Exploring the vulnerabilities of WiFi hacking through different lenses

1st Ryan Freas
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
ryanfreas19@augustana.edu

2st Elnatan Mesfin Tesfa
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
elnatanmesfintesfa20@augustana.edu

3st Max Sellers
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
maxsellers20@augustana.edu

4st Paul Addai
Dept of Math and Computer Science
Augustana College
Rock Island, Illinois
pauladdai19@augustana.edu

***Abstract*—Wireless Fidelity, better known as "Wi-Fi," is a family of wireless network standards and protocols. These protocols are most often used for local area networking (LAN) of devices and for internet access, allowing devices that are in close proximity to exchange many different types of data. A router is a device that interacts with a Wi-Fi network, controlling all of the traffic between devices connected to the Wi-Fi signal and the internet. In our paper, we will describe how someone may attempt to breach your wireless network and steal your sensitive information. This is known as Wi-Fi hacking. We will also compare and contrast the different types of Wi-Fi security protocols. The words Wi-Fi, wireless network, and wireless connection, may be used in the same context as one another throughout the paper.**

***Index Terms*—Wi-Fi, Wi-Fi signal, wireless network, Wi-Fi hacking, cyber attack**

I. Introduction

The pace of life in the 21st century is exhausting. It seems like we can never get a break from communication; whether our communication is in the form of texting with a friend or looking up a question on the web, we are always compelled to pull out a device that is connected to the internet. Whether we like it or not, this is how life is and consequently, our life is governed by the signals being sent and received from these devices. The entity that governs these interactions is called Wi-Fi. Wi-Fi uses radio waves to transmit these signals between a router and your device via frequencies. Although a wireless connection makes communication easy and convenient, it is also susceptible to cyber attacks. When your network is breached via your Wi-Fi signal, this is known as W-Fi hacking [14]. Wi-Fi hacking means that the security protocols in your wireless network were cracked, consequently granting a hacker full access to any information transmitted over that network. The things that an attacker may have access to includes but is not limited to the following: any web pages you visit, your IP address, any saved info on your browser such as passwords/browsing history, and any important financial information that is saved within your device. The motives of these 'Wi-Fi hackers' can include selling your information or impersonating you to take money out of your bank account. One important thing to note is that your connection to public Wi-Fi is more susceptible to being hacked than on your home Wi-Fi.

II. Related Work

WiFi networks has become accessible and can be found almost everywhere in our society. Most of these networks are protected by passwords and also username which prevents unauthorized user from accessing it. Due to this, a lot of people has discovered also ways to access these networks using various hacking tools such as aircrack-ng which is usually used for cracking WEP/WPA/WPA2 logins/passwords, Reaver, Pixiewps, etc. These types of tools or softwares allows attackers with little knownledge or no form of experience to easily launch an attack on a WiFi network.

There was a research paper that talked about the entire process of cracking a (Wired Equivalent Privacy) encryption of WiFi [16]. It focused on finding the vulnerabilities related to 802.11-based wireless networks to help secure them. They were about to launch an attack using tools such as Cain and Abel which is a popular password cracking tool along with NetStumbler, Kismet and MiniStumbler.

WiFi calling has become popular in our societies nowadays which also draw the attention of hackers. There was another research paper that explores the vulnerabilities of WiFi calling and how the attacks are launched and how to prevent these attacks [17]. It explained that the key issue is connecting to unsecured WiFi networks which exposes users to security threats. The researchers discovered two proof-of-concept attacks which were telephony harassment or denial of voice service and user privacy leakage. These two attacks were about to bypass the existing security defenses and to

provide a solution to this vulnerability, WiFi Calling Guardian was invented which seeks to reduce overall damage in case of any attack. WiFi Calling Guardian working by first checking the status of a WiFi connection whether WPA3 is enabled and lastly check the ARP table on the client device to verify if two devices share the same MAC address. If two devices share the same address, then it is likely that there is an ARP spoofing attack hence the connection is not safe.

