Effects of the WPA2 KRACK Attack in Real Environment

Dávid János Fehér[1], Barnabás Sándor[2]
[1]Keleti Károly Faculty of Business and Management, Óbuda University, Budapest, Hungary
[2]Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University
david.janos.feher@gmail.com; sandor.barnabas@gmail.com

Abstract—**The World's most used Wi-Fi protocol, the WPA2, contained vulnerability and several problems discovered and published by cybersecurity researchers. It has affected the IT World, and further changes can be expected. This article examines the details and effects of this change alongside of user behavior.**

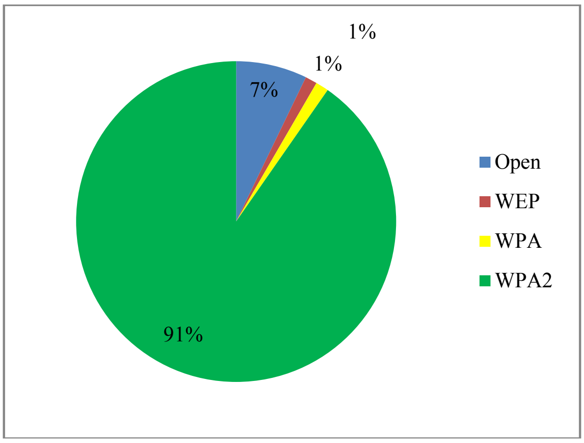
Keyword: Wi-Fi, WPA2, KRACK, WPA3, wireless vulnerability, cybersecurity

I. INTRODUCTION

The whole IT world was dumbfounded when security researchers found several management vulnerabilities in the WPA2 protocol in October of 2017. This vulnerability allows the attacker to gain access to the private Wi-Fi network. It is in the Wi-Fi security protocol itself, so most of the WPA2 protocol using the device was affected by it. Without the right patches, the KRACK (Key Reinstallation Attack) can be effective against most of the WPA2 devices in personal or enterprise network with the WPA-TKIP, AES-CCMP and GCMP cipher. We investigated the conditions, effects and the expected developments of the WPA2 protocol vulnerability. [1]

II. BACKGROUND

The evolving technology forced back the wired connections, and the present and the future is the wireless network connection. Wi-Fi devices make it more convenient to connect to a network and make the installation of the device much more accessible for the average user and enterprise professionals. Benefits usually come with disadvantages. Wireless solutions are more accessible for unauthorized users and attackers. A hacker can attack a Wi-Fi network from the neighboring building or from farther away with the right signal booster antenna heightening the security risk. The latest wireless protocol is related to vulnerabilities, and attacks always were widespread, but the World is changing with the technology. The industry 4.0, the Internet of Things, the smart cars are about to exchange data and work with each other. The user base is growing with the consumption andutilization of wireless devices, so the present is and the future will be about wireless connections. The growing confidential usage increases the interest of attackers to gather information from this technology and the information security professionals to make the network and the workflow continuous and secure. Wireless risks are high in an enterprise environment, so the cybersecurity professionals endeavor to use the most secure protocol which is WPA2. The upgraded WPA protocol was released in 2004, and in 2018 it is the most used protocol. We can say that the WPA2 protocol is the most used Wi-Fi protocol nowadays. The latest wireless devices come with WPA2 protocol setting by default. The latest wireless devices come with WPA2 protocol setting by default, so the whole manufacturer environment is trying to improve the security of their users. the whole manufacturer environment is trying to improve the security of their users. Based on a Wardriving measurement 91% of available wireless access points use WPA2 protocol in Budapest and the remaining 1% uses WPA, 1% uses WEP and 7% of available sources are open. Access points usually have the option to use the WPA2 next to WPA to solve the compatibility problems if the connecting devices cannot communicate with the WPA2 protocol, 43% of the measured devices working with this setting. [Figure 1] [2] [3] [4] [5]



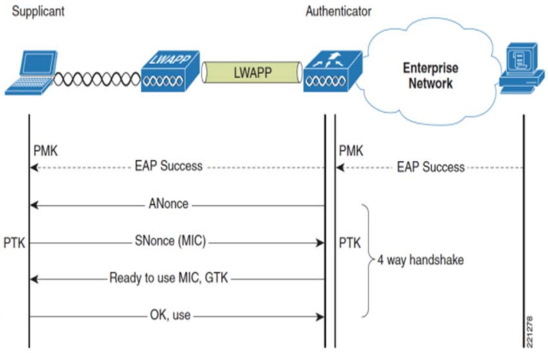
1. Figure: WiFi protocols based on the Wardriving measurement [2]

