Wi-Fi Security: Do We Still Have to Look Back?

Karim Lounis
Intelligent Systems Engineering Department
The National School of Artificial Intelligence
Sidi AbdAllah, Algiers, Algeria
karim.lounis@ensia.edu.dz

***Abstract*—Wi-Fi is a wireless communication technology that has been around since the late nineties. Nowadays, it is the most adopted wireless short-range communication technology in various IoT (Internet of Things) applications and on many wireless AI (Artificial Intelligent) systems. Although Wi-Fi security has significantly improved throughout the past years, it is still having some limitations. Some vulnerabilities still exist allowing attackers to generate different types of attacks. These attacks can breach the authentication, confidentiality, and data integrity of Wi-Fi systems. At the same time, many vulnerabilities have been fixed or patched, and the attacks that were relying on those vulnerabilities would fail on modern Wi-Fi systems. Therefore, it is important for security engineers, in general, and for wireless intelligent system designers, in particular, to be aware of the existing vulnerabilities and feasible attacks on modern Wi-Fi systems and their respective countermeasures. That would help them to not have to look back and care about attacks that can no longer be generated on today's Wi-Fi systems. In this light, we devote this paper to extensively review the attacks on Wi-Fi. We group the attacks into feasible and unfeasible. Also, for each attack, we discuss the possible countermeasures to mitigate it.**

***Index Terms*—Wi-Fi, Wi-Fi Security, and Wi-Fi attacks.**

I. Introduction

WI-FI technology is being widely adopted as a short-range wireless communication technology for many IoT (Internet of Things) applications, such as smart homes and healthcare. The technology is also embedded in many AI (Artificial Intelligent) systems. Nevertheless, due to the new security concerns introduced by new computing and networking paradigms, such as IoT and AI systems, the security of Wi-Fi systems, in general, and Wi-Fi devices, in particular, has increased and it has become a serious issue. Another issue is that many people are still promoting the feasibility of some attacks that rely on fixed, patched, or even eradicated vulnerabilities. Security and Wi-Fi systems engineers must have a concise reference that catalogs the attacks that are still feasible and the attacks that are no longer feasible on modern Wi-Fi systems. Furthermore, in this new type of computing environment, the impact of attacks is not limited to data being stolen as it use to be in classical Wi-Fi systems but may also include the loss of humans. Thus, the impact of attacks has to be known so as the countermeasures to mitigate these attacks.

The current literature about Wi-Fi security usually presents Wi-Fi attacks that are either a variant of known attacks or attacks that are no longer possible. Only a few of them present new attacks. Also, there are many research works that provide a classification of Wi-Fi attacks, regardless of their feasibility on modern Wi-Fi systems. Therefore, we devote this paper to extensively review the attacks on Wi-Fi by grouping them into feasible and unfeasible. Also, for each attack, we discuss the possible countermeasures to mitigate it.

The rest of the paper is organized as follows. In Section II, we provide an overview of Wi-Fi and present its security mechanisms. In Section III, we extensively review various attacks on Wi-Fi and discuss their possible countermeasure. We group the attacks into feasible and unfeasible based on their feasibility on modern Wi-Fi systems. Also, for better readability and referencing, we arrange these attacks based on the security service that each attack aims to compromise. We consider authentication, confidentiality, integrity, and availability. We conclude the paper in Section IV.

II. Wi-Fi Communication Technology

A. Wi-Fi Overview

Wi-Fi (Wireless Fidelity) is a wireless communication technology based on the IEEE 802.11 standard. It allows the construction of WLANs (Wireless Local Area Networks) over both unlicensed radio bands, the 2.4 GHz ISM (Industrial Scientific and Medical) band and the 5 GHz UNII (Unlicensed National Information Infrastructure) band. It was first introduced in 1999 allowing the implementation of WLANs over a short range with a basic transmission rate of 2Mbps. Later, Wi-Fi significantly evolved in many aspects, such as power management, quality of service, data rate, infrastructure modes, and security. Nowadays, a Wi-Fi network can send data at 6.75Gbps [1] and reach a range up to 382km [2]. It is commonly used in domestic places, such as houses, hotels, hospitals, universities, and enterprises.

Wi-Fi allows the construction of WLANs following four different configurations: Infrastructure, Ad Hoc, bridge, and repeater. The first two modes define how Wi-Fi devices can directly or indirectly communicate with each other, whereas, the last two modes define how to extend the range of a Wi-Fi network. In the infrastructure mode, an access point, called coordinator, controls and coordinates a certain number of wireless devices called wireless clients or stations (viz., Fig. 1). These wireless stations have to be associated and authenticated to the access point to be fully connected to the network. The set of wireless stations along with the access point constitutes a BSS (Basic Service Set) structure which is identified by a BSSID (Basic Service Set Identifier).

