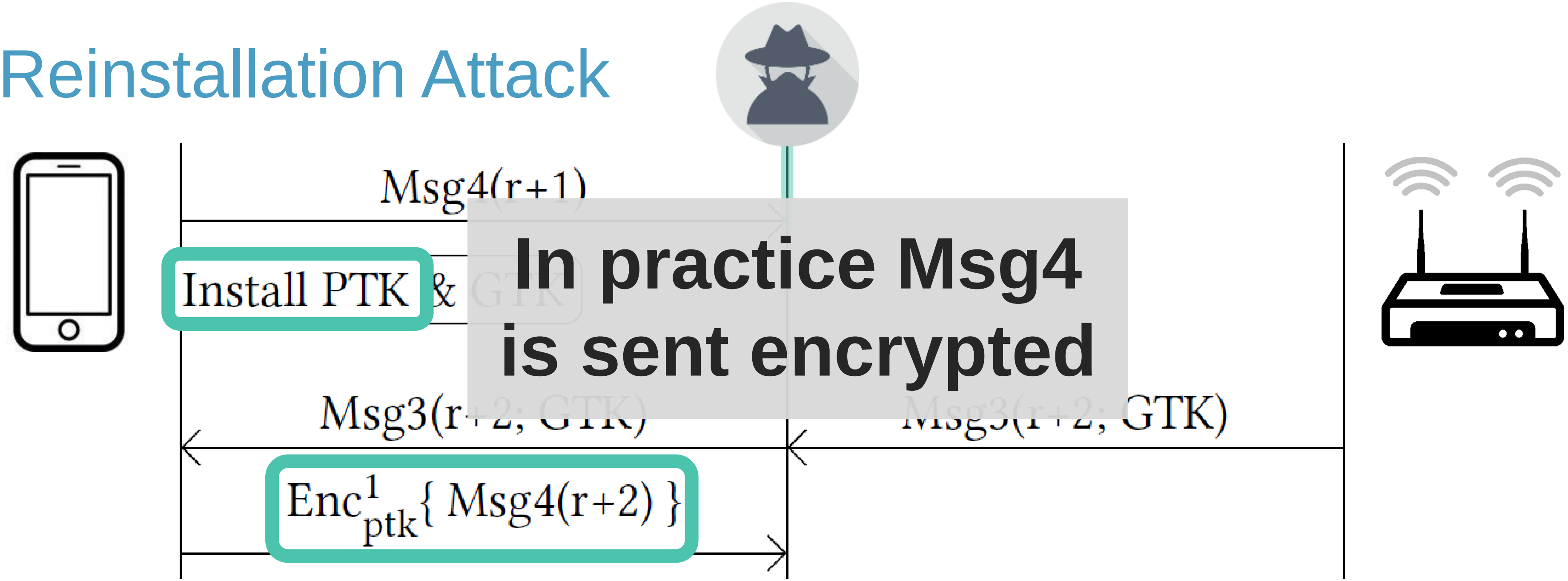
Install PTK & GTK

Msg3(r+2; GTK)

Msg3(r+2; GTK)

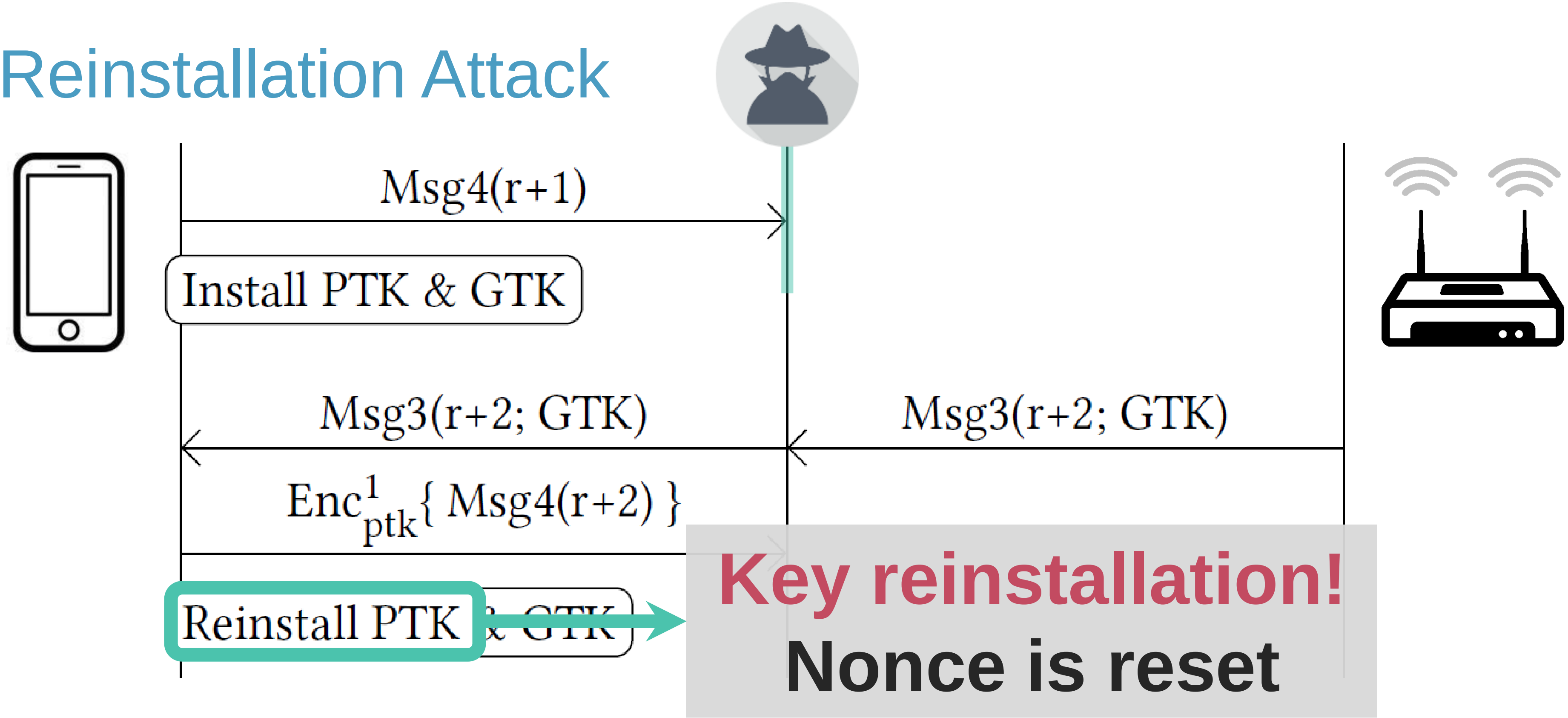
$\mathrm{Enc}^{1}_{\mathrm{ptk}}\{\ \mathrm{Msg4}(r+2)\ \}$