A. Hacking Encrypted WiFi Networks

Encrypted wifi networks can also be hacked. There was a research done to investigate how the encryption protocols Wired Equivalent Privacy(WEP) can easily be attacked. WEP put in place safeguards to prevent the most obvious attacks on the protocol. These attacks entail decrypting ciphertexts encrypted with the same keystream as well as flipping bits in the cipher stream and seeing which bits are flipped in the resulting plaintext. [1].They discovered that while WEP provided safeguards against these attacks, it did so inadvertently, making it conceivable for an attacker who listens to enough data to crack a WEP key. The invader only needs to gather enough traffic to run a statistical analysis and find the key in order to access a WEP network. In contrast, they discovered that the WPA's handshake is its greatest weakness. During the four-step process of logging on to an access point, a client exchanges the hash of the access point's key, which is then utilized for the duration of the session and rotated on a per-packet basis. [1]. The Service Set Identifier (SSID) of the access point, which is the name of the wireless network, is added to the hash. It is possible for the attacker to recover the key if they can deduce it from that hash. Utilizing the rainbow table is feasible. A 40GB lookup table known as the coWPAtty database was created by the Church of WiFi, a disparate group of wireless security experts, using a list of a million passwords salted with the top 1000 SSIDs [1]. In a reauthentication attack, the attacker only needs to remove a trustworthy client from the network and force it to reauthenticate.

B. Packet Injection Exploiting Attack

Using OpenFlow technology, software-defined networking (SDN) decouples the control plane from the data plane and enables flexible network control. It has received a lot of attention in the future network and is used widely in many different fields. As the SDN has grown, its security issue has emerged as a pressing area that requires research. Researchers suggest to learn the packet injection exploiting attack. Attackers can further leverage them by fraudulently introducing bogus hosts into the SDN network topology to conduct a denial of service (DoS) attack. The results have an impact on the controller's throughput and processing power, severely deplete data plane resources, and ultimately have an impact on the entire network.

How the packet injection attack works is described in a series of steps [10]:

1) : Through host A, the attacker transmits a large number of packets to the SDN network with falsified source MAC addresses.

2) : There isn't a matching forwarding rule in the flow table when the switch gets an unknown data packet from host A. It will forward the packet to the controller after encasing it in a Packet-In message.

3) : The SDN controller will get the Host Profile file when it receives a Packet-In message from the switch. The host tracking service will believe a new host has joined the network because the attacker spoofs the source MAC address, as explained in Section 2, adding a phony host to the SDN topology.

4) : The attacker can then create particular packets through host B, identify the destination MAC address as a forged fake MAC address, produce the destination IP address or port at random, and send the packet to the SDN network after injecting numerous false hosts.

5) : The SDN topology now includes the bogus hosts, thus the controller won't be able to remove these erroneous packets from host B. This is the aspect of the assault that differs the most from the one that fakes the target MAC address. The controller installs flow table rules to the switch and determines the forwarding strategy for unidentified packets.

6) : The controller's processing power and the switches' flow tables will be overloaded if the attacker often sends unknown packets through host B. These mismatched flows would also use an excessive amount of the southbound interface's capacity, potentially affecting the entire network. To confirm the viability and effectiveness of the packet injection exploitation attack, experiments were run in a software environment. Mininet simulates the experiment topology [10]. The southbound interface is Openflow1.3, and the controller they choose is Floodlight v1.2. To mimic the attack, they choose h1 and h6 (of the 6 hosts) as the attacking hosts and the rest as regular network users. The host h1 injects phony hosts into the SDN network using Scapy, a potent interactive packet manipulation software, and the host h2 launches a DoS attack using these fake hosts. The host h1 creates data packets and periodically injects them into the test network. The built-in RandMAC() function of Scapy that was used to construct the source MAC address of the forged data packet, and the destination MAC and IP address refer to the host h6. As additional device information is not intuitively displayed by Floodlight, they modify the source code to output the device MAC. As a result, the device management service correctly learns the injected host and adds it to the SDN network topology. They introduced 50 fake devices using this method.