Fig. 1. Interconnection of Wi-Fi smart and AI devices.

This BSSID corresponds to the MAC address[1] of the access point. When multiple BSSs are connected, they form an ESS (Extended Service Set) structure identified by an ESSID (Extended Service Set Identifier) or SSID (Service Set Identifier). In an Ad Hoc mode however, wireless devices connect to each other to form different flexible network architectures such as mobile and mesh networks. In such network configurations, each wireless device can be both a wireless station and a wireless coordinator. The set of all connected wireless stations forms the structure of an IBSS (Independent Basic Service Set) identified by an SSID.

Wi-Fi adopts the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) protocol to access the radio channel. This protocol allows Wi-Fi devices to send their data while avoiding collisions by applying the binary exponential back-off algorithm. In the exponential back-off algorithm, Wi-Fi devices promptly sense the radio channel for its availability and back off for a random time if the channel is busy. If a Wi-Fi device detects that the radio channel is not busy, it starts transmitting its data (i.e., IEEE 802.11 frames).

B. Wi-Fi Security

Wi-Fi technology provides a number of security mechanisms. In the following paragraphs, we briefly present these mechanisms that help understand the reviewed Wi-Fi attacks and countermeasures. Interested readers are referred to the IEEE 802.11 specification documents [3] for more details.

WEP (Wired Equivalent Privacy). This security mechanism was introduced as part of the IEEE 802.11 standard in 1997 to provide authentication, encryption, and data integrity. For authentication, WEP provides two security modes, the OSA (Open System Authentication) and the SKA (Shared Key Authentication). In the first mode, any Wi-Fi station can get connected to any access point that adopts this mode. The second mode however, is based on the use of a pre-shared secret key and a challenge-response protocol. If a Wi-Fi station proves to the access point the right possession of the secret key, it gets authenticated. For encryption, WEP applies the RC4 (Ron's Code 4) stream cipher algorithm along with an encryption key and uses the CRC-32 algorithm to generate an ICV (Integrity Check Value) code for data integrity.

IEEE 802.11i Standard. Few years after WEP was shown to be containing serious vulnerabilities [4]–[8], the IEEE proposed the 802.11i framework [9]. This framework provides stronger security mechanisms for authentication, encryption, and data integrity. Notwithstanding, due to the high demand and pressure for a secure solution to be implemented and released, the Wi-Fi Alliance quickly (in April 2003) started certifying devices based on a draft version of 802.11i under the name of WPA (Wi-Fi Protected Access). In June 2004, the final version implementing the 802.11i specification was ratified under the name of WPA2.

The IEEE 802.11i standard defines two possible authentication modes: enterprise mode, also known as WPA-Enterprise, and personal mode, also known as WPA-PSK. In the first mode, an 802.1X infrastructure is adopted. Such infrastructure consists of an authentication server, e.g., RADUIS (Remote Authentication Dial-in User Service); a network controller (authenticator) usually an access point; and the use of the EAP (Extensible Authentication Protocol). This infrastructure allows any Wi-Fi device, also known as a supplicant, to join the network and to be uniquely identified and authenticated. In the second authentication mode, a pre-shared password is used to derive a cryptographic keychain that is used for authentication, encryption, and data integrity. As the IEEE 802.11i standard was not compatible with WEP, two new encryption mechanisms have been introduced, TKIP (Temporal Key Integrity Protocol) and CCMP (CTR with CBC-MAC Protocol) [10]. A third mode called GCMP (Galois Counter Mode Protocol) was introduced in 2012 [1], [11]. Similar to WEP, TKIP mechanism uses RC4 algorithm but with a longer encryption key. It uses Michael algorithm to compute a code called MIC (Message Integrity Code) for data integrity. CCMP however, is more secure as it uses AES (Advanced Encryption Standard)[2] for encryption and CBC-MAC (Cipher Block Chaining-Message Authentication Code) algorithm for data integrity [10].

WPS (Wi-Fi Protected Setup). This security mechanism was introduced by the Wi-Fi Alliance in 2006 to provide an easy and secure procedure to join a Wi-Fi network. Currently, four procedures have been defined: (1) PIN-based procedure, where the user introduces an 8-digit PIN code shown on the new device into the access point memory or vice-versa. (2) PBC (Push Button Configuration), where the user has to simultaneously push a virtual or physical WPS-button on both devices (i.e., access point and the new device). (3) NFC (Near Field Communication), where the user approaches the new

[1]MAC (Media Access Control) address is a 48-bit hardware address uniquely associated to the network interface of a device to connect to a network. This address is generally used at the link and MAC protocol-layer.

[2]AES (Advanced Encryption Standard), also known as Rijndael, is a symmetric cipher established by the U.S. National Institute of Standards and Technology (NIST) in 2001 [12].

device next to the access point so that a near-field contactless authentication can be performed. (4) USB (Universal Serial Bus) mode, where the user needs a USB pendrive to transfer authentication data between Wi-Fi devices.

