Responding to KRACK: Wi-Fi Security Awareness in Private Households*

Jan Freudenreich[1], Jake Weidman[2][0000−0003−4727−4271], and Jens Grossklags[1][0000−0003−1093−1282]

[1] Technical University Munich, Germany
jan.freudenreich@tum.de jens.grossklags@in.tum.de
[2] The Pennsylvania State University, PA, USA
jakeweidman@google.com

Abstract. In this paper, we study the update and security practices of individuals in private households with an exploratory interview study. In particular, we investigate participants' awareness regarding KRACK, a patched key vulnerability in the WPA/WPA2 protocol, and similar vulnerabilities in the context of usage and management scenarios in Wi-Fi networks. We show that while most people are aware of certain dangers, they struggle to address Wi-Fi related vulnerabilities. The findings could prove to be beneficial in identifying not only the current security status of average users regarding Wi-Fi security, but also to improve update and information propagation to mitigate related threats in the future.

Keywords: WPA/Wi-Fi Security · KRACK Attack · Interview Study

1 Introduction

Today, Wi-Fi devices are used in nearly every household with an installed base reaching 13 billion devices in 2019 [19], while Wi-Fi Protected Access (WPA and WPA2) serves as the most commonly used encryption protocol [20].

While WPA2 was widely believed to be secure against direct attacks on the protocol, Vanhoef and Piessens described a practical attack against both WPA and WPA2 networks, allowing for decryption and manipulation of data sent in these networks. The so-called Key Reinstallation Attack (KRACK) [16] was the first non-vendor-specific attack described to allow full decryption of data sent through the Wi-Fi stream.

KRACK makes use of flaws in cryptographic handshakes used to authenticate clients in wireless networks secured by WPA and WPA2. Most importantly, the 4-Way Handshake and the Group Handshake can be attacked. In an attack scenario, a victim is 'tricked' to reinstall an already used session key, severely undermining the security of the wireless network. A successful attack on the 4-Way Handshake allows for replay attacks and decryption of the data stream in

* Jake Weidman is now with Google. The work was partially completed while being a visiting scholar at the Technical University of Munich.

networks secured by the TKIP and CCMP protocols. In TKIP-secured networks, the attacker is also able to forge the traffic between client and access point. The attack settings are not restricted to certain scenarios, and could, therefore, be used in private, commercial, and policy settings.

The newly developed WPA3 standard replaces the 4-Way Handshake with Simultaneous Authentication of Equals (SAE) and thereby mitigates the previously described KRACK attack vector. However, recently discovered vulnerabilities, including Denial-of-Service (DoS) and downgrade attacks, may allow an attacker to force access points to revert back to the WPA2 protocol and effectively circumvent the stronger protection of WPA3 [17]. Such vulnerabilities could possibly slow down the adoption of WPA3. Further, in early 2020, related flaws were discovered in common Wi-Fi chips, affecting an estimated number of one billion devices [4].

In addition, older devices, which are not provided with security updates anymore (or slow update behavior by users) could leave large numbers of devices unpatched even after corrective updates are introduced. This is especially true for operating systems on mobile devices - smartphones and tablets - which often have a far shorter support life cycle than desktop devices [7–9].

The main goal of this work is to analyze the awareness and security measures taken in a sample of private households concerning KRACK and, more generally, Wi-Fi security via an exploratory interview study. Our work aims to help better understand and tackle the existing problems in Wi-Fi security and to outline possible ways for improvements of update and information propagation practices in this problem domain.

2 Related Work

Relevant to our study are the update support practices by vendors, which vary substantially. Microsoft offers support for their Windows desktop products for five to ten years [9]. For Apple, the average time of support for OS X 10 variants is around 40 months [13]. Apple's iPhone products receive updates generally for a period of three to five years [11]. Updates for Android - a more open ecosystem - depend heavily on the vendor [6]. Google's Nexus and Pixel devices are supported with updates for about three years [8].