A. WPA2

The WPA2 certification was introduced in September 2004 by the Wi-Fi Alliance as a mirror of the IEEE 802.11i security amendment. This new certification includes AES algorithm in CCMP based on NIST FIPS 140-2 government-grade security requirement. The WPA2 is backward-compatible with the WPA and supports the 802.1X/EAP authentication or PSK. The core protocol of the WPA2 certification is the Counter Mode with CBC-MAC Protocol (CCMP). [6]

978-1-5386-6841-2/18/$31.00 ©2018 IEEE

The WPA2 wireless communication works with a 4-way handshake structure. When a client tries to join a protected Wi-Fi network the handshake is executed and is used to verify that both the client and access point possess the accurate credentials (e.g., the pre-shared password of the network). Simultaneously the 4-way handshake settles a new encryption key encrypting all subsequent traffic. Currently, the 4-way handshake is used by all modern protected Wi-Fi networks.[Figure 2] [6]



2. Figure: 4-way Handshake

B. *WPA2 Passphrase Vulnerability*

One of the well known existing vulnerabilities of the WPA2-Personal protocol was based on passphrases. Most of the home users do not use 802.11X/EAP solution with RADIUS server for authentication. The weaker WPA2-Personal is using PSK authentication with static passphrase which is vulnerable to an offline brute-force dictionary attack.

C. *Key Reinstallation Attack*

On the Black Hat USA (LV, NV) conference in October 2017, Mathy Vanhoef and Frank Piessens presented the Key Reinstallation Attack (KRACK) process, which exploits the vulnerability of the older version of the Wi-Fi Protected Access (WPA), and the latest WPA2 protocol-protected networks. This method is directed against the current method of WPA (4-way handshake). The different attack works against personal and enterprise Wi-Fi networks, and even against networks that only use AES. [7] [8]

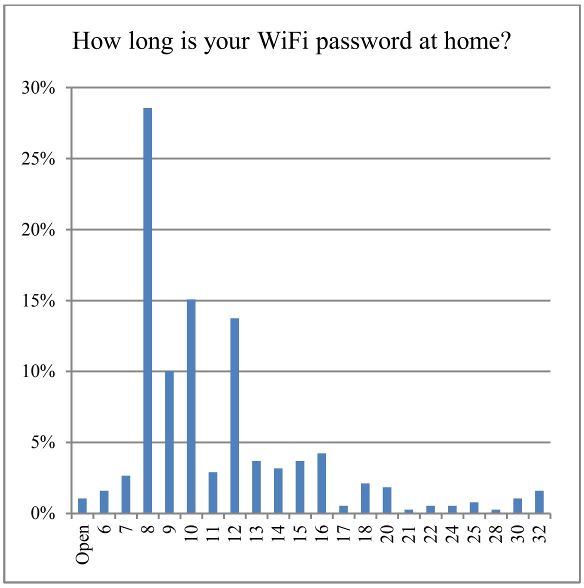
The attack tricks the victim into reinstalling the already used key / already-in-use key by manipulating and replaying cryptographic handshake messages. [9]

D. *Related Common Vulnerabilities and Exposures*

- CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
- CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
- CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.