III. Research and Findings

There are 4 Wifi Security protocols upto date. These are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA 2), Wi-Fi Protected Access 3 (WPA 3). Wired Equivalent Privacy is on the older side of Wi-Fi security protocols, dating back to the late 1990's. This protocol came into existence attempting to address how hackers would snoop on wireless data as it was transmitted between clients and APs. Soon after its release, experts identified major faults in the protocol. WEP was used throughout

the industry, but was gradually phased out in the 2000's. This phenomenon happened in both enterprise and consumer devices. The final straw was in 2009, when there was a large scale attack against the retail store T.J Maxx. This attack was carried out by hackers looking to steal information on T.J. Maxx's customers. They were successful because the retailer's WiFi was secured by WEP, which was very vulnerable. Almost 100 million customers got their information stolen. The effects of this attack were so significant that the Payment Industry Data Security Standard began to completely ban retailers from processing important data, such as credit card data, using the Wired Equivalent Privacy protocol. The reason WEP is so vulnerable is because it only uses a 24-bit initialization vector, but this is rather small and the nature of the vector only being 24 bots makes it more likely for users to recycle keys. This makes it easier for the key to be cracked [2].

A. WEP Weakness

There are several weakness in WEP, which are detrimental for the safety of the WiFi networks and have led to several hackers gaining access [7]. Here is a list of some of the weakness that have led to these vulnerabilities:

- WEP does not prevent forgery of packets.
- WEP does not prevent replay attacks. An attacker can simply record and replay packets as desired and they will be accepted as legitimate.
- WEP uses RC4 improperly. The keys used are very weak, and can be brute-forced on standard computers in hours to minutes, using freely available software.
- WEP reuses initialization vectors. A variety of available cryptanalytic methods can decrypt data without knowing the encryption key.
- WEP allows an attacker to undetectably modify a message without knowing the encryption key.
- Key management is lacking.

B. WPA

WPA, or Wi-Fi Protected Access, was a protocol created in response to WEP being exposed as insufficient. WPA as a protocol was only a short term alternative. This was because in reality, it took many years to come up with an advanced and long term replacement for a Wi-Fi protocol. With that said, now that WEP was exposed, the Wi-Fi alliance had to come up with a new protocol fast [9]. WPA has two modes: one is for enterprise users, and the other is for personal use. The enterprise mode, which would handle more data and needed to be more secured, required the use of an authentication server. The personal mode utilized a pre-shared key for easier implementation in smaller offices or for individual consumers. This also made it easier to manage. WPA improved on WEP by using longer keys and a larger initialization vector. The IV for WPA was 48 bits, while the IV for WEP was 24 bits, as we have discussed previously. The WPA protocol was designed to be compatible with the WEP protocol. The reason for this was to encourage a fast and easy transition to using the WPA protocol.

C. WPA Weaknesses

As we have mentioned breifly previously, One of the largest weaknesses in the WPA protocol is something known as KRACK. This stands for Key Re-installation Attack. This attack targets the 4-way handshake in the potocol. In order to maintain a secure key when utilizing WPA, the access point and the user/client have to use an initialization vector. This is the number that is increased and put into the next messagess. The key and the vector form a keystream. This is then used to encrypt the WiFi data. For WPA to maintain security, it is imperative that the keystream is only used a single time [5]. Researchers uncovered a weakness that was revealed when replaying parts of the handshake. This causes the access point to reset, and consequently, the keystream is reused. [3]

D. WPA2

The successor to Wi-Fi Protected Access protocol was WPA2. This standard was published in 2004 by the IEEE (Institute of Electrical and Electronics Engineers). Similiar to WPA, WPA2 offers both an enterprise mode and a personal mode. The improvements WPA2 made upon WPA is as follows: WPA2 replaces the encryption and authentication mechanisms in WPA with more advanced ones called AES (Advanced Encryption Standard) and CCMP (Counter Mode with Cipher Block Chaining Messsage Authentication Code Protocol . The specifics of these mechanisms are complicated, but they are a major improvement over the ones in WPA. With that said, it is important to note that WPA2 requires more computing power than WPA. Improvements in computer hardware have attempted to mitigate these performance worries. WPA2 also featured better roaming, enabling consumers to go from one AP to a different one on the same Wi-Fi without having to re-authenticate themselves. In 2017, a cybersecurity researcher from Belgium discovered a vulnerability in WPA2. This vulnerability exploited the feature of reinstalling encryption keys that were specifically wireless. Hackers can capture and analyze transmissions until they are able to determine what the encrypted key is and gain access to any and all network data [8].

