CYBERSECURITY
EXPERTS ON YOUR SIDE

# KrØØk: Serious Vulnerability Affected Encryption of Billion+ Wi-Fi Devices

Robert Lipovsky | Stefan Svorencik

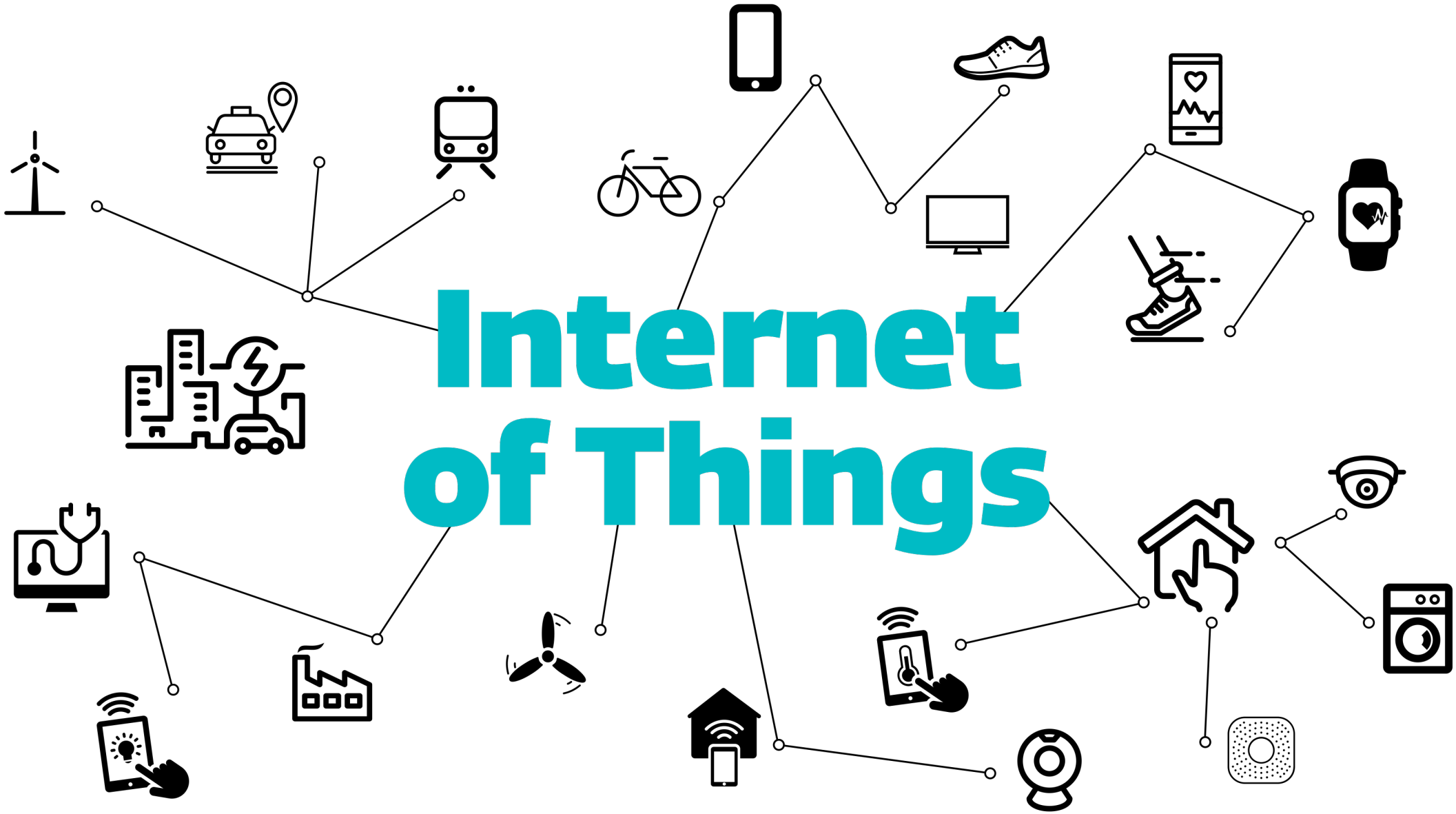
# IoT research

***Consumer IoT Devices Are Expanding The Enterprise Attack Surface***

**Forrester:** *Managing the Security Risks Posed by Your Employees' IoT Devices, by Chris Sherman, February, 2020*

***Most Consumer IoT Devices Can Be Exploited***

**Forrester:** *Managing the Security Risks Posed by Your Employees' IoT Devices, by Chris Sherman, February, 2020*


Internet
of Things

**Robert Lipovsky**

Senior Malware Researcher

**Stefan Svorencik**

Head of Experimental Research & Detection

**Miloš Čermák**

Malware Researcher
Experimental Research & Detection

**Martin Kalužník**

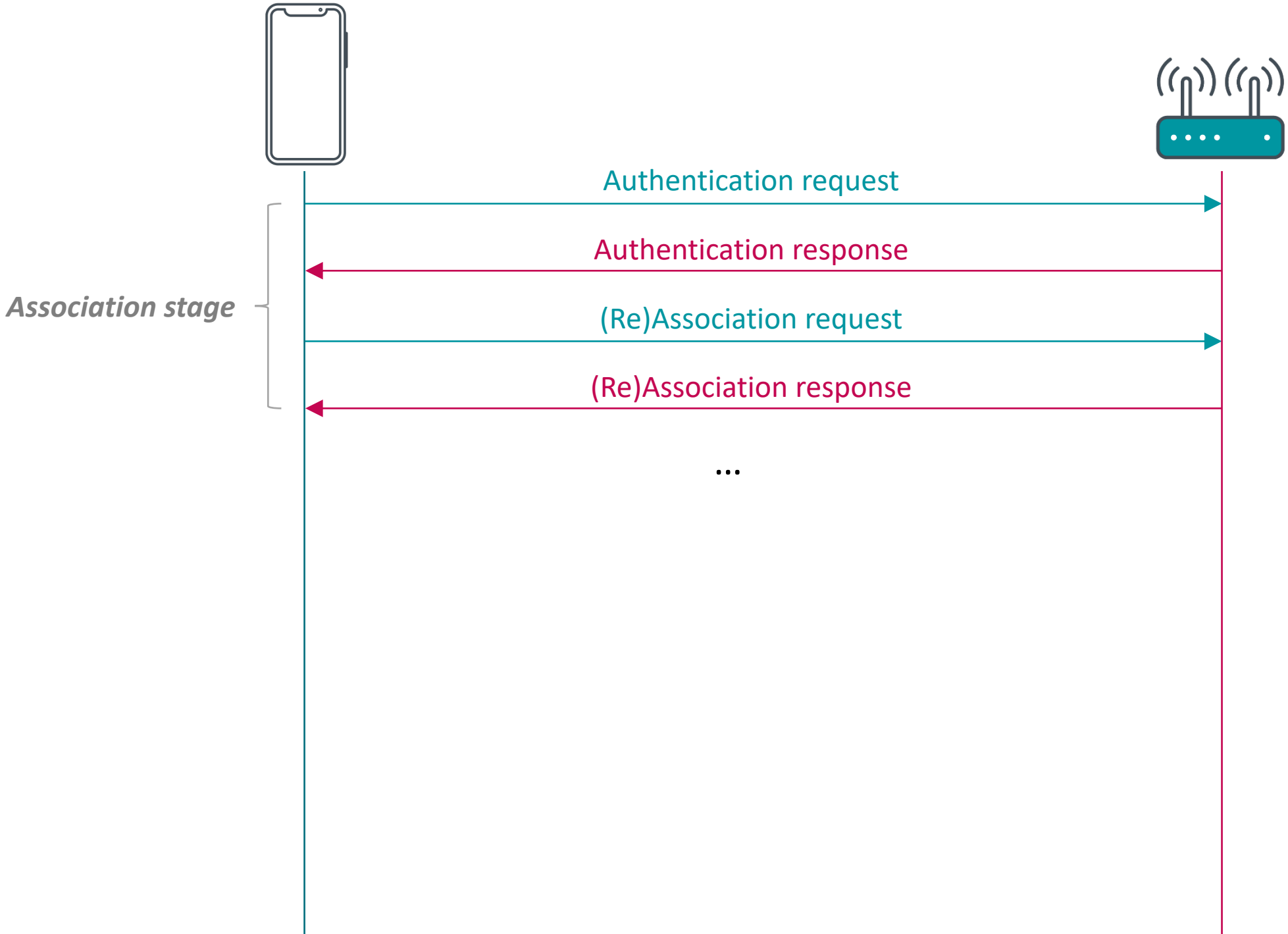
Malware Researcher
Experimental Research & Detection