Reinstallation Attack



In practice Msg4 is sent encrypted

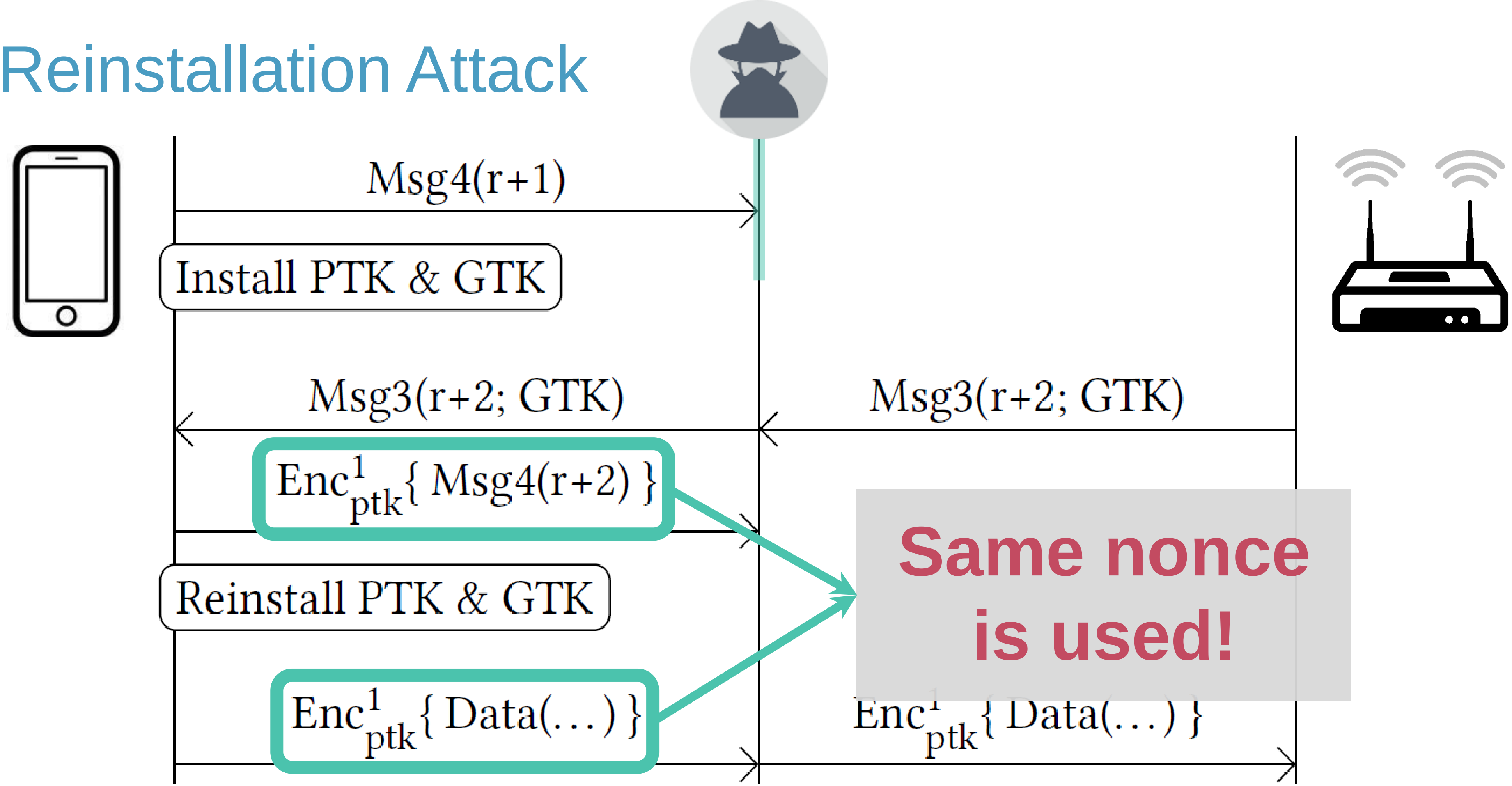
Reinstallation Attack



Key reinstallation!

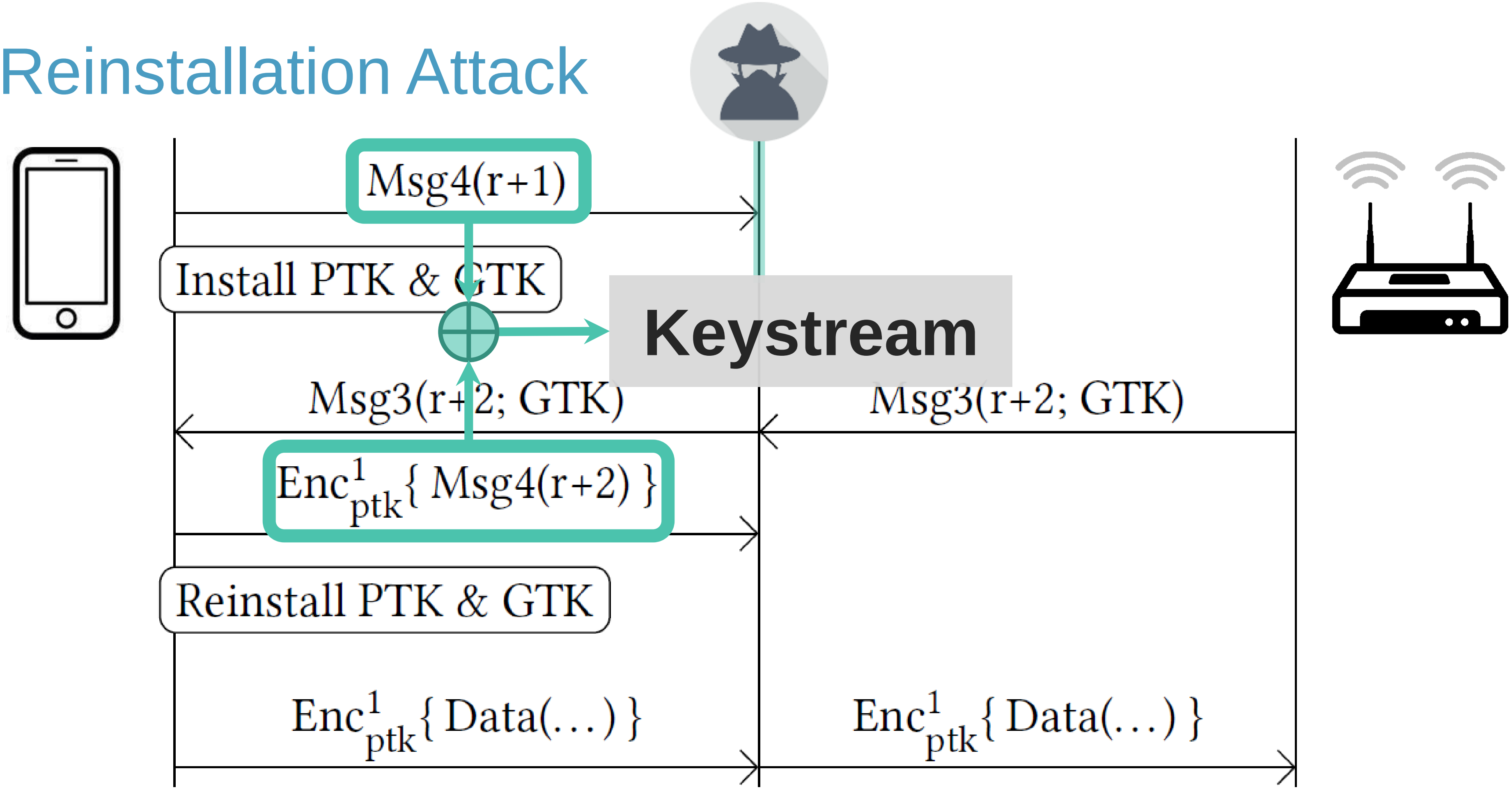
Nonce is reset

Reinstallation Attack


Msg4(r+1)
Install PTK & GTK
Msg3(r+2; GTK)
Msg3(r+2; GTK)
$\text{Enc}^1_{\text{ptk}}\{\text{ Msg4(r+2) }\}$
Reinstall PTK & GTK
$\text{Enc}^1_{\text{ptk}}\{\text{ Data(…) }\}$
$\text{Enc}^1_{\text{ptk}}\{\text{ Data(…) }\}$

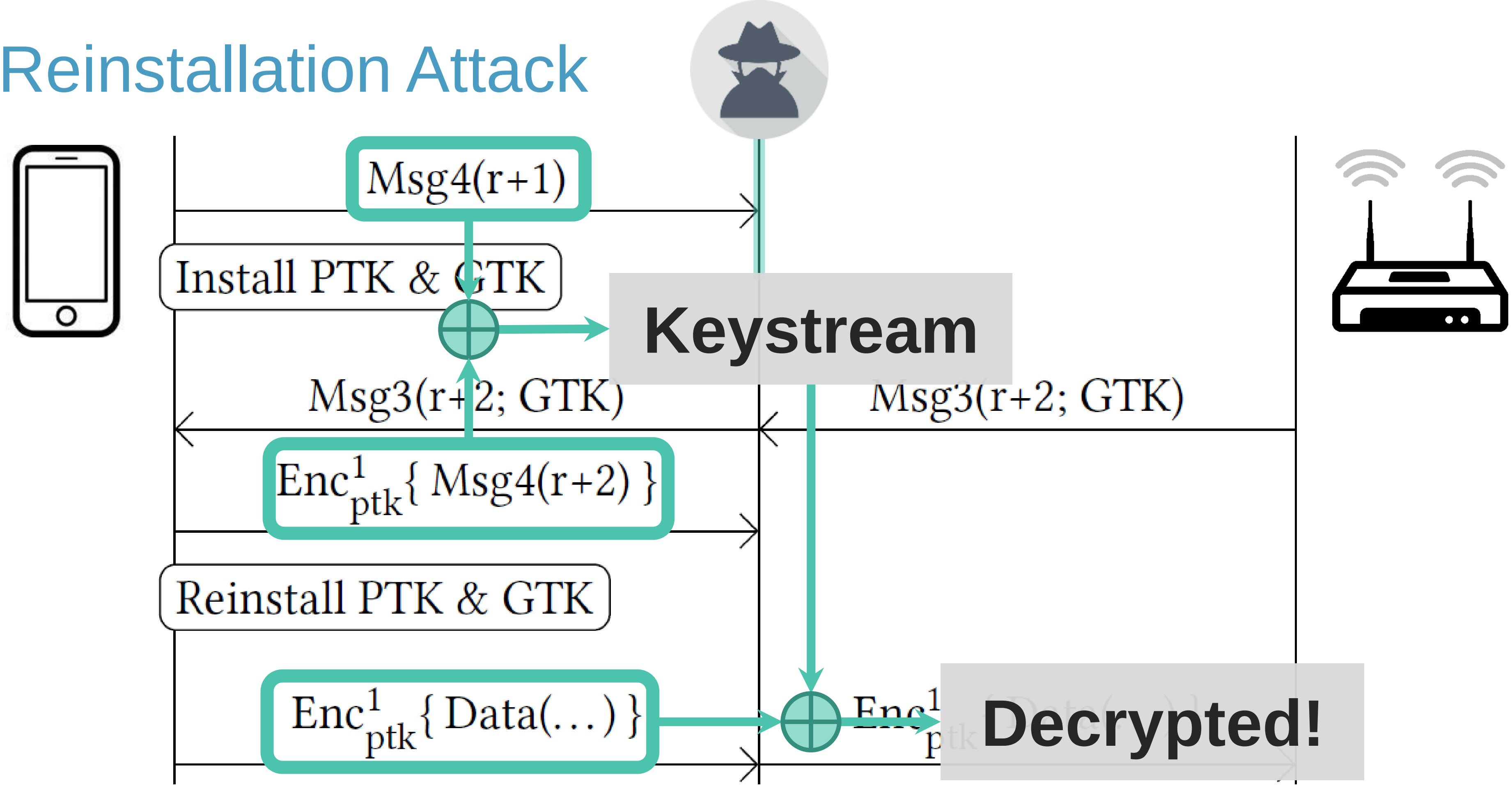
Same nonce is used!

