



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

Robert Lipovsky | Stefan Svorencik







IoT research



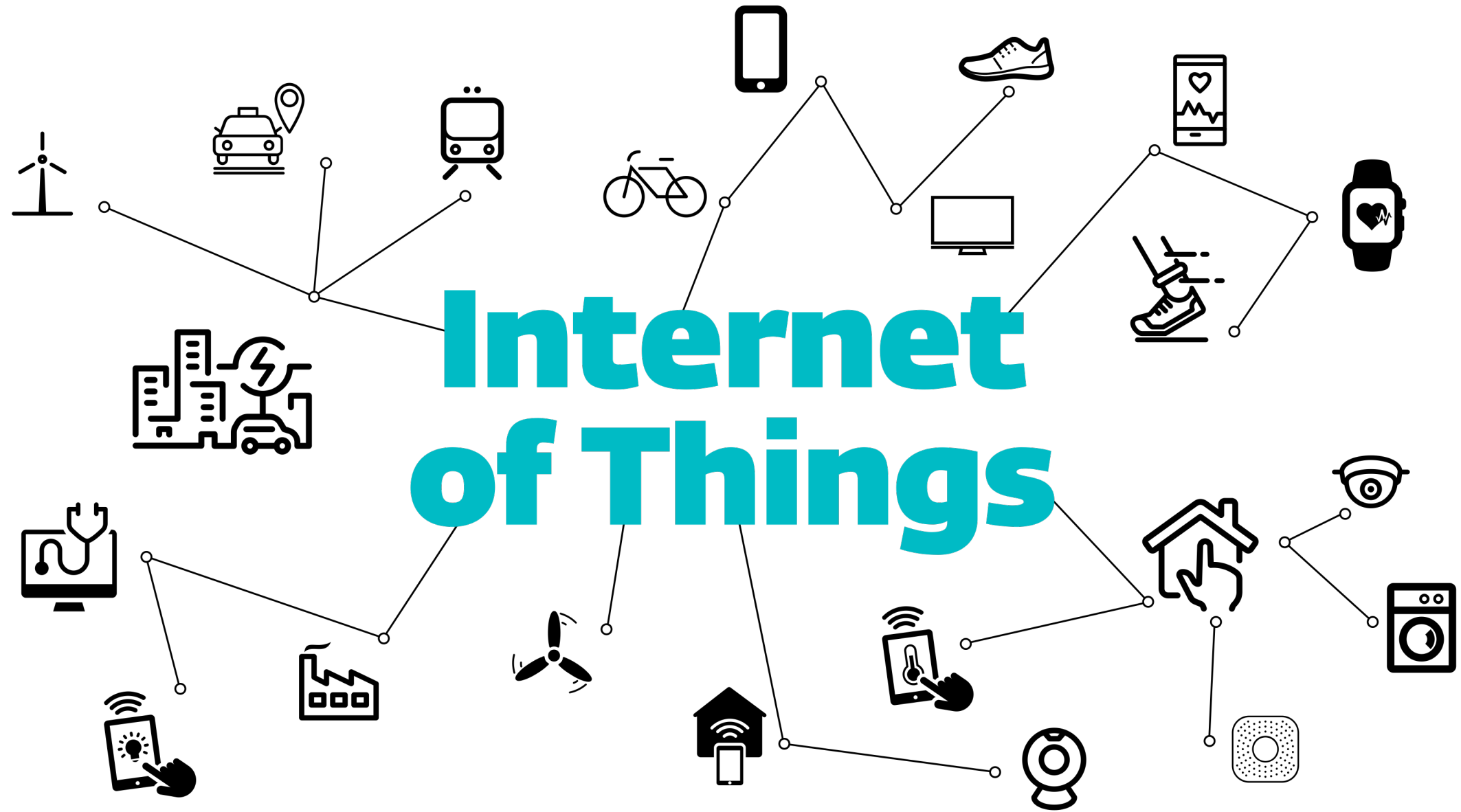
***Consumer IoT Devices
Are Expanding The
Enterprise Attack
Surface***

***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





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



eset®

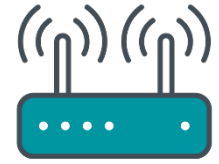
The image shows a control room with several computer monitors. The top row of monitors displays 'GLOBAL VIEW' and 'EUROPE VIEW' maps with data points. The bottom row shows people working at desks with multiple monitors. A large white 'eset' logo with a registered trademark symbol is overlaid in the center.

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**

The background features a dark, futuristic cityscape with glowing blue lines and data streams. The lines radiate from the center, creating a sense of depth and movement. The buildings in the background are stylized and also glow with blue light. The overall aesthetic is high-tech and digital.

Wi-Fi Security Primer



Association stage

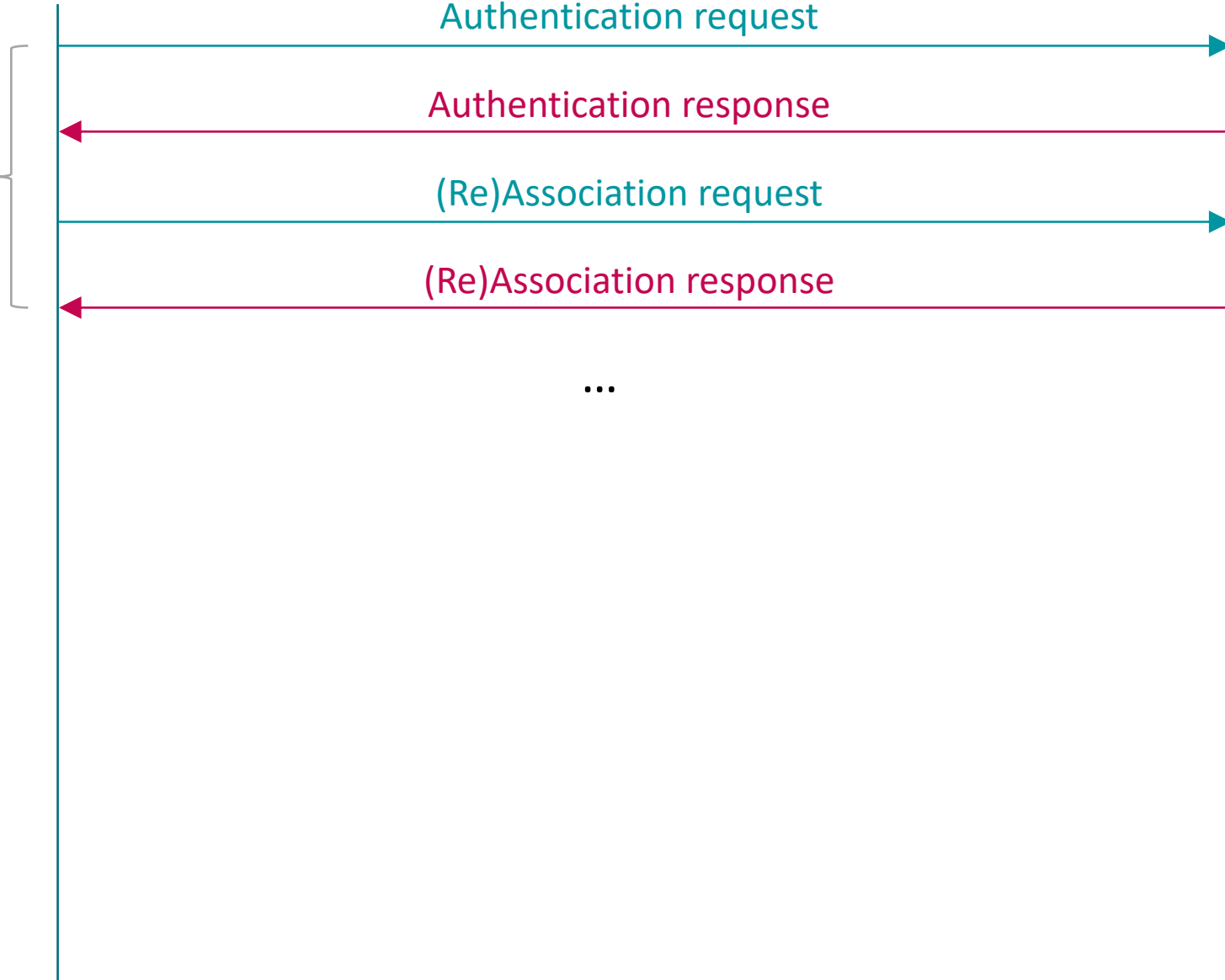
Authentication request

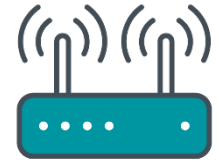
Authentication response

(Re)Association request

(Re)Association response

...





