Wireless security iterations and vulnerabilities

476/576 Class Project: Team 6A
Boyuan Gao, Michael Jereza, Inyong Kim Oregon State University, Corvallis, OR, USA,
gaob,jerezam,kiminy@oregonstate.edu

***Abstract*—Wireless local area network (WLAN) is a breakthrough technology that allows remote devices to communicate and integrate with local area networks, which were previously only accessible from a physical connection. Wireless connection allows networks to integrate an entirely new ecosystem of remote devices that connect and disconnect frequently, also known as roaming. As technology has improved and now with the advent of 5G technology, transmission of data through wireless fidelity (Wi-Fi) provides speeds comparable to Ethernet connections. The difficulty is to provide equivalent security. Protecting information sent through the air does not have the same privacy as an electrical signal over a copper wire. In some instances a malicious actor can intercept that traffic to divulge information. In others they can craft malicious traffic that appears to come from a legitimate source, tricking a victim's system. Network threats like these are only possible by the discovery and disclosure of vulnerabilities in wireless security mechanisms, allowing them to exploit vulnerable networks that haven't implemented a developed solution. However this game of cat and mouse over many iterations of international standards, has made the technology stronger. The majority of the modern world utilizes this wireless technology to avoid the limitations of physically connected infrastructure. More and more devices use Wi-Fi, and it is now common to provide free Wi-Fi in public places. Along with increasing Wi-Fi usage, attempts to attack Wi-Fi security vulnerabilities are increasing. This report explains wireless security protocols, how past vulnerabilities were leveraged against them, and the how the iterations of Wireless Protected Access that led to the modern standard of WPA3 improved the technology by learning from the past. This new protocol, WPA3, also has current vulnerabilities which will be analyzed, simulated, and possibly prevented by an implemented countermeasure.**

key word - WEP, WPA, WPA2, WPA3, Dragonblood

I Introduction: Motivation and Objectives

The importance and contemporary problems of Wi-Fi security

The Internet of Things (IOT), Unmanned aerial vehicles (UAV), and Smartphones are utilizing the Internet; even more state of the art devices are being developed to utilize Wireless Local Access Networks (WLAN) due to the convenience and efficiency of wireless communication. In proportion to such WLAN usage, hacking attempts for monetary gains and information collection have been rapidly increasing in recent times. According to a report in *European Societies*, the increase in telecommuting and indoor activity since the outbreak of Covid-19 has led to a sharp increase in attempts that threaten cyber-security for specific gains [1]. Cybercrimes such as leakage of intellectual property, fraud based on identity theft, and financial extortion through the acquisition of personal information are carried out through hacking such as Man-in-the-middle attacks. The majority of the hacking attempts can be prevented with the security protocols developed by the Wi-Fi Alliance. However, early security protocols like Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) are vulnerable to certain attacks. After identifying these specific attacks, the Wi-Fi Alliance has continually improved its security protocols to defend against them. Despite these efforts by the Wi-Fi Alliance, new ways of exploiting the protocol implementations are constantly being found. In short, security protocols must continue to evolve with the discovery of new vulnerabilities, otherwise they risk exposing attack surfaces that could be used to harm the users or devices on a network. The Wi-Fi Alliance is strengthening the Wi-Fi security protocol through continuous research, and currently provides the latest security protocol called WPA3. The Wi-Fi Alliance eliminated most of the security vulnerabilities found in previous protocols that before WPA3, but this iteration of the protocol is still not widely adopted. The biggest problem is that vulnerabilities have been discovered in this new technology before enough people have adopted it. Vulnerabilities in this recently developed protocol will make people reluctant to switch, especially since older hardware must be upgraded for the capability of WPA3. Maintaining the older security protocol is to settle for a technology that has been made obsolete due to a critical security flaw, which leaves user

vulnerable to external threats. With the proliferation of cybercrime, the rapid transition to WPA3 is urgent to mitigate critical vulnerabilities in Wi-Fi technology.