How Wi-Fi-related security vulnerabilities can create high risk scenarios for the user has been previously shown, for example, by Petters [21]. In 2012, he presented a flaw in routers manufactured by Arcadyan, including so-called Easy-Boxes distributed by Vodafone. The patents of Arcadyan revealed how the factory WPA key was calculated using the publicly broadcasted BSSID of the router. This allowed an attacker to gain complete access to a secured network by only recording the public MAC-address of the router. In 2013, Viehböck showed that through a similar flaw in the WPS algorithm it was possible to hack affected routers, even if the device password had been changed [18].

For the user perspective, a series of AOL/NCSA Online Safety Studies (see, for example, the 2004 version [1]) used an approach (partly exemplary for our

study) where security perceptions of participants were directly correlated with the factual security status of the devices *in their own homes*. Poole et al. [10] further elaborated on the high need for IT support in private households and the problems arising as the result of using different providers and vendors, as well as having different sources of user knowledge.

3 Methodology and Participant Data

The research topic was approached in a qualitative way by performing exploratory semi-structured interviews in interviewees' own homes. Prior to the interview, a short questionnaire was given to the participants, which included questions about demographics and participants' Wi-Fi usage and management as well as their network topology. During the interview, more in-depth questions were provided; structurally divided in five segments. The objective of the first three segments was to provide a deepening structural tree from more broad Wi-Fi and security questions before focusing on the topic of KRACK. The questions in the fourth segment were focused on a broader understanding of security and update-related issues, aiming to find possible mitigations for challenges regarding security updates and insufficient information propagation (to learn about security problems and mitigations). The final part consisted of three questions, tracking possible behavioral changes and reactions to the interview process itself. Following the interview, an additional survey was provided to the participants, allowing us to gather information about update practices and to further evaluate participants' security assessments.

Participants were recruited (in March 2018) through snowball sampling with a focus on achieving a relatively diverse distribution of participants from different social environments and anticipated technological backgrounds to allow the gathering of insights from different perspectives. They were required to be living in a multi-person household and to have their own Wi-Fi network. The interviews were recorded, and subsequently transcribed and anonymized such that no personally identifiable information was present during the analysis process. During the design and execution of the study, we followed recommended community practices for running security usability studies [12].

The study was conducted in the Munich area, Germany. Of the 16 participants, 2 were female, and 14 were male. Nine of the participants were students from different universities and fields of study. Other occupations included a nurse, a pensioner, an unemployed and a self-employed individual. All participants had reached matriculation standard in their education. Two, additionally, had completed vocational education, one a bachelor's degree, and two held a diploma. The average age of the participants was 28.75 years (min = 20; max = 61). Laptops were present in every household; only one household did not have smartphones present. Desktop and tablet devices were used in about half of the households.

4 Results

Wi-Fi usage and sensitive data. Questions about Wi-Fi usage (from the survey) allowed for gathering of information about general Wi-Fi practices and the possibility of (sensitive) data leakage. On a scale from 1 (rarely used) and 5 (always used), browing ranked highest (4.0) followed by streaming (3.8), office work (3.6), social media (2.7) and eventually gaming (2.1). Every person in our sample was using their Wi-Fi for office work and media streaming at least sometimes, whereas some people never used it to play games or to access social media platforms. All of these scenarios could possibly leak private data, which should not be publicly available.

Higher level encryption not ensured. Since the KRACK attack is performed through intercepting data in transmission, securing the transfer layer could be one possible mitigation; also for similar forms of attack. When asked whether participants pay attention to Transport Layer Security (TLS) and to the Hypertext Transfer Protocol Secure (HTTPS), the answers were rather ambiguous. The evaluation shows that there was no clear tendency in this sample group. The statement from Participant 3 is transferable to most others: "*It depends on the context. If I do some unimportant activities no, but if it is concerned with user or banking data yes.*"

The data also shows, that 10 participants (62.5%) had never used a VPN before. Only one participant used a VPN service most of the time to achieve a higher level of security. Others used the technology for work or study purposes; mostly to get access to remote file locations. We found that 13 participants (81.25%) had never used TOR, or a similar onion routing technique, before. Most of them did not recall ever hearing about this way of anonymization. Only one participant did use TOR on a regular basis.