Association stage

Authentication request

Authentication response

(Re)Association request

(Re)Association response

Message 1

Construct PTK

Message 2

Construct PTK

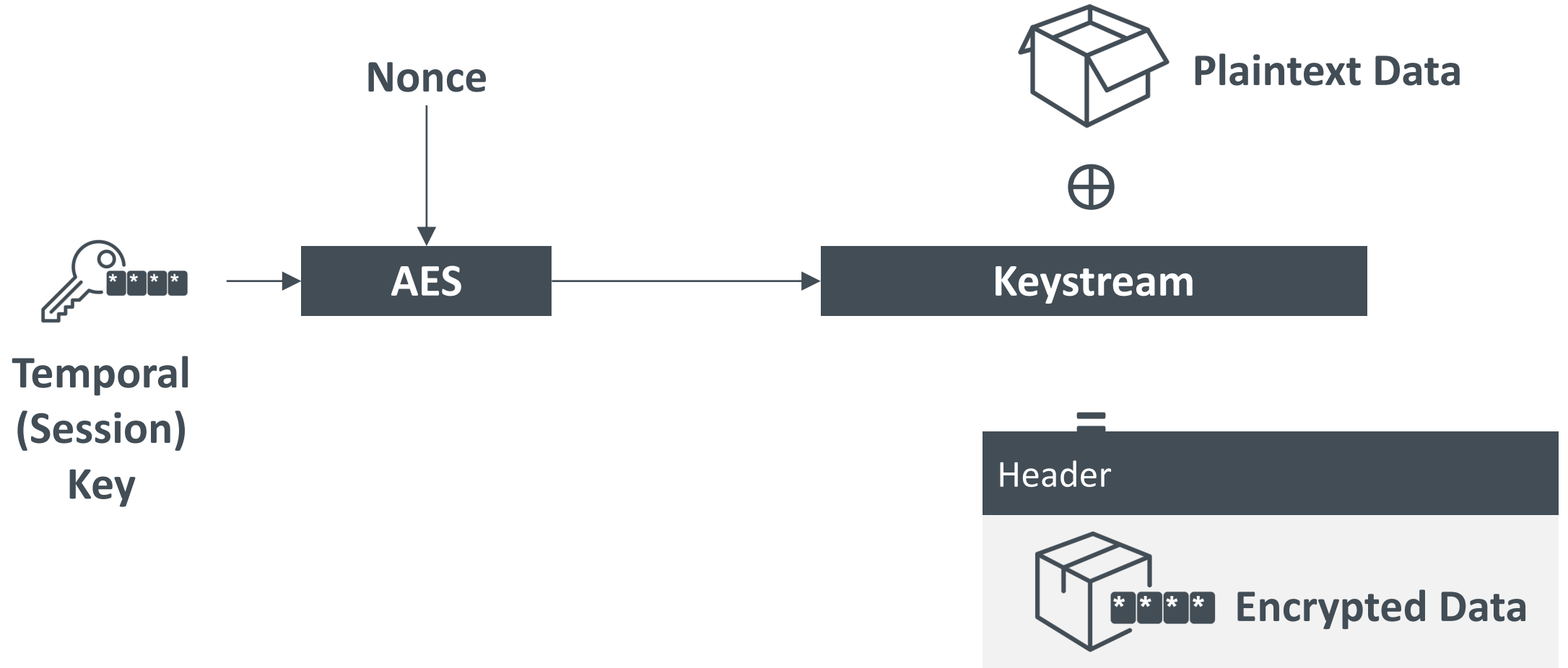
Message 3

Message 4

...

4-way handshake

Encryption in WPA2-CCMP

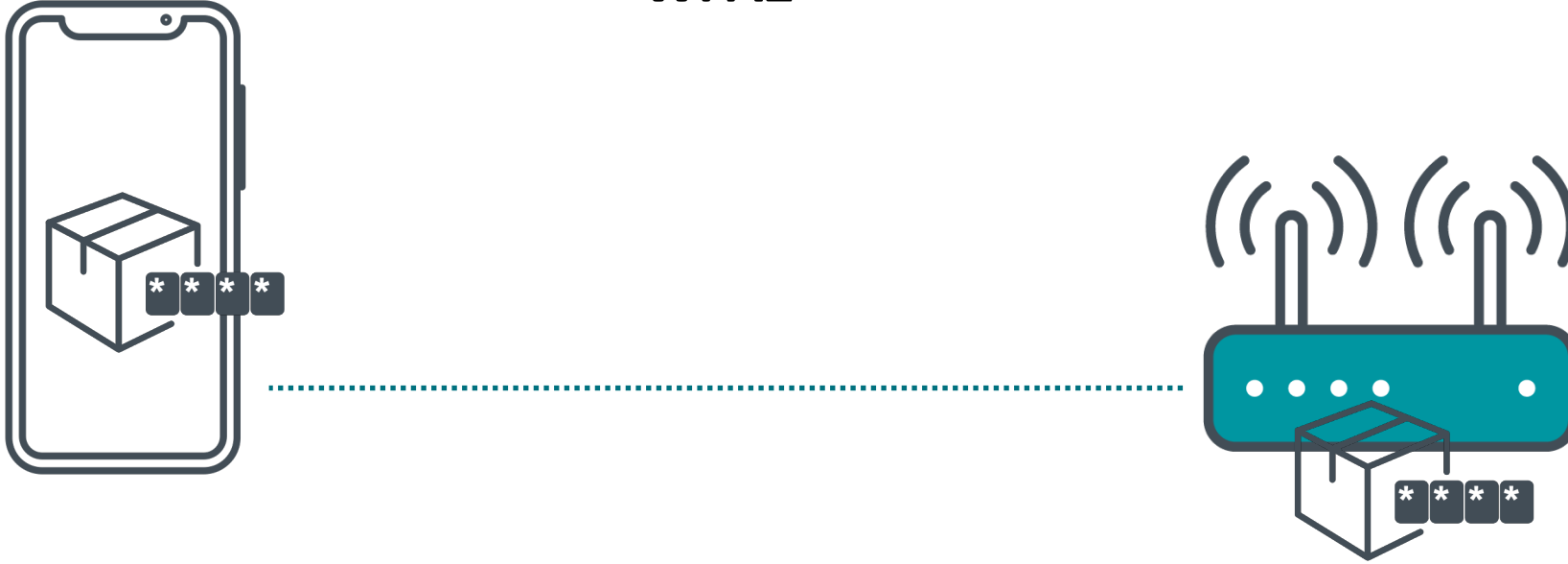


The background features a futuristic digital cityscape with glowing blue lines and structures. The scene is dominated by a central perspective of a glowing blue path that recedes into the distance, flanked by various digital buildings and structures. The overall color palette is dark with vibrant blue highlights, creating a high-tech, cybernetic atmosphere.