Technical objectives and Goals

In 2018 the Wi-Fi Alliance launched the WPA3 protocol. In this survey, it will discuss the recently discovered vulnerabilities of the WPA3 protocol. According to new research published by Vanhoef (2020), the recently discovered security issue was named Dragonblood, a reference to the Dragonfly handshake method featured by WPA3 [2]. There are several aspects to Dragonblood with different classifications, among which this paper will focus on the downgrade attack and the resource consumption attack. The technical objectives for this demonstration of the Dragonblood vulnerability, is to simulate the potential threats utilizing Wireshark and Kali Linux. The goal is to present the countermeasures for the simulated threat and reflect it in the simulation to show how much the security level has improved based on the derived key parameters.

This report is organized into the following sections. Section II describes the elements that make up a basic WLAN network and a background knowledge of Wi-Fi security. Section III describes the process leading up to the most advanced security protocols at the present time, in the perspective of challenge and solution. In Section IV, the challenges that have still not been solved in the latest protocol are described in detail. Finally Section V provides conclusion and suggestion for the direction of future work.

II Background and Fundamental Concepts

Introduction to WLAN technology

The wireless local area network (WLAN) mainly uses radio frequency (RF) technology to transmit electromagnetic waves for data transmission, dethroning the established transmission mode which utilizes twisted-pair copper wires. With WLAN networks, including Wi-Fi networks, users can integrate individual devices in simple information transmission structures for data transmission and communications [3]. Currently, 802.11n, which has been widely used in various fields, stands out among many existing communication protocols due to its prominent advantages in terms of data transmission effectiveness, efficacy, and security [4], [5].

Architecture of WLAN network

The wireless local area network is generally composed of several parts, including wireless communication medium, devices, terminal stations, and access points.

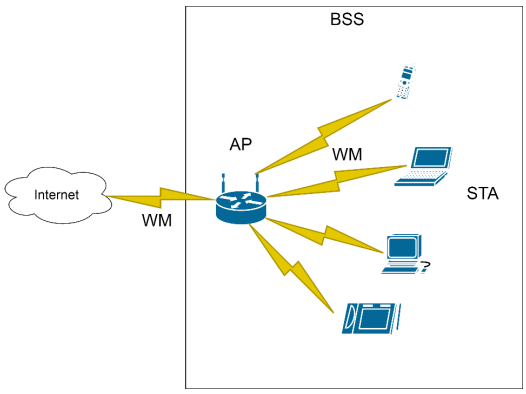

Fig. 1: Topology of a Typical WLAN Network

- **Station (STA)**

STA is the basic component of the WLAN network. It generally refers to the terminal device using the WLAN network, also known as the client, which can be fixed or mobile [5]. This includes mobile phones, computers, and workstations.

- **Access point (AP)**

The function of the AP in the WLAN is similar to that of the base station. The main function is to complete the communication between the STA and the distributed system. APs are often located in the center of BSA (Basic Service Area) and are nodes of wireless and wired networks [5].

- **Wireless medium (WM)**

The wireless medium is the transmission medium used for transmission and communication between the STAs and the AP. For example the air is a typical WM for radio waves. In addition, the wireless medium can also be defined by the physical layer standard in the WLAN [5].

- **Distributed system (DS)**

The physical layer coverage in the wireless local area network determines the communication distance of an access point. The basic service set (BSS) includes AP and the corresponding STA. Multiple BSSs connect through the network to form a network, and the network components used for connection are distributed systems (DS) [5]. As a critical component of WLAN networks, including Wi-Fi networks, the access point mainly plays the role of relaying signals of data communication and transmission in the WLAN networks. For wired networks, applied network architecture and protocols are essentially determined by physical structure and topology which makes it unnecessary to alter their processes, with access points designed to be physically connected

to the network [5]. In the contrast, the designed AP technology for wireless networks is required to realize its functions with the characteristics of formatting and error checking calculations for wired and wireless data frames. This allows wireless connection to be capable of transferring, and verifying through calculation, data to the neighbor local area network without inputting the path table and parameters by administrators [3].

