KRACK and the Ethics of Disclosure

Adon Shapiro

December 13, 2017

Abstract

Vulnerabilities and exploits in software are discovered every day. This is a well-known fact in the cyber-security industry. What is not so universally agreed-upon is the proper way for an ethical hacker or security researcher to disclose a vulnerability they have discovered, and the argument re-surfaces with the disclosure of each new high-profile bug. The most recent such bug is KRACK. In October 2017, researchers at the University of Leuven published details of a vulnerability they had discovered in the WPA2 protocol that secures Wi-Fi connections. They called it KRACK (Key Reinstallation AttaCK) because of the way it takes advantage of a bug in WPA2 that allows the re-use of insecure cryptographic keys. KRACK is significant because it is a fundamental weakness not in a specific piece of software, but rather in the Wi-Fi standard itself, and so everyone who uses Wi-Fi was susceptible to the attack. Because of its recentness and its far-reaching impact, KRACK is a perfect lens through which to view the problem of ethical disclosure.

Introduction

Disclosure, as it pertains to cyber-security, refers to the manner in which people are made aware of vulnerabilities in their software. This can mean many different things, however. To formalize different approaches to disclosure, it is helpful to define three roles in the process: Vendors, Customers, and Reporters.[1] As defined by Christey and Wysopal, a Vendor is "an individual or organization who provides, develops, or maintains software, hardware, or services, possibly for free." A customer is an "end user of the software, hardware, or service that may be affected by the vulnerability," and a Reporter is an "individual or organization that informs (or attempts to inform) the Vendor of the vulnerability."[1] The crux of the debate is how different approaches to disclosure affect Customers. The "different methods" refer to the actions and reactions of Reporters and Vendors. At the extreme ends of the disclosure spectrum we have full disclosure and full secrecy. Full disclosure is when a Reporter makes their discovery completely public with little to no consideration given to the consequences of publicizing an exploit. The reasoning behind this method is generally that the best way to fix a vulnerability is to have it be as noticeable as possible, and that the consequences of malicious individuals learning of the attack are negligible. Full secrecy is when a Reporter alerts a Vendor, but neither Reporter nor Vendor alert the public, sometimes even after the vulnerability has been taken care of. The rationale being that Customers will be safest if the exploit is kept completely secret. Keeping software vulnerabilities secret, the argument goes, keeps them out of the hands of the hackers.[2] Of course, these are both extremes and in reality, most vulnerabilities are disclosed in a manner somewhere between these two approaches. Most people try to identify a happy medium that they call "responsible disclosure," but what this actually means is also a matter of contention.

KRACK is an inherent weakness in the WPA2 protocol that secures protected Wi-Fi networks. Essentially, the vulnerability allows an attacker to authenticate themselves by

[1] Christey & Wysopal
[2] schneier

forcing the network to reinstall an already in-use cryptographic key (thus the name KRACK, for Key Reinstallation AttaCK). The exploit was discovered by Belgian researchers Mathy Vanhoef and Frank Piessens at KU Leuven in 2016 and published a paper with the results of their findings in October 2017, however some affected vendors were notified earlier than this.[3] On the spectrum of disclosure, this is what most people would label responsible disclosure with perhaps a bit of a bent towards full disclosure. Though some vendors were alerted before the bug was fully disclosed, ultimately the vulnerability was made fully known to the public, and vendor's soon realized patches to their implementations of WPA2.

To the Community

So far, it may seem that KRACK is unremarkable. It was discovered by academic researchers, disclosed in a relatively uncontroversial manner, and quickly patched. But it is easy to overlook the severity of the exploit. For one thing, almost anyone who uses the internet is susceptible to it. WPA2 is the standard for secure wireless access and is relied upon for protecting almost every modern Wi-Fi network. It is also such a recently disclosed bug that many people are likely still susceptible to the attack if their vendor has not yet patched their WPA2 implementation or even if the customer fails to keep their system regularly up-to-date.

In terms of disclosure, KRACK's fresh discovery allows to view the ramifications of its disclosure in real time, and its academic source gives it an unusual amount of legitimacy. All told, it is a new and interesting opportunity to gain new perspective on the old debate.