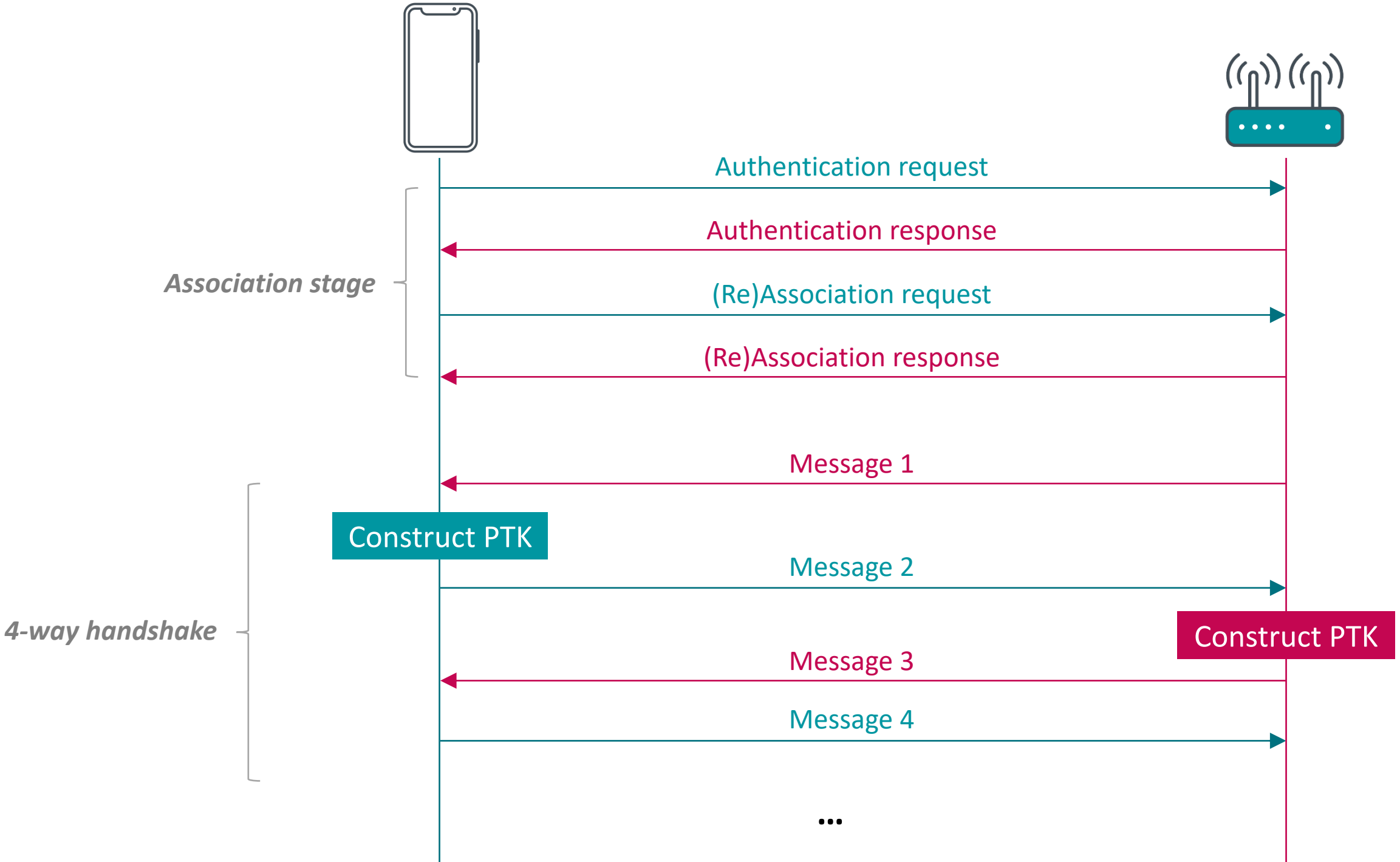

GLOBAL VIEW
EUROPE VIEW
GLOBAL VIEW
EUROPE VIEW
eset
NASA

# Agenda

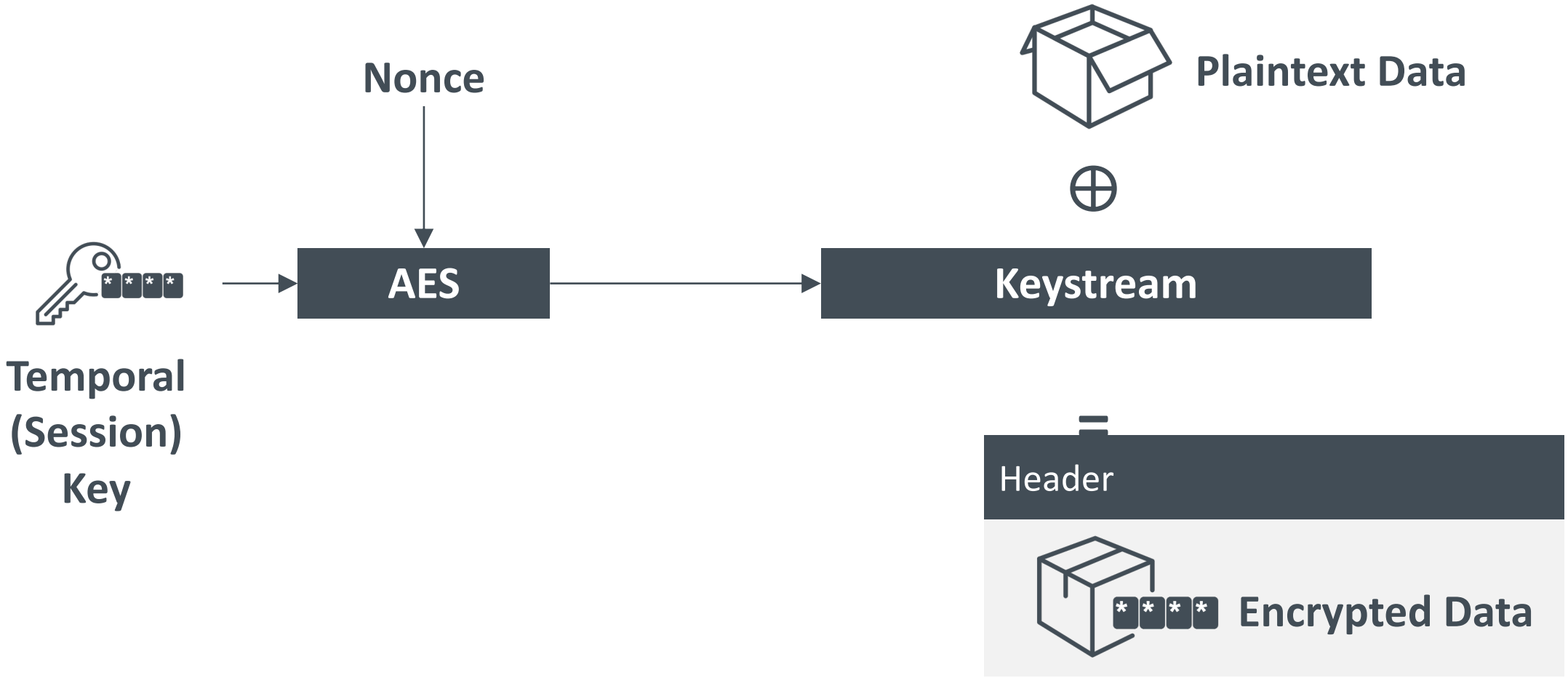
1. **Quick intro to WPA2**
2. **The Kr00k vulnerability**
3. **Impact**
4. **What does this have to do with KRACK and Amazon devices?**
5. **Latest research / related vulnerabilities**
6. **Conclusion**


Wi-Fi Security Primer


Authentication request
Authentication response
Association stage
(Re)Association request
(Re)Association response
...

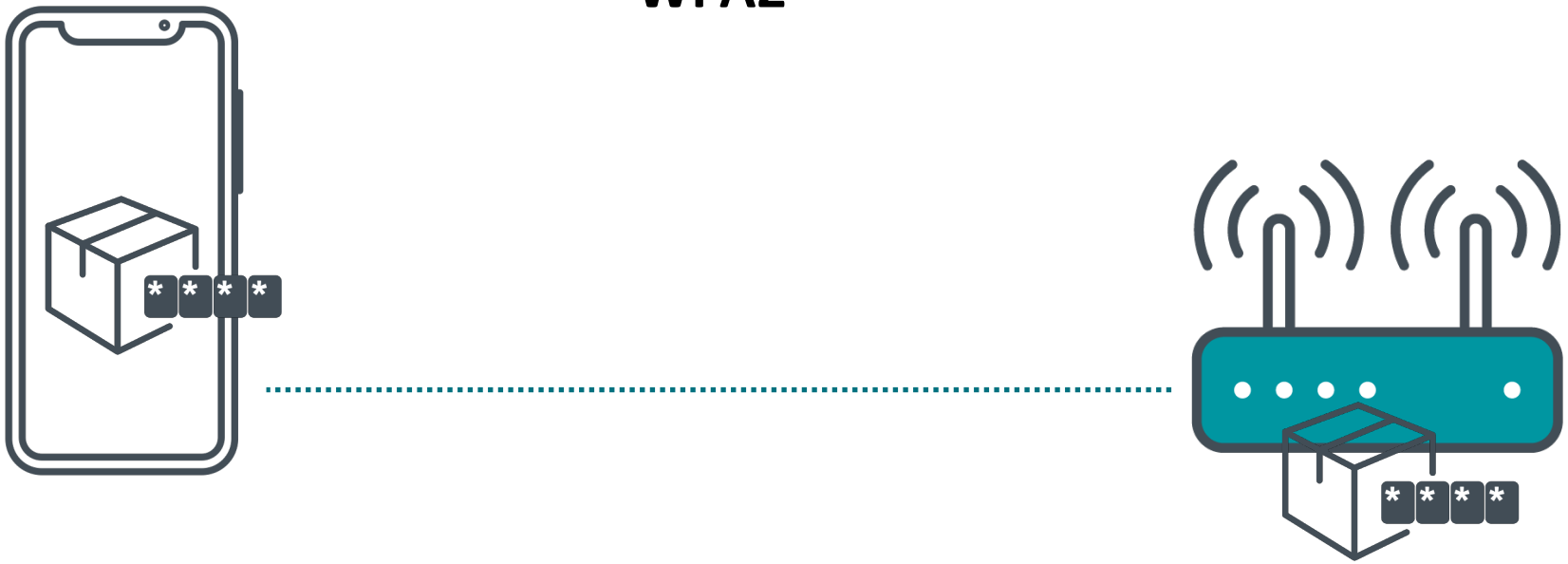

Authentication request
Authentication response
Association stage
(Re)Association request
(Re)Association response
Message 1
Construct PTK
Message 2
4-way handshake
Construct PTK
Message 3
Message 4
...