Background of WLAN and Wi-Fi security

The progress and development of modern society has given wireless LAN ample opportunity for improvement, and as a result its functions and security have been continuously improved. Despite its features of convenience that are considerably popular with people, there is plenty of technical concerns in terms of security [6]. As peoples' awareness of the importance of security and protecting personal information increases, the improvement of wireless local area network security is also an inevitable to suffice practical needs related to WLAN security and robustness against cyber-attacks [7]. Due to various incidents of security breaches and leaked information that has more frequently occurred in recent times, the security of network communication is often pushed to the cusp of the storm. With the advancement of technology and increased attention to modern wireless network security mechanisms, these security mechanisms have also shown a state of continuous improvement. As a result the technology's security strength has naturally increased to a new unprecedented level [8]. As a typical and most widely used wireless local area network communication technology, the security techniques, mechanisms, and protocols applied for Wi-Fi communications have been hot topics among academia and the industry. Wi-Fi technology has experienced four generations of encryption technology since its introduction around 2000 [6]. At the same time, the security risks and security vulnerabilities of Wi-Fi encryption schemes and security protocols have been disclosed from time to time [6], [7]. In order to enable readers to deeply understand Wi-Fi encryption technology and security risks from the technical source, this paper is designated to investigate and analyze Wi-Fi security techniques, mechanisms, and protocols at different stages in detail.

III Advances on the State-of-the Art: Challenges and Solution Approaches

The Wi-Fi Alliance has experienced four technical stages indicated by different Wi-Fi security schemes since the first use of Wi-Fi encryption technology and security protocols in 2000 [9]. This includes WEP, WPA, WPA2, and WPA3. According to the security strength and the iterative development of encryption methods, the four stages can be alternatively classified into weak-key, symmetric-key, and asymmetric-key stages.

WEP security protocol

The earliest Wi-Fi communication used the WEP security protocol. The earliest WEP security protocol and encryption technology were not applied in wireless communication, instead they were developed for encrypting important data in Ethernet communication [10]. The encryption operation of WEP uses the RC4 algorithm, which is a common XOR algorithm implementation. The encryption idea at this stage was relatively simple. A fixed-length wireless message can be encrypted by performing a round of RC4 calculation using an encryption key with a length of 128 bits [9]. WEP encryption does not have a key management method [9]. A receiving end is considered a legitimate user by default if its WEP key match the AP's encryption key. Wireless packets can be easily cracked through RC4 inverse calculation. Essentially, the encryption keys of WEP are not spread casually, and not all users can grasp the correct key. In the early days of wireless statistical technology, WEP had an advantage with its simple and easy-to-implement algorithm composition [9], [10]. Nonetheless, with the rapid growth of computer computing speed, a 128-bit key can be verified by a capable attacker in a considerably short time. The WEP encryption scheme thereby became vulnerable, as the communication data of all users in the network will be instantly exposed once the WEP key is exposed [11].

WPA security protocol

In order to address the shortcomings of the WEP encryption scheme, WPA-TKIP was designed to introduce various new security mechanisms including message integrity check (MIC) and TKIP sequence counter (TSC). This was provided on the basis of WEP encryption hardware utilizing software upgrades, taking into account the continuity of the Wi-Fi inventory market at that time [12]. In the initial stage of message encryption, the Michael calculation module is used to extract the message retrieval information, the first round of encryption processing is performed, and the sequence count is added before the session is encrypted. This method can effectively reduce the risk of security attacks and prevent message tampering [13]. To be more specific, if the message is replaced or tampered with during the transmission phase, the information is retrieved by decrypting the extracted message during message decoding. The counter information will be different from the message itself. Therefore, the

receiving side will easily find that the message has been tampered with or substituted[12]. The WPA-TKIP encryption technology also adopted the pre-shared key (PSK) mechanisms for the first time and introduced a 4-way handshake mechanism to separate the network key held by the user from the session key [12]. The master key of WPA-TKIP is a combination of a 512-bit key, which is designed to be split into five groups during the encryption process for message integrity checking, encryption, and verification [13]. The session encryption scheme of WPA-TKIP was inherited from the RC4 encryption algorithm that had been applied in WEP [14]. The original intention of this design is to meet the security upgrade of Wi-Fi products, modules, and chips in the inventory market. The hardware requirements of WPA encryption technology and protocol are consistent with WEP, which means that the Wi-Fi-enabled products currently deployed on the market did not become obsolete by merely conducting software upgrades to update the encryption scheme [12]. Differentiated with the WEP encryption scheme, the security level of the WPA-TKIP encryption architecture and the design of the handshake process was greatly improved. Nevertheless, due to the low complexity of the encryption operation module of RC4, it cannot effectively prevent brute force attacks, for example pre-shared key traversal of the password dictionary attacks [11].