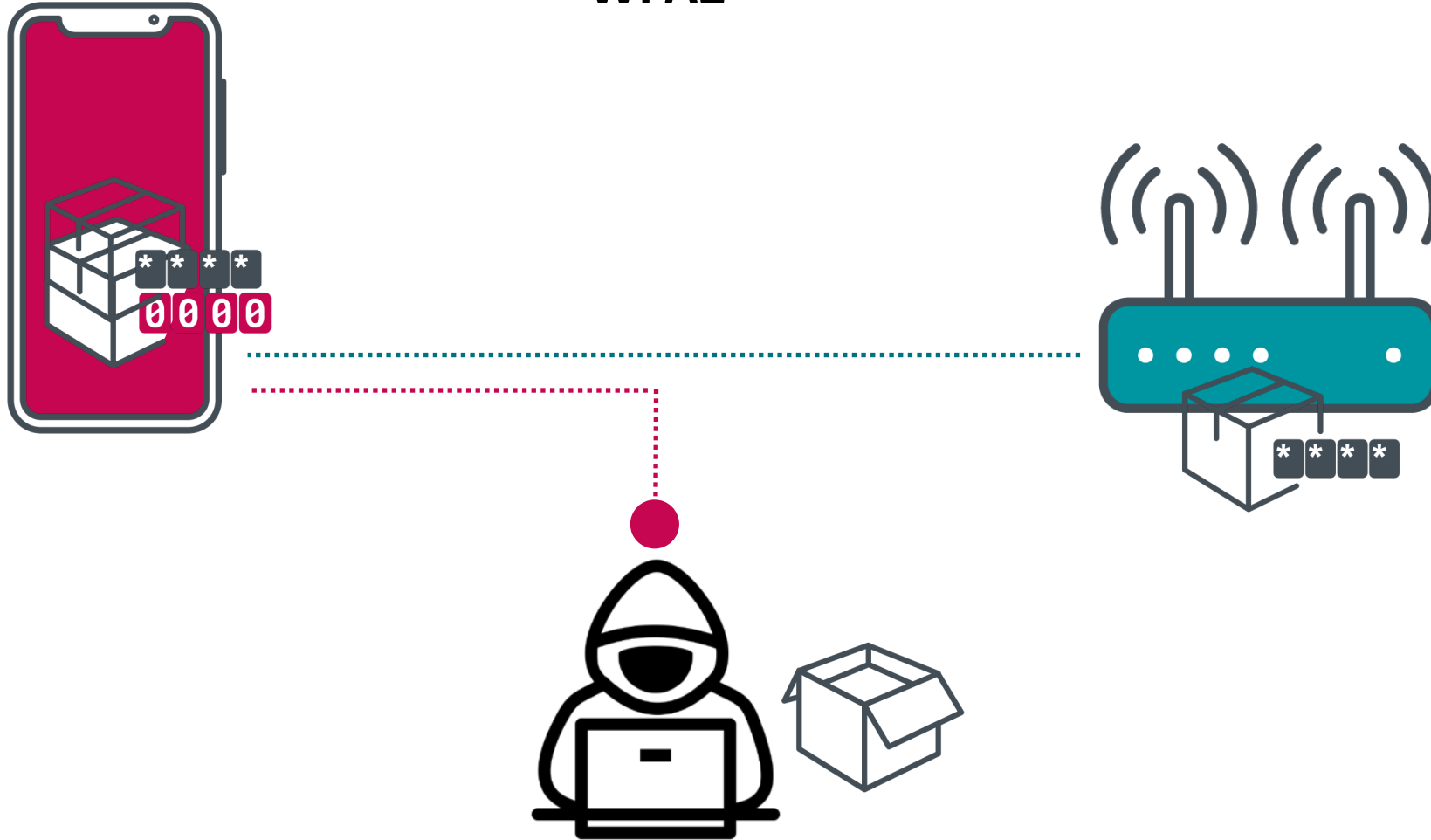
Krøøk

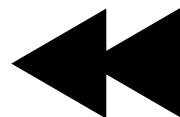
CVE-2019-15126

WPA2



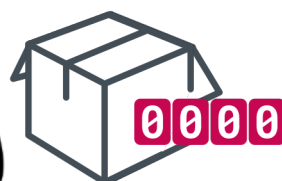
WPA2





Rewind

WPA2



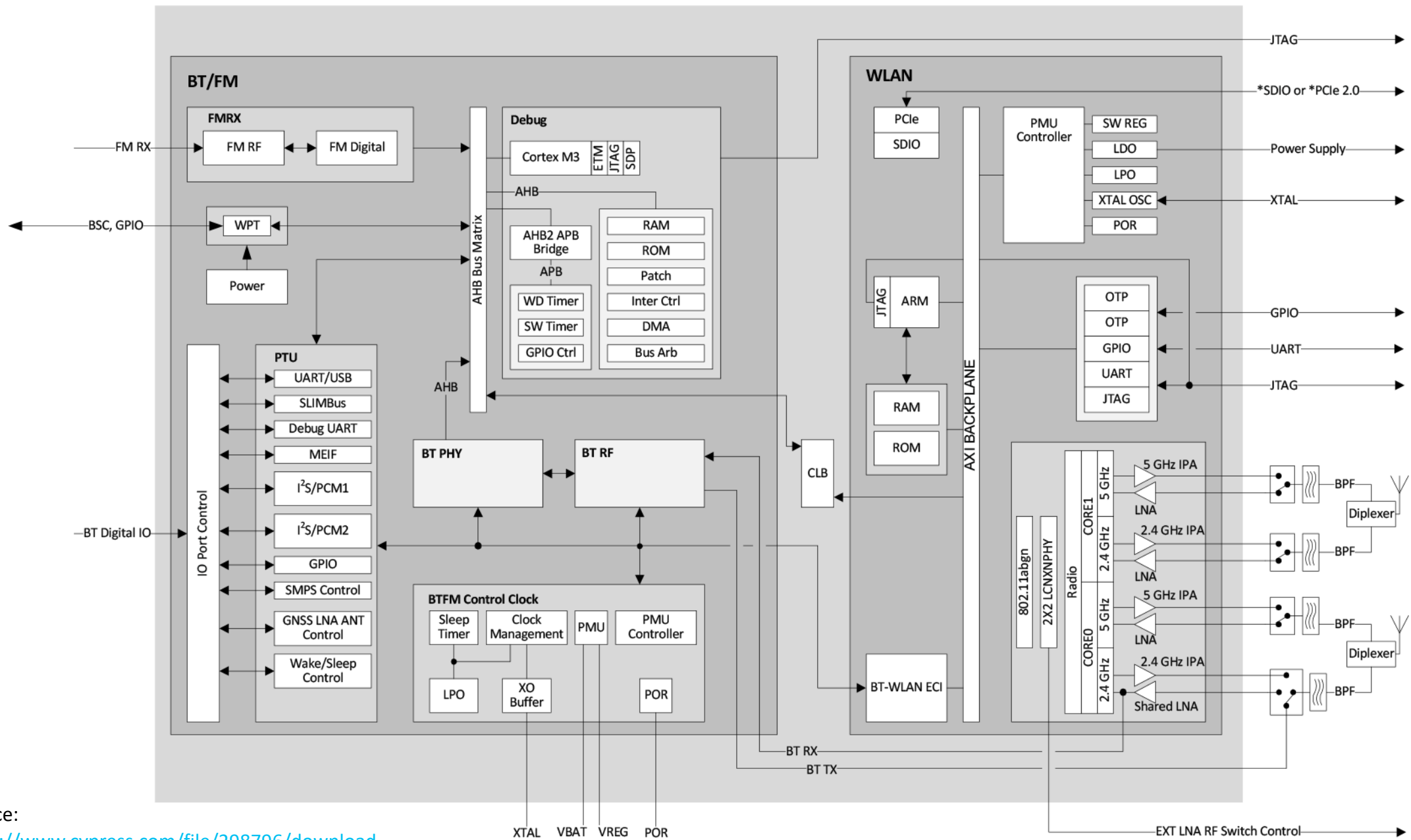




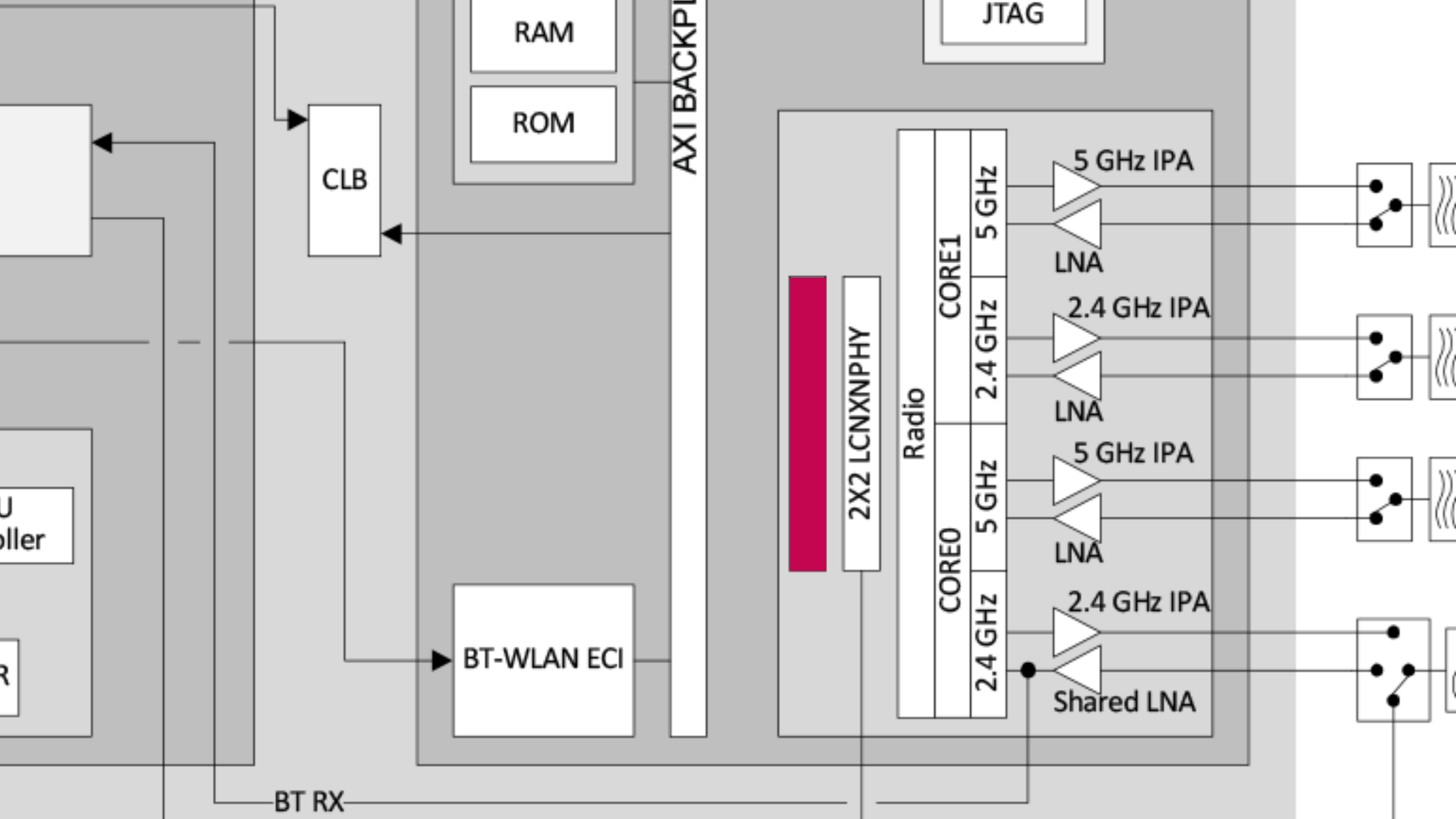
BROADCOM®
BCM4343WKBG
HE1713 P11
614225-16 3E
11-81