# Encryption in WPA2-CCMP

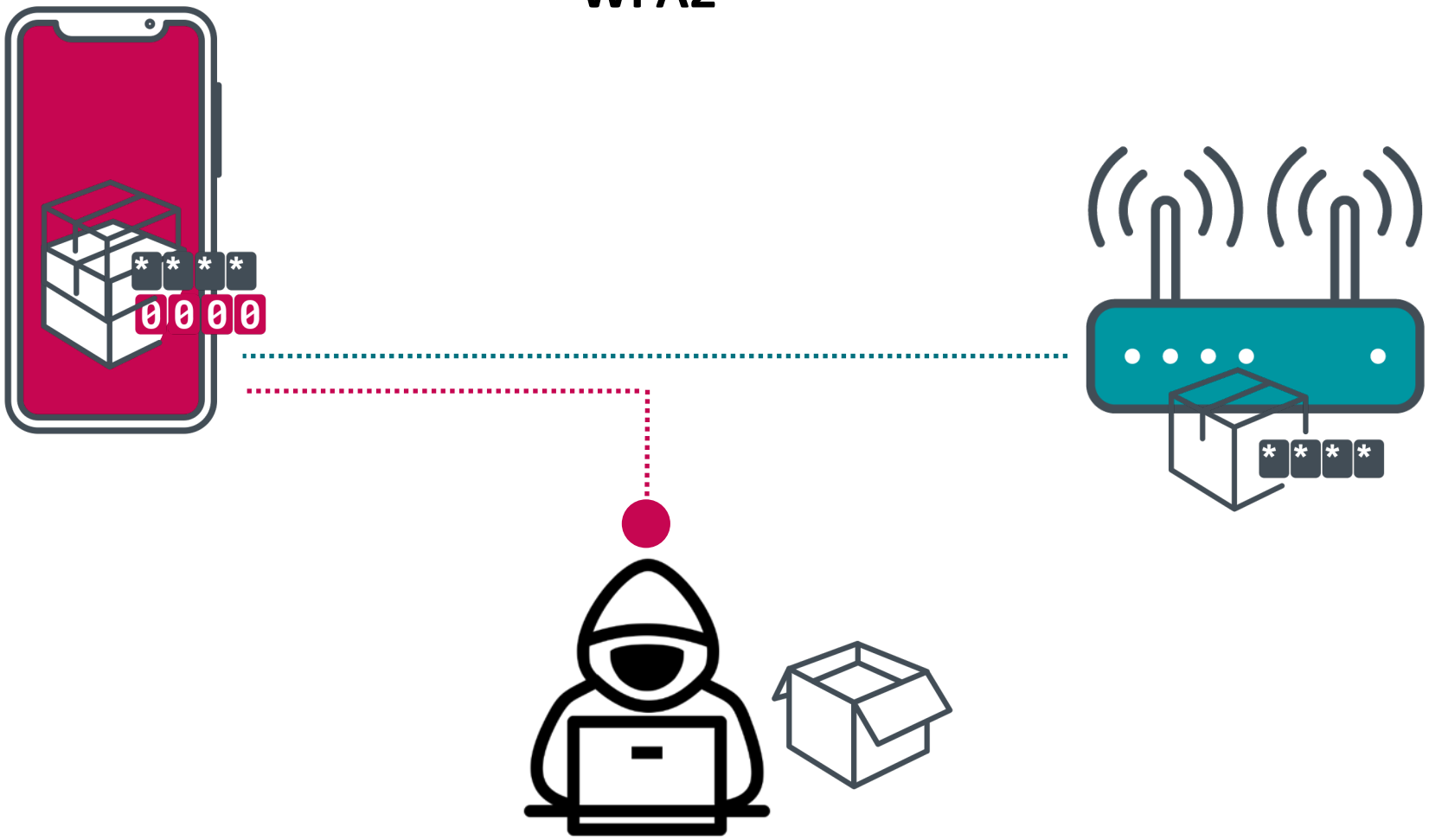



KrØØk
CVE-2019-15126

# WPA2

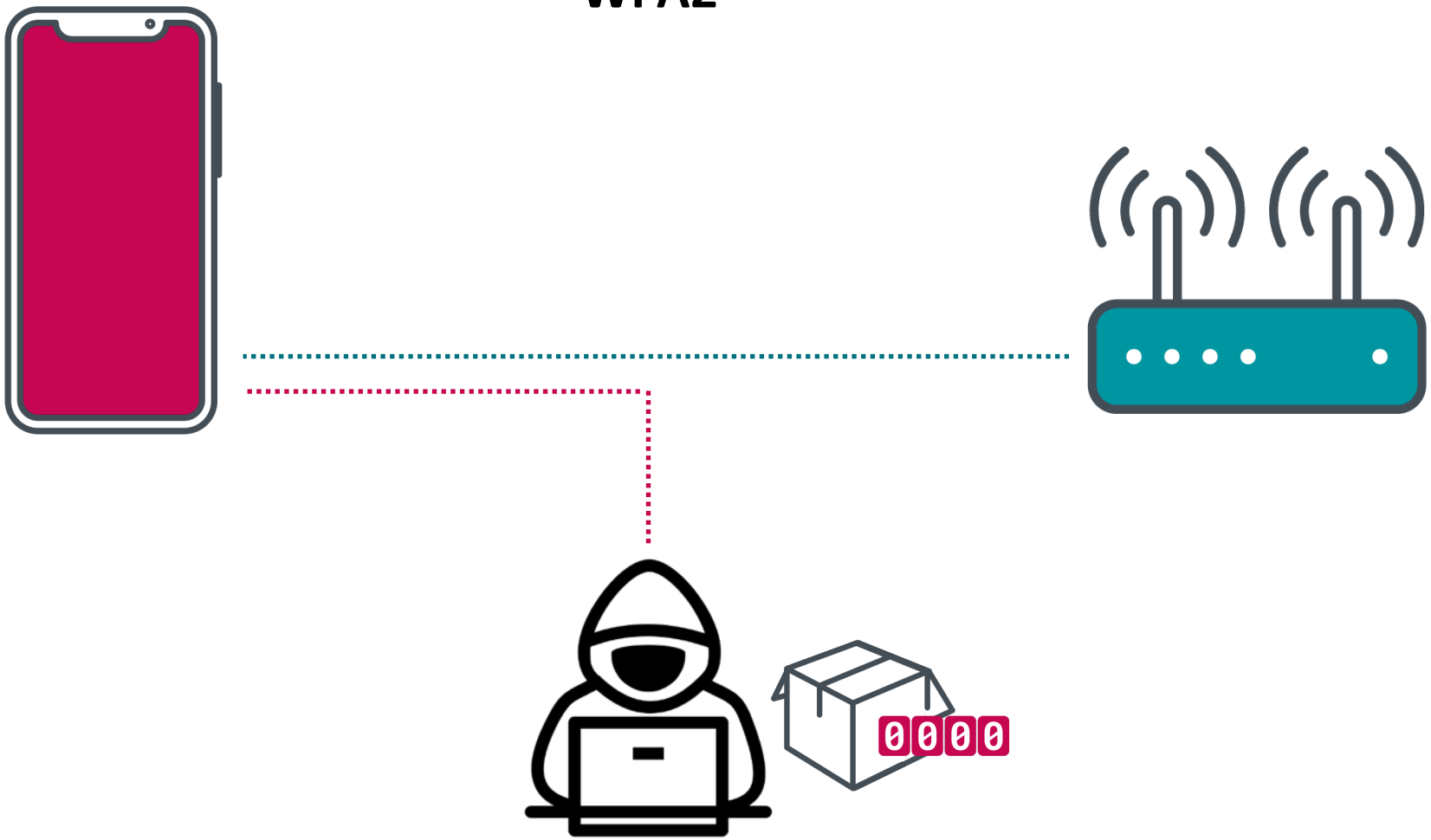


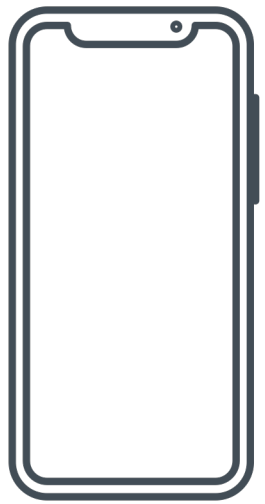
# WPA2

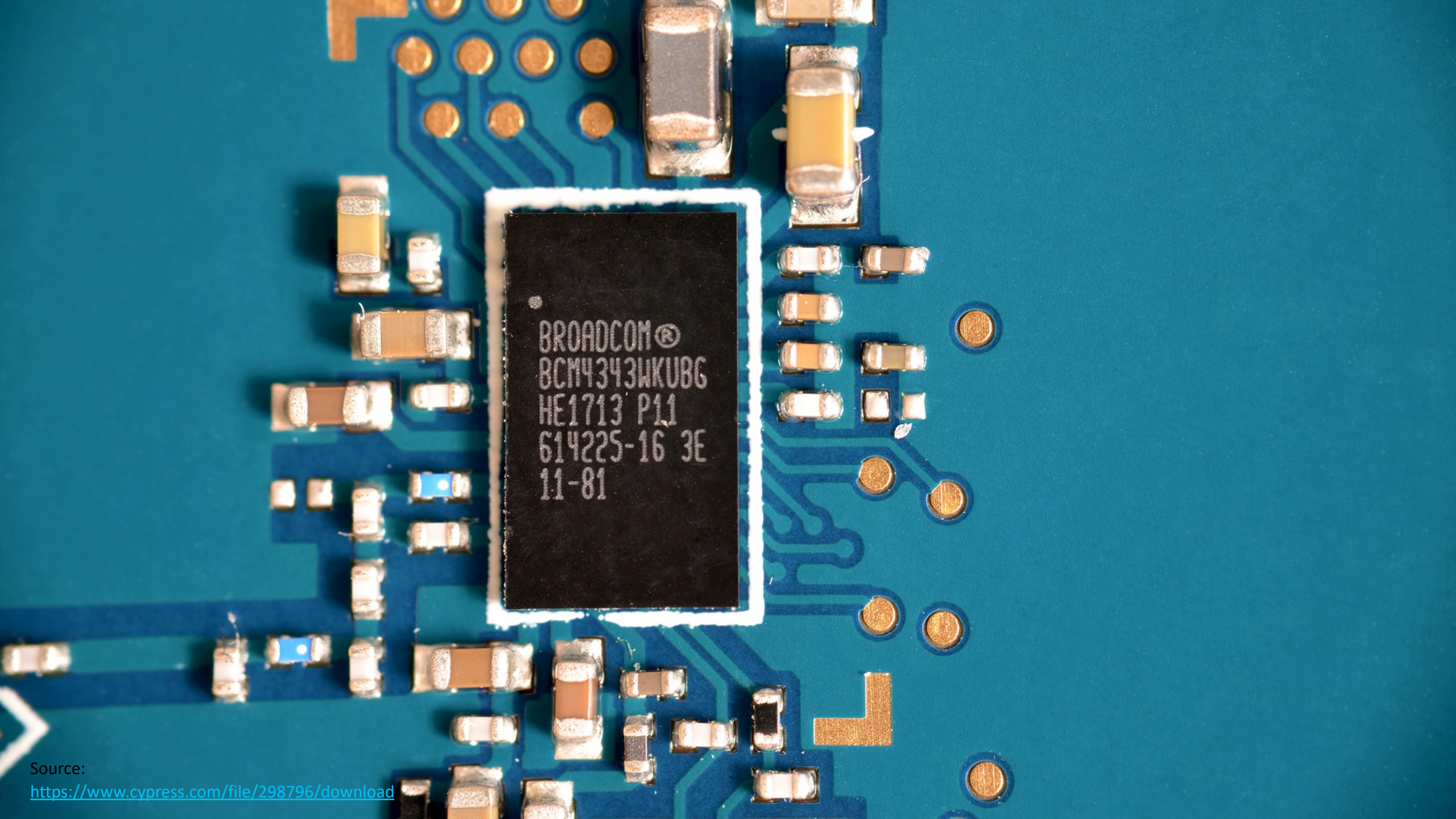


Rewind

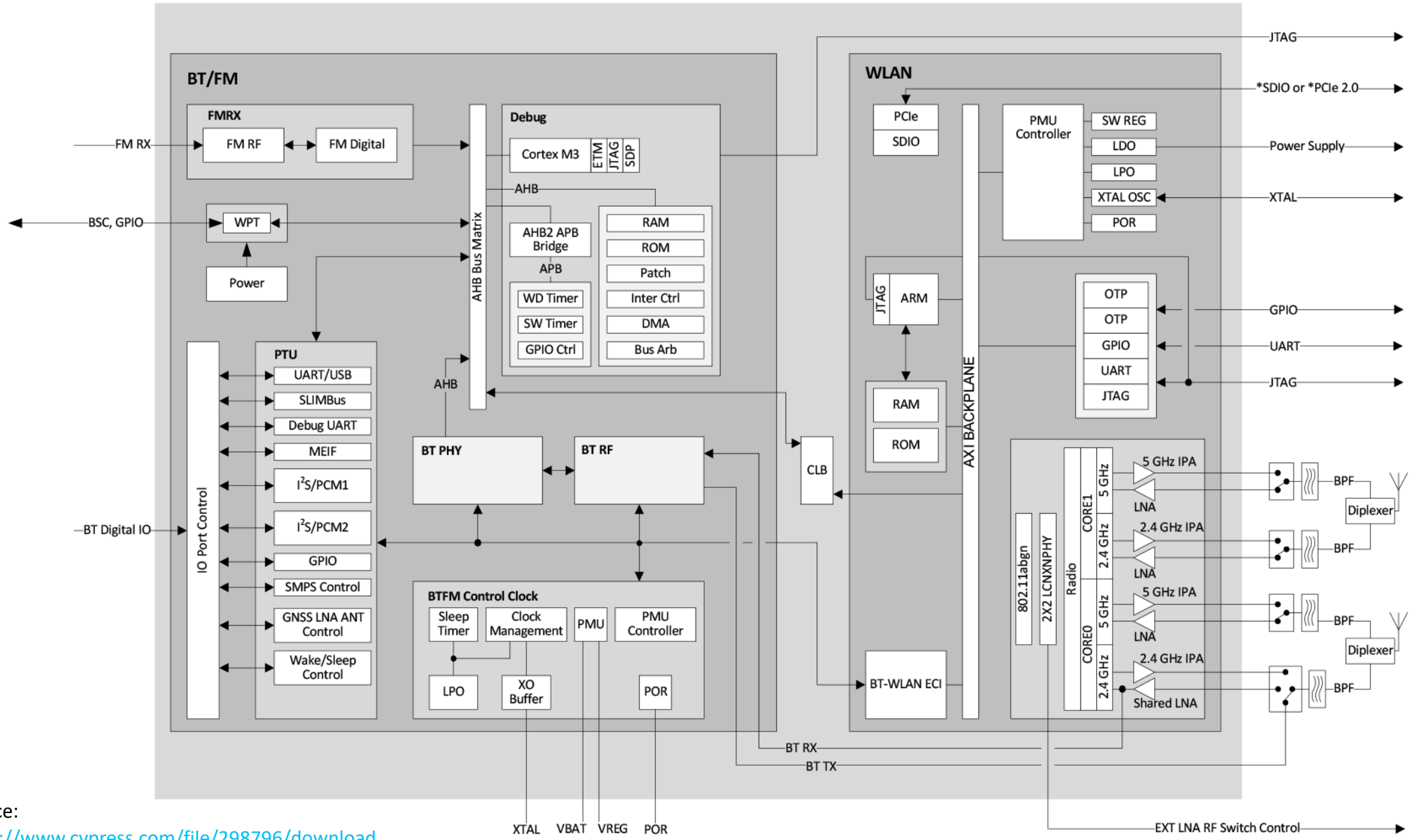
# WPA2



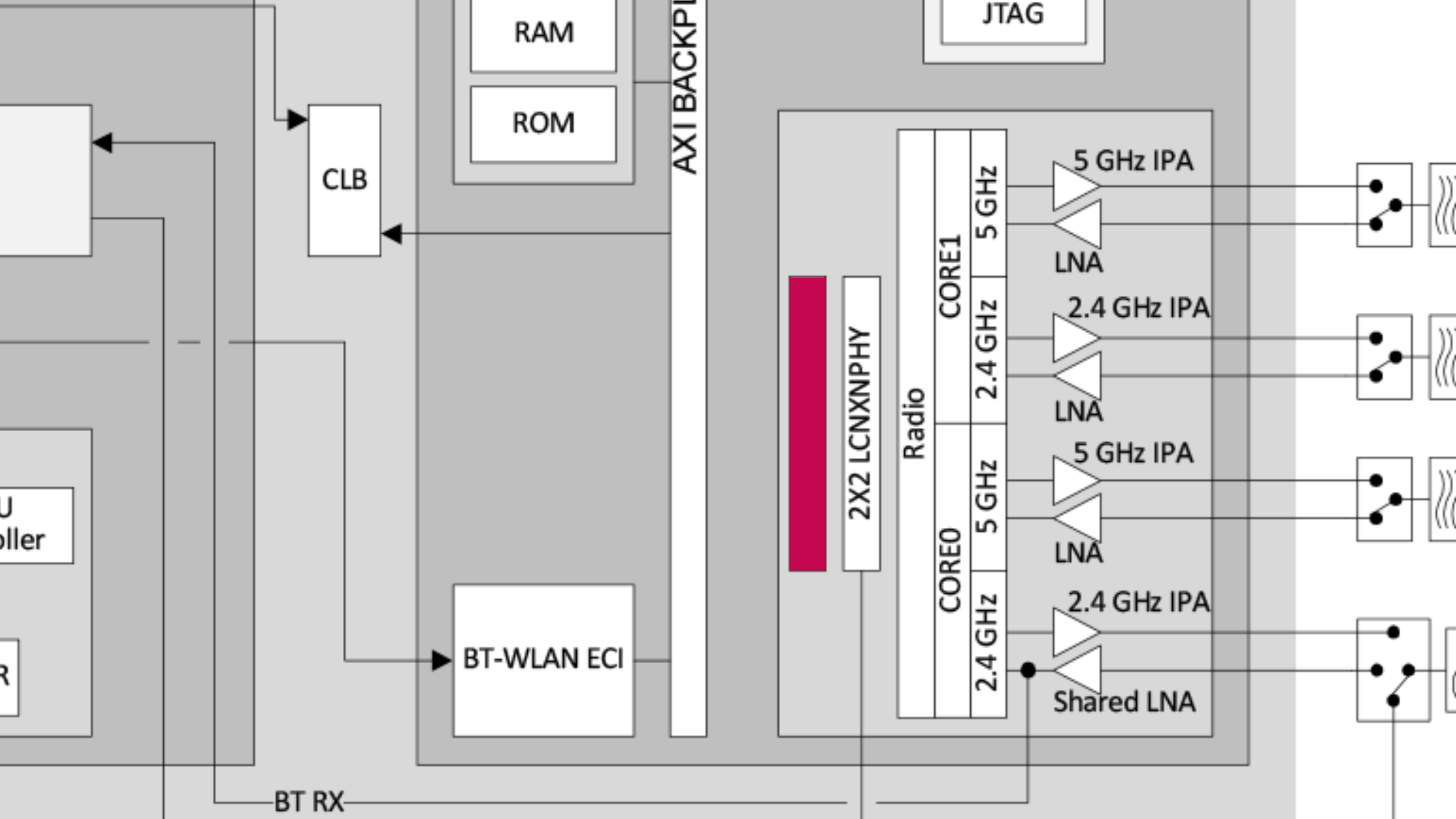


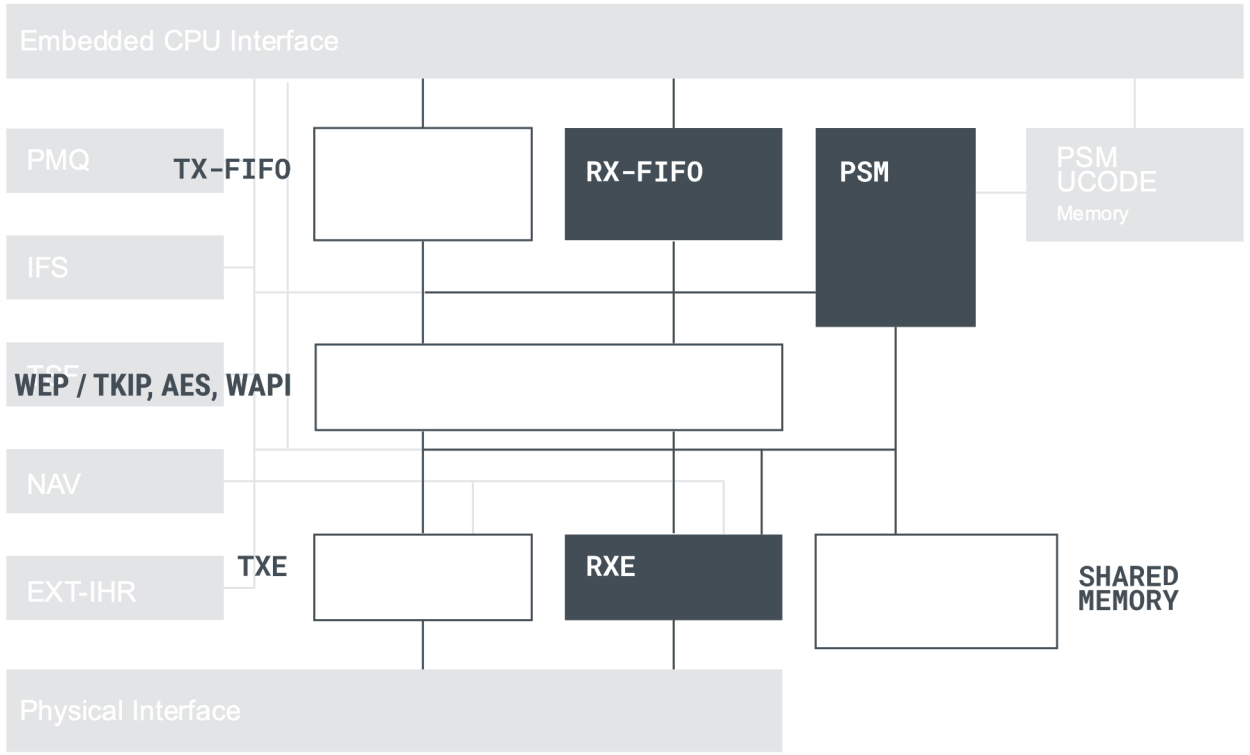


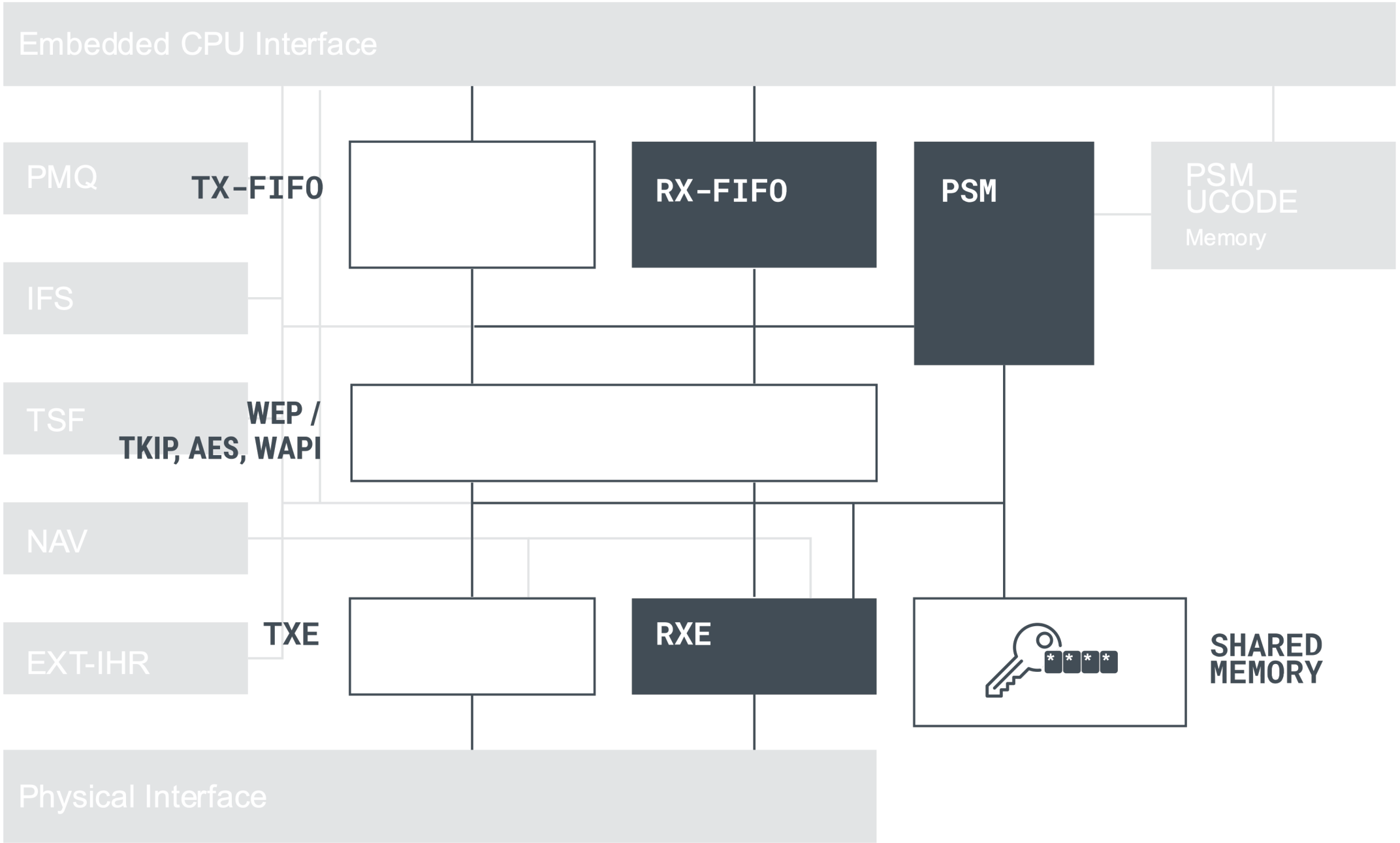