WPA2 security protocol

In 2006, the Wi-Fi Alliance launched the WPA2 technology globally and used it as an encryption solution for wireless LAN communications. The WPA2 encryption scheme abandons the RC4 encryption method and uses the AES encryption scheme to encrypt the message. AES encryption technology was the highest security symmetric key encryption algorithm invented at the end of the 20th century and the beginning of the 21st century [11]. The WPA2 encryption method first cuts the message subject into data blocks and then uses the corresponding key array to perform multiple rounds of interleaving nonlinear encryption operations [15]. The encryption operation of WPA2 can be completed with considerably limited processor resources, and the installation speed of the key is also quite fast. WPA2 uses a multi-round interleaving non-linear encryption method, which greatly increases the difficulty of reverse cracking, and can ensure the avalanche effect of excellent key design. To be more specific, every time the encryption key is modified by 1 bit, the encrypted message corresponds to the original message, which produces significant resistance against brute force attacks [13]. At the same time, the WPA2 encryption algorithm also draws on the concept of information integrity security verification in the WPA encryption process design and uses a higher level of security CCM and CBC-MAC calculation method to complete the extraction of the MIC code [15].

The WPA2 encryption scheme is the longest-used Wi-Fi encryption technology scheme thus far. By adopting block-based encryption, it can be ensured that the information sent by the same user in different time periods uses different encryption and decryption keys [15]. In the meantime, different wireless users in the same wireless LAN use different encryption and decryption keys, thus achieving a superior encryption-decryption isolation effect. Based on this, it is fundamentally not viable for adversaries to crack the key through commonly used brute-force cracking methods, including the dictionary cracking method [11]. Subsequently, Wi-Fi networking using WPA2 encryption has gradually exposed two major problems as time goes on. The first problem is related to the protection of management frames. The encryption mechanism established by WPA2 through the 4-way handshake is usually only for data information in communication, which does not form effective protection for some management messages in the Wi-Fi networking environment, specifically the management frame message in the Wi-Fi communication network is transparently transmitted on the wireless air interface [15]. The management frame message usually carries critical network information. As soon as the information is exposed or maliciously imitated or tampered with, it will cause damage to the communication network. For instance, two important sets of management frames for establishing terminal connections in Wi-Fi networks are association/de-association and authentication/de-authentication request and response frames [6]. These two types of management frames are never encrypted in traditional Wi-Fi network transmission, and these two types of management frames support unicast and multicast methods [11], [15]. This means that if an attacker is in any Wi-Fi group continuously broadcasting de-association requests or de-authentication request messages in the network, it will force all users on the network to disconnect, leading to the denial of service for the entire network and traffic will be paralyzed instantly. Another problem exposed by Wi-Fi networking using the WPA2 encryption scheme is the WPA2 key reinstallation attack (KRACK) vulnerability disclosed by Vanhoef (2017). The key reinstallation attacks occur in the 4-way handshake phase of WPA2 networking. Through the 4-way handshake, both parties

can rely on a pre-shared key or a pairwise master key (PMK) derived from a certificate to negotiate the WPA2 pairwise temporal key (PTK) during the communication. Commonly, the key used for session encryption is generated and installed on the devices of both parties in the third stage of the 4-way handshake [15]. To elaborate, the principle of KRACK's attack is that a fake terminal continuously sends replies that have not received the third handshake message in the third stage of the 4-way handshake, which will cause the PTK in the 4-way handshake to be substituted into the counter as constantly being recalculated and reinstalled. As the number of reinstallation increases, the counter will have a chance to return to the all-zero state [11]. At this time, the PTK generated by the counter will become the all-zero key, and the data transmission applying the encryption will be virtually transparent. As a result, it cannot avoid the passive situation where the encrypted data is completely equal to the plaintext even with the subsequent encryption mechanism of WPA2. After the KRACK vulnerability was disclosed, the United States Department of Homeland Security also released and confirmed the security risks of KRACK, which made the WPA2 encryption method no longer secure [16].

WPA3 security protocol

In view of the unprecedented large number of application scenarios of Wi-Fi technology, the Wi-Fi Alliance launched a new generation of Wi-Fi security scheme named WPA3 in 2018. WPA3 was created in order to protect the privacy and communication security of the vast Wi-Fi application fields and users against evolved cyber threats and attacks. WPA3 technology is the first Wi-Fi protocol using the asymmetric key method in wireless communication. Relying on the most advanced cryptography technology and the increasing computing power worldwide, WPA3 technology is expected to escort the succeeding stage of wireless communication based on Wi-Fi technology [11].

