TLP: WHITE

ENJOY SAFER TECHNOLOGY™

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

CONTENTS

EXECUTIVE SUMMARY 2
INTRODUCTION 3
TECHNICAL BACKGROUND 3
THE Kr00k VULNERABILITY 4
ATTACK VECTORS: EXPLOITING THE VULNERABILITY 5
UNAUTHORIZED READING - DECRYPTION OF DATA 5
AFFECTED DEVICES 6
VULNERABLE ACCESS POINTS 7
HOW KR00K RELATES TO KRACK 7
HOW KRACKING AMAZON ECHO LED TO THE DISCOVERY OF Kr00k 7
COMPARING KRACK AND Kr00k 8
CONCLUSION 8
ACKNOWLEDGEMENTS 9
TIMELINE OF DISCOVERIES AND RESPONSIBLE DISCLOSURE 9

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

EXECUTIVE SUMMARY

ESET researchers discovered a previously unknown vulnerability in Wi-Fi chips and named it Kr00k. This serious flaw, assigned CVE-2019-15126, causes vulnerable devices to use an all-zero encryption key to encrypt part of the user's communication. In a successful attack, this vulnerability allows an adversary to decrypt some wireless network packets transmitted by a vulnerable device.

Kr00k affects devices with Wi-Fi chips by Broadcom and Cypress that haven't yet been patched. These are the most common Wi-Fi chips used in contemporary Wi-Fi-capable devices such as smartphones, tablets, laptops, and IoT gadgets.

Not only client devices but also Wi-Fi access points and routers with Broadcom chips were affected by the vulnerability, thus making many environments with unaffected or already patched client devices vulnerable anyway.

Our tests confirmed that prior to patching, some client devices by Amazon (Echo, Kindle), Apple (iPhone, iPad, MacBook), Google (Nexus), Samsung (Galaxy), Raspberry (Pi 3), Xiaomi (RedMi), as well as some access points by Asus and Huawei, were vulnerable to Kr00k. This totaled to over a billion Wi-Fi-capable devices and access points, at a conservative estimate. Further, many other vendors whose products we did not test also use the affected chipsets in their devices.

The vulnerability affects both WPA2-Personal and WPA2-Enterprise protocols, with AES-CCMP encryption.

Kr00k is related to KRACK (Key Reinstallation Attacks), discovered in 2017 by Mathy Vanhoef, but is also fundamentally different. In the beginning of our research, we found Kr00k to be one of the possible causes behind the "reinstallation" of an all-zero encryption key, observed in tests for KRACK attacks.

We responsibly disclosed the vulnerability to chip manufacturers Broadcom and Cypress, who subsequently released updates during an extended disclosure period. We also worked with the Industry Consortium for Advancement of Security on the Internet (ICASI) to ensure that all potentially affected parties – including affected device manufacturers using the vulnerable chips, as well as any other possibly affected chip manufacturers – were aware of Kr00k.

According to our information, patches for devices by major manufacturers have been released by now. To protect yourself, as a user, make sure you have applied the latest available updates on all your Wi-Fi-capable devices, including phones, tablets, laptops, IoT devices with Wi-Fi, and Wi-Fi access points and routers. As a device manufacturer, please inquire about patches for the Kr00k vulnerability directly with your chip manufacturer.

INTRODUCTION

This white paper introduces Kr00k – a serious vulnerability in Wi-Fi chips, formally known as CVE-2019-15126.

It details the mechanics of the vulnerability, the culprits behind it and demonstrates some of the possible ways in which Kr00k can be exploited by adversaries. In the Conclusion section, we cover the state of patching and ways in which organizations and users should address the issue.

We also provide the backstory that led ESET researchers to their findings, as well as detail the complex disclosure process that was necessary to fix a flaw hidden deep down in over a billion devices that form the Internet of Things.

But before we get into the Kr00k vulnerability, we provide a simplified introduction to WPA2 security. This information is a necessary pre-requisite to understand how and why Kr00k arose.

TECHNICAL BACKGROUND

This section provides basic explanations of selected key terms, needed to understand the rest of the paper.