Source:
https://www.cypress.com/file/298796/download

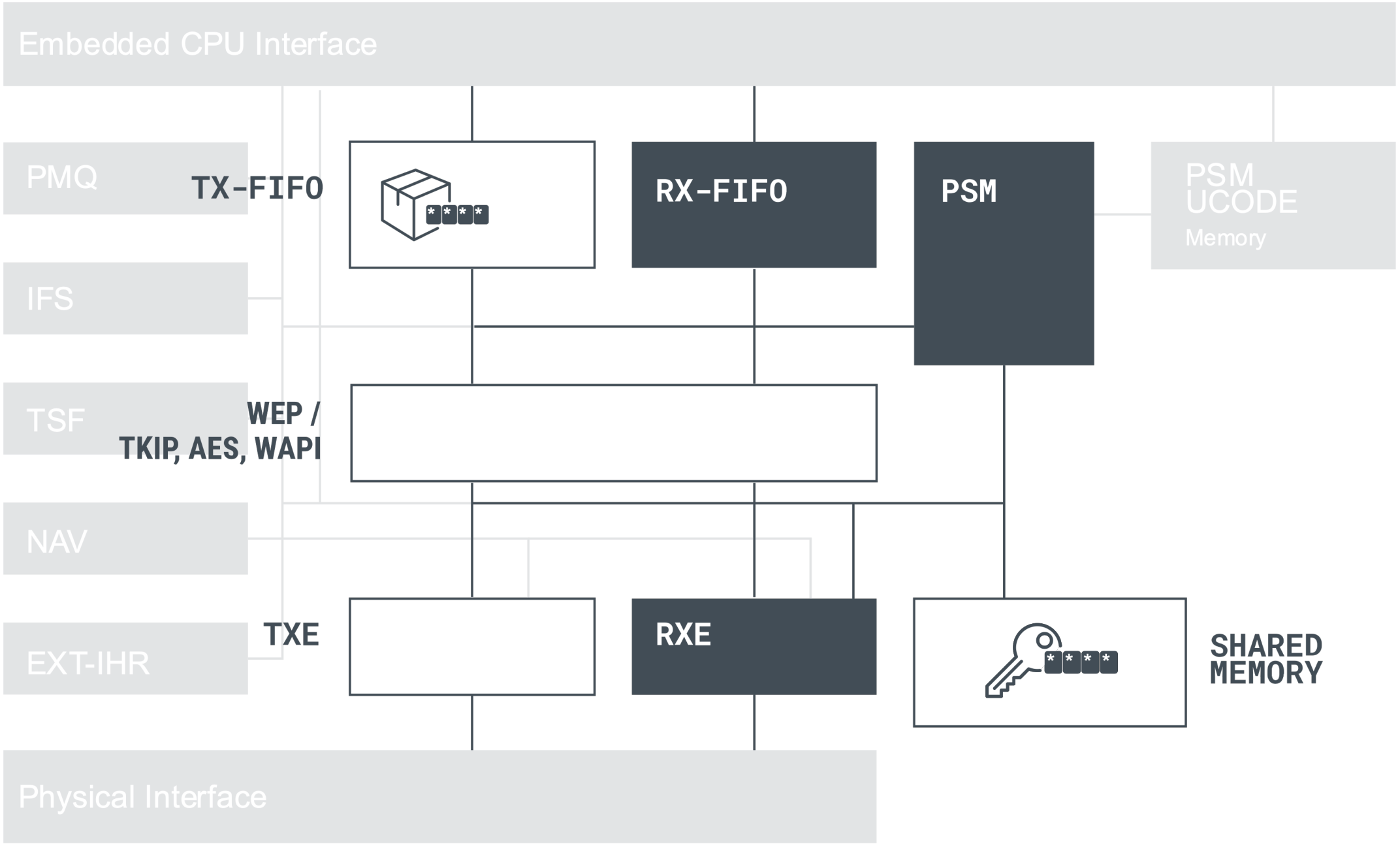



Source:
https://www.cypress.com/file/298796/download

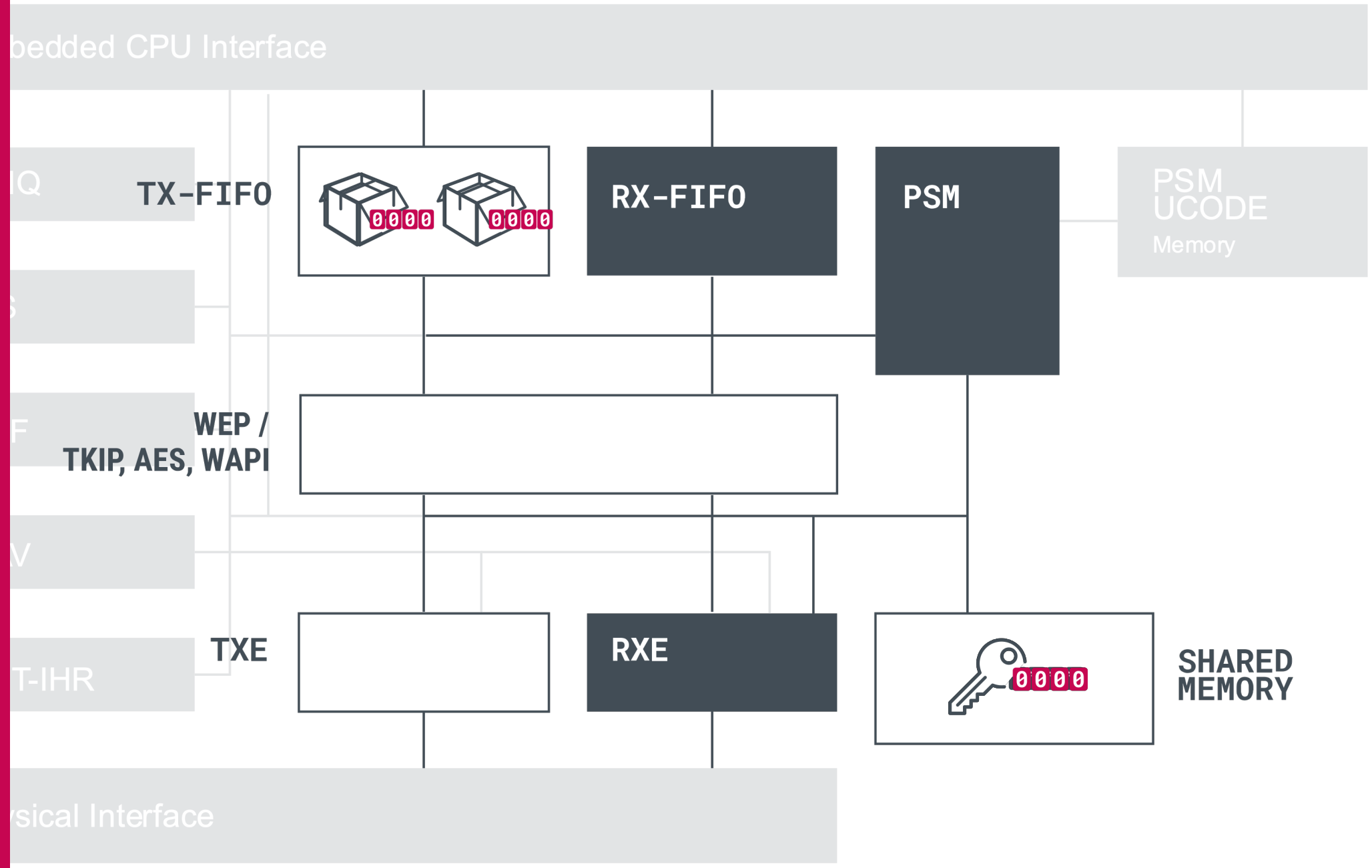

RAM
ROM
JTAG
AXI BACKPL
CLB
2X2 LCNXNPHY
Radio
CORE1
CORE0
5 GHz
2.4 GHz
5 GHz
2.4 GHz
5 GHz IPA
LNA
2.4 GHz IPA
LNA
5 GHz IPA
LNA
2.4 GHz IPA
Shared LNA
BT-WLAN ECI
BT RX


Embedded CPU Interface
PMQ
TX-FIFO
RX-FIFO
PSM
PSM
UCODE