With the rapid development of computer network technology, digital social media, electronic commercial, online business, and other applications have made unprecedented prosperity, and the encryption scheme using symmetric keys as the cryptographic system was gradually showing signs of fatigue. For example, in terms of key management overhead, the network equipment must manage C(n,2)=n(n-1)/2 keys to ensure secure communication between n users, which is not practically affordable for modern Wi-Fi or WLAN data communication. With the explosion of network users, the management of keys has become a heavy burden [16]. In addition, applications represented by e-commerce put forward the need for secret communication between network users who do not know each other, and key distribution is usually performed based on an asymmetric key system under the default sharing mechanism [6], which will not be able to meet novel security requirements as declared above.

The principle of asymmetric keys is that each node in the network that needs to communicate will use a pair of keys for encryption or decryption. The public key is published by the network management center or the key management center, and each communication node stores its own private key. In the stage of session encryption, the message is encrypted and transmitted by the public key, and the message is decrypted by the private key at the recipient's side [16]. The keys used for message encryption and decryption are different, it is thereby an asymmetric key as the name implies. The SAE point-to-point communication key exchange system used in WPA3 encryption is an asymmetric key group generation method represented by elliptic curve cryptography. The elliptic curve equation can perfectly generate a large enough asymmetric key set to suffice the demands of point-to-point communication encryption [6], [11], [16].

Comparison and contrast between the proposed techniques

Both WPA and WPA2 protocols are relatively advanced Wi-Fi security protocols. The difference between the two is that WPA uses the TKIP protocol and WPA2 introduces the CCMP protocol on this basis, which means that 802.11i users can choose one of these two encryption methods. The WPA protocol can be deemed as an upgraded version of the WEP protocol [11]. The reason is that the most important algorithm of TKIP is still the RC4 algorithm, while more stringent improvements have been made in key length and encryption methods to greatly improve the capacity of preventing attacks and cracking. The key to the WPA2 protocol is the introduction of CCMP, and its core algorithm is AES. The AES algorithm effectively overcomes the disadvantages of the RC4 algorithm and improves the security capability. Whereas, the WPA2 can be used only after replacing the hardware, which means that it cannot be used on WEP devices only by upgrading the software. To better achieve the hardware compatibility between WPA and WPA2 protocols, 802.11i was designed to include TKIP compliances [6], [11], [16].

In WPA2, the cipher block chaining message protocol used in CCMP is a designated encryption method. Differentiated from WEP and TKIP's RC4 algorithm, its core algorithm is an AES encryption algorithm

that uses a 128-bit key and a 128-bit data block for encryption operations. This cipher block chaining message protocol has higher hardware requirements and is related to the processor. Thus, the obsolete devices can support WEP and TKIP, while cannot support CCMP/AES encryption [11].

Compared with the WPA/WPA2 protocol, the encryption scheme of the WPA3 protocol cannot only address the security risks in the previous Wi-Fi network communication but also enable a specific management frame protection mechanism for management frames, i.e. the protected management frame (PMF), which is even more effective. The value is to provide more ideal encryption measures in the face of future massive Wi-Fi networking equipment and point-to-point wireless device communications [6], [11], [16]. The bottleneck problem of key management has also been solved. For an increasing number of new Internet applications of e-commerce, the digital signature feature of the public-key encryption scheme that is adopted by the WPA3 protocol can effectively trace the encryption operation of each node, which will have a profound impact on new applications based on Wi-Fi communication mode in the future [11], [16].

Aspects	WEP	WPA	WPA2	WPA3
Release Year	1997	2003	2004	2018
Security Level	Extremely low	Relatively low	Relatively high	Extremely high
Core Encryption	RC4	TKIP with RC3	AES-CCMP	AES-CCMP & AES-GCMP
Key Size	64-bit & 128-bit	128-bit	128-bit	128-bit & 256-bit
Authentication	WEP open & shared	WPA-PSK & 802.1X with EAP	WPA-PSK & 802.1X with EAP	AES-CCMP & AES-GCMP
Integrity	CRC-32	64-bit MIC	CCMP with AES	SHA-2
Pre-Shared Key	PSK	PSK	PSK	SAE
Key Management	None	4-way handshake	4-way handshake	Elliptic curve cryptography methods.
Vulnerability	Brute-force attack, including dictionary attack, vulnerabilities	Brute-force attack, including dictionary attack, vulnerabilities	Brute-force attack, including dictionary attack, vulnerabilities / key reinstallation attack vulnerabilities	No significantly fatal vulnerabilities