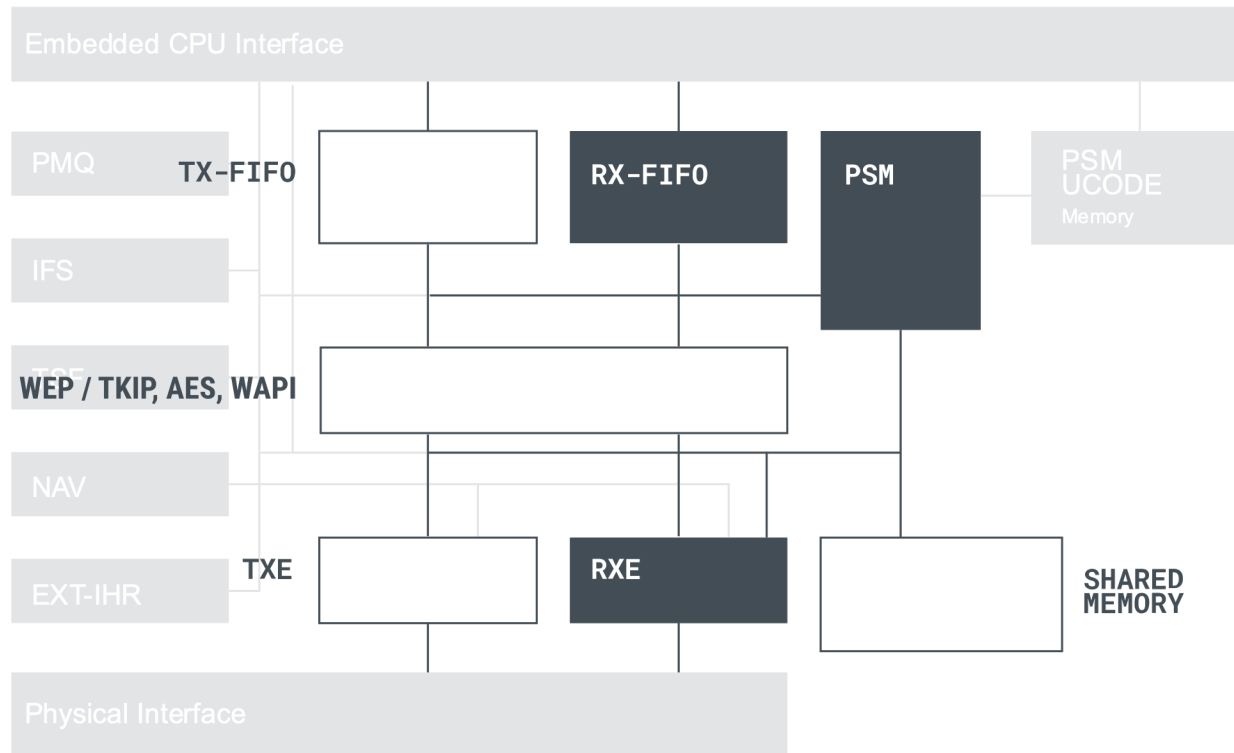
Source:

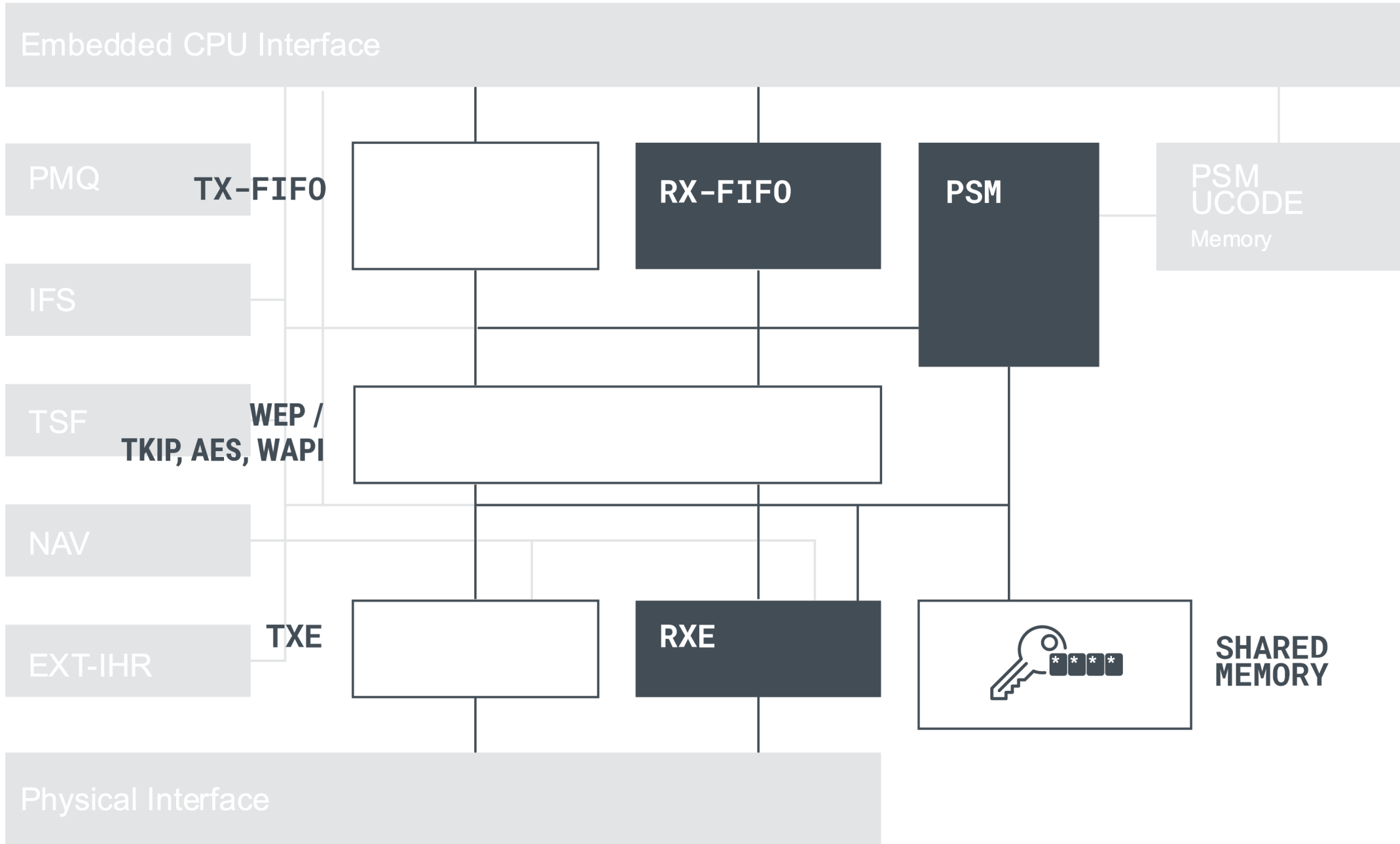
<https://www.cypress.com/file/298796/download>