Opportunistic Wireless Encryption. This mechanism is defined in the RFC810. It aims to add a security layer for Wi-Fi networks that adopt the open system authentication such as public and guest networks. It uses the Diffie-Hellman key establishment protocol [13] to establish a shared key, known as PMK (Pairwise Master Key). This key is then used to derive other keys to guarantee message authentication, confidentiality, and integrity. Note that this protocol allows a Wi-Fi client and an access point to establish a shared secret key without having shared any credentials a priori.

PMF (Protected Management Frames). Before IEEE 802.11w (a.k.a., Protected Management Frames, or PMF[3]), only data frames could be protected in Wi-Fi. Management and control frames were used without any protection. The IEEE 802.11w amendment came to provide certain protection to some specific management frames, known as Robust Management Frames (RMF). These frames include, deauthenticaiton frames, disassociation frames, and certain action frames, e.g., QoS action frames and Block ACK frames. Also, the mechanism provides protection, through Security Association teardown protection (a.k.a., Security Association Query Procedure, cf., next subsection), to association and authentication frames exchanged during an existing connection to prevent disconnection of connected Wi-Fi supplicants. The IEEE 802.11w provides data integrity and freshness for broadcast and multicast robust management frames through the use of the Broadcast Integrity Protocol (BIP). This protocol uses the Message Integrity Code (MIC) to protect the integrity of the frames and provide freshness to prevent the replay of old frames. Tampered or replayed frames are passively discarded when they are detected. This for example mitigates broadcast deauthentication attack, where all connected supplicants get instantly disconnected after processing (without any verification) a spoofed deauthentication frame. On the other hand, unicast robust management frames benefit from data confidentiality in addition to data integrity and data freshness protection. Finally, as IEEE 802.11w provides protection to only some management frames, DoS attacks based on other management frames (i.e., Class 1 frames) are unfortunately still possible.

WPA3 (Wi-Fi Protected Access 3). In June 2018, the Wi-Fi Alliance announced WPA3 [14] as the next generation of Wi-Fi security. This new security mechanism aims to completely replace WPA2 mechanism. It provides multiple advantages over WPA2 such as protections against dictionary attacks (through the use of Simultaneous Authentication of Equals protocol [15], also known as dragonfly), forward secrecy, side-channel attacks, and authentication of management frames (through MFP). It allows three possible operational modes: WPA3-SAE (Wi-Fi Protected Access 3-Simultaneous Authentication of Equals), which is used when Wi-Fi devices only support WPA3; WPA3-SAE transition, also known as mixed mode, which allows Wi-Fi devices that only support WPA2 to connect to a WPA3 network; and WPA3-Enterprise 192-bit, which is used in sensitive enterprise environments, such as government and industry. WPA3-Enterprise, in particular v2.0 (December 2019), adds additional security measures to WPA2-Enterprise. For example, in WPA3-Enterprise, supplicants would not have the option of "skip certificate validation" or "accept any certificate" to complete an authentication with an authentication server, e.g., RADIUS, which was not the case with WPA2-Enterprise. This would mitigate possible evil twin attacks. Other versions were released, v3.0 (December 2020) and v3.1 (November 2022), to enhance the mechanism with respect to transition modes and privacy extension mechanisms.

[3]Note that PMF should not be confused with Cisco MFP (Management Frame Protection), which was developed in 2005. In MFP, there are two modes: (1) Infrastructure mode, where the access point sings beacon frames and other broadcast management frames (to detect Rogues). (2) Client mode, where the AP signs management frames that are sent to the client in addition to beacon and broadcast management frames

III. Attacks on Wi-Fi Technology

In this section, we extensively review various attacks on Wi-Fi systems and discuss their possible countermeasures. We divide this section into two parts. The first part (Subsection III.A) reviews attacks that are still possible on modern Wi-Fi systems. The second part (Subsection III.B) reviews attacks that became no longer possible on modern Wi-Fi systems due to security standard upgrades. Also, for better readability and referencing, we group these attacks based on the security service that each attack aims to compromise. We consider authentication, confidentiality, integrity, and availability. Besides the considered security services, we do not deny the existence of many other overlapping security services, which include but are not limited to, non-repudiation, access control, auditability, accountability, authorization, trust, trustworthiness, traceability, anonymity, liveness, and synchronization. It is not possible to derive a useful orthogonal grouping of attacks by considering all the existing security services.

In the following paragraphs, we provide a brief definition of the considered security services. This would allow a better understanding of the attacks when the latter are discussed.