Fig. 2: Summary of Comparison and Contrast between WEP, WPA, WPA2 and WPA3

IV Unsolved Technical Challenges

Despite the protocol improvements that have been provided by WPA3, there are still several Wi-Fi security problems that have not been resolved. The unsolved tasks raised in the report by Kohlios are shown in the Fig.3 [17].

Attack	Solved by WPA3
Deauthentication	Yes
Handshake Capture Dictionary Attack	Yes
PMKID Hash Dictionary Attack	Yes
Rouge Access Point	Partially
Evil Twin Attack	No
Handshake Capture En/Decryption	Yes
KRACK Exploit	Yes
ARP Spoofing	Partially
SSL Stripping	No
DNS Spoofing	No

Fig. 3: Attack table

Evil Twin Attack

The Evil Twin Attack is an attack that extends the Rogue Access Point. Specifically, it is a method attackers use to obtain the MITM status by inducing the user to accidentally connect to a malicious AP that is set up in a place where the user can physically reach [17]. By mimicking the existing AP's SSID and MAC address, a malicious AP capable of outputting an illegal level of a signal attracts the users to access the wrong AP without even realizing it. The attack method is effective primarily when targeting APs in public places, and is more intimidating because it targets multiple users [18]. In order to block unintentional access to the AP, a common countermeasure is to pop up notifications and warnings stating 'this is an unidentified network' to users. However, using methods such as warnings/notifications is not effective to block users from voluntarily accessing an unsecured network[19].

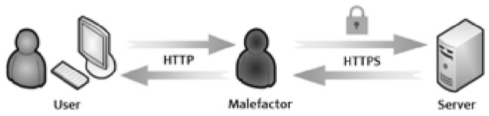

Fig. 4: SSL Stripping

SSL Stripping

Secured Socket Layer (SSL) Stripping is an attack method targeting users who use a website to which HyperText Transfer Protocol Secure (HTTPS) is applied when the MITM status is achieved [17]. An attacker with MITM downgrades the user's website access from HTTPS to an unencrypted HTTP. As shown in the Fig. 4, the information sent by the user is transmitted to the attacker without encryption, and the attacker communicates with the secured site based

on this information[19]. Since it is an attack method that assumes that the MITM state is obtained, so the attack that can be effectively stopped by preemptively blocking MITM. However, the development of protocol security targeting SSL stripping as a double security aspect seems to be a way to increase security.

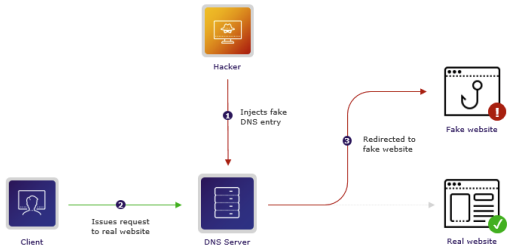

Fig. 5: DNS spoofing

DNS Spoofing

As shown in the Fig.5, assuming that the MITM state has been obtained, Domain Name Server(DNS) Spoofing is one of an attack stealing critical information by leading the user to a convincingly disguised fake website[20]. Users who access a similarly duplicated fake site enter their personal information, including various IDs and passwords, and are exposed to serious security threats. As similar with SSL stripping case, countermeasures against DNS spoofing tend to be left to the individual's responsibility. The reason that the response to DNS spoofing remains the responsibility of the individual is that the protocol that enforces the choice of DNS is also related to violating the individual's choice of websites they want to visit freely, so a careful approach is necessary.