Reinstallation Attack

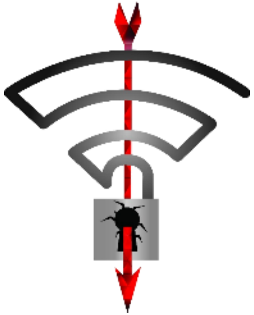


Msg4(r+1)
Install PTK & GTK
Keystream
Msg3(r+2; GTK)
Msg3(r+2; GTK)
$\text{Enc}^1_{\text{ptk}}\{\text{ Msg4(r+2) }\}$
Reinstall PTK & GTK
$\text{Enc}^1_{\text{ptk}}\{\text{ Data(...) }\}$
$\text{Enc}^1_{\text{ptk}}\{\text{ Data(...) }\}$

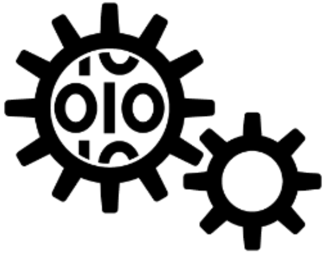
Reinstallation Attack


Msg4(r+1)
Install PTK & GTK
Keystream
Msg3(r+2; GTK)
Msg3(r+2; GTK)
$\text{Enc}^1_{\text{ptk}}\{\text{Msg4(r+2)}\}$
Reinstall PTK & GTK
$\text{Enc}^1_{\text{ptk}}\{\text{Data(...)}\}$
$\text{Enc}^1_{\text{ptk}}\{\text{Data(...)}\}$
Decrypted!

Overview



Key reinstalls in 4-way handshake



New KRACKs

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:

- Recover Message Integrity Check key from plaintext[2,3]
- **Forge/inject** frames sent by the device under attack

Handshake specific

Group key handshake:

- Client is attacked, but only AP sends real broadcast frames
- Can only replay broadcast frames to client

4-way handshake:

- Client is attacked → replay/decrypt/forge

Implementation specific

iOS 10 and Windows: 4-way handshake not affected

- **Cannot decrypt unicast traffic** (nor replay/decrypt)
- But group key handshake is affected (replay broadcast)
- Note: iOS 11 does have vulnerable 4-way handshake[6]