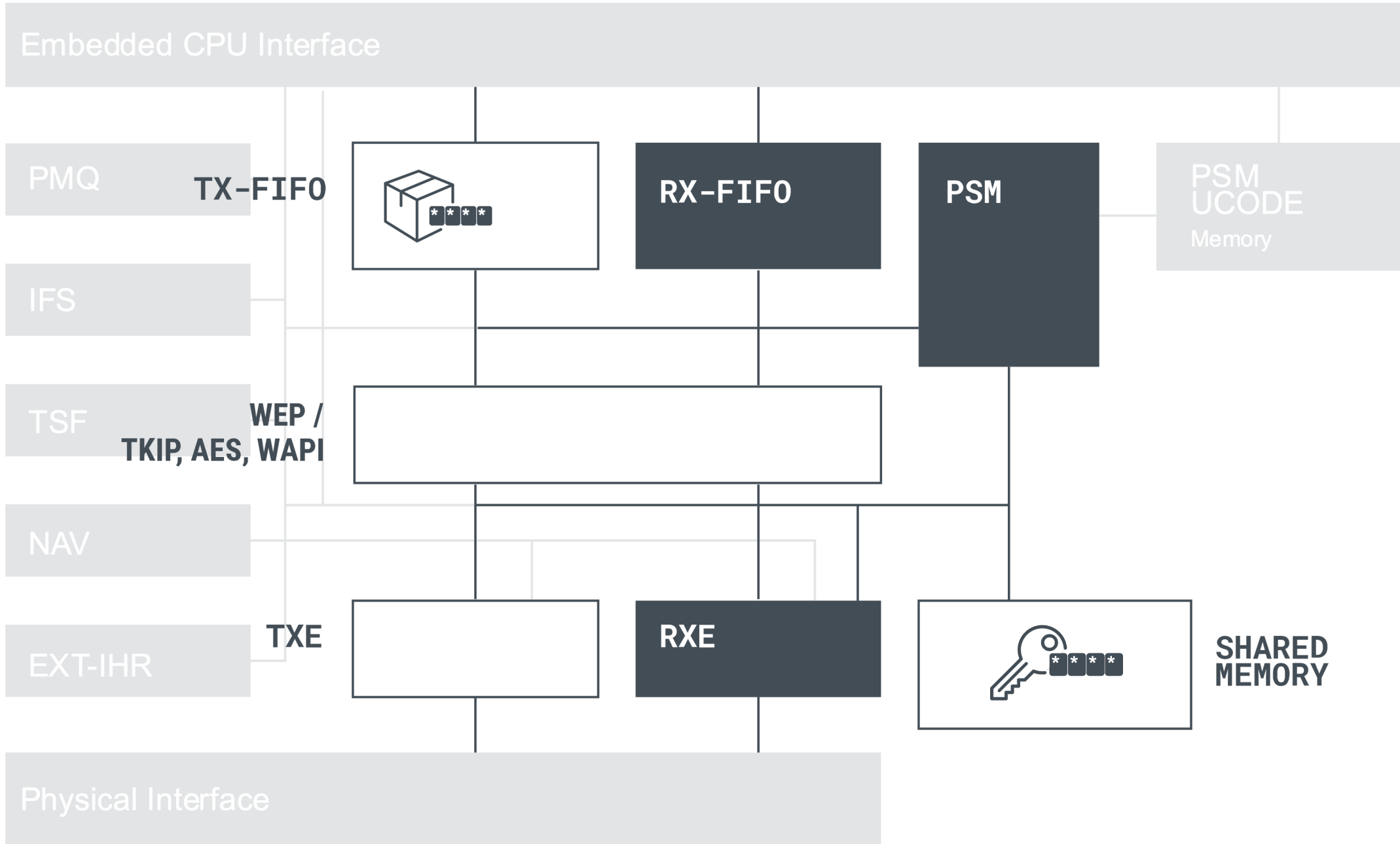


Source: <https://www.cypress.com/file/298796/download>

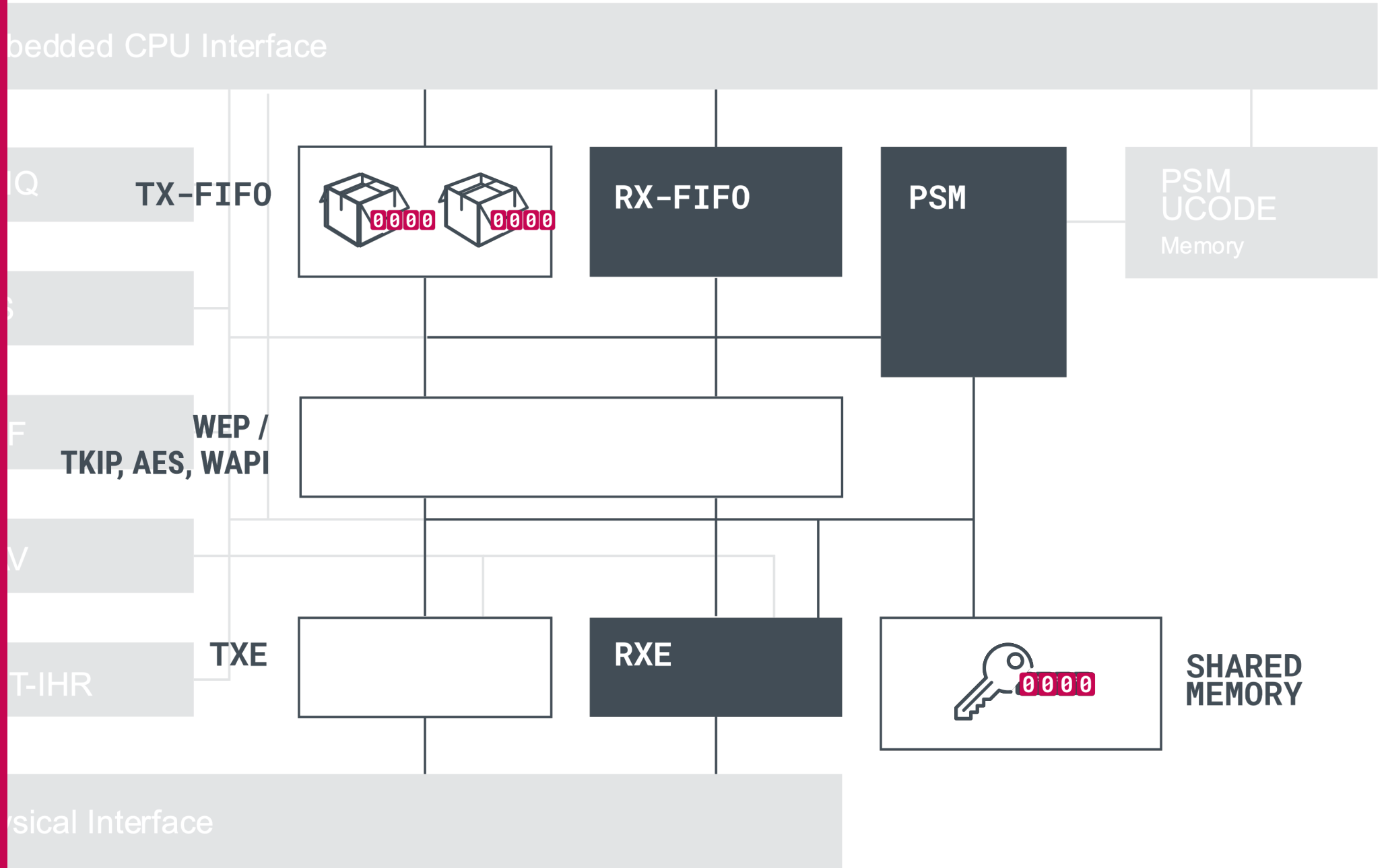




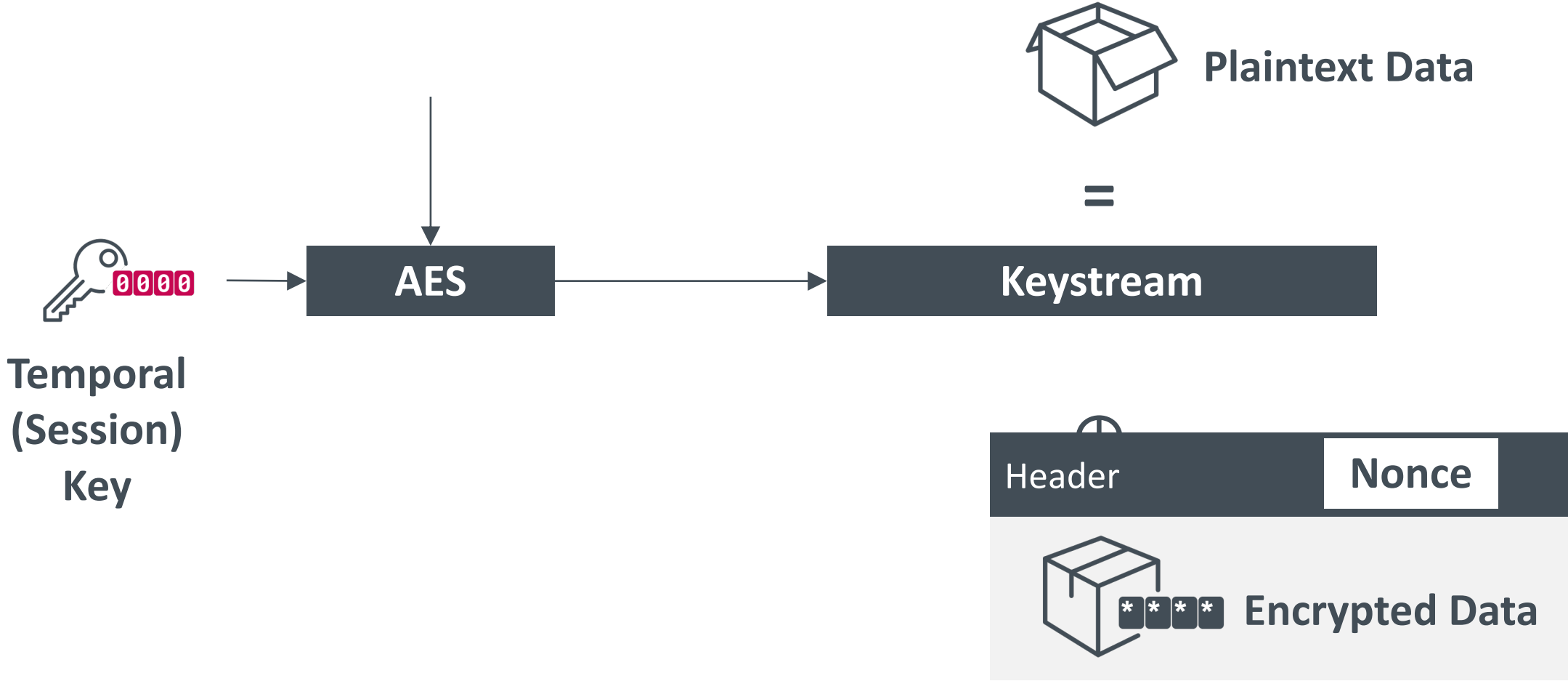




Disassociation



Decryption in WPA2-CCMP



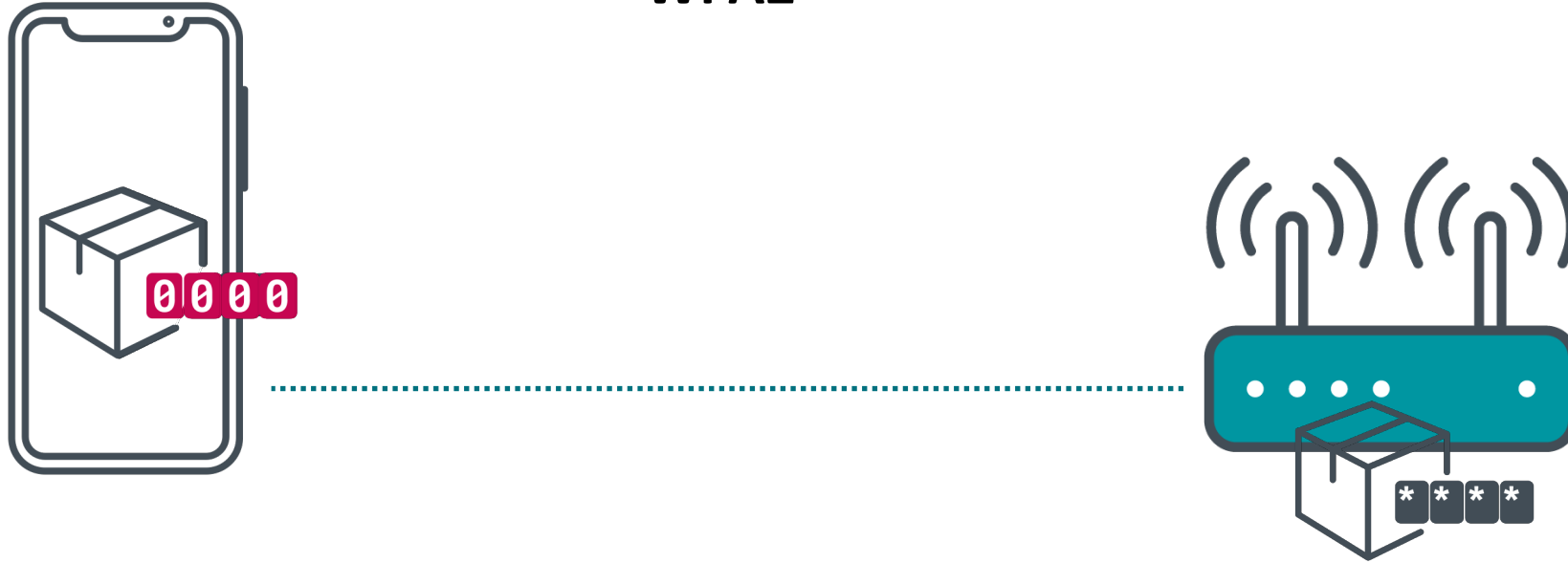
The background is a dark, futuristic digital cityscape. It features various rectangular structures and vertical pillars, all outlined with glowing blue lines that resemble circuit traces or data paths. Some of these structures have a grid-like pattern on their faces. In the lower right area, there are clusters of small, bright blue dots, possibly representing data points or network nodes. The overall color palette is dominated by dark blues and blacks, with the glowing blue lines providing the primary source of light and contrast.

Impact

What can an attacker do with this vulnerability?