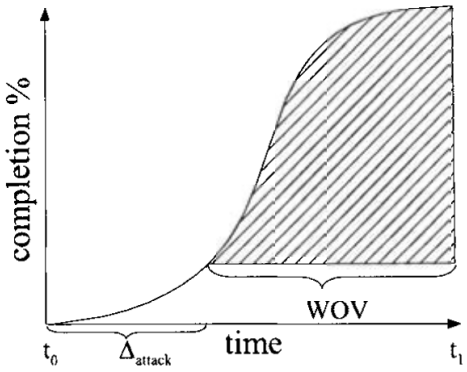

Fig. 6: Window of vulnerability

Zero-day attack

When security vulnerabilities on the state of art protocol are announced, attempts to abuse them until they are fixed or solved is called a zero-day attack. The authors of *IFIP International Information Security Conference*, named the period during which this vulnerability was exerted as Windows of Vulnerability (WOV). As depicted in Fig.6, WOV is the time from the time it takes until the security patch is finally completed, excluding the time period from the time the vulnerability is announced to the adversary preparing for an attack [21]. If the organization that discovers the vulnerability is the one who developed the operating system or protocol, it is possible to secure stability by dividing the patch twice. On the contrary, if adversary discovers this security vulnerability and publishes it, it is almost impossible to deal with it, and the resulting WOV increases. The situation worsens when adversary developed attack tools are maliciously disclosed. The attack case against the National Security Agency (NSA) in 2017 is a representative case in which the situation became serious caused by an adversary. To prepare for a malicious zero-day attack, the layer of security is thickened so that even if a vulnerability is found in one security, the rest of the security can effectively block it. In other words, it is necessary to study a method for thickening the security layer.

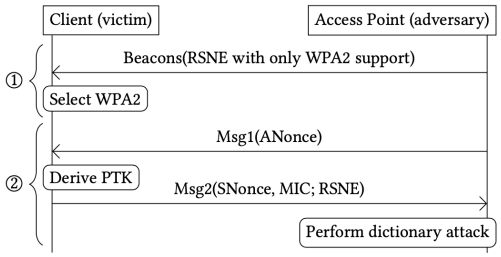

Fig. 7: Dictionary attack exploiting Transition mode

Vulnerabilities in WPA3

Simultaneous Authentication of Equals (SAE) adopted in WPA3 is equipped with a transition mode for compatibility with users using WPA2. However, *2020 IEEE Symposium on Security and Privacy* found that in this mode, a hacker can recover the network password through the previously existing WPA2 security attacking methods such as KRACK and PMKID [2]. The flow of attack is called a downgrade attack. As shown in the Fig. 7, the adversary makes the state vulnerable to security by forcing the hardware containing WPA3 to use only WPA2 and to disable the countermeasure for KRACKs and PMKID [2].

In addition to downgrade attacks using SAE compatibility, there is the vulnerability against the attack that exploits the high overhead of Dragon

fly-handshake used in WPA3. The Dragon Fly Handshake performs a hash-to-curve operation, which has a high overhead. By exploiting such high overhead, it is possible for an attacker to impersonate a user and transmit a commit frame, and to deliberately delay the response speed at the access point with subsequent attacks to perform a DOS attack. Dragon Blood is considered the most challenging task as of now. Since a problem that has occurred in the latest security protocol WPA3, it is a problem that must be treated in the shortest time, and must it be corrected before WPA3 becomes more common.

V Conclusion

The security of Wi-Fi has become increasingly important over time as the usage of the technology grow more frequent and in higher volume. In this survey project, it showed the concepts of the basic hardware that composes a WLAN. It discussed how the security protocol developed over time, and the reasons behind the different iterations from WEP to the modern WPA3. Additionally, the report presented the current challenges that exist for the WPA3 protocol, slowing the adoption rate of this iteration as no solution has yet been developed. Finally, the following assignment will implement a simulation and countermeasure for the Dragonblood vulnerabilities in a WPA3 access point. The predicted difficulty is that the Wi-Fi network simulation should be conducted at a close distance, but since face-to-face meetings due to COVID-19 are difficult, the project's efficiency will decrease. Moreover, having a device that supports WPA3 is expensive in terms of hardware. Since research cannot be conducted together in one network, this part is considered to be a significant limitation.

VI Group Member Contributions

Boyuan Gao : Responsible for completing sections 2 and 3.

Michael Jereza : Responsible for writing slides, presentation, abstract, conclusion, editing, and proofreading.

Inyong Kim : Responsible for writing abstract, sections 1, 4, and 5. Responsible for synthesizing reports in Overleaf form.