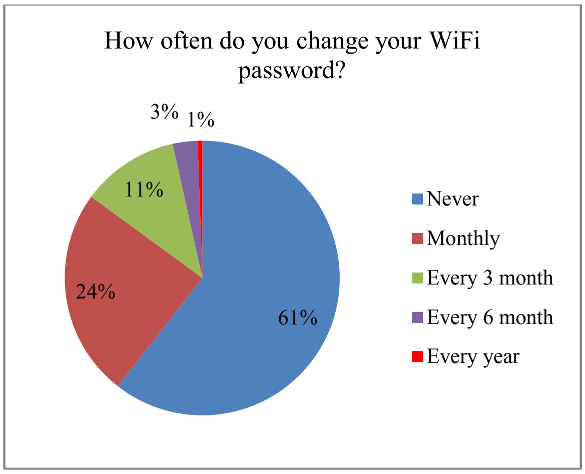
SOLUTION

We created quantitative survey research to gather more information about the average user behavior, security awareness and to identify the compromised user groups. Based on the survey 87,3% of the respondents have Wi-Fi in their home. The survey was filled out by 379 people and widely distributed to gain more varied results, so we can not separate the vulnerable and the not-vulnerable persons, but we see the two ends of the scale. Based on the gathered information we can declare that the problems are generally accumulating. The main problem in this situation is the high number of affected users. The most experienced users have already updated the firmware of their Wi-Fi routers and devices to avoid this type of problems, but most of the device owners are average final users. This problem consists of several consistent elements, like too weak and too short password. The acquired encrypted password is easily crackable if the password is weak, furthermore the computing capacity is growing year by year. Based on our survey we know that 108 people, 29% of the examined users, have 8 characters long password on their Wi-Fi. Most of the passwords contain uppercase and numbers next to the lowercase letters, which means it would take an average computer about 2 hours to crack these passwords with a simple brute force attack.[Figure 3] [10] [11]



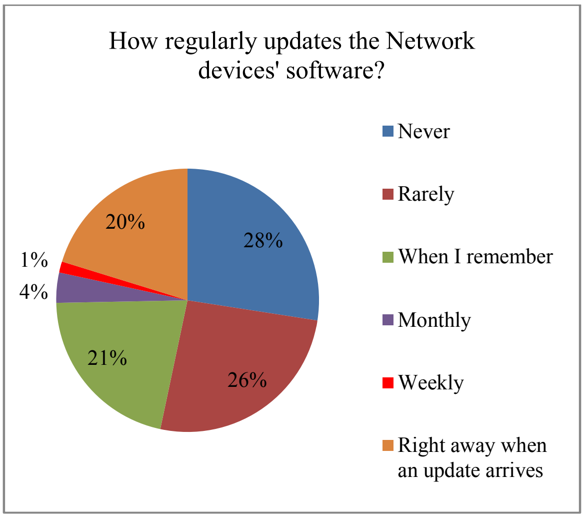
3. Figure: Home WiFi password choosing behavior

Most of the users, 61% of the respondents never change the password of the Wi-Fi access point It is the cause of many problems. If the password already leaked, the attacker can use it for a long period of time.[Figure 4]



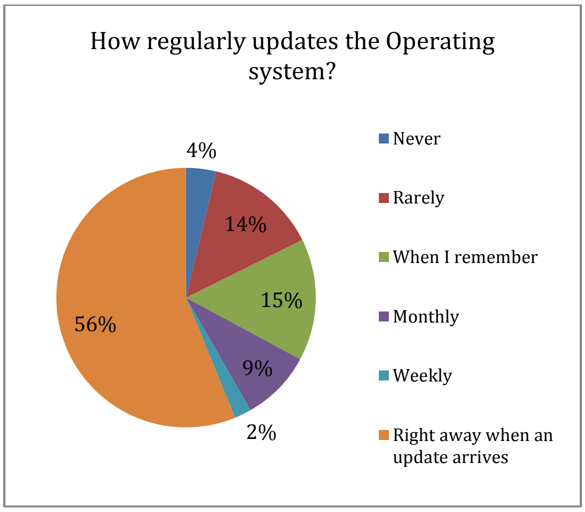
4. Figure: User password changing behavior

The most important part of the mitigation are device updates. The most known manufacturers usually publish updates to fix the most critical security vulnerabilities as soon as possible. Most of the end user devices are trying to automatize or push the updates on the devices, but the network device update rates are not ideal. 28% of the respondents never update their network devices. [Figure 5]



5. Figure: Network device updating behavior

The Wi-Fi Alliance published its protocol specification, and in 2019 the first WPA3 devices might finally arrive. Attacks against Wi-Fi devices are working with an ever growing arsenal, against which the market's steady participant, the WPA2 cannot give full protection anymore. It was about time to get information about which device manufacturers already have taken care of this vulnerability. The WPA3 will make the protocol and standard more efficient, and simplify the Wi-Fi security with a line of new security functions. The new generation promises more complicated authentication, stronger encryption and better support of critical business networks, while weeding out the old obsolete protocols and making the use of PMF (Protected Management Frames) mandatory. Update protocols – just like before – come with two safety modes, the Wi-Fi Alliance separates WPA3-Personal and WPA3-Enterprise variables depending on the use environment. The previous one is more extensive and safe providing password-safe authentication for the protection of personal users: in the case of WPA3-Personal the used PSK (Pre-shared Key) is going to be changed to SAE (Simultaneous Authentication of Equals), which can withstand dictionary-based brute force attacks when the attacker is trying out all the possible combinations for the log in identification from an automatized database. These attacks are frequent, but only work against the short and straightforward log-in data – they are not very useful with a 30 character password, but most of the users are not very good at giving a complicated enough password. [8] [12]