Memory
IFS
WEP / TKIP, AES, WAPI
NAV
TXE
RXE
EXT-IHR
SHARED
MEMORY
Physical Interface

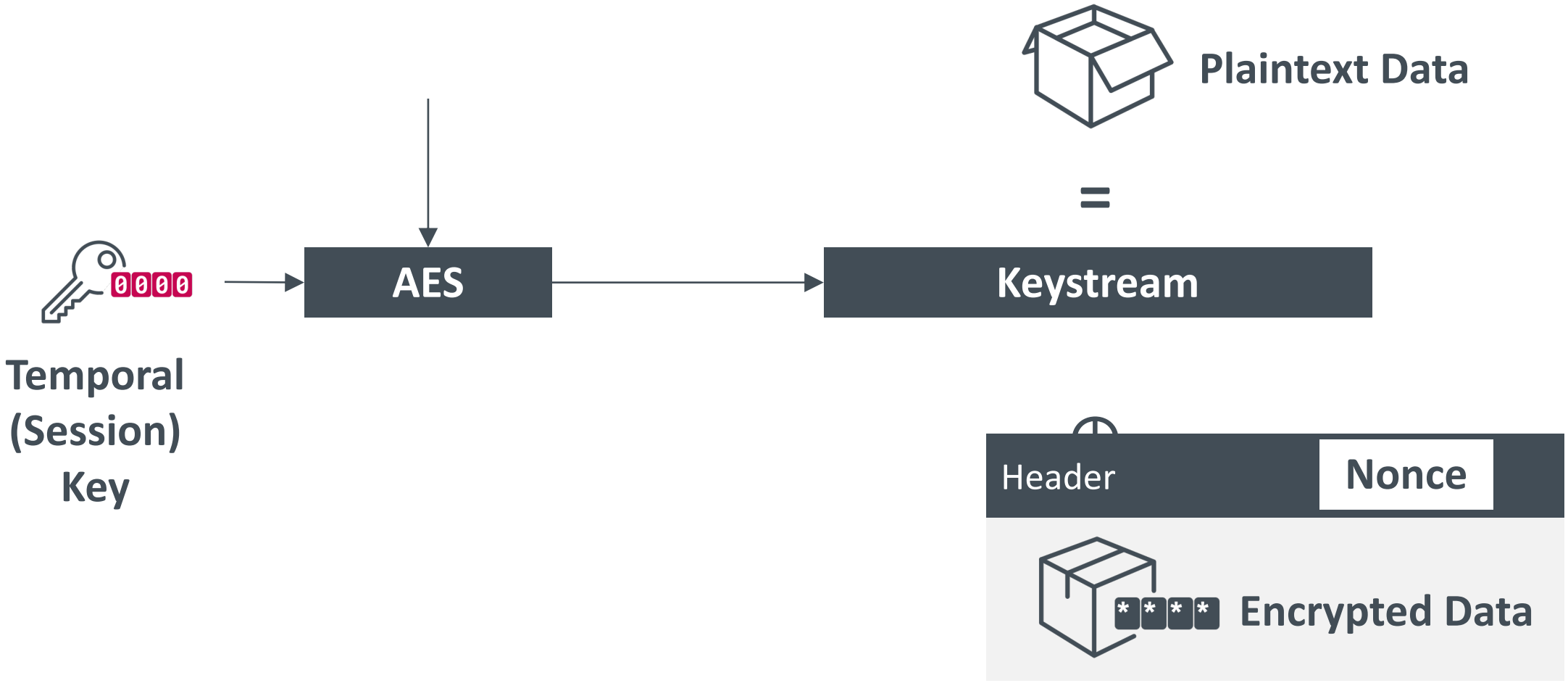

Embedded CPU Interface
PMQ
TX-FIFO
RX-FIFO
PSM
PSM
UCODE
Memory
IFS
TSF
WEP /
TKIP, AES, WAPI
NAV
TXE
RXE
EXT-IHR
SHARED
MEMORY
Physical Interface


Embedded CPU Interface
PMQ
TX-FIFO
RX-FIFO
PSM
PSM
UCODE
Memory
IFS
TSF
WEP /
TKIP, AES, WAPI
NAV
TXE
RXE
EXT-IHR
SHARED
MEMORY
Physical Interface