Our research focuses on *WPA2* with *CCMP* used as the data confidentiality and integrity protocol. This is the most ubiquitous standard used in contemporary Wi-Fi networks.

Whenever a client device establishes a connection with an access point, the initial stage is called an association. For our purposes, the reverse – a **disassociation** – and the combination of the two – a reassociation – are most relevant. Disassociations and reassociations occur for a number of reasons:

for example, when a client roams from one Wi-Fi access point to another, due to signal interference, or simply when a user turns off Wi-Fi on their device.

Associations and disassociations are governed by *management frames*. The important thing to note here is that these are unauthenticated and unencrypted – hence, an attacker can forge a management frame to manually trigger a disassociation, which will be processed by the targeted device.

With WPA2, secure communication is established by the *4-way handshake*. It ensures mutual authentication of the client and the access point (for example, by confirming that they both know the Pre-Shared Key (PSK) aka the Wi-Fi access password). During the 4-way handshake, the client and access point also construct and install cryptographic keys for data confidentiality and integrity. One of the keys that is negotiated is the PTK (Pairwise Transient Key), which itself is split into different keys serving different purposes. The one which is most relevant for our discussion of Kr00k is the 128-bit **TK (Temporal Key)**, which is used to encrypt unicast data frames transmitted during the client-AP session. In the text, we'll be using the terms TK and "session key" interchangeably.

THE Kr00k VULNERABILITY

Figure 1 provides a schematic overview of the bug at the chip level. While we do not have detailed visibility into the inner workings of the affected chips, we believe the schematic (based on the *CYW4356 chip specification*) captures the cause and basic idea of the vulnerability.

Kr00k manifests itself after a disassociation. Once a station's WLAN session gets disassociated (1), the session key (TK) stored in the Wireless Network Interface Controller's (WNIC) Wi-Fi chip is cleared in memory – set to zero (2). This is expected behavior, as no further data is supposed to be transmitted after the disassociation.

However, we discovered that all data frames that were left in the chip's Tx (transmit) buffer were transmitted (4) after being encrypted with this all-zero key (3).