6. Figure: OS updating behavior

The complexity of the information security allows approaching the problem from another angle. Update a PC or mobile device OS or application is easy and obvious, 56% of the respondents do it right away when an update arrives. The market leader companies try to improve the end user experience, and the security is a part of this. Most of the web browsers try to force the HTTPS (Hypertext Transfer Protocol Secure) communication in every website to provide a more secure way of browsing.[Figure 6] [14]

A VPN (Virtual Private Network) is a means to confidentially send data or information over a shared network infrastructure or a compromised network. VPNs defend the data that transferred over this network by encrypting the data. VPN (Virtual Private Network) solutions more available and cheaper than some years before so it is a user-friendly solution.[15]

III. CONCLUSION

Until the publishing of WPA3 and the spread of the new protocol, the best solution to mitigate the risk of the new vulnerability is to patch the firmware of the affected devices. Sadly, older devices are unsupported by the manufacturer, most of them are vulnerable, so it is necessary to replace them. The hardest part in this situation is to reach the average users and motivate them to update or replace their devices or use software based mitigations. Some Internet Service Provider offers Wi-Fi network devices with their subscription. They can manage their well-known devices to handle the highest security vulnerabilities. The most critical essential element is the user awareness and user knowledge because the market is full of different unsupportable devices without the automated update. [12]

REFERENCES

[1] Swati Khandelwal: KRACK Demo: Critical Key Reinstallation Attack Against Widely-Used WPA2 Wi-Fi Protocol https://thehackernews.com/2017/10/wpa2-krack-wifi-hacking.html - Downloaded: May 11, 2018

[2] Zsolt Illési, Áron Halász and Péter János Varga. "Wireless Networks and Critical Information Infrastructure" SACI 2018 • IEEE 12th International Symposium on Applied Computational Intelligence and Informatics •2018, May 17-19 • Timişoara, Romania

[3] Lasi, Heiner, et al. "Industry 4.0." Business & Information Systems Engineering 6.4 (2014): 239-242.

[4] Afaqui, M. Shahwaiz, E. G. Villegas, and E. L. Aguilera. "IEEE 802.11 ax: Challenges and requirements for future high-efficiency WiFi." IEEE Wireless Communications 99 (2016): 2-9.

[5] Dalibor Dobrilovic, Zeljko Stojanov, Stefan Jäger, Zoltán Rajnai: A Method for Comparing and Analyzing Wireless Security Situations in Two Capital Cities. Acta Polytechnica Hungarica Vol. 13, No. 6, 2016

[6] Coleman, David D., David A. Westcott, and Bryan E. Harkins. CWSP Certified Wireless Security Professional Study Guide Second Edition: Exam CWSP-205. John Wiley & Sons, 2017. 78-79

[7] Mathy Vanhoef: Key Reinstallation Attacks: Breaking the WPA2 Protocol www.blackhat.com/docs/eu-17/materials/eu-17-Vanhoef-Key-Reinstallation-Attacks-Breaking-The-WPA2-Protocol.pdf - Downloaded: May 17, 2018

[8] Wi-Fi Alliance: www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-security-enhancements Visited: May 17, 2018

[9] Mathy Vanhoef and Frank Piessens: Key Reinstallation AttacksBreaking WPA2 by forcing nonce reuse, www.krackattacks.com Visited: May 15, 2018

[10] Gibson Research Corporation - Security: How Big is Your Haystack? www.grc.com/haystack.htm - Visited: May 2, 2018

[11] Farik, Mohammed, and A. S. Ali. "Analysis of default passwords in routers against brute-force attack." International Journal of Technology Enhancements and Emerging Engineering Research 4.9 (2015): 341-345

[12] Wi-Fi Alliance www.wi-fi.org/discover-wi-fi/security - Visited: May 17, 2018

[13] Kornélia Lazányi, Zuzana Virglerová, Ján Dvorský, Rimantas Dapkus: An Analysis of Factors Related to "Taking Risks" , according to Selected SocioDemographic Factors. Acta Polytechnica Hungarica Vol. 14, No. 7, 2017

[14] Hernacki, Brian, and William E. Sobel. "Detecting man-in-the-middle attacks via security transitions." U.S. Patent No. 8,561,181. 15 Oct. 2013.

[15] Bartlett, Graham, and Amjad Inamdar. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. Cisco Press, 2016.