Disassociation



# Decryption in WPA2-CCMP

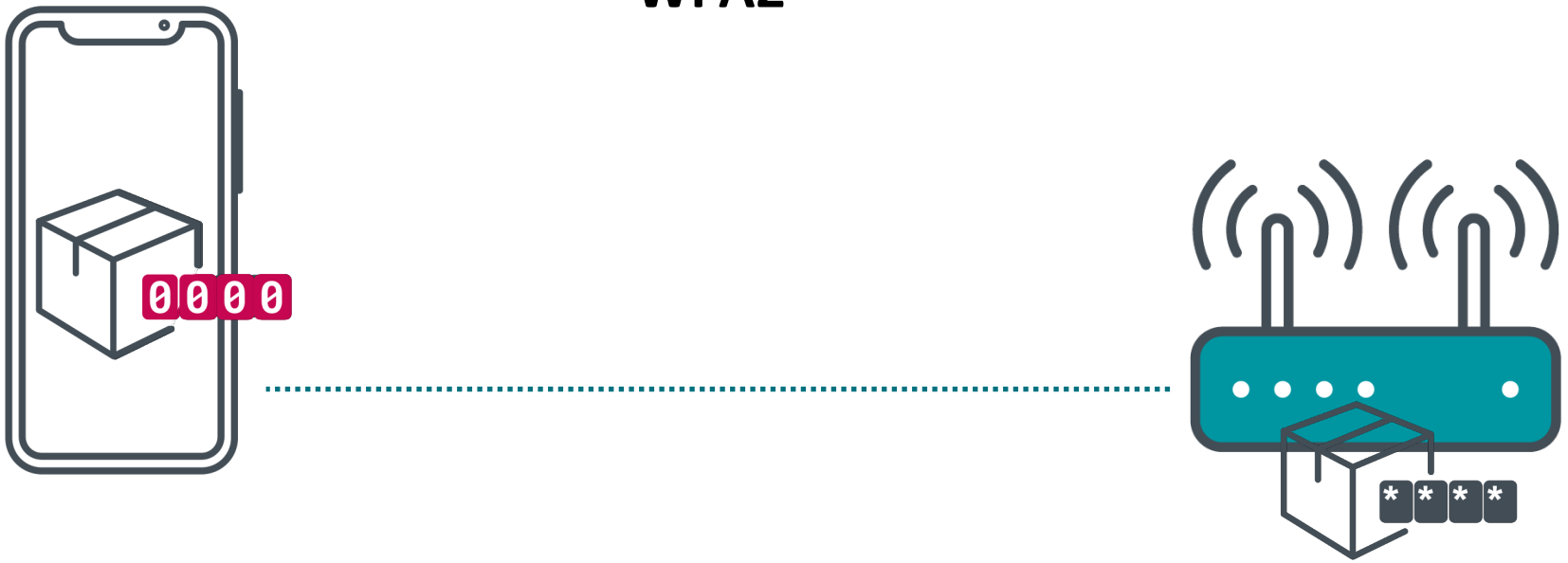


# Impact

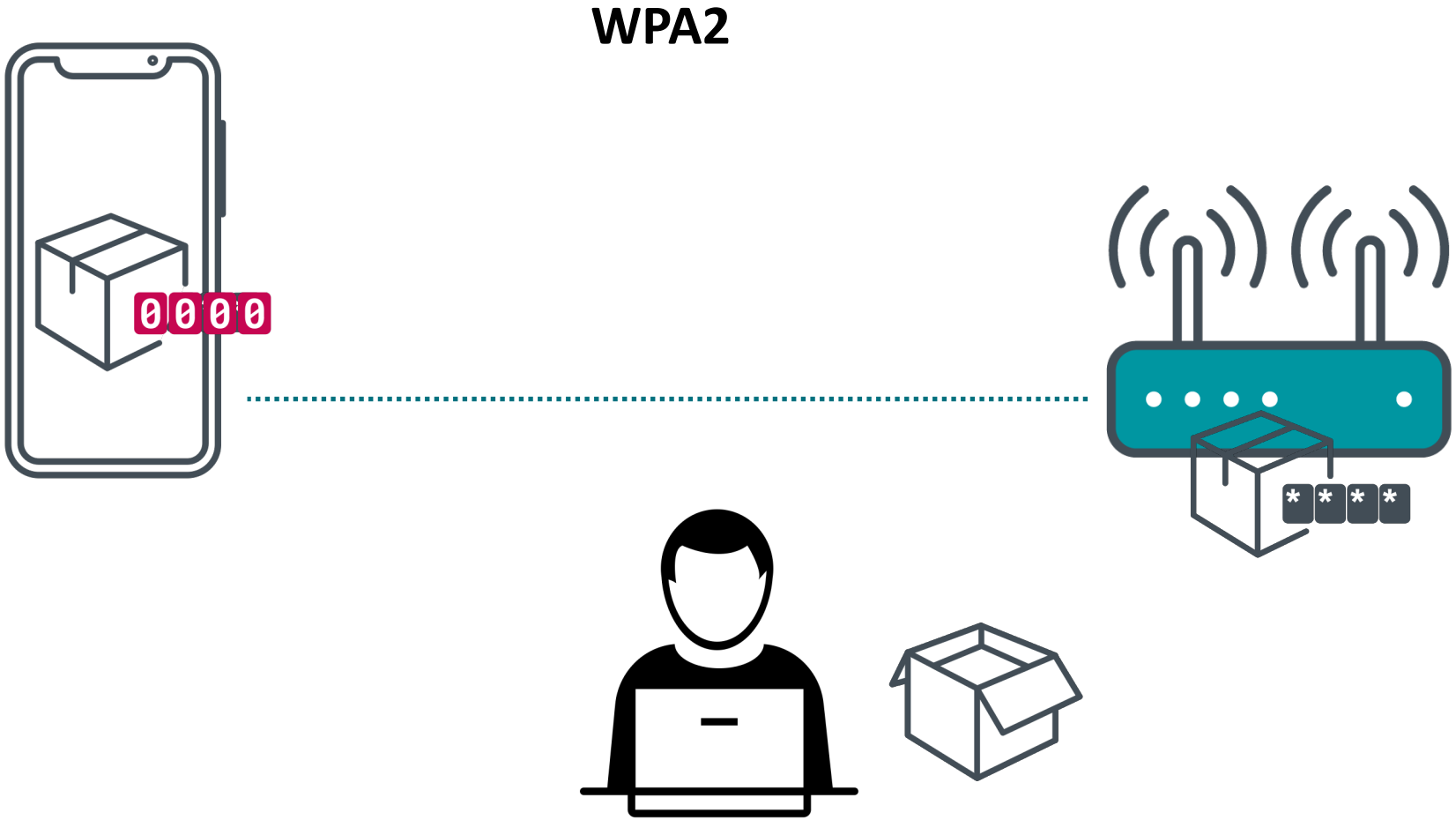
What can an attacker do with this vulnerability?

# Eavesdropping – Passive

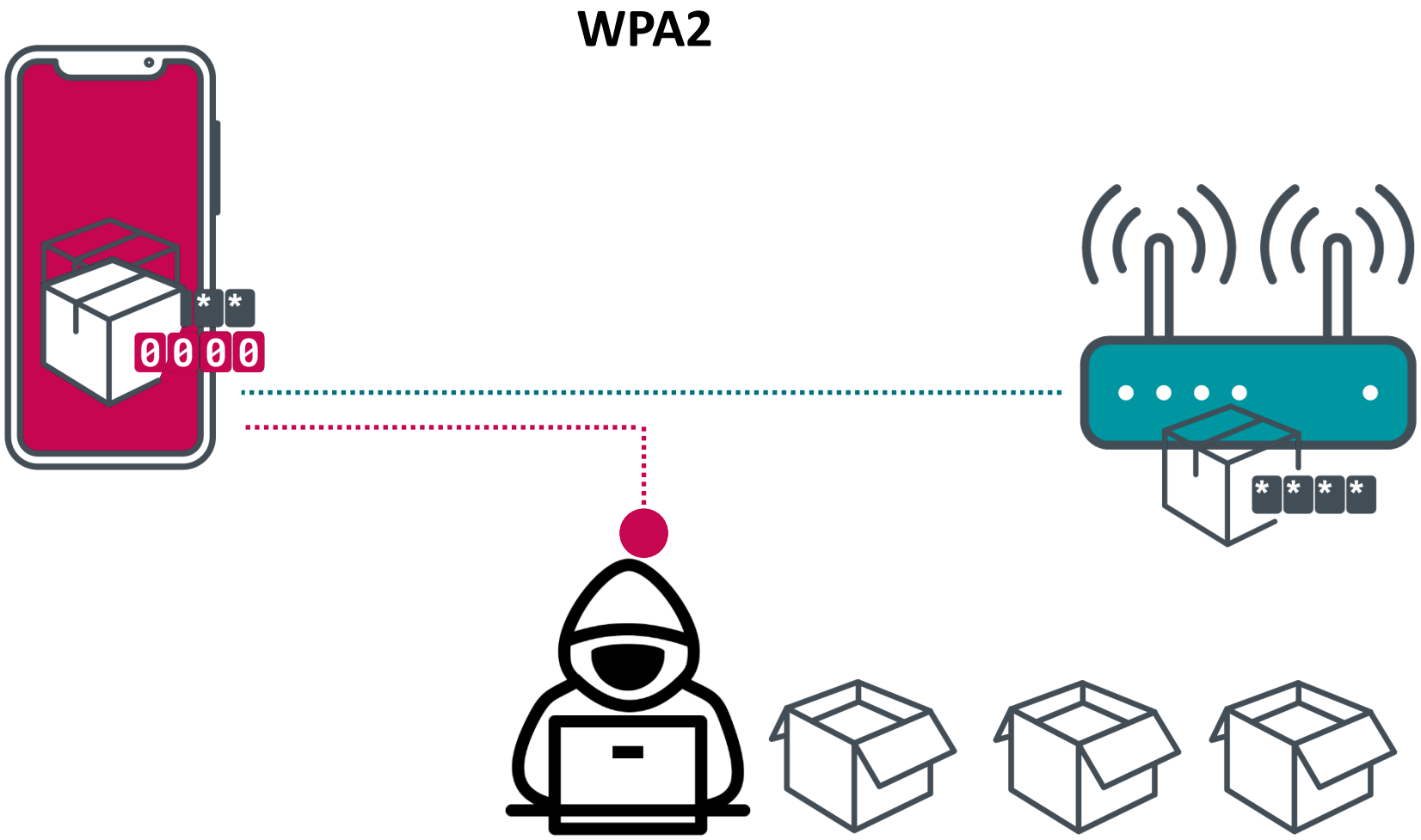
**WPA2**



# Eavesdropping – Passive

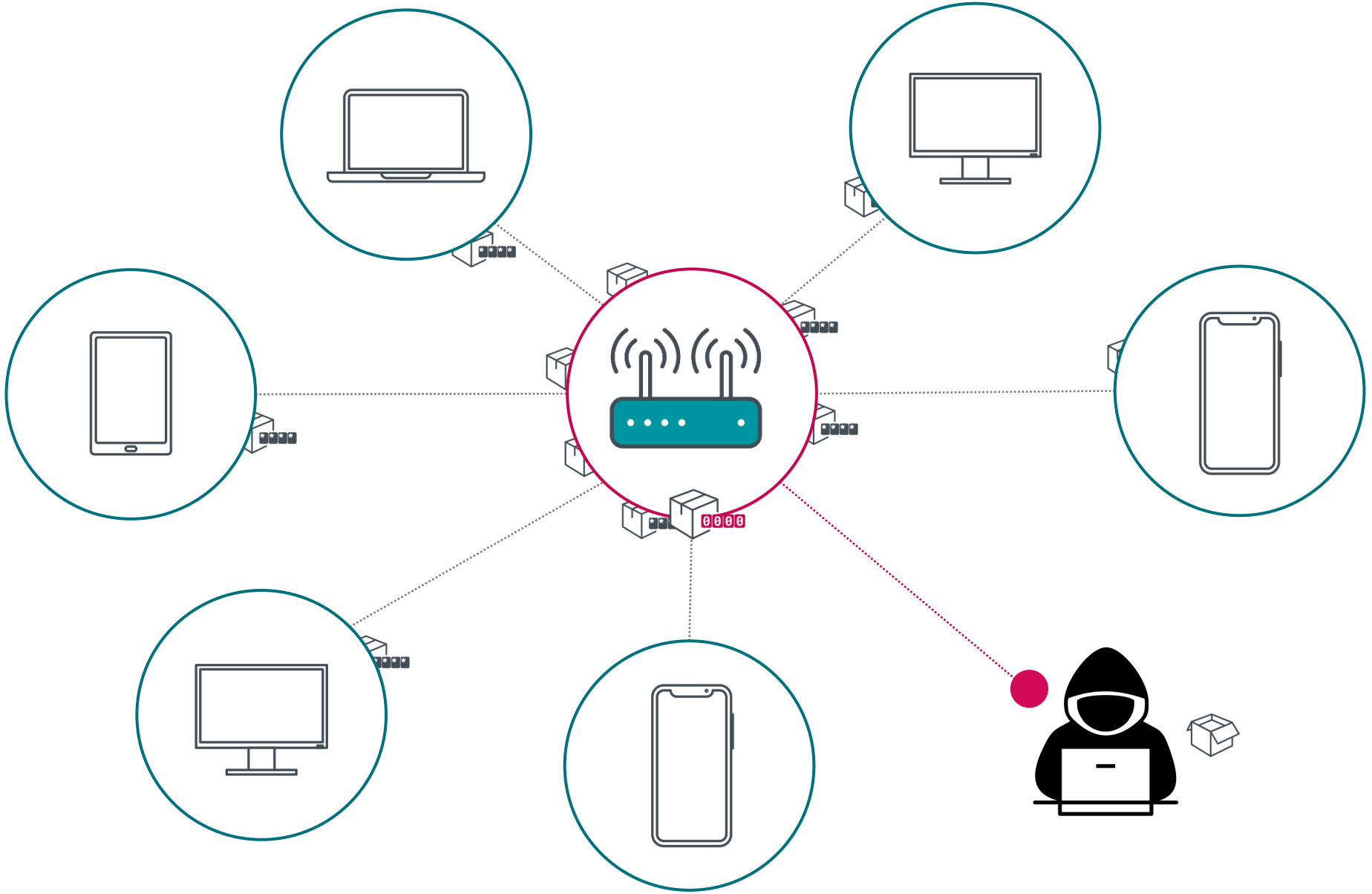


# Eavesdropping – Active



# DEMO

# Vulnerable Access Point vs. Secure Devices



# What devices are affected?

- Devices with Broadcom and Cypress FullMAC Wi-Fi chips

- We positively tested:
  - Apple iPhones
  - Apple MacBooks
  - Samsung Galaxy phones
  - Google Nexus phones
  - Raspberry Pi 3
  - Amazon Echo 2
  - Amazon Kindle 8
  - ASUS Wi-Fi routers
  - Huawei Wi-Fi routers