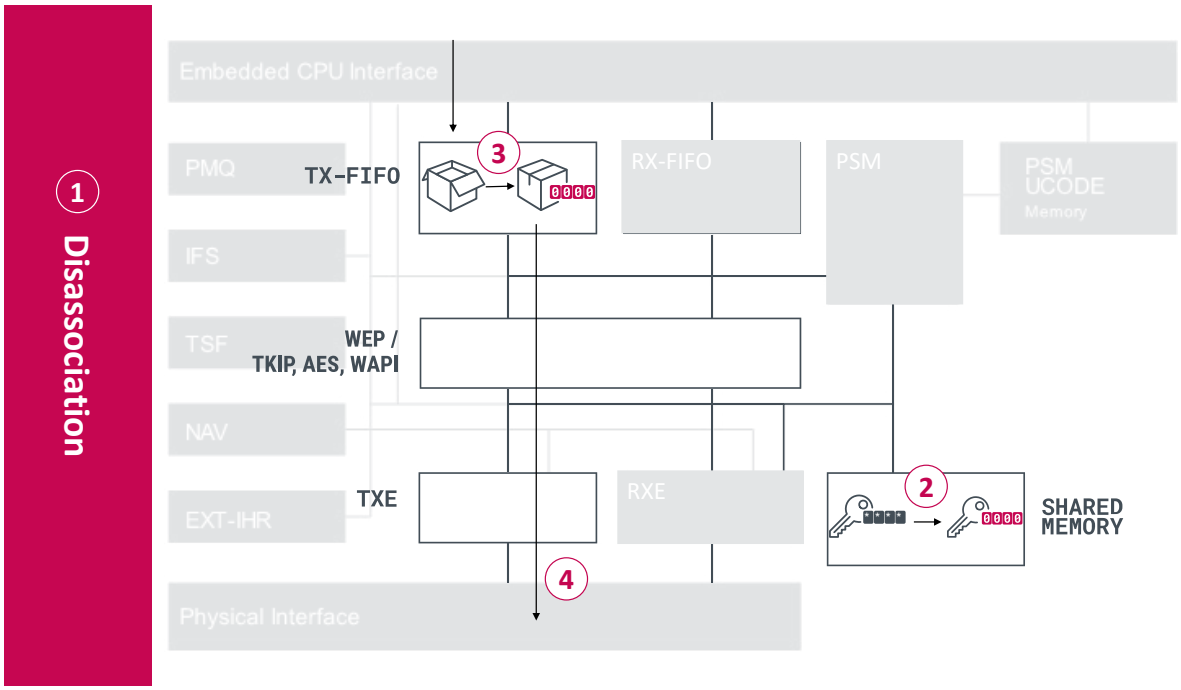


Figure 1 // Kr00k causes transmission of data encrypted with an all-zero key

ATTACK VECTORS: EXPLOITING THE VULNERABILITY

Since Kr00k (encryption with an all-zero TK) manifests itself following a disassociation, an adversary can exploit this by manually triggering disassociations – as opposed to the disassociations that occur naturally.

This is possible, because a disassociation can be triggered by a management data frame that's unauthenticated and unencrypted. There are possibly even other methods or events that can cause a disassociation (e.g. transmitting malcrafted packets, *EAPOLs*, etc.) – and/or to trigger Kr00k.

Unauthorized reading - decryption of data

As explained in the previous section, after a disassociation occurs, data from the chip's Tx buffer will be transmitted encrypted with the all-zero TK. These data frames can be captured by an adversary and subsequently decrypted. This data can contain several kilobytes of potentially sensitive information.

This is possible even if the attacker is not connected (authenticated and associated) to the WLAN (e.g. doesn't know the PSK) – by using a WNIC in *monitor mode* – which is what would make Kr00k advantageous for the attackers, compared to some other attack techniques used against Wi-Fi security.

By repeatedly triggering disassociations (effectively causing reassociations, as the session will usually reconnect), the attacker can capture more data frames.

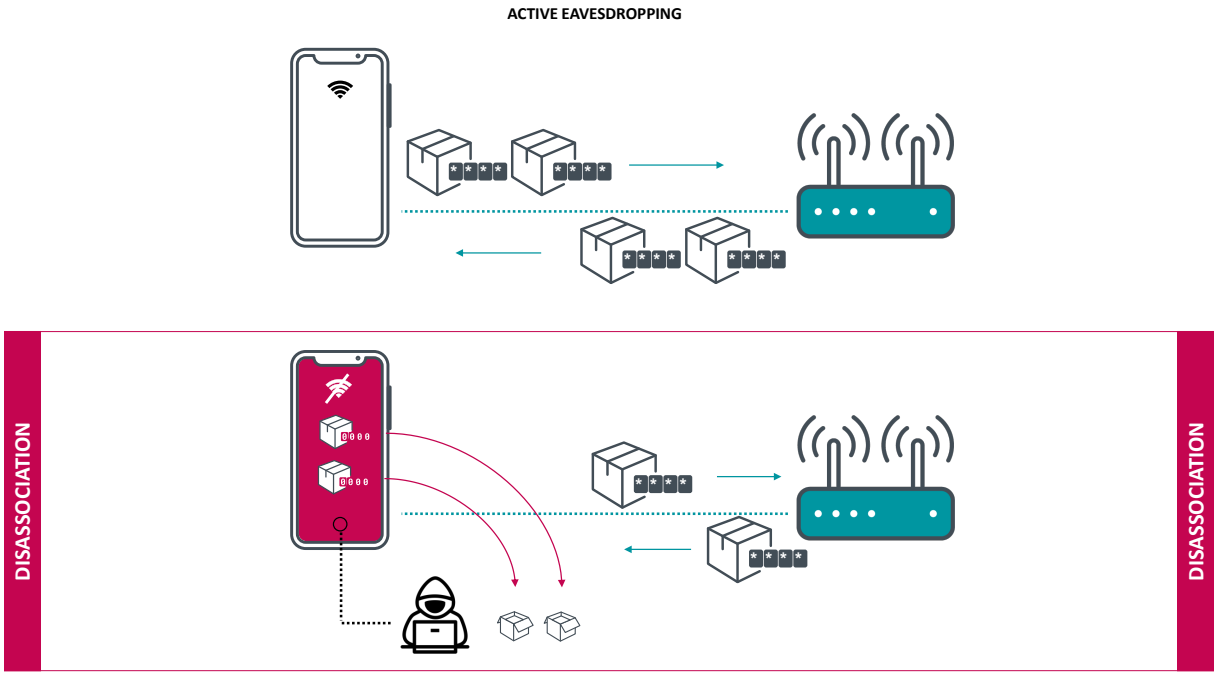
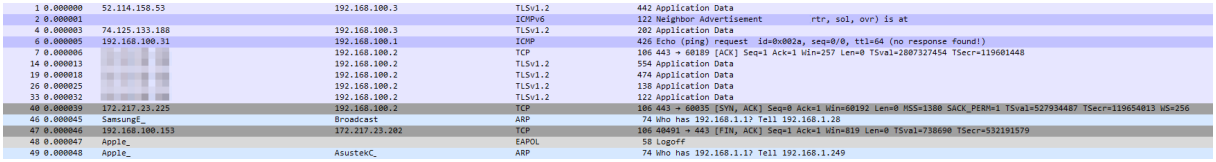