Is your Wi-Fi safe? Even though every participant used their Wi-Fi on a daily basis with several devices, half of them perceived their Wi-Fi network as insecure (50.0%). In contrast, only 6 participants (37.5%) believed their Wi-Fi network to be secure, while two individuals considered their networks partly secure (12.5%). Most argued that the lack of security comes from their own actions, mostly from choosing and handling their respective Wi-Fi passwords in an insecure fashion. One example included giving the password to outside parties, like Participant 2: *"No [...] because my password is [***].*[3] *It is really weak. Why else? Probably, because everyone in the house knows my password."* Another reported practice was taking pictures of the factory settings and sending them using messenger apps to other individuals.

Another rather peculiar case was Participant 8 (and a flatmate), who wrote the factory password on a sheet of paper and put it on a kitchen cabinet. This alone would be problematic, because it would empower anyone having access to the kitchen to attain the password. However, their password is also visible for people outside passing by their flat, since it is hung directly beside a window:

[3] The password was given without any questioning and despite we asked the participant not to tell passwords or similar compromising information.

"*We have it hanging there. [...] This would be such a critical point. If you look through the window, you can see our Wi-Fi password.*"

Factory Settings. Another potential vulnerability for home networks is not changing the default password and continuing using the factory setting. Indeed, many participants still use their routers with the implemented factory settings, although every manufacturer should have instructed them to change these settings. Awareness of the potential threat through an unchanged factory password differed widely across the interviewed participants. Whereas some were aware of a potential vulnerability and changed their password accordingly, like Participant 15, who when asked about why he believes his Wi-Fi network to be secure, said: "*Because of the password. Which was not the original password.*" Others did not show such awareness at all (Participant 14): "*No. I trust it.*" Interestingly, some participants were aware of this possible threat, and even recognized it as an attack vector, but still did not change their password.

Perceived risks. A possible explanation for such observed behavior may be related to the perceived threat model. Most of the participants see similar hazards concerning Wi-Fi networks. A commonly stated risk was the leakage of personal or sensitive data and the possibility of someone getting access to the network and thereby allowing the attacker to use the internet under the resident's identity. The possibility of attackers gaining access to personal and private data was described, for example, by Participants 10 and 13. Such data could then also be leaked to be publicly available. Participant 10 stated: "*That everything I do is accessible to others - which websites I use.*" Participant 13 mentioned: *"Getting your personal data hacked and having it presented to the whole public.*" Participant 1 remarked the possibility of gaining further access to other devices and the possibility of identity theft: "*He could get in my home network, see my hard drives, and surely could get remote access to my computer - at least I could imagine. And of course he could take my identity by using my network.*" Similarly, Participant 8 stated: "*Or he could do some strange internet stuff with our IP. Doing something illegal and stuff like that with our IP.*"

When taking a deeper look into what participants see as sensitive data, it was firstly defined as connected to information related to financial holdings. Among these were passwords for online banking or credit card PINs. Participant 2 remarked: "*Banking information. Everything directly connected to money.*" Secondly, more sophisticated and indirect attacks to gain access to privacy-concerning data were also mentioned. Indeed, several participants identified data as sensitive which would make themselves or others victims of blackmail and extortion. Participant 2 stated: "*Or pornos and stuff which would allow for blackmailing. Maybe if you Google for medical or embarrassing stuff. Or drug related things.*" The listed information could pose a high risk for the victim when leaked publicly. Perceived risks could be the loss of their job, or being shamed in public or by family or friends.

Victims. Most participants were certain that they would not be the target of cyberattacks. Some argued this based on the environment they were living in, like Participant 11 who resides in a small village: "*If I would be living in a bigger*

city or something like that, I would be more concerned." Others, like Participant 8 noted: "*There are many old people in our neighborhood. They are happy if their computer is starting.*"

However, most argued that their own data or information would be irrelevant to others. As an example, Participant 14 stated: "*If I had sensitive data, I would be more concerned.*" Likewise, as participant 15 put it: "*It is exactly like your smartphone: When you type something into Google or when Google tracks you regardless whether your location is on or off. It is the same - it is as bad as if someone would get your data through such an attack.*" These sentiments represent a potential hindrance for further investments in security. Many participants had a "Not Me" mindset, meaning that they do not see themselves as possible victims. The present culture of data collection and data privacy invasions further appears to feed such mindsets as the quotes indicate [14].