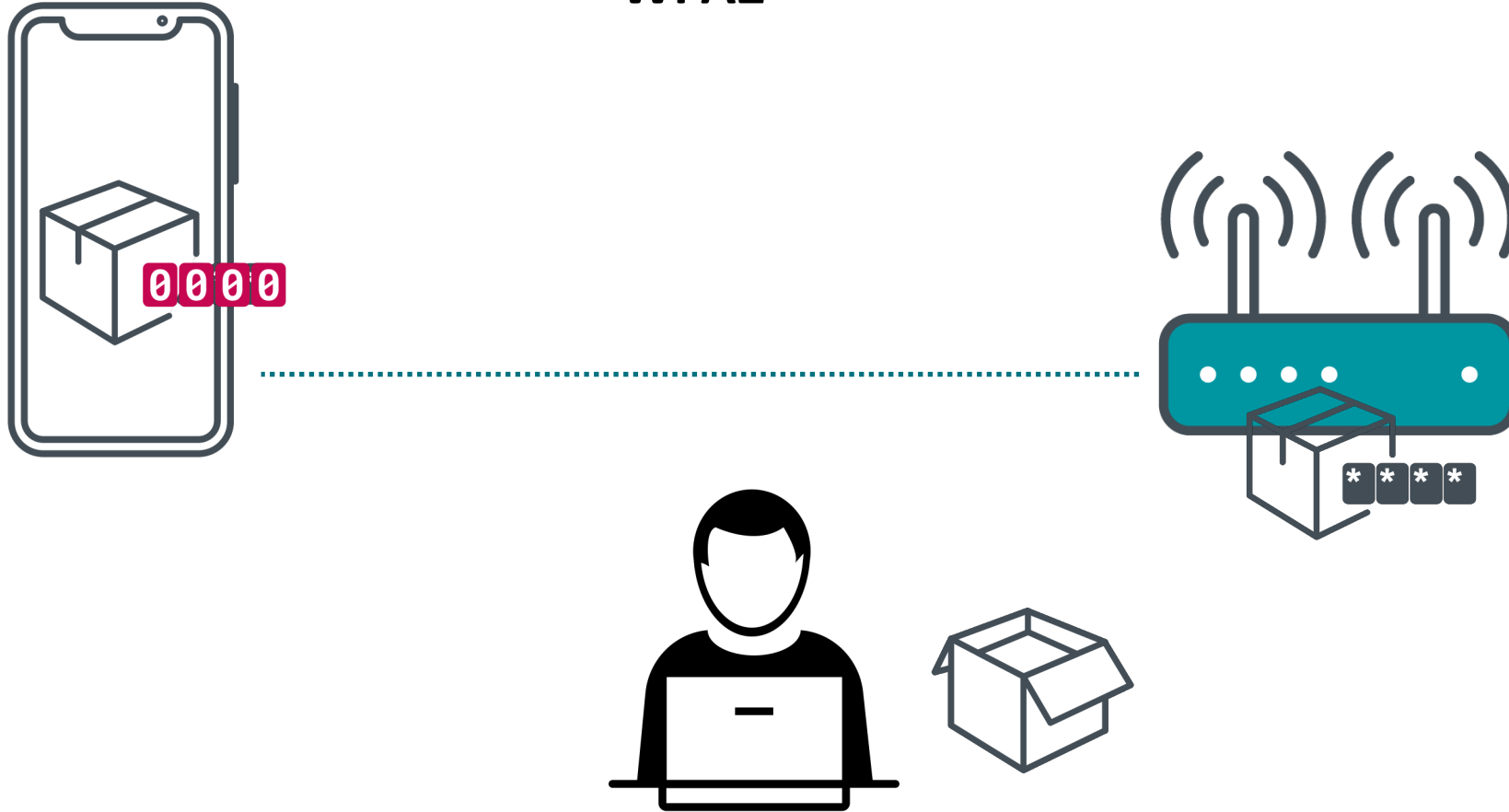
Eavesdropping – Passive

WPA2



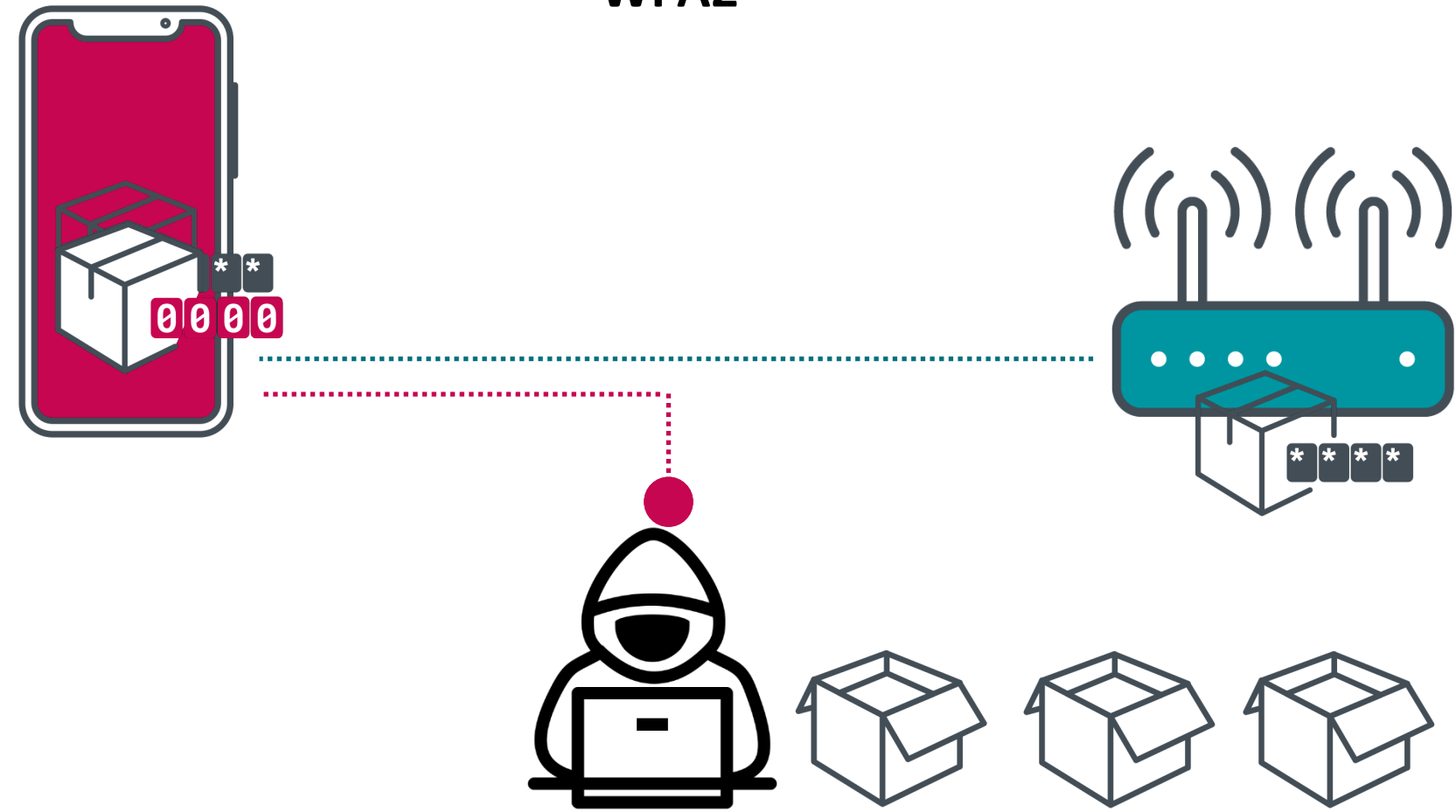
Eavesdropping – Passive

WPA2



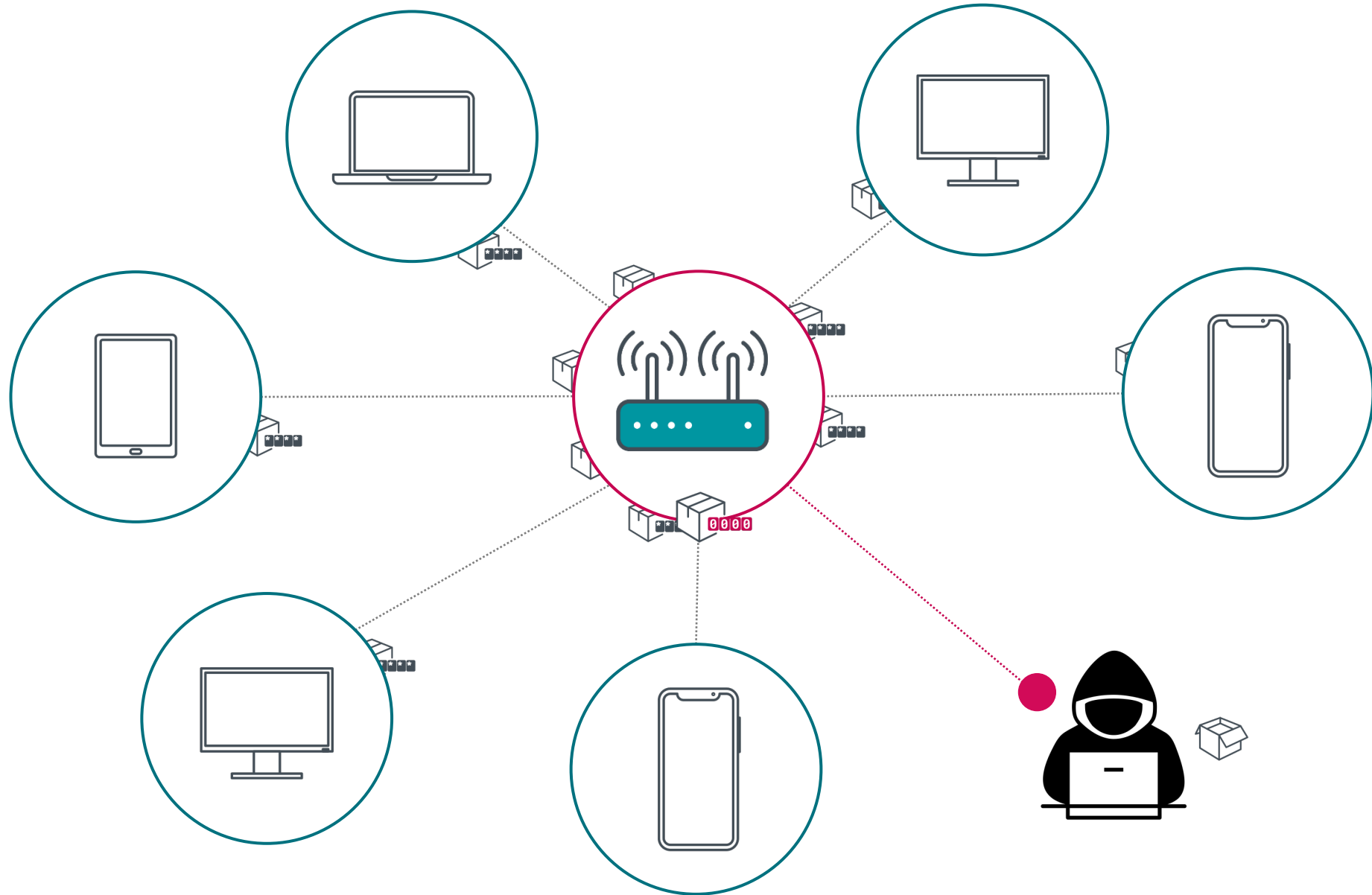
Eavesdropping – Active

WPA2



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

The background is a complex, glowing blue digital environment. It features a perspective view of a grid of small, bright blue lights that recede into the distance. On the left, there are several tall, vertical, rectangular structures with glowing outlines, resembling server racks or data centers. On the right, there are more complex, layered structures with glowing lines and surfaces. The overall atmosphere is one of a high-tech, futuristic digital world.