Figure 2 // An active attacker can trigger disassociations to capture and decrypt data

As a result, the adversary can capture more network packets containing potentially sensitive data, including DNS, ARP, ICMP, HTTP, TCP, and TLS packets – similar to what they would see on an open WLAN network without WPA2. (Of course, TLS provides another layer of encryption, which is not affected by this attack.)



1	0.000000	52.114.158.53	192.168.100.3	TLSv1.2	442 Application Data
2	0.000001			ICMPv6	122 Neighbor Advertisement rtr, sol, ovr) is at
4	0.000003	74.125.133.188	192.168.100.3	TLSv1.2	202 Application Data
6	0.000005	192.168.100.31	192.168.100.1	ICMP	426 Echo (ping) request id=0x002a, seq=0/0, ttl=64 (no response found!)
7	0.000006		192.168.100.2	TCP	106 443 → 60189 [ACK] Seq=1 Ack=1 Win=257 Len=0 TSval=2807327454 TSecr=119601448
14	0.000013		192.168.100.2	TLSv1.2	554 Application Data
19	0.000018		192.168.100.2	TLSv1.2	474 Application Data
26	0.000025		192.168.100.2	TLSv1.2	138 Application Data
33	0.000032		192.168.100.2	TLSv1.2	122 Application Data
40	0.000039	172.217.23.225	192.168.100.2	TCP	106 443 → 60035 [SYN, ACK] Seq=0 Ack=1 Win=60192 Len=0 MSS=1380 SACK_PERM=1 TSval=527934487 TSecr=119654013 WS=256
46	0.000045	Samsungf_	Broadcast	ARP	74 Who has 192.168.1.1? Tell 192.168.1.28
47	0.000046	192.168.100.153	172.217.23.202	TCP	106 40491 → 443 [FIN, ACK] Seq=1 Ack=1 Win=819 Len=0 TSval=738690 TSecr=532191579
48	0.000047	Apple_		EAPOL	58 Logoff
49	0.000048	Apple_	AsustekC_	ARP	74 Who has 192.168.1.1? Tell 192.168.1.249

Figure 3 // Example of captured WLAN traffic that was divulged due to the Kr00k vulnerability

AFFECTED DEVICES

The vulnerability primarily affects FullMAC WLAN chips manufactured by Broadcom and Cypress. These chip manufacturers have a high market share – it is safe to say that Broadcom chips are used by the majority of today's Wi-Fi capable devices. Cypress chips are widely used in IoT devices.