E. WPA2 Weaknesses

Although WPA2 was a major upgrade from WPA and it still is a widely used security protocol, there remain many different vulnerabilities in the protocol. Some researchers have found a collection of exploitations in the WPA2 protocol that were named "FragAttacks." One of these so called "FragAttacks" goes by the name of an "Aggregation Attack." This attack exploits the frame aggregation feature in Wi-Fi. The purpose of this feature is to increase the speed of a network by merging smaller frames into a bigger 'aggregated' frame. These aggregation frames contain a flag that says whether or not the data is aggregated or not, The problem here is that the 'is aggregated' flag is never authenticated. This means that a

threat actor can modify the flag and trick a user into processing data within the frame in a malicious manner. The threat actor can use this to insert network packets by fooling the user into connecting to their server and then altering the 'is aggregated flag' of packets of their choosing. Another vulnerability that falls under the branch of these "FragAttacks" is an attack that is called the Fragment Cache Attack. This is a design flaw that is located within Wi-Fi's frame fragmentation feature. Here, the issue is present when a user disconnects from a network. When they do this, the Wi-Fi device is not forced to get rid of non-reassembled fragments from its memory. A scenario where this can be abused is against hotspot-like networks. The threat actor can inject a malicious fragment inside of the fragment cache of the access point and if the client sends the malicious fragmented frames to the router, it can exfiltrate sensitive data. [15]

F. WPA3

WPA3, the most modern wireless security standard and the one that experts today deem to be the most secure, was certified by Wi-Fi Alliance in 2018. All devices aiming to receive Wi-Fi certification by July 2020 must enable WPA3.

Protected Management Frames, which assist prevent eavesdropping and forgeries, are required by WPA3. It also forbids the use of antiquated security techniques and standardizes the 128-bit cryptography suite. For enhanced protection of confidential business, financial, and governmental data, WPA3-Enterprise offers an optional 192-bit security encryption and a 48-bit IV. AES-128 and CCMP-128 are used by WPA3-Personal [6].

Simultaneous Authentication of Equals (SAE), a variation of the Internet Engineering Task Force's dragonfly handshake in which either client or AP can begin communication, replaces the PSK four-way handshake in WPA3 to mitigate the KRACK issue in WPA2. Then, rather than engaging in a multipart conversation with other devices, each device provides its authentication credentials in a discrete, one-off message. Importantly, SAE forbids the use of encryption keys and demands a fresh code for each communication. Cybercriminals are less able to eavesdrop or interject themselves into an interaction when there isn't open-ended communication between the AP and client or encryption key reuse.

Users are only permitted to make active, on-site authentication attempts, and SAE flags anyone who has attempted too many password guesses. The conventional Wi-Fi network should be more resistant to offline dictionary assaults because of these capabilities. SAE also allows a feature known as forward secrecy, which seeks to prevent attackers who have cracked a passcode from using it to decrypt data they have already acquired and preserved. Forward secrecy works by requiring a new encryption passphrase for each connection.

In addition to WPA3, Wi-Fi Alliance also unveiled a brand-new protocol dubbed Wi-Fi Easy Connect, which streamlines the setup procedure for Internet of Things (IoT) devices by using a mechanism like a QR code scan. Wi-Fi Enhanced Open is a further feature that automatically encrypts data while connecting to public Wi-Fi networks, making it safer to do so.

In practice, of course, WPA3 is not impervious to threats. Vanhoef, the security expert who discovered KRACK, and Eyal Ronen, a researcher at Tel Aviv University, published several new security flaws in WPA3 in 2019. The so-called Dragonblood vulnerabilities included two downgrade attacks, in which an attacker forces a device to revert to WPA2, and two side-channel attacks, which enable offline dictionary attacks. Wi-Fi Alliance downplayed the risks, however, saying vendors could readily mitigate them via software upgrades. Regardless of its potential vulnerabilities, experts agree WPA3 is the most security wireless protocol available today [13].