# What was done about this?

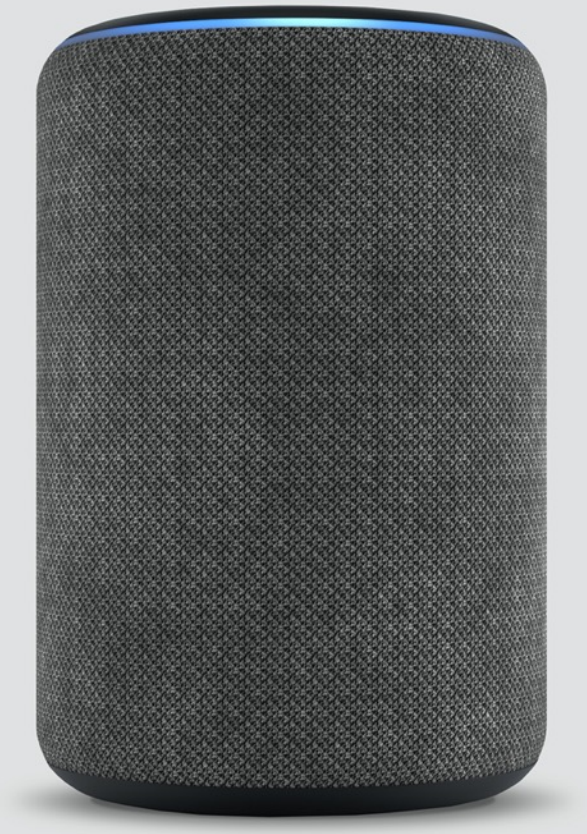
- ESET responsibly disclosed to Broadcom and Cypress
  - Granted 120 day grace period
- Broadcom and Cypress pushed patches to individual device manufacturers
- ESET worked with ICASI to ensure all possibly affected parties were aware of the bug


KRACKing Amazon Echo
How it all started…


localhost:4000
Key Reinstallation Attacks
Breaking WPA2 by forcing nonce reuse
Discovered by Mathy Vanhoef of imec-DistriNet, KU Leuven, 2017
INTRO
DEMO
DETAILS
PAPER
TOOLS
Q&A
INTRODUCTION
We discovered serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks. An attacker within range of a victim can exploit these weaknesses using key reinstallation attacks (KRACKs). Concretely, attackers can use this novel attack technique to read information that was previously assumed to be safely encrypted. This can be abused to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, and so on. The attack works against all modern protected Wi-Fi networks. Depending on the network configuration, it is also possible to inject and manipulate data. For example, an attacker might be able to inject ransomware or other malware into websites.

# AMAZON
# ECHO 1ST GEN

Vulnerable to **KRACK** attack



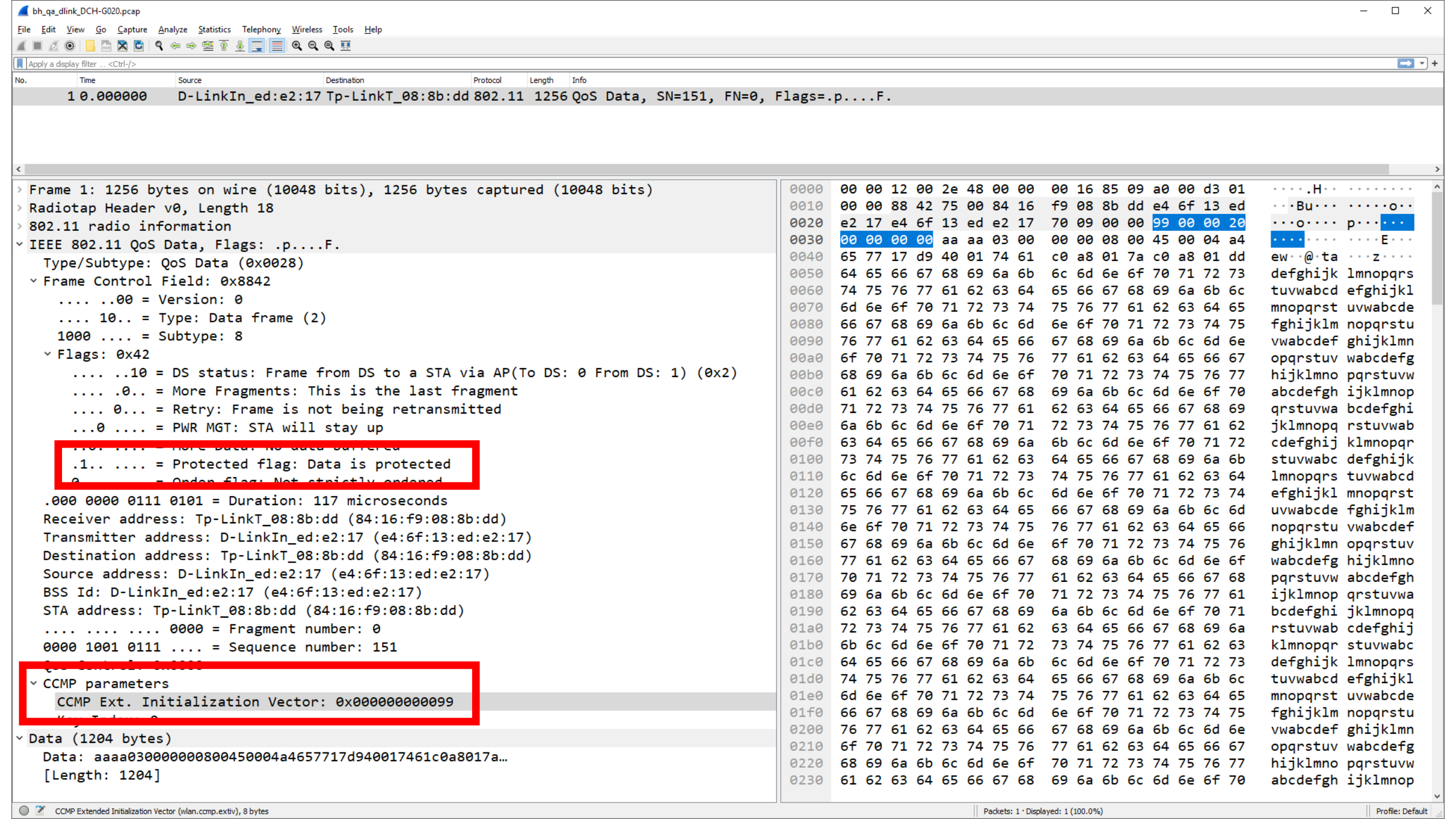
# AMAZON ECHO 2ND GEN

Vulnerable to… **Kr00k**

# KRACK vs. KR00K

| KRACK | KR00K |
| --- | --- |
| Attack / exploit | Vulnerability / bug |
| Nonce reused to acquire keystream | Data encrypted with all-zero session key |
| Triggered during the 4-way handshake | Triggered after a disassociation |
| Affects most Wi-Fi capable devices | Affects the most widespread Wi-Fi chips (Broadcom & Cypress) |


Follow-up research


bh_qa_dlink_DCH-G020.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 D-LinkIn_ed:e2:17 Tp-LinkT_08:8b:dd 802.11 1256 QoS Data, SN=151, FN=0, Flags=.p....F.
Frame 1: 1256 bytes on wire (10048 bits), 1256 bytes captured (10048 bits)
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p....F.
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8842
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x42
.... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
.1.. .... = Protected flag: Data is protected
.000 0000 0111 0101 = Duration: 117 microseconds
Receiver address: Tp-LinkT_08:8b:dd (84:16:f9:08:8b:dd)
Transmitter address: D-LinkIn_ed:e2:17 (e4:6f:13:ed:e2:17)
Destination address: Tp-LinkT_08:8b:dd (84:16:f9:08:8b:dd)
Source address: D-LinkIn_ed:e2:17 (e4:6f:13:ed:e2:17)
BSS Id: D-LinkIn_ed:e2:17 (e4:6f:13:ed:e2:17)
STA address: Tp-LinkT_08:8b:dd (84:16:f9:08:8b:dd)
.... .... .... 0000 = Fragment number: 0
0000 1001 0111 .... = Sequence number: 151
CCMP parameters
CCMP Ext. Initialization Vector: 0x000000000099
Data (1204 bytes)
Data: aaaa03000000800450004a4657717d940017461c0a8017a…
[Length: 1204]
0000 00 00 12 00 2e 48 00 00 00 16 85 09 a0 00 d3 01
0010 00 00 88 42 75 00 84 16 f9 08 8b dd e4 6f 13 ed
0020 e2 17 e4 6f 13 ed e2 17 70 09 00 00 99 00 00 20
0030 00 00 00 00 aa aa 03 00 00 00 08 00 45 00 04 a4
0040 65 77 17 d9 40 01 74 61 c0 a8 01 7a c0 a8 01 dd
0050 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
0060 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c
0070 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65
0080 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75
0090 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e
00a0 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67
00b0 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77
00c0 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70
00d0 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69
00e0 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62
00f0 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72
0100 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b
0110 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64
0120 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74
0130 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d
0140 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66
0150 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76
0160 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f
0170 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68
0180 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61
0190 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71
01a0 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a
01b0 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63
01c0 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
01d0 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c
01e0 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65
01f0 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75
0200 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e
0210 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67
0220 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77
0230 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70
CCMP Extended Initialization Vector (wlan.ccmp.extiv), 8 bytes
Packets: 1 · Displayed: 1 (100.0%)
Profile: Default