The client devices that we positively tested in our lab to be vulnerable to Kr00k include:

- Amazon Echo 2nd gen
- Amazon Kindle 8th gen
- Apple iPad mini 2
- Apple iPhone 6, 6S, 8, XR
- Apple MacBook Air Retina 13-inch 2018
- Google Nexus 5
- Google Nexus 6
- Google Nexus 6S
- Raspberry Pi 3
- Samsung Galaxy S4 GT-I9505
- Samsung Galaxy S8
- Xiaomi Redmi 3S

We estimate that the number of affected devices, prior to patching, was well over a billion as the billion mark is passed by counting only the number of affected iPhone generations we tested.

We have also tested some devices with Wi-Fi chips from other manufacturers, including Qualcomm, Realtek, Ralink, Mediatek and did not see the vulnerability manifest itself. Obviously, we have not tested every possible Wi-Fi chip by every manufacturer, so while we are currently not aware of other affected chips, we also cannot rule this out.

Vulnerable access points

Of great concern is that not only client devices but also Wi-Fi access points and routers are affected by Kr00k.

This results in scenarios where client devices that are unaffected (either patched or using different Wi-Fi chips not vulnerable to Kr00k) can be connected to an access point (often times beyond an individual's control) that is vulnerable. The attack surface is greatly increased, since an adversary can decrypt data that was transmitted by a vulnerable access point to a specific client (which may or may not be vulnerable itself).

In our lab, we were able to confirm that some wireless routers by ASUS and Huawei were vulnerable in this way. Specifically, we positively tested:

- Asus RT-N12
- Huawei B612S-25d
- Huawei EchoLife HG8245H
- Huawei E5577Cs-321

HOW Kr00k RELATES TO KRACK

Our discovery of the chipset-level Kr00k vulnerability follows our previous research known as KRACK (Key Reinstallation Attacks). This section provides the background story behind our research, as well as a comparison of Kr00k and KRACK, as the two are related but also fundamentally different.

KRACK attacks revealed serious weaknesses in the WPA2 protocol – these were alarming discoveries by Mathy Vanhoef in 2017. The plural in KRACK is important: there were a number of variants of the attacks, and a number of CVEs were assigned to cover these.

In the worst case scenarios, KRACK attacks can result in the setting of an all-zero TK under a number of different circumstances, as is explained in Vanhoef's *paper*.

How KRACKing Amazon Echo led to the discovery of Kr00k

Even two years after KRACK received widespread attention, not all devices were fully patched. For example, ESET's IoT research team discovered that *the first generation Amazon Echo was vulnerable to KRACK*. Following our responsible disclosure, Amazon promptly issued a patch.

More importantly, though, we later found that while the second generation Amazon Echo was not affected by the original KRACK attacks, it was vulnerable to one of the KRACK variants, specifically: *PTK reinstallation in 4-way handshake when STA uses Temporal PTK construction, random ANonce*.

We also reported this flaw to Amazon and – following a number of productive calls with their security team – discovered that the culprit was actually the Cypress WLAN chip used in the second generation Echo. It was vulnerable to the bug we later named Kr00k, and we believe that the KRACK testing scripts revealed it by triggering a disassociation.

It should be noted that encryption with an all-zero TK can have number of causes – Kr00k is just one of them, although a very significant one, due to the widespread distribution of the vulnerable Broadcom and Cypress chips.

Comparing KRACK and Kr00k

As explained above, KRACK and Kr00k are related. Further, both enable unauthorized decryption of data.

Kr00k is one of the possible reasons behind the "reinstallation" of an all-zero TK, which has been observed while testing for KRACK attacks.

A few key differences between the two are highlighted in Table 1.

KRACK	Kr00k
KRACK, as the expanded acronym suggests, is a series of attacks – exploits	Kr00k, on the other hand, is a vulnerability – bug
The basic idea behind KRACK is that the Nonce is reused to acquire the keystream	The main idea behind Kr00k is that data is encrypted with an all-zero session key (TK)
Triggered during the 4-way handshake	Triggered after a disassociation
Affects most Wi-Fi capable devices, as it exploits implementation flaws in the WPA2 protocol itself	Affects the most widespread Wi-Fi chips (by Broadcom & Cypress)

Table 1 // Comparing KRACK and Kr00k

CONCLUSION

Kr00k – CVE-2019-15126 is a vulnerability that affected billions of devices, potentially causing the leak of sensitive data and opening a new attack vector for blackhats.