From our research most of the WiFi password cracking tools works best on WEP and WPA. This due to the fact that these protocols have some security flaws in them which make them vulnerable to attacks. Comparing the two, WPA is more secure than WEP because it uses a 256-bit key for encryption which is larger than 64 and 128-bit key for WEP.

In the WPA3 authentication protocol, there was also a vulnerability found. A race-condition attack can take advantage of the bad-token vulnerability to deny Wi-Fi clients service. In order to prevent trustworthy clients from joining to a WPA3 network, the attacker delivers fake authentication messages that are compromised with a faulty token (WPA3 authentication confirm value). Moreover, WPA3 is susceptible to two denial-of-service attacks linked to WPA2 as well. Using Linux software tools hostapd-2.7 and wpa supplicant-2.7 on Raspberry Pis, an experiment was conducted to test the WiFi vulnerability. The experiment demonstrated the impact of the attack on a legitimate WPA3 network using the WPA3-SAE mechanism [11].

G. Password Cracking

Brute force assaults have been present since the early 1990s, when a DOS program named L0phtcrack first surfaced. In these attacks, the hacker iterates through all conceivable combinations of the alphanumeric characters that make up a password. The discovery made by L0phtcrack was that hashes are one-way processes, in contrast to rainbow password attacks, which take use of the fact that passwords are typically stored as a hash function's output [4]. It is simply not possible for a hacker to recreate a password using only the hash value, even if they had access to the hashed version of the password. Rainbow tables, which are enormous, pre-calculated lists of hash values for each possible combination of characters within a given set, can, nevertheless, be used to decipher the hashed value of your password. These tables speed up brute force password cracking procedures considerably, but they consume a substantial amount of computer memory or hard drive space—typically 2 TB or more. In essence, you exchange memory and storage space for a faster password-cracking timescale.

Another way to crack the WiFi password is by creating a Brute Force Dictionary using Crunch. Crunch is a wordlist generator where you can specify a standard character set or

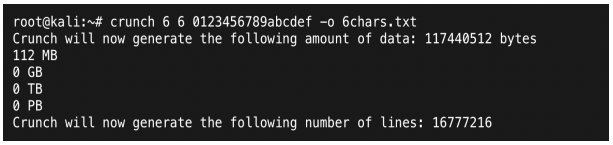

Fig. 1. Crunch Tool Usage

Fig. 2. iwconfig command in the terminal

any set of characters to be used in generating the wordlists. The wordlists are created through combination and permutation of a set of characters and you can determine the amount of characters and list size. The Brute Force Dictionary will take up a lot of disk space. For example, it will produce 5, 925, 787, and 425GB file size, containing 636, 954, 190, 679, 126, and 528 passwords to create a length of 1-to-12-bit dictionary, containing the uppercase and lowercase letters, numbers, underscores, spaces, special characters. Figure 1 also shows a similar example where we are generating a dictionary file containing words with a minimum and maximum length of 6 (6 6) using the given characters (0123456789abcdef), saving the output to a file (-0 6chars.txt).

Numerous systems, including web servers, routers, switches, firewalls, IDS/IPS, web applications, domain systems, and database systems are set up with weak or default passwords. [18] These passwords are simple to crack and judge. Strong passwords are advised for this, and default passwords should be avoided. For instance, let's say we buy a D-Link wireless access point for home use. It is set up using the login "admin" and password "admin" by default. By using these password strategies, any attacker has simple access to our wireless network. Therefore, passwords need to be updated frequently and be difficult so that hackers cannot access our system.