wpa_supplicant 2.4+

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

Overview

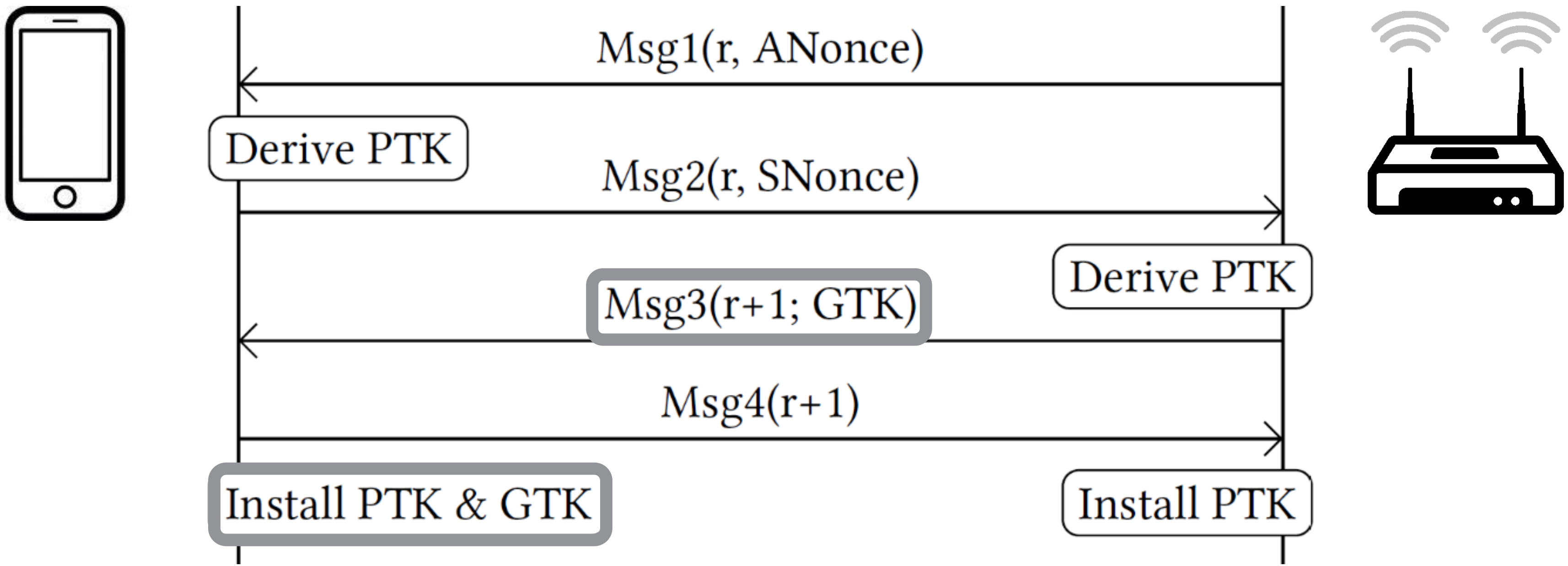
Key reinstalls in 4-way handshake

New KRACKs

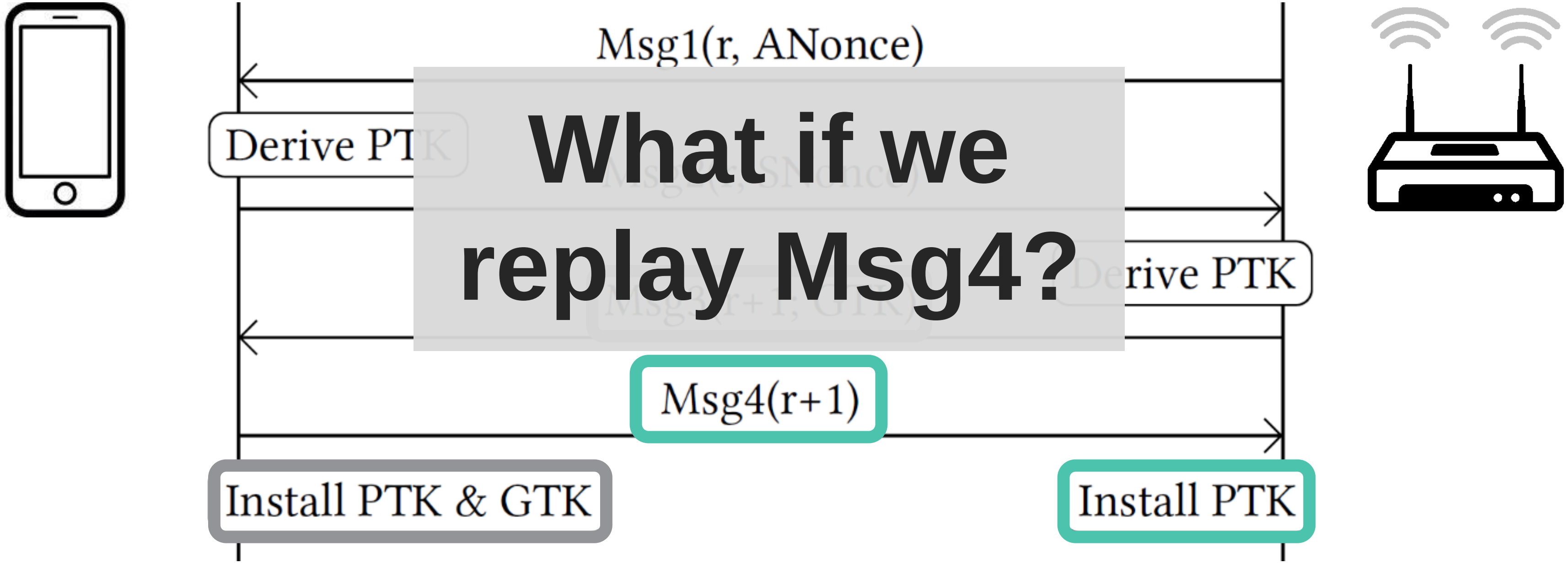
Practical impact

Lessons learned

Idea 1: replay other handshake messages?



Idea 1: replay other handshake messages?



What if we replay Msg4?

MediaTek drivers vulnerable!

- Certain MediaTek Drivers accept replayed Msg4's
- Used in 100+ devices → **many vulnerable products**[9]

ASUS RT-AC51U

TP-Link RE370K

Idea 2: A/SNonce renewed during rekey?

AP can start new handshake to refresh the PTK

- Same messages exchanged as initial handshake
- New ANonce and SNonce must be used

macOS:

- Patched default KRACK attack
- But **reuses the SNonce during a rekey**
- SNonce reuse patched in macOS 10.13.3

Exploiting SNonce reuse

No problem if ANonce does change

- But Linux’s hostapd reused ANonce …
- Previous key was renegotiated and reinstalled
- Can **decrypt old captured traffic**!

Adversary can replay old handshake

- Tricky because messages must now be encrypted
- But feasible under specific circumstances

Idea 3: further audit patches

Several users reported:

“**Patched client still vulnerable**

to group key reinstallations”

- Either our patches are flawed …
- … or device always accepts replayed broadcast frames?!

No broadcast replay checks!

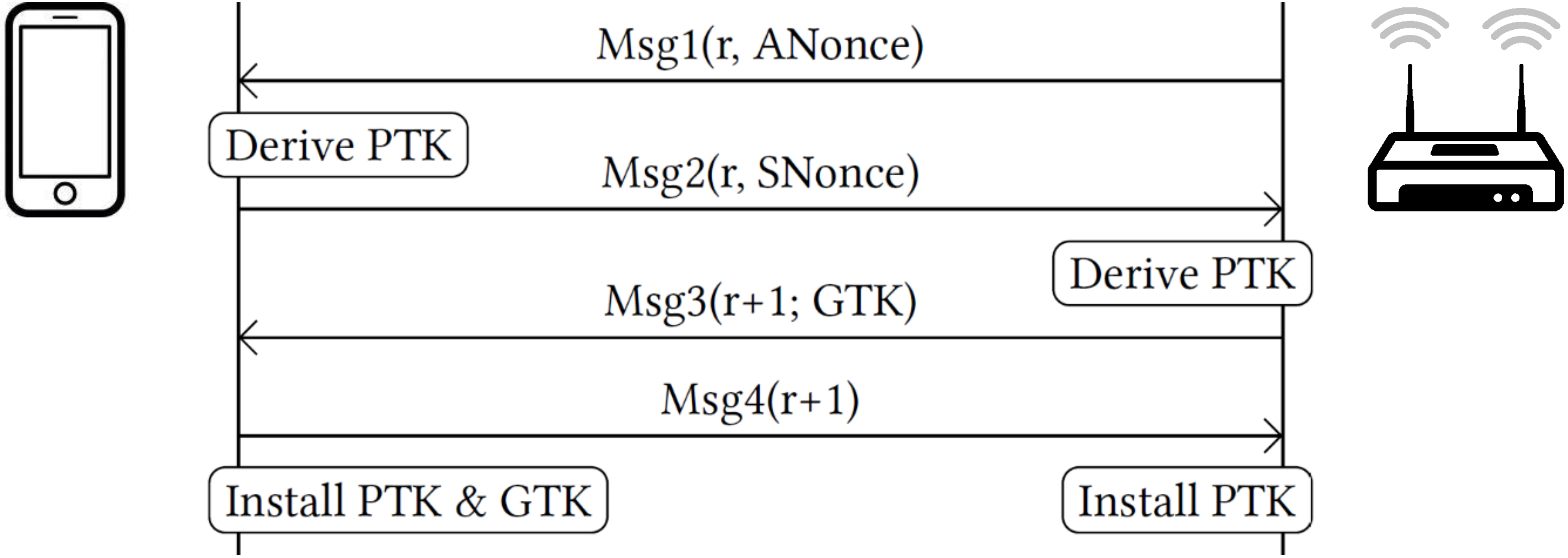
Netis WF-2120

AWUS036NH

Nexus 5X

- 8 of out 16 tested devices vulnerable
- Likely caused by **faulty hardware/firmware decryption**

Related issue: group key improperly installed



Msg1(r, ANonce)

Derive PTK

Msg2(r, SNonce)

Derive PTK

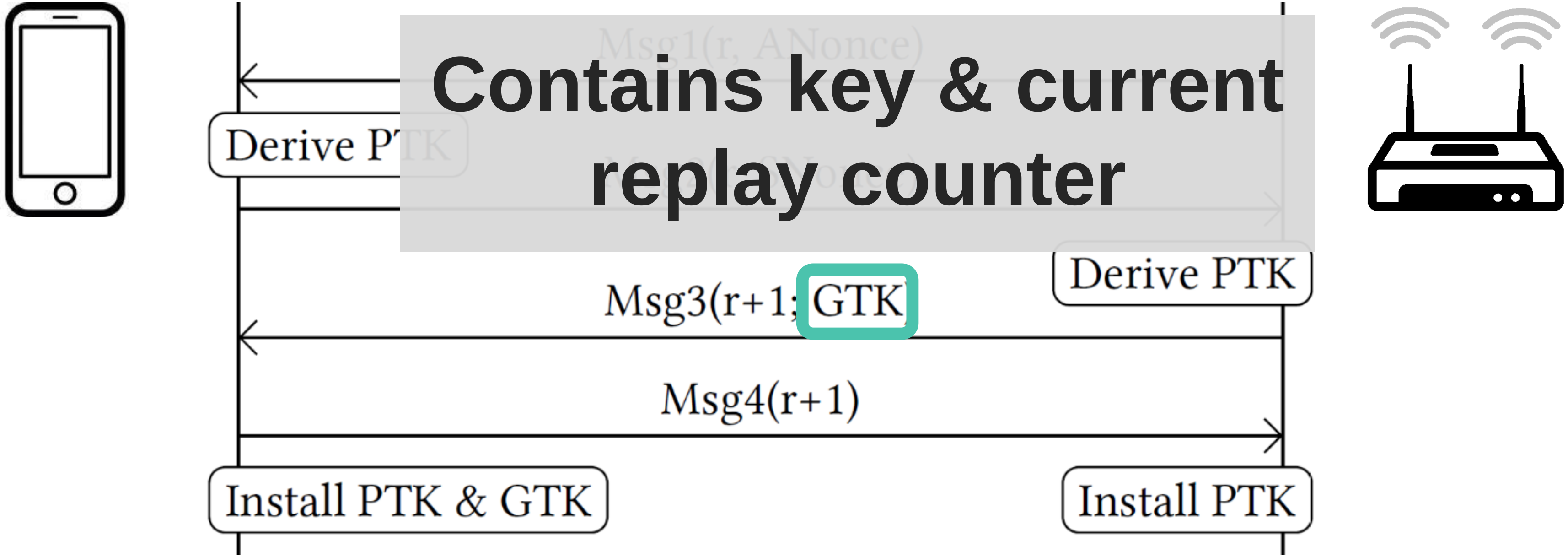
Msg3(r+1; GTK)

Msg4(r+1)

Install PTK & GTK

Install PTK

Related issue: group key improperly installed



Msg1(r, ANonce)