Through the linking of sensitive data with money and the potential for extortion, certain other classes of possible victims were named. Among these were politicians, prominent figures and, interestingly, professors. As Participant 2 stated, when asked if he does see himself as a possible victim: "*No. Celebrities maybe or professors. People who are more important than me.*" Different to these mostly general assumptions about possible victims, Participant 14 was able to describe an example from his work-related situation: "*One of my clients is an interior architect and among other things deals with alarm systems. That's very important data. Knowing that she has designed a certain house, she explicitly could be attacked.*"

The responses show that participants were able to connect sensitive data and attack scenarios. But, interestingly, they do not see such a connection given their own situation or personal environments.

Attackers. The description of possible attackers, which could make use of flaws in Wi-Fi networks or IT vulnerabilities in general, differed between participants. Nevertheless, three basic types can be extracted from the answers given in the interviews: intelligence agencies, monetary interests and corporate and economic espionage, and miscreants.

One quote (by Participant 4), in particular, highlights the perceptions regarding information gathering or extortion and thereby gaining political power: "*There are people - spies - which are interested in what people do or say. Everyone knows that government surveillance agencies - keyword Trojan*[4] *- have the possibilities. And they use them, too.*" The motives of blackhat hackers are either described as being about gathering money, or like Participant 13 noted, as wanting to cause destruction: "*People who do this as some kind of hobby. They don't get anything from it, but do it solely to harm others.*" This point outlines a problem with the "Not Me" mindset: Someone without a well-defined agenda is not prone to economically rational modes of operations, since his benefits do not lay in gaining money or political power, but are solely hedonistic - in this

[4] Participant refers to the so-called "Bundestrojaner", a controversial German state sponsored Trojan access tool used to secretly examine IT devices [3].

case causing mayhem. Such scenarios do not offer a clear distinction between non-victims and victims and are thereby potentially dangerous for everyone.

The presented descriptions of dangers and pictorials of victims and attackers quite possible indicate the cause of participants' lack of secure behavior; especially their feelings of unimportance and the presence of a "Not Me" mindset.

Knowledge about KRACK. From all participants in this study, only two did recall hearing about KRACK beforehand (12.5%). However, most participants previously stated that they felt informed about security and technology in general - some would even try to gather specific information and news concerning IT and computer security. However, most of them did not recall the reports connected to the KRACK Attack and the underlying WPA flaws, even though the attack was covered by major German mainstream media, like the Süddeutsche Zeitung [15] and the Handelsblatt [5]. These observations clearly show a problem in information propagation.

In our sample, only 6 participants (37.5%) were concerned about attacks like KRACK. When going into detail, it became clear that again most did not see themselves among the potential victims [2]. Nearly all agreed, that the possible dangers for others could be quite high, which is consistent with findings from above: Assessing a vulnerability as problematic, but not counting themselves among the likely victims.

Security assessment. No participant in this group reported to have checked the security status with respect to KRACK. Seven participants (43.75%) believed their devices to be safe, since they recalled doing security updates in the past few months or made use of automated update procedures. Only two participants (12.5%) believed their devices to be affected. The rest was unsure (43.75%).

Mobile Devices: We found that 37.5% of Android devices (6/16) and 62.5% of iOS devices (5/8) in this sample were still vulnerable to KRACK. It appears that the rather short overall update period for smartphones, mostly between two and four years, does not suit the longer usage period of such devices. Most vulnerable devices were indeed not eligible for security updates anymore; only two iOS devices, which could have been updated, were not updated by the user. *Desktop and Notebook Devices:* No macOS (0/2) or Linux (0/7) devices were still vulnerable, and only a minority of Windows PCs (18.75%, 3/16) were still vulnerable. It should be noted that the only affected Windows PCs were either older XP models, or in one case a Windows 10 PC were the user used a registry hack to prohibit the operating system from updating. All others were running Windows 7 or 10 and had the appropriate security updates installed.