H. WiFi Cracking

The WiFi access point (AP) uses radio waves to disseminate its information to the surrounding area. Before the penetration test starts, the penetration tester needs a network card that supports a promiscuous mode of operation in order to have access to all the data flowing through the test site. A promiscuous mode network card can read all the data that flows through it, whether or not the destination address is it. We must first put the network into monitor mode before scanning the target network to get its essential data, such as the number of APs, working channel, signal strength, and client-specific data. Find the wireless router's name and the concealed Service Set Identifier (SSID). The AP typically broadcasts its own SSID, but for security reasons, it hides it to safeguard the WiFi network, allowing only clients who are aware of the SSID to connect to the AP. A disguised SSID does not, however, adequately safeguard the WiFi network. Genuine clients that connect to the AP exchange authentication information that includes non-encrypted SSID information. On WiFi networks with disguised SSIDs, penetration tests are carried out by extracting the SSID. Only clients with a valid MAC address are allowed to connect to some APs that have the MAC address filter function enabled. The goal of client MAC logging is to find a solution for MAC filtering protection. MAC address filtering prevents the attacker from connecting to the WiFi network by allowing only authorized MAC clients to connect to the AP. This safeguards the WiFi network. The AP is tricked by sniffing the legitimate MAC and then logging in under the cover of the authentic MAC because the MAC information is not encrypted. Monitoring of a certain target network can be implemented after getting accurate information about the target network. The attack is reinjected once the modified legitimate data packet has been intercepted in listening mode. [12] By listening to the target network and obtaining the target AP's genuine data, it may also analyze. WiFi Protected Setup (WPS), Wired Equivalent Privacy (WEP), and WiFi Protected Access (WPA) are currently the three main authentication encryption mechanisms used by WiFi networks. In order to successfully crack a password, one must first study the encryption mechanism used by the target network. For instance, in order to crack the WEP password, we must collect a sizable amount of data from the client and AP for analysis and calculation. In order to decrypt WPA, we must first take the four handshake protocol packets sent between the legitimate client and the AP, evaluate them, and determine the access codes.

IV. Our Experiment

We attempted to crack a WiFi network using a raspberry pi computer. We attempted to perform a dictionary attack on a network using a program Aircrack. This program generates passwords to brute force attack a WiFi network at an extremely fast rate. Even though this attack may not always crack the password, it is extremely easy to perform and can has the potential to break into many different networks. Aircrack is used to assess WiFi security and has many features. These includes monitoring. The program can capture packets and export the information it finds to text files for further analysis. It can also perform many types of attacks such as replay attacks, packet injection, and dictionary attacks. In our experimentation, we discovered that the raspberry pi is insufficient to perform the types of attack we wanted to carry out. We needed something more powerful. Instead of using the raspberry pi, we opted to use a VM (virtual machine) hosted on a macbook. We then used Kali Linux, an operating system for penetration testing, ethical hacking, and network security assessments to perform the attack.

With Kali Linux, we open the Kali terminal and install aircrak-ng feature. In the terminal we initiate airmon-ng which

is used to monitor the Wi-Fi. Then we selected the monitor name we wanted to crack. After that we used the "iwconfig" command 2 to enable monitoring the Wi-Fi. Next, we used the command "airodump-ng mon0" get all of the router names. The terminal lists all of the routers in our surrounding area but we targeted our mobile hotspot connection. The list of routers included all of the basic information we needed for each router, but we needed specific information in order for the hack to work properly. Next, we had to make sure that the router was WPA or WPA2 Security and we found this out by making sure our hotspot had it's WPA name. After we made sure it was WPA or WPA2, we selected our hotspot. Once that ran it automatically created a .cap file which we renamed to our hotspot name. Next, we used the dictionary keylist txt file generated by crunch to help launch a dictionary attack on the wifi. Since this was just an experiment to prove to others than wifi passwords can be hacked, we used a simple password ("123456abc") on the first trial.

V. Conclusion

WiFi has been revolutionary in our every day lives. It allows us to connect to the internet wherever we want in a convenient manner. Although the security protocols started out as primitive, they progressively advanced, becoming more and more secure. Even though the WEP protocol is considered prehistoric and obsolete at this point, it was once seen as a secure protocol. Obviously, we can crack a network secured by WEP in many different ways today, but this was always not the case. The same can be seen in the other protocols, such as WPA and WPA2. At the time of their release, they were certainly far better than their predecessors. Unfortunately, hackers with malicious intentions always catch up to the security experts. As such, the protocols WPA and WPA2 are now seen as insufficient. Today, we have the most secure protocol named WPA3. Even though it is the most secure, clients have trouble adopting it, as it can be costly and complicated to change entire systems. Additionally, despite the fact that it was just recently released, there have already been a few flaws discovered. It is important to note how susceptible these security protocols can be to attacks. Even primitive types of attacks such as dictionary attacks work on WEP, WPA, and even WPA2. As we can see, there are many different ways to take advantage of a vulnerability in a system. With too many variables and possible flaws in a protocol, it is necessary to always try to stay one step ahead of the hackers. This is why bodies such as the Institute of Electrical and Electronics Engineers and the WiFi alliance exist.