Derive PTK

Contains key & current replay counter

Derive PTK

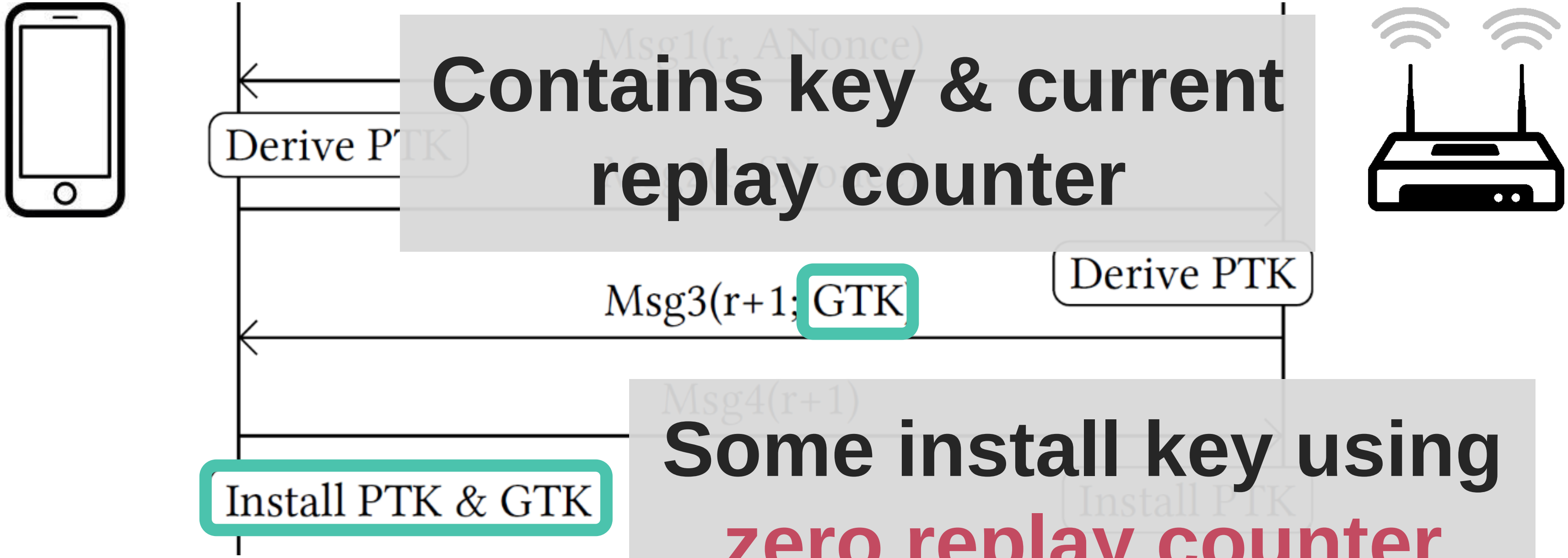
Msg3(r+1; GTK)

Msg4(r+1)

Install PTK & GTK

Install PTK

Related issue: group key improperly installed



Contains key & current replay counter

Some install key using zero replay counter

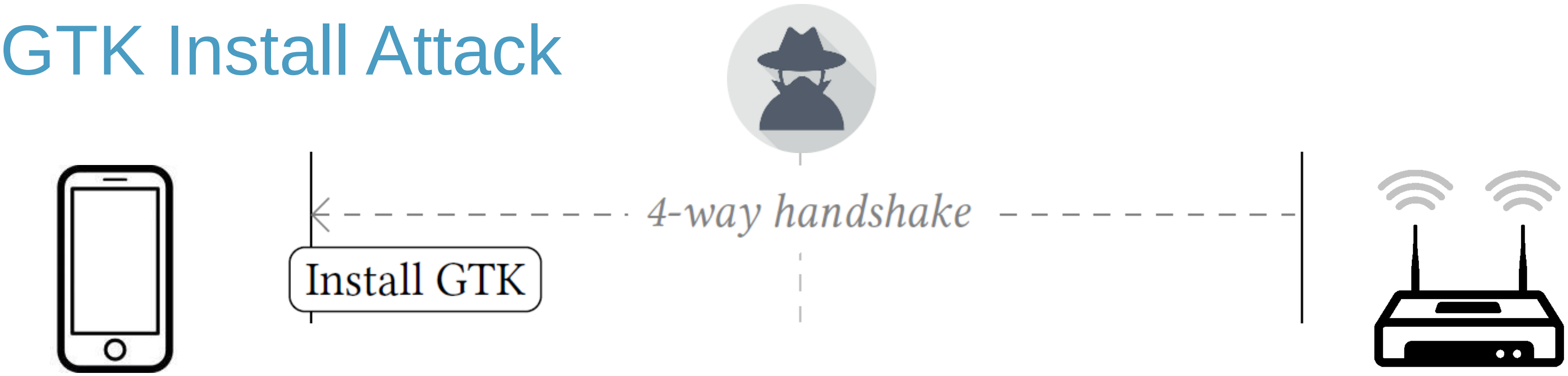
Related issue: group key improperly installed

Affected devices:

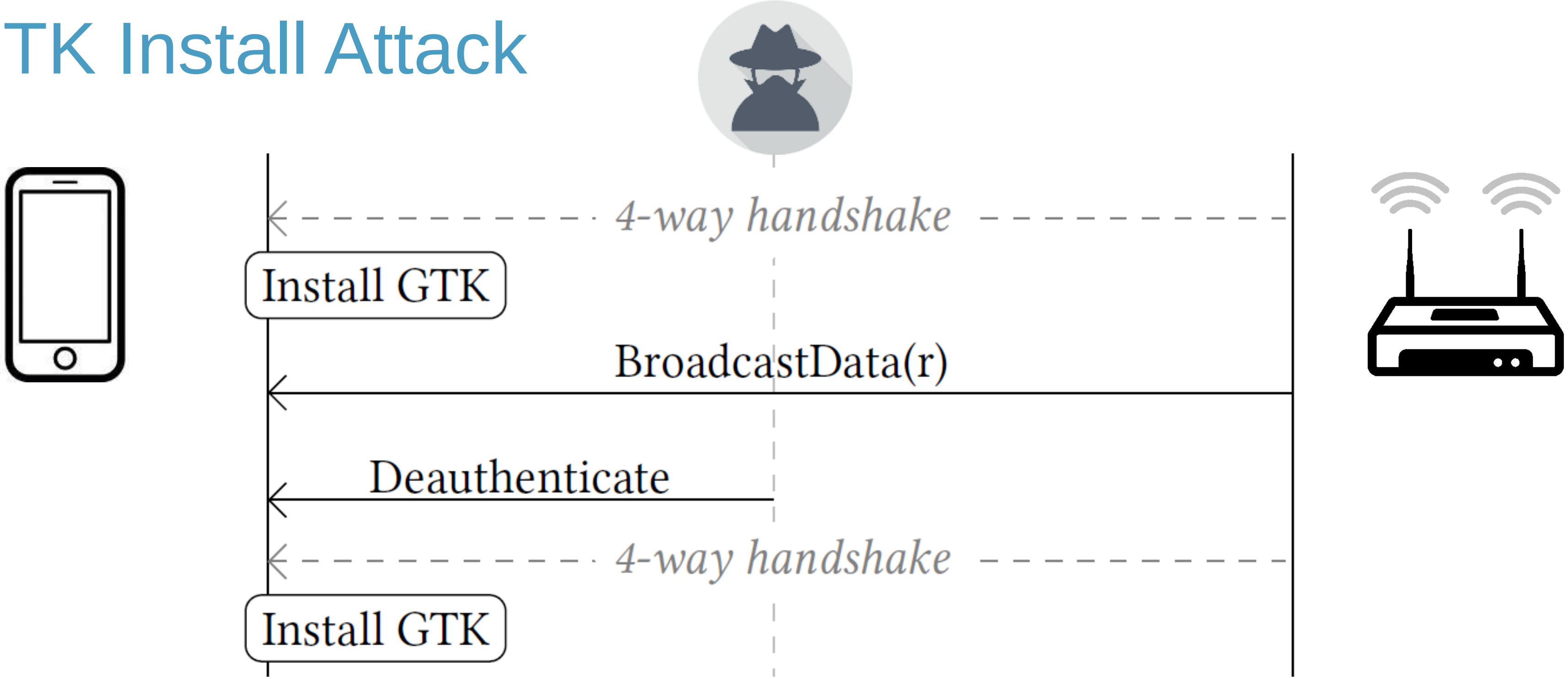
- Samsung S3 LTE
- $POPULAR_CLIENT

How to abuse this?