In our sample, mobile devices were far more often vulnerable to the KRACK Attack. Further, nearly all vulnerable devices were outside of the respective support time frame, which for mobile devices is usually far shorter than for desktop devices. Taken together, in this sample, 10 out of the 16 households (62.5%) had at least one vulnerable device present, and several had multiple vulnerable devices. It is important to note that the attack and also the first security updates were made available more than half a year before our study.

Further, a significant difference between the assessment of security and the actual security was observed. Interestingly, the two participants who believed their devices to be still affected had in reality no vulnerable devices present in their households. In contrast, four participants of those who noted that their devices should be in an updated and secure state, had at least one vulnerable device present in their households.

Communication. One question covered the widely discussed topic of enforcing updates without direct user consent. Most participants were clearly against this kind of enforcement. They mostly cited a loss of independence and the fear of losing functionality. Participant 9 stated, for example: "*I don't want any enforcement. They should know that an update is available, but they shouldn't be pressured.*"

Therefore, a suitable way to achieve a higher level of security, and not in opposition to the participants, would be to improve the communication between users and providers. Several communication channels should be implemented simultaneously. These should be both direct channels (e.g., email) and indirect channels (e.g., newspapers, websites). Most participants want providers to inform them directly, and also seek to receive information from the media. In contrast, government, and in particular intelligence agencies seem to be suffering from a widespread lack of trust in governmental institutions. Participant 7 stated: "*I would say better by news or public media. Instead of the government, which would make me feel like my mobile phone is monitored by the government. Any message from them could mean they monitor this.*"

5 Discussion and Concluding Remarks

Update Supply and Propagation. When updates are provided, participants seem to perform them on a regular basis. However, our data suggests that desktop devices are far better secured against such attacks than mobile devices. Desktop devices are usually supported with updates over a longer period of time. In opposition to that, support cycles for smartphones are far shorter. Nearly all mobile devices are highly dependent on the manufacturer of these devices. When the support period expires, a switching of operating systems is usually impossible.

The widespread usage of proprietary software and firmware - in this case contrary to open source software - extends the manufacturers' field of responsibility, since it is impossible for non-expert users, even with some technical knowledge and abilities, to control these software parts. Such software and the subordination to specific providers are prone to be problematic, since they further increase the dependence on these providers and hinder other parties from taking care of flaws or insufficient update provision.

Lack of Wi-FI Security and Wi-Fi Security Consciousness. Participants often do not engage in secure practices when using or managing their Wi-Fi infrastructure. Most prominently, many do not change factory settings, do not choose or handle passwords appropriately, and do not concern themselves with security updates for these devices (in contrast to computers and phones).

In contrast, nearly all participants seem to be generally aware that a variety of security threats and attack scenarios may exist. But they do not apply these dangers to themselves. Users often do not see themselves as potential victims, because of a perception of lack of importance of their devices and data, and an overall missing consciousness regarding data privacy.

Knowledge and Information Propagation. Judging from the presented findings, participants seem not to be informed about security flaws and vulnerabilities regarding their devices or the underlying techniques in general. The same applies for dangers associated with insecure devices or data leakages, both in personal and social settings.

How these issues could be addressed cannot be satisfactorily discussed in this short work. Nevertheless, the somewhat variable findings suggest that multiple ways should be present simultaneously. These ways include direct and indirect communication. For specific persons and vulnerability situations, a direct approach, in which households are contacted through mail or other direct communication channels, seems to be fitting. This form of information should be done by the manufacturers or providers themselves. However, this direct communication cannot fully substitute public announcements - especially in scenarios where high portions of the deployed devices are affected, like in the example of KRACK. However, the preferences for ways of informing about security flaws and dangers were very diverse necessitating a flexible approach using different ways of communication.

Update Without Consent. Users want to keep sovereignty over their owned devices, meaning that almost all of the participants in this sample did not want their devices to update without direct consent. In addition to the possible loss of functionality, most are concerned with a general loss of control over their device. However, in today's complex setting of connected devices, this desire can only be securely satisfied if people are generally able to fulfill the underlying responsibilities; likely in conjunction with adequate novel tools. On the one hand, we have the individuals' wish for sovereignty and control; on the other hand, the need for ensuring a secure collective infrastructure.