# Qualcomm WLAN chips

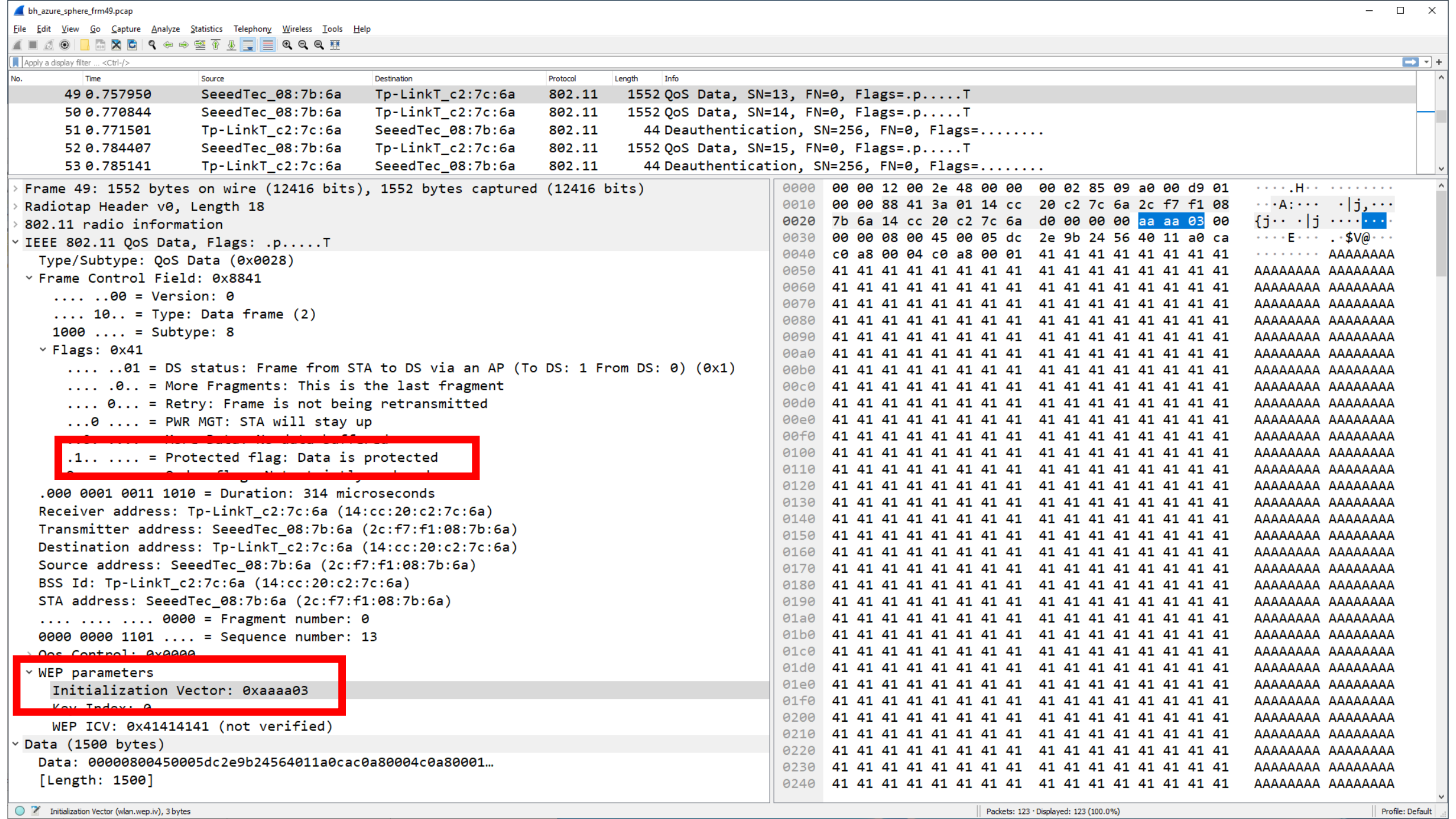
- **CVE-2020-3702**
- Affected chip: **QCA9531**

- Mitigation:
  - **Proprietary driver** patched July 2020
  - **Open source drivers?!**

# Mediatek WLAN chips

- Affected tested devices:
  - **ASUS RT-AC52U router**
  - **Azure Sphere MT3620** (OS ver.20.05)

- Mitigation:
  - SW patches issued March - April 2020
  - Azure Sphere – patch in latest/upcoming OS update


bh_azure_sphere_frm49.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
49 0.757950 SeeedTec_08:7b:6a Tp-LinkT_c2:7c:6a 802.11 1552 QoS Data, SN=13, FN=0, Flags=.p.....T
50 0.770844 SeeedTec_08:7b:6a Tp-LinkT_c2:7c:6a 802.11 1552 QoS Data, SN=14, FN=0, Flags=.p.....T
51 0.771501 Tp-LinkT_c2:7c:6a SeeedTec_08:7b:6a 802.11 44 Deauthentication, SN=256, FN=0, Flags=........
52 0.784407 SeeedTec_08:7b:6a Tp-LinkT_c2:7c:6a 802.11 1552 QoS Data, SN=15, FN=0, Flags=.p.....T
53 0.785141 Tp-LinkT_c2:7c:6a SeeedTec_08:7b:6a 802.11 44 Deauthentication, SN=256, FN=0, Flags=........
Frame 49: 1552 bytes on wire (12416 bits), 1552 bytes captured (12416 bits)
Radiotap Header v0, Length 18
802.11 radio information
IEEE 802.11 QoS Data, Flags: .p.....T
Type/Subtype: QoS Data (0x0028)
Frame Control Field: 0x8841
.... ..00 = Version: 0
.... 10.. = Type: Data frame (2)
1000 .... = Subtype: 8
Flags: 0x41
.... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
.... .0.. = More Fragments: This is the last fragment
.... 0... = Retry: Frame is not being retransmitted
...0 .... = PWR MGT: STA will stay up
.1.. .... = Protected flag: Data is protected
.000 0001 0011 1010 = Duration: 314 microseconds
Receiver address: Tp-LinkT_c2:7c:6a (14:cc:20:c2:7c:6a)
Transmitter address: SeeedTec_08:7b:6a (2c:f7:f1:08:7b:6a)
Destination address: Tp-LinkT_c2:7c:6a (14:cc:20:c2:7c:6a)
Source address: SeeedTec_08:7b:6a (2c:f7:f1:08:7b:6a)
BSS Id: Tp-LinkT_c2:7c:6a (14:cc:20:c2:7c:6a)
STA address: SeeedTec_08:7b:6a (2c:f7:f1:08:7b:6a)
.... .... .... 0000 = Fragment number: 0
0000 0000 1101 .... = Sequence number: 13
WEP parameters
Initialization Vector: 0xaaaa03
WEP ICV: 0x41414141 (not verified)
Data (1500 bytes)
Data: 00000800450005dc2e9b24564011a0cac0a80004c0a80001…
[Length: 1500]
0000 00 00 12 00 2e 48 00 00 00 02 85 09 a0 00 d9 01 .....H..
0010 00 00 88 41 3a 01 14 cc 20 c2 7c 6a 2c f7 f1 08 ...A:... .|j,...
0020 7b 6a 14 cc 20 c2 7c 6a d0 00 00 00 aa aa 03 00 {j.. .|j ........
0030 00 00 08 00 45 00 05 dc 2e 9b 24 56 40 11 a0 ca ....E... ..$V@...
0040 c0 a8 00 04 c0 a8 00 01 41 41 41 41 41 41 41 41 ........ AAAAAAAA
0050 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0060 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0070 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0080 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0090 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00a0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00b0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00d0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00e0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
00f0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0100 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0110 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0120 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0130 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0140 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0150 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0160 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0170 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0180 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0190 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01a0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01b0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01c0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01d0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01e0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
01f0 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0200 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0210 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0220 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0230 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
0240 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 AAAAAAAA AAAAAAAA
Initialization Vector (wlan.wep.iv), 3 bytes
Packets: 123 · Displayed: 123 (100.0%)
Profile: Default


Wrapping up…

Kudos to


amazon


BROADCOM


Qualcomm


icasi™


CYPRESS
EMBEDDED IN TOMORROW™


Microsoft

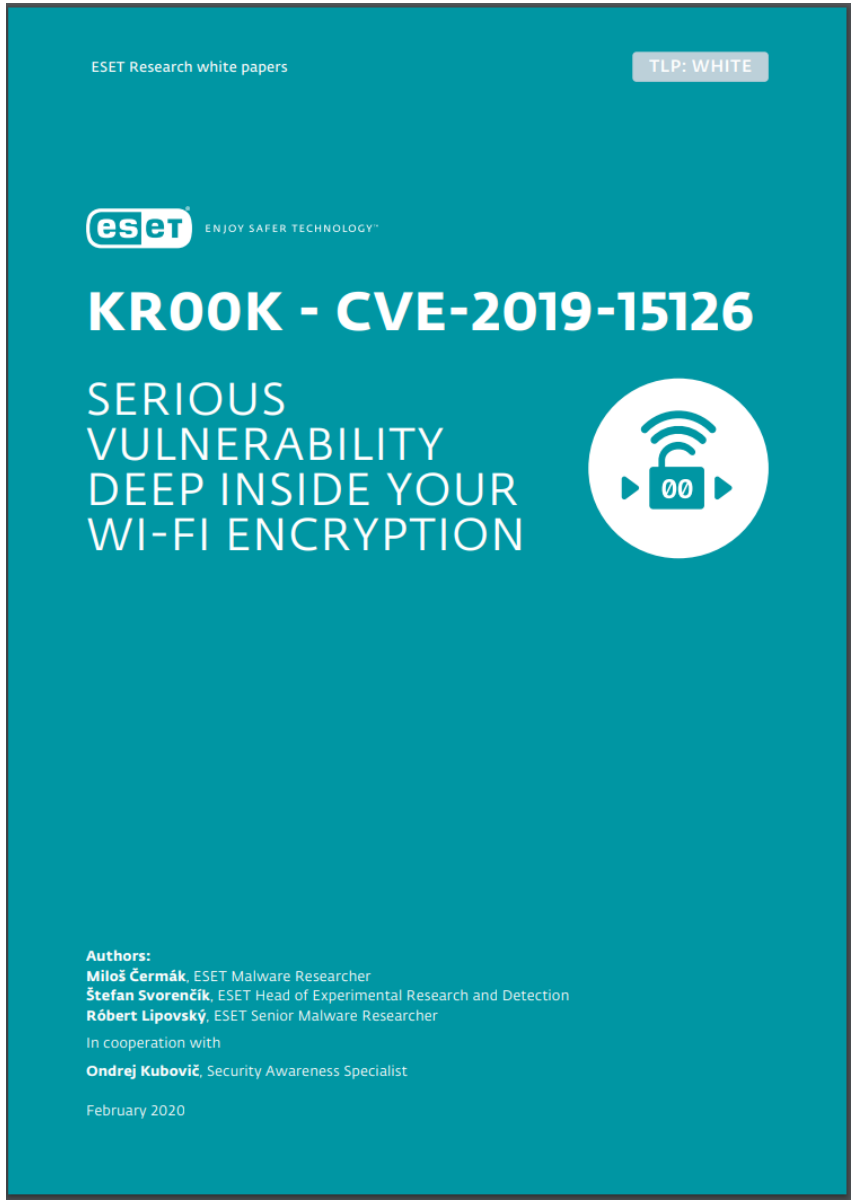

Aruba Product Security Advisory
Advisory ID: ARUBA-PSA-2020-003
CVE: CVE-2019-15126
Publication Date: 2020-Mar-26
Status: Confirmed
Revision: 3
Title
WPA and WPA2 Disassociation Vulnerability ("Kr00k")
timing flaw in certain Wi-Fi chip firmware may all
limited amount of WPA2-encrypted frames using a kn
uba products are affected by this vulnerability.
ZEBRA
ASUS
New Kr00k Vulnerability Lets Attacke
Subscribe To LifeGuard Updates
The Kr00k vulnerability potentially affec
Broadcom or Cypress. This includes se
Mac
About the security
iPadOS 13.2
This document describes the securit
About Apple security
For our customers' protection, Apple
HUAWEI
Security Notice - Statem
About the Vulnerability
Kr00k in Wi-Fi Chips
Initial Release Date: Feb 28, 2020
Last Release Date: May 27, 2020
After getting
2019-15126)
has started inv
Huawei
CISCO
Security Advisories
Cisco
SAMSUNG
Mobile Security
Security Post
Mist
A Juniper Company
Documentation › Security Alerts › Mist Se
Mist Security Ad
FAQ
What is this vulnerability?
Kr00k – formally known as CVE-20
unauthorized decryption of some
frames without proper MAC lev
CONSUMER
BUSINESS
SERVICE PROVIDERS
SUPPORT
D-Link
Kr00k ESET
Date: 03/09/2020

# What should you do?

- Update all your devices ~~with Broadcom & Cypress chips~~

  Even APs / Wi-Fi routers!  Not just Personal – but Enterprise too!

- As a manufacturer of Wi-Fi capable devices:
  - Contact the Wi-Fi Alliance and check with your Wi-Fi chip manufacturer that your devices have been patched




**www.ESET.com/int/Kr00k**

CYBERSECURITY
EXPERTS ON YOUR SIDE

# Thanks for watching!

@ESETResearch | WeLiveSecurity.com