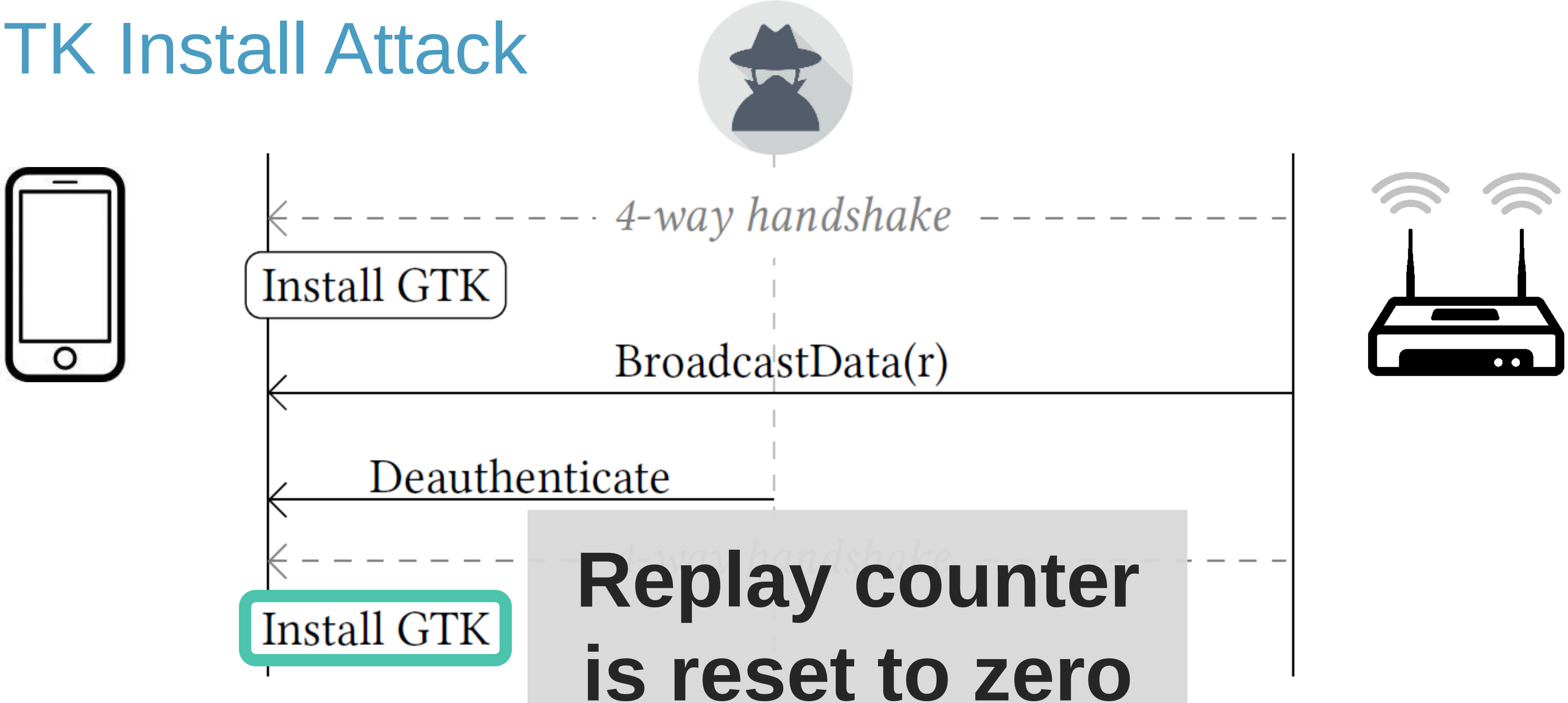
GTK Install Attack



GTK Install Attack

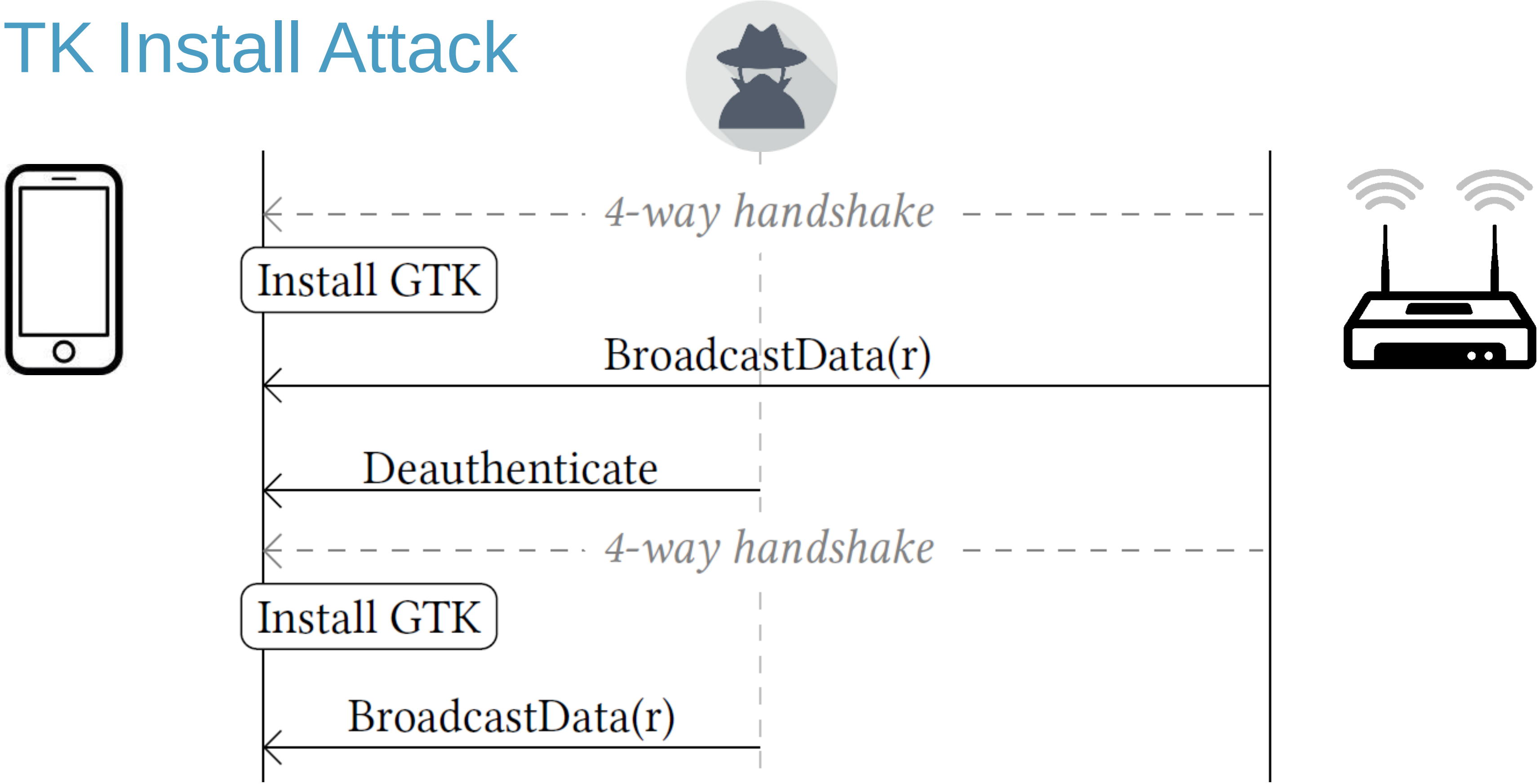


GTK Install Attack



Replay counter is reset to zero

GTK Install Attack



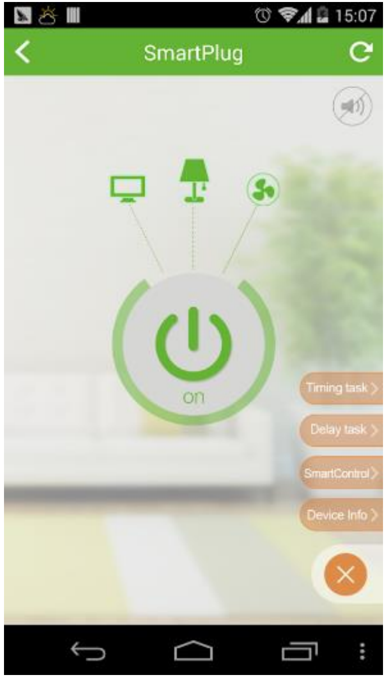
Idea 4: Impact of replaying broadcast frames?