Acknowledgements: We thank the anonymous reviewers for their constructive feedback.

References

1. America Online and the National Cyber Security Alliance: AOL/NCSA online safety study (2004)
2. Bidgoli, M., Grossklags, J.: End user cybercrime reporting: What we know and what we can do to improve it. In: 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). pp. 1–6 (2016)
3. Buermeyer, U.: Gutachterliche Stellungnahme zur öffentlichen Anhörung zur Formulierungshilfe des BMJV zur Einführung von Rechtsgrundlagen für Online-Durchsuchung und Quellen-TKUe im Strafprozess - Ausschussdrucksache (2017)

4. Cermak, M., Svorencik, S., Lipovsky, R.: KR00K - CVE-2019-15126: Serious vulnerability deep inside your Wi-Fi encryption. https://www.welivesecurity.com/wp-content/uploads/2020/02/ESET_Kr00k.pdf (2020)
5. DPA: Forscher entdecken Sicherheitslücken bei WPA2. https://www.handelsblatt.com/technik/it-internet/wlan-verschluesslung-forscher-entdecken-sicherheitsluecken-bei-wpa2/20461320.html (2017), accessed: 23.06.2020
6. Farhang, S., Kirdan, M.B., Laszka, A., Grossklags, J.: An empirical study of Android security bulletins in different vendors. In: Proceedings of The Web Conference (WWW). pp. 3063–3069 (2020)
7. Farhang, S., Weidman, J., Kamani, M.M., Grossklags, J., Liu, P.: Take it or leave it: A survey study on operating system upgrade practices. In: Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC). pp. 490–504 (2018)
8. Google LLC: Learn when you'll get Android updates on Pixel phones & Nexus devices. https://support.google.com/nexus/answer/4457705 (2020), accessed: 21.06.2020
9. Microsoft Inc.: Windows lifecycle fact sheet. https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet (2020), accessed: 21.06.2020
10. Poole, E.S., Chetty, M., Morgan, T., Grinter, R., Edwards, K.: Computer help at home: Methods and motivations for informal technical support. In: SIGCHI Conference on Human Factors in Computing Systems. pp. 739–748. ACM (2009)
11. Richter, F.: How long does Apple support older iPhone models? https://www.statista.com/chart/5824/ios-iphone-compatibility/ (2019), accessed: 21.06.2020
12. Schechter, S.: Common pitfalls in writing about security and privacy human subjects experiments, and how to avoid them. Tech. rep., Microsoft, January (2013)
13. SCS Computing Facilities: Operating system support lifecycle. https://computing.cs.cmu.edu/desktop/os-lifecycle (2020), accessed: 21.06.2020
14. Solove, D.: I've got nothing to hide and other misunderstandings of privacy. San Diego Law Review **44**, 745 (2007)
15. Tanriverdi, H.: Forscher durchlöchern Wlan-Sicherheit. http://www.sueddeutsche.de/digital/it-sicherheit-krack-attack-forscher-durchloechern-globalen-wlan-standard-1.3711399 (2017), accessed: 23.06.2020
16. Vanhoef, M., Piessens, F.: Key reinstallation attacks: Forcing nonce reuse in WPA2. In: ACM SIGSAC Conference on Computer and Communications Security (CCS). pp. 1313–1328 (2017)
17. Vanhoef, M., Ronen, E.: Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd. In: IEEE Symposium on Security & Privacy (S&P). IEEE (2020)
18. Viehboeck, S.: Vodafone Easybox default WPS PIN algorithm weakness. https://sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20130805-0_Vodafone_EasyBox_Default_WPS_PIN_Vulnerability_v10.txt (2012), accessed: 23.06.2020
19. Wi-Fi Alliance: Wi-Fi in 2019. https://www.wi-fi.org/news-events/newsroom/wi-fi-in-2019 (2019), accessed: 23.06.2020
20. Wigle.net: Statistics. https://wigle.net/stats (2020), accessed: 21.06.2020
21. Wischnjak, D.: Immer Ärger mit der Easybox. https://www.heise.de/security/artikel/Immer-Aerger-mit-der-EasyBox-2294914.html (2014), accessed: 23.06.2020