Technical Details of the Exploit

Since KRACK is a fundamental vulnerability in the WPA2 protocol, some understanding of the protocol is necessary to understand the specifics of KRACK. Wi-Fi Protected Access II (WPA2) is the name given to implementations of the standard outlined in IEEE 802.11i-

[3] bleepingcomputer

2004. The standard augments a Robust Security Network (RSN) with the addition of a four-way Handshake and a Group Key Handshake. First a user must provide a pre-shared keyy for initial authentication (the Wi-Fi password). A secret Pairwise Master Key (PMK) is then generated for the session. Next, the four-way handshake verifies that both the access point and the client have the proper PMK without needing to disclose the key. Once this is established, two more keys are generated: the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK).[4]

KRACK exploits a vulnerability in the four-way handshake process of the protocol. An attacker can intercepts the encrypted traffic of the handshake and need only resend the third handshake to reset the WPA2 encryption key. Every time the key is reset the data sent over the network will be encrypted with the same values, allowing traffic to be gradually decrypted until the entire key is decrypted and the network no longer secure. [5] The attack is particularly devastating against wpa_supplicant, the open-source Wi-Fi client typically used on Linux operating systems. This implementation, which is also found in many Android phones, allows the attacker to simply install an all-zero encryption key with no need at all for the real key.

Defense

Unfortunately, without a patched implementation of WPA2, there is no way to defend against a KRACK attack. Fortunately, many vendors have released patches that completely fix the issue. Mathy Vanhoef, the researcher who discovered the vulnerability provides scripts to test your machine for the vulnerabiliy.

[4] IEEE802.11i

[5] krackattacks

Disclosure as it Pertains to KRACK

I said earlier that most people would consider Vanhoef's disclosure "responsible." Let us now define what responsible disclosure entails. As defined by Christey & Wysopal, responsible disclosure aims to:

1. Ensure that vulnerabilities can be identified and eliminated effectively and efficiently for all parties.
2. Minimize the risk to customers from vulnerabilities that could allow damage to their systems.
3. Provide customers with sufficient information for them to evaluate the level of security in vendors' products.
4. Provide the security community with the information necessary to develop tools and methods for identifying, managing, and reducing the risks of vulnerabilities in information technology.
5. Minimize the amount of time and resources required to manage vulnerability information.
6. Facilitate long-term research and development of techniques, products, and processes for avoiding or mitigating vulnerabilities.

KRACK seems to follow this model by first notifying vendors, etc. following Christey & Wysopal's process outline for responsible disclosure. C & W also outline the responsibilities of the reporter.

KRACK is somewhat unique in that it is a product of academic research, but is otherwise unremarkable in terms of its disclosure. Most would agree that it was disclosed in a "responsible" manner. Vendors were alerted first and then customers later. So what can we learn from this? First of all, it is worth mentioning that despite its severity, the overall impact of KRACK has been low. There have been no documented, high-profile cases of serious data being compromised by a KRACK attack and many vendors (google) took almost a whole month to roll out patches.

use other examples to explain how krack was minimal.

KRACK was disclosed “responsibly,” but what good did it really do. Vendors were notified months before the paper was published, but in many cases patches were not released until a month after the disclosure date, and some products still have yet to be patched. Bruce Schneier.

Essentially, the “responsible” aspects of KRACK’s disclosure did nothing to mitigate its effect and its impact was minimal after full disclosure despite being quite severe. The problem is that a reporter can act perfectly responsibly but the whole thing can be ruined by vendors who cannot be held accountable. So the vendors are useless and full disclosure really doesn’t have that many risks.

Conclusion

KRACK was easily the most significant vulnerability discovered in 2017. Affecting nearly every internet user and limited only by being in range of a wireless access point, it had the farthest-reaching scope of any such bug in recent memory. However, it has not had nearly as large of an impact as its potential implies. A significant mitigating factor in this and all software exploits is the manner in which the Reporter chooses to disclose the vulnerability. KRACK was by all means disclosed in a “responsible” manner, but could have been done better. If vendors were alerted early, they should have fixed it. They didn’t, so what’s the point. We only saw patches after full disclosure. Thus, an earlier full disclosure would have been more ethical.

References

https://www.krackattacks.com/

https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html

https://web.archive.org/web/20060328012516/http://infosecuritymag.techtarget.com/articles/january01/columns_curmudgeons_corner.shtml

https://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00

https://www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932

https://www.bleepingcomputer.com/news/security/new-krack-attack-breaks-wpa2-wifi-protocol/

IEEE 802.11i-2004

https://www.kb.cert.org/vuls/id/228519