Kankun smart power plug

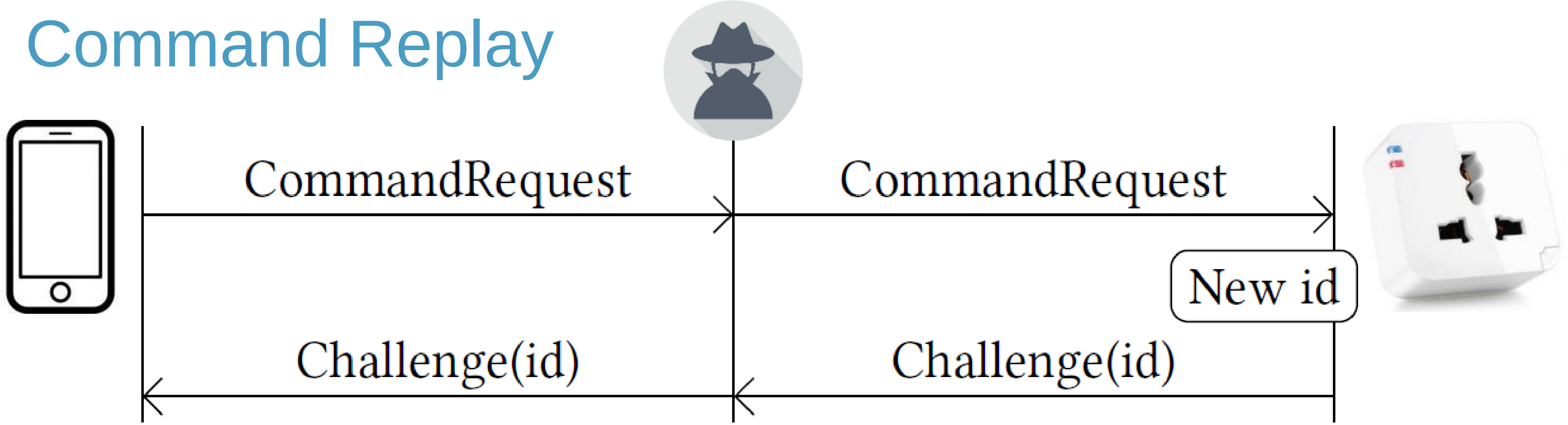
- Android app to control it

Commands are broadcast UDP

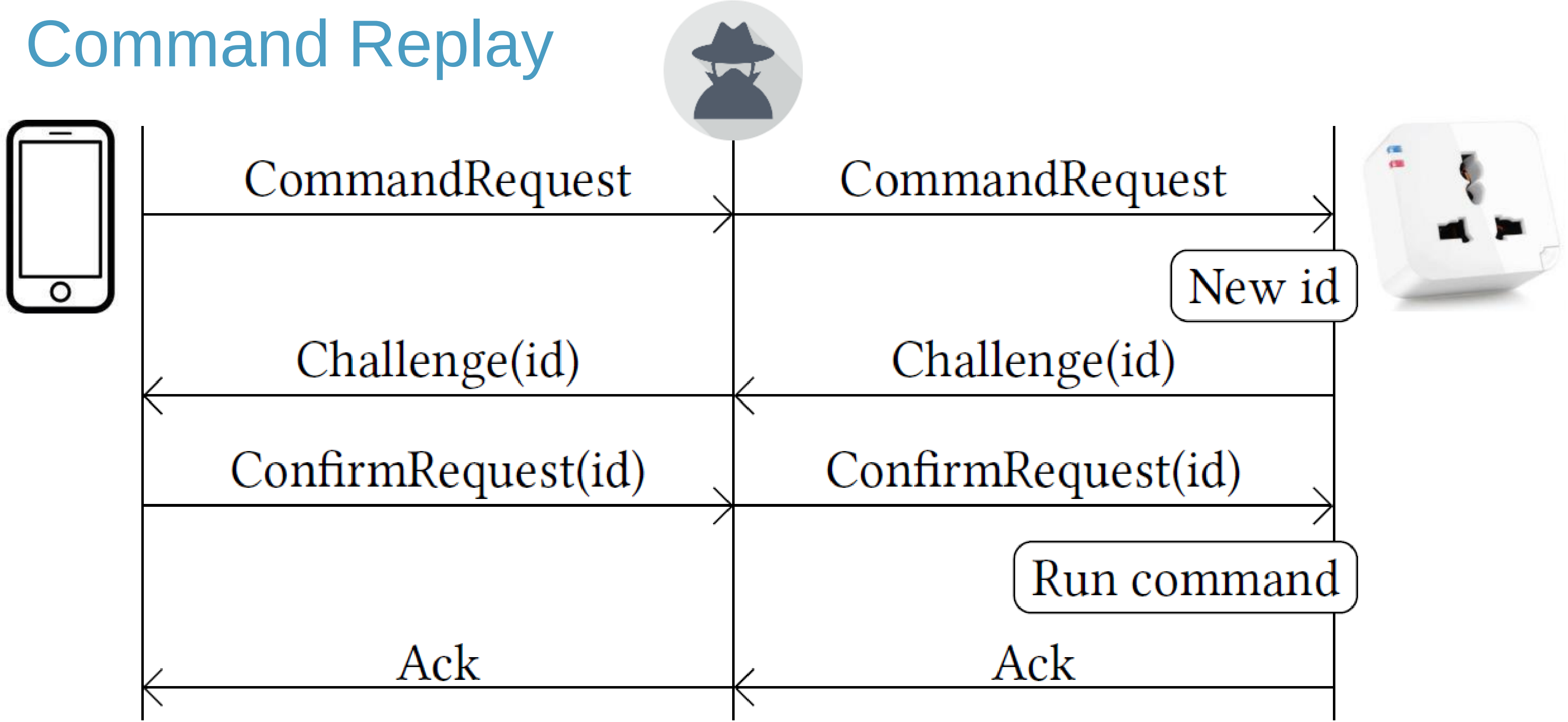
- Destination MAC in payload (?!)
- Challenge/response protocol