References

[1] D. Buil-Gil, F. Miró-Llinares, A. Moneva, S. Kemp, and N. Díaz-Castaño, "Cybercrime and shifts in opportunities during covid-19: a preliminary analysis in the uk," *European Societies*, pp. 1–13, 2020.

[2] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 517–533.

[3] V. Jones and H. Sampath, "Emerging technologies for wlan," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 141–149, 2015.

[4] D. Bhaskar and B. Mallick, "Performance evaluation of mac protocol for ieee 802. 11, 802. 11ext. wlan and ieee 802. 15. 4 wpan using ns-2," *International Journal of Computer Applications*, vol. 119, pp. 25–30, 06 2015.

[5] S. Banerji and R. S. Chowdhury, "On ieee 802.11: Wireless lan technology," *International Journal of Mobile Network Communications Telematics*, vol. 3, no. 4, p. 45â64, Aug 2013. [Online]. Available: http://dx.doi.org/10.5121/ijmnct.2013.3405

[6] S. Malgaonkar, R. Patil, A. Rai, and A. Singh, "Research on wi-fi security protocols," *International Journal of Computer Applications*, vol. 164, no. 3, pp. 30–36, Apr 2017. [Online]. Available: http://www.ijcaonline.org/archives/volume164/number3/27465-2017913601

[7] D. Coleman, *CWSP: certified wireless security professional study guide CWSP-205*, second edition ed. Indianapolis, IN: John Wiley and Sons, 2017, oCLC: on1005831581.

[8] M. Waliullah and D. Gan, "Wireless lan security threats vulnerabilities," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 1, 2014. [Online]. Available: http://dx.doi.org/10.14569/IJACSA.2014.050125

[9] A. Sari and M. Karay, "Comparative Analysis of Wireless Security Protocols: WEP vs WPA," *International Journal of Communications, Network and System Sciences*, vol. 08, no. 12, pp. 483–491, 2015. [Online]. Available: http://www.scirp.org/journal/doi.aspx?DOI=10.4236/ijcns.2015.812043

[10] V. Deotare, S. Wani, and S. Shelke, "Wired equivalent security algorithm for wireless lan."

[11] B. I. Reddy and V. Srikanth, "Review on wireless security protocols (wep, wpa, wpa2 & wpa3)," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2019.

[12] A. Sari, M. Karay *et al.*, "Comparative analysis of wireless security protocols: Wep vs wpa," *International Journal of Communications, Network and System Sciences*, vol. 8, no. 12, p. 483, 2015.

[13] M. Prastavana and S. Praveen, "Wireless security using wi-fi protected access 2 (wpa2)," *International Journal of Scientific Engineering and Applied Science (IJSEAS)*, vol. 2, pp. 374–382, 2016.

[14] M. Rana, M. Abdulla, and D. Arun, "Common security protocols for wireless networks: A comparative analysis," *International Journal of Psychosocial Rehabilitation*, vol. 24, pp. 3887–3896, 04 2020.

[15] S. Malgaonkar, R. Patil, A. Rai, and A. Singh, "Research on wi-fi security protocols," *International Journal of Computer Applications*, vol. 164, no. 3, pp. 30–36, 2017.

[16] V. Poddar and H. Choudhary, "A comparitive analysis of wireless security protocols (wep and wpa2)," *Int. J. Ad Hoc Netw. Syst*, vol. 4, no. 3, pp. 1–7, 2014.

[17] C. P. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," *Electronics*, vol. 7, no. 11, p. 284, 2018.

[18] P. Shrivastava, M. S. Jamal, and K. Kataoka, "Evilscout: Detection and mitigation of evil twin attack in sdn enabled wifi," *IEEE Transactions on Network and Service Management*, vol. 17, no. 1, pp. 89–102, 2020.

[19] N. Sombatruang, L. Onwuzurike, M. A. Sasse, and M. Baddeley, "Factors influencing users to use unsecured wi-fi networks:

Evidence in the wild," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019, pp. 203–213.

[20] S. V. Vliet, "What is dns poisoning? (aka dns spoofing)." [Online]. Available: https://blog.keyfactor.com/what-is-dns-poisoning-and-dns-spoofing

[21] H. Johansen, D. Johansen, and R. van Renesse, "Firepatch: Secure and time-critical dissemination of software patches," in *IFIP International Information Security Conference*. Springer, 2007, pp. 373–384.