KRACKing Amazon Echo

How it all started...



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

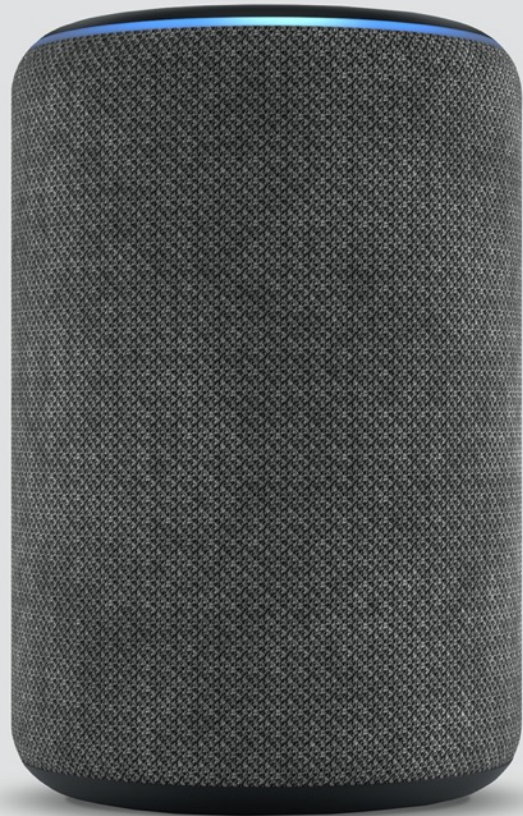
INTRODUCTION

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. KROOK

KRACK

Attack / exploit

Nonce reused to acquire keystream

Triggered during the 4-way handshake

Affects most Wi-Fi capable devices

KROOK

Vulnerability / bug

Data encrypted with all-zero session key

Triggered after a disassociation

Affects the most widespread Wi-Fi chips
(Broadcom & Cypress)

The background is a complex, futuristic digital environment. It features a grid of glowing blue dots on the ground, which recedes into the distance. The scene is filled with various geometric shapes, lines, and structures, all rendered in a glowing blue color. The overall atmosphere is one of high-tech and digital connectivity.

Follow-up research

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
v IEEE 802.11 QoS Data, Flags: .p....F.
  Type/Subtype: QoS Data (0x0028)
  v Frame Control Field: 0x8842
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  v 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
    ...0... = Order flag: Not strictly ordered
    .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
  v CCMP parameters
    CCMP Ext. Initialization Vector: 0x000000000099
  v Data (1204 bytes)
    Data: aaaa030000000800450004a4657717d940017461c0a8017a...
    [Length: 1204]

```

0000	00 00 12 00 2e 48 00 00 00 16 85 09 a0 00 d3 01H.....
0010	00 00 88 42 75 00 84 16 f9 08 8b dd e4 6f 13 ed	...Bu... ..o..
0020	e2 17 e4 6f 13 ed e2 17 70 09 00 00 99 00 00 20	...o... p... ..
0030	00 00 00 00 aa aa 03 00 00 00 08 00 45 00 04 a4E...
0040	65 77 17 d9 40 01 74 61 c0 a8 01 7a c0 a8 01 dd	ew..@.ta ...z....
0050	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
0060	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwabcd efghijkl
0070	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mnoqrst uvwabcde
0080	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu
0090	76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	vwabcdef ghijklmn
00a0	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstuv wabcdefg
00b0	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvwxyz
00c0	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefghijklm nop
00d0	71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69	qrstuvwxyz abcdefghi
00e0	6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62	jklmnopq rstuvwab
00f0	63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72	cdefghij klmnopqr
0100	73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b	stuvwabc defghijk
0110	6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64	lmnopqrs tuvabcd
0120	65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74	efghijkl mnopqrst
0130	75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d	vwabcde fghijklm
0140	6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66	nopqrstu vwabcdef
0150	67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76	ghijklmn opqrstu
0160	77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f	wabcdefg hijklmno
0170	70 71 72 73 74 75 76 77 61 62 63 64 65 66 67 68	pqrstuvwxyz abcdefgh
0180	69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61	ijklmnop qrstuva
0190	62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71	bcdefghi jklmnopq
01a0	72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 6a	rstuvwab cdefghij
01b0	6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63	klmnopqr stuvwabc
01c0	64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73	defghijk lmnopqrs
01d0	74 75 76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c	tuvwabcd efghijkl
01e0	6d 6e 6f 70 71 72 73 74 75 76 77 61 62 63 64 65	mnoqrst uvwabcde
01f0	66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75	fghijklm nopqrstu
0200	76 77 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e	vwabcdef ghijklmn
0210	6f 70 71 72 73 74 75 76 77 61 62 63 64 65 66 67	opqrstu wabcdefg
0220	68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77	hijklmno pqrstuvwxyz
0230	61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70	abcdefghijklmno

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

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
- QoS Control: 0x0000
- WEP parameters
 - Initialization Vector: 0xaaaa03**
 - Key Index: 0
 - 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 01H.....
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 caE... ..\$V@...
0040	c0 a8 00 04 c0 a8 00 01 41 41 41 41 41 41 41 41 AAAAAAAAA
0050	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0060	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0070	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0080	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0090	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00a0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00b0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00c0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00d0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00e0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
00f0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0100	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0110	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0120	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0130	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0140	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0150	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0160	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0170	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0180	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0190	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01a0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01b0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01c0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01d0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01e0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
01f0	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0200	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0210	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0220	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0230	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA
0240	41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41	AAAAAAAA AAAAAAAAA

Initialization Vector (wlan.wep.iv), 3 bytes

Packets: 123 · Displayed: 123 (100.0%) Profile: Default

The background is a dark teal color with a complex digital aesthetic. On the left side, there are several thick, glowing teal lines that curve from the bottom left towards the center. The rest of the background is filled with a fine, grid-like pattern of small, glowing teal dots and lines, creating a sense of depth and data flow. The overall effect is that of a high-tech, futuristic digital environment.

Wrapping up...

Kudos to



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")

Overview
=====

A timing flaw in certain Wi-Fi chip firmware may allow an attacker to inject a limited amount of WPA2-encrypted frames using a known vulnerability. Some Aruba products are affected by this vulnerability.



SAMSUNG
Mobile Security
Security Post



Documentation > Security Alerts > Mist Security Alerts
Mist Security Ad
FAQ



Security Notice - Statement About the Vulnerability Kr00k in Wi-Fi Chips

Initial Release Date: Feb 28, 2020
Last Release Date: May 27, 2020

What is this vulnerability?
Kr00k – formally known as CVE-2019-15126 – is a vulnerability that allows an attacker to perform unauthorized decryption of some WPA2-encrypted frames without proper MAC level authentication.



New Kr00k Vulnerability Lets Attackers
New Kr00k Vulnerability Lets Attackers
Subscribe To LifeGuard Updates
The Kr00k vulnerability potentially affects some ASUS products that use Broadcom or Cypress Wi-Fi chips.

About the security update for iPadOS 13.2

This document describes the security update for iPadOS 13.2.

About Apple security updates

For our customers' protection, Apple regularly releases security updates. An investigation has occurred and patches are available on the [Apple Support](#) page.

CONSUMER BUSINESS SERVICE PROVIDERS SUPPORT



Security
After getting
2019-15126)
has started inv
Huawei

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

ESET Research white papers

TLP: WHITE



KROOK - CVE-2019-15126

SERIOUS
VULNERABILITY
DEEP INSIDE YOUR
WI-FI ENCRYPTION



Authors:

Miloš Čermák, ESET Malware Researcher

Štefan Svorenčík, ESET Head of Experimental Research and Detection

Róbert Lipovský, ESET Senior Malware Researcher

In cooperation with

Ondrej Kubovič, Security Awareness Specialist

February 2020

www.ESET.com/int/Kr00k





CYBERSECURITY
EXPERTS ON YOUR SIDE

Thanks for watching!

@ESETResearch | [WeLiveSecurity.com](https://www.welivesecurity.com)