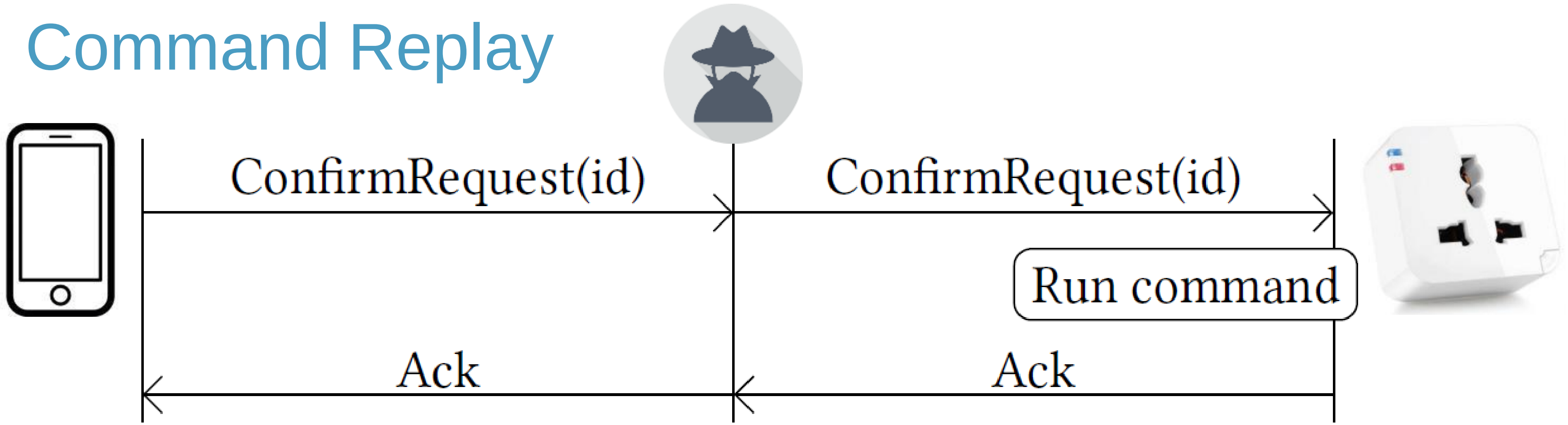
Command Replay



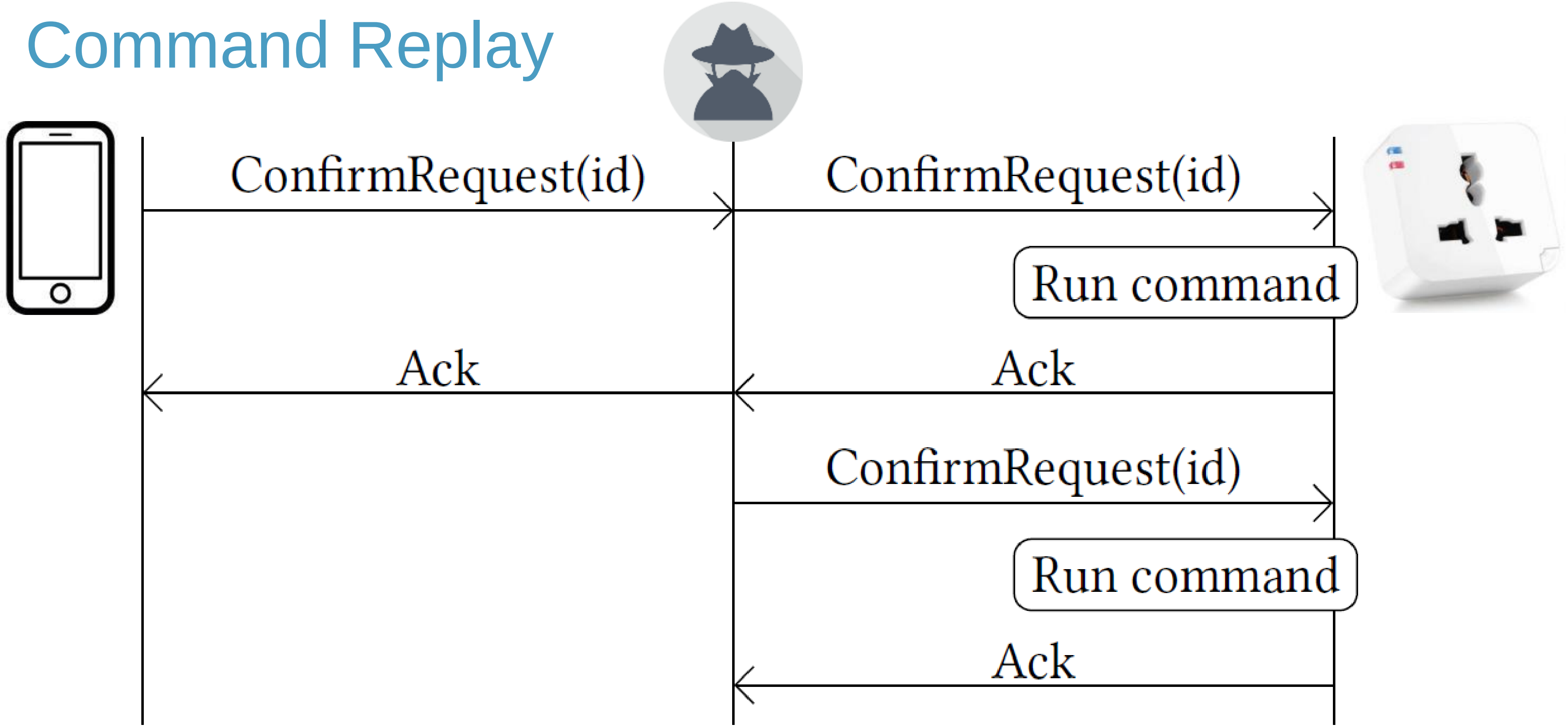
Command Replay



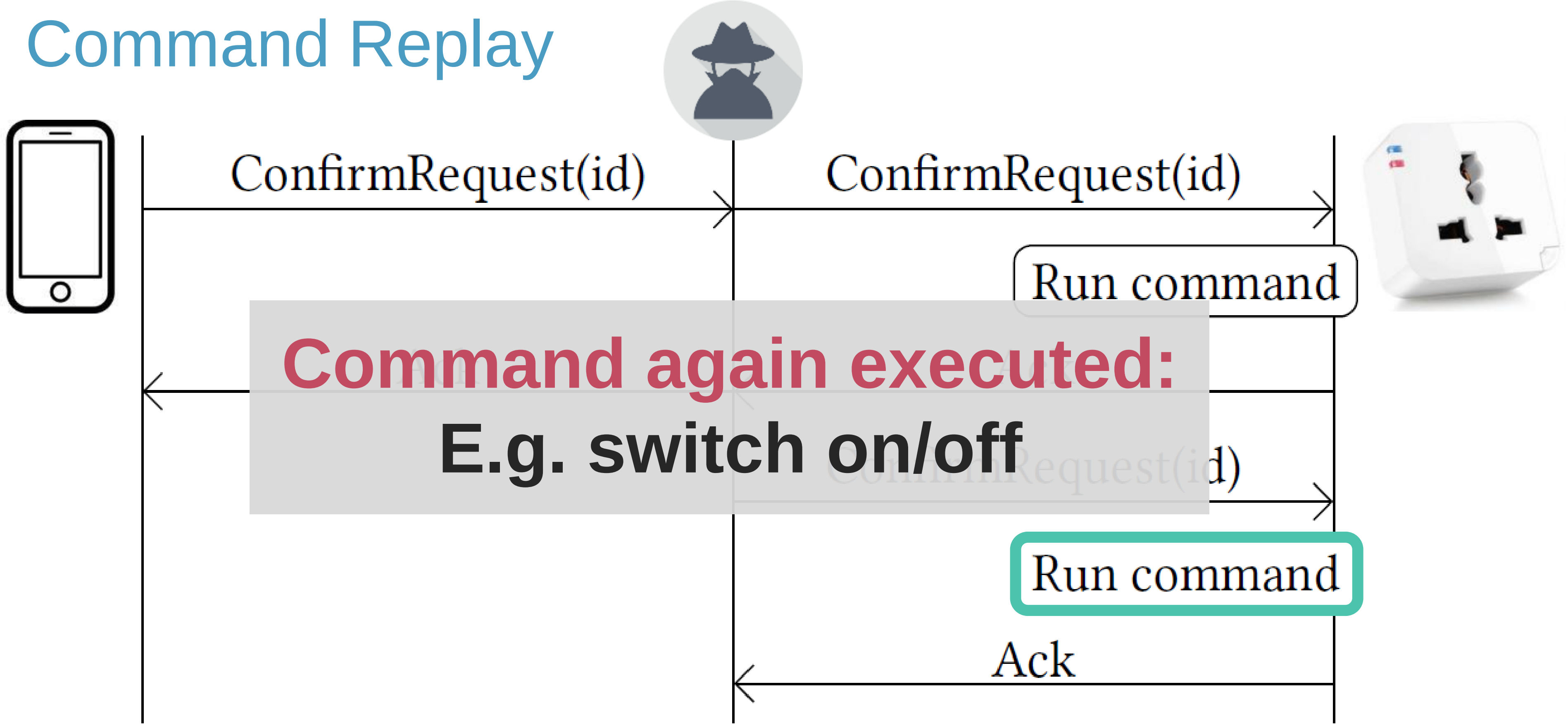
Command Replay



Command Replay



Command Replay



Command again executed:

E.g. switch on/off

Is your device affected?

github.com/vanhoefm/krackattacks-scripts

- Tests clients and APs
- Works on Kali Linux

Remember to:

- Disable hardware encryption
- **Use a proper Wi-Fi dongle!**

Overview

Key reinstalls in 4-way handshake

New KRACKs

Practical impact

Lessons learned

Limitations of formal proofs

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

The combination was not proven secure!

Multi-party vulnerability coordination

Widespread issue! How to disclose?

Guidelines and Practices for Multi-Party Vulnerability Coordination (Draft)[7]

Remember:

- Goal is to protect users
- There are various opinions

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

References

1. C. He, M. Sundararajan, A. Datta, A. Derek, and J. Mitchell. A Modular Correctness Proof of IEEE 802.11i and TLS. In CCS, 2005.
2. E. and M. Beck. Practical attacks against WEP and WPA. In WiSec, 2009.
3. M. Vanhoef and F. Piessens. Practical verification of WPA-TKIP vulnerabilities. In ASIA CCS, 2013.
4. A. Joux. Authentication failures in NIST version of GCM. 2016.
5. J. Jonsson. On the security of CTR+ CBC-MAC. In SAC, 2002.
6. Apple. About the security content of iOS 11.1. November 3, 2017. Retrieved 26 November from https://support.apple.com/en-us/HT208222
7. Multi-party vuln coordination
8. M. Vanhoef and F. Piessens. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In CCS, 2017.
9. WikiDevi. MediaTek MT7620. Retrieved 2 April from https://wikidevi.com/wiki/MediaTek_MT7620A
10. US Central Intelligence Agency. Network Operations Division Cryptographic Requirements. Retrieved 5 December 2017 from https://wikileaks.org/ciav7p1/cms/files/NOD%20Cryptographic%20Requirements%20v1.1%20TOP%20SECRET.pdf