Following the discovery of the vulnerability, ESET responsibly disclosed it to the affected chip manufacturers Broadcom and Cypress (and, initially, to Amazon). We also contacted ICASI to ensure that the vulnerability would be disclosed to other (possibly) affected parties – device manufacturers using the vulnerable chips and other chip manufacturers.

While the source of the bug lies in the Wi-Fi chips, fortunately, it can be mitigated through software or firmware updates.

According to some vendor publications and our own (non-comprehensive) tests, devices should have received patches for the vulnerability by the time of publication. Depending on the device type, this might only mean ensuring the latest OS or software updates are installed (Android, Apple and Windows devices; some IoT devices), but may require a firmware update (access points, routers and some IoT devices).

Thus, users and organizations should update devices with Broadcom or Cypress chips to the latest software versions. This includes both client devices, as well as access points. Manufacturers using Broadcom or Cypress chips should check with those vendors that their devices have been patched.

ACKNOWLEDGEMENTS

Special thanks to our colleagues Juraj Bartko and Martin Kaluznik, who greatly contributed to this research.

We'd also like to extend a hat-tip to Mathy Vanhoef for his great research on KRACK that led us to our discoveries.

Lastly, we'd like to commend Amazon, Broadcom, and Cypress for their good cooperation on dealing with the reported issues and ICASI for their assistance in informing as many of the impacted vendors as possible.

We are publishing Broadcom's official statement regarding our disclosure:

"Broadcom appreciates the good work ESET did in identifying potential vulnerabilities in some wireless local area network (WLAN) devices. By working through a responsible disclosure process, Broadcom was notified and was able to take appropriate measures to ensure end-users are protected."

TIMELINE OF DISCOVERIES AND RESPONSIBLE DISCLOSURE

Q3 2018	ESET Research started testing Amazon Echo and Amazon Kindle for vulnerabilities.
Jan 9, 2019	ESET Research reported to Amazon the vulnerability that later turned out to be Kr00k.
Jan 12, 2019	Amazon's security team confirmed it had replicated the reported issues and requested further consultation.
H1 2019	ESET Research continued investigating for the source of the vulnerability.
Jul 18, 2019	ESET Research identified FullMAC Wi-Fi chip by Cypress as a source of the Kr00k vulnerability and contacted the chip manufacturer.
July 20, 2019	Cypress's security team confirmed it had replicated the Kr00k vulnerability
Aug 14, 2019	ESET Research identified that the vulnerability affects not only IoT devices (with Cypress Wi-Fi chips) but also devices with Broadcom chips. Broadcom was contacted.
Aug 16, 2019	Broadcom's security team confirmed the reported vulnerability. They requested an extended grace period (90 to 120 days) to create and publish patches for the vulnerability, which was granted.
Aug 17, 2019	Kr00k has been assigned CVE-2019-15126.
Q4 2019 – Q1 2020	Patches for Kr00k released to manufacturers that use affected Broadcom and Cypress Wi-Fi chips in their devices.
Jan 16, 2020	Kr00k vulnerability reported to ICASI as part of a broader disclosure.
Feb 26, 2020	ESET discloses Kr00k vulnerability to the public.

Table 2 // Timeline of discoveries and ESET's responsible disclosure

ABOUT ESET

For 30 years, *ESET®* has been developing industry-leading IT security software and services for businesses and consumers worldwide. With solutions ranging from endpoint and mobile security, to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give consumers and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn *100 Virus Bulletin VB100* awards, identifying every single "in-the-wild" malware without interruption since 2003. For more information, visit www.eset.com or follow us on *LinkedIn*, *Facebook* and *Twitter*.

ENJOY SAFER TECHNOLOGY™