References

[1] Danny Bradbury. Hacking wifi the easy way. *Network Security*, 2011(2):9–12, 2011.

[2] Matthieu Caneill and Jean-Loup Gilis. Attacks against the wifi protocols wep and wpa. *Journal, no. December*, 2010.

[3] Dávid János Fehér and Barnabás Sandor. Effects of the wpa2 krack attack in real environment. In *2018 IEEE 16th international symposium on intelligent systems and informatics (SISY)*, pages 000239–000242. IEEE, 2018.

[4] Steve Gold. Cracking wireless networks. *Network Security*, 2011(11):14–18, 2011.

[5] Mahmoud Khasawneh, Izadeen Kajman, Rashed Alkhudaidy, and Anwar Althubyani. A survey on wi-fi protocols: Wpa and wpa2. In *International conference on security in computer networks and distributed systems*, pages 496–511. Springer, 2014.

[6] Christopher P Kohlios and Thaier Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 7(11):284, 2018.

[7] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, and Seema Shrawne. Vulnerabilities of wireless security protocols (wep and wpa2). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 1(2):34–38, 2012.

[8] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, and Behrang Samadi. A survey on wireless security protocols (wep, wpa and wpa2/802.11 i). In *2009 2nd IEEE international conference on computer science and information technology*, pages 48–52. IEEE, 2009.

[9] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, and Behrang Samadi. A survey on wireless security protocols (wep, wpa and wpa2/802.11i). In *2009 2nd IEEE International Conference on Computer Science and Information Technology*, pages 48–52, 2009.

[10] Jishuai Li, Sujuan Qin, Tengfei Tu, Hua Zhang, and Yongsheng Li. Packet injection exploiting attack and mitigation in software-defined networks. *Applied Sciences*, 12(3), 2022.

[11] Karim Lounis and Mohammad Zulkernine. Bad-token: denial of service attacks on wpa3. In *Proceedings of the 12th International Conference on Security of Information and Networks*, pages 1–8, 2019.

[12] He-Jun Lu and Yang Yu. Research on wifi penetration testing with kali linux. *Complexity*, 2021, 2021.

[13] B Indira 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*, pages 28–35, 2019.

[14] S Vinjosh Reddy, K Sai Ramani, K Rijutha, Sk Mohammad Ali, and CH Pradeep Reddy. Wireless hacking-a wifi hack by cracking wep. In *2010 2nd International Conference on Education Technology and Computer*, volume 1, pages V1–189. IEEE, 2010.

[15] Mathy Vanhoef and Frank Piessens. Advanced wi-fi attacks using commodity hardware. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 256–265, 2014.

[16] S Vinjosh Reddy, K Sai Ramani, K Rijutha, Sk Mohammad Ali, and CH. Pradeep Reddy. Wireless hacking - a wifi hack by cracking wep. In *2010 2nd International Conference on Education Technology and Computer*, volume 1, pages V1–189–V1–193, 2010.

[17] Tian Xie, Guan-Hua Tu, Bangjie Yin, Chi-Yu Li, Chunyi Peng, Mi Zhang, Hui Liu, and Xiaoming Liu. The untold secrets of wifi-calling services: Vulnerabilities, attacks, and countermeasures. *IEEE Transactions on Mobile Computing*, 20(11):3131–3147, 2021.

[18] Irfan Yaqoob, Syed Adil Hussain, Saqib Mamoon, Nouman Naseer, Jazeb Akram, and Anees ur Rehman. Penetration testing and vulnerability assessment. *Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org*, 7(8), 2017.