Authentication. This service aims to prove that an entity, e.g., an individual, software, or device, is effectively what it claims to be. It is generally set up by proving the possession of a secret (something you know, e.g., Wi-Fi password or key), possession of a personal physical item (something you have, e.g., smart access card), and/or personal features (something you are, e.g., fingerprints, facial, and iris recognition).

Confidentiality. It is also known as secrecy. This service aims to protect the content of the stored and transmitted data from being disclosed to unauthorized parties. In Wi-Fi, it is essentially carried out using encryption techniques.

Integrity. This service aims to guarantee that the content of stored or transmitted data has not been accidentally or intentionally been modified.

Availability. This service assures that system services and resources, software, or hardware, are instantly and continuously available for users, when needed.

A. Feasible Attacks on Wi-Fi

In this subsection, we present various attacks that we believe are still possible and feasible on modern Wi-Fi systems.

A.1. Authentication-related Attacks on Wi-Fi

We present attacks that violate the authentication in Wi-Fi. These attacks are mainly due to a partial implementation of frame authentication or due to some flaws in the protocols.

Identity Spoofing. In this scenario, an attacker spoofs the identity of a Wi-Fi device to impersonate it and gain certain privileges. This can be done by spoofing the MAC address[6] of the target Wi-Fi device, the SSID (i.e., in case of spoofing an access point), or both. This attack is easy to implement since nowadays most Wi-Fi network interfaces support the MAC address changing option as well as the "Master mode" to emulate Wi-Fi access points.

Although it is not that easy to mitigate spoofing, detecting such activity is rather possible. Using wireless intrusion detection systems [16], it is possible to detect the presence of two identical devices operating in the network [17]. For instance, a spoofing access point can be localized by analyzing synchronization frames[4] generated by access points and detecting the presence of frames carrying the same BSSID and SSID, but with different timestamps.

Packet Forging. As authentication is not available in Wi-Fi management and control frames, attackers can easily forge them. In most cases, the attacker creates a frame and indicates the source address as the address of a device that has higher privileges, such as the access point. The devices which receive those forged frames accept them and process them as if they were sent from the true source, i.e., the access point.

Packet forging can be mitigated by requiring authentication on all types of Wi-Fi frames. For instance, every connected device should be able to verify whether a received frame is coming from a legitimate source or not. To that end, Wi-Fi devices can employ PMF (Protected Management Frame) mechanism, which is optional in WPA and WPA2, but mandatory in WPA3. An alternative consists of using WPA-Enterprise with X509 digital certificates.

Access Point Cloning. This attack is also known as Evil twin. In this scenario, the attacker sets its Wi-Fi adapter into master mode (i.e., access point mode) and adapts its network settings to be similar to a target access point settings (i.e., same MAC address, SSID, and radio channel). The attacker then boosts the signal strength to monopolize the radio channel and leaves the network with no security mechanism. This attracts careless Wi-Fi users to connect to the attacker's access point and use free Internet. Since no security is setup, the attacker analyzes the network traffic to extract any credentials. A more interesting scenario occurs when WPA-Enterprise is used with one-way authentication, where Wi-Fi supplicants do not have to authenticate the WPA authenticator (server). The supplicants would have the option of "skip certificate validation" or "accept any certificate" to complete the authentication. The attacker may mislead supplicants to connect to the attacker's access point instead of the legitimate one.

This attack can be detected by setting a wireless IDS (Intrusion Detection System), such as Kismet [16], that can detect the presence of identical access points within the same area [17]. The IDS captures and analyzes the network traffic to detect access points with the same SSID, same MAC address, same (or different) security mechanism, but with different beacon timestamps. When WPA-Enterprise is used, mutual authentication must be established. Supplicants should not have the choice of "skipping certificate validation" or "accepting any certificate". Such a policy is enforced in WPA3-Enterprise.

A.2. Confidentiality-related Attacks on Wi-Fi

Wi-Fi networks have been demonstrated to be vulnerable to interception attacks [4]–[6], [18], [19]. This is fundamentally related to the broadcast nature of the wireless medium along with the implementation flaws discovered in the adopted encryption mechanisms, e.g., RC4. Notwithstanding, after the implementation of WPA2-AES and WPA3, these confidentiality-related issues have come to an end, making some various attacks unfeasible on modern Wi-Fi systems.

Sniffing and Packet Analysis. Wi-Fi allows the use of a non-secure mode called open mode. In this mode, no confidentiality is provided and all Wi-Fi frames are sent unencrypted over the radio channel. An attacker can easily capture a number of Wi-Fi frames to analyze them and extract sensitive information such as credentials and private information.

The most obvious security initiative that can be adopted to mitigate this attack is to use the AES encryption mechanism provided by WPA2 and WPA3. However, in some circumstances, certain Wi-Fi networks are intentionally left open for user flexibility, such as the ones provided in supermarkets, large retail shops, or even airports. In such networks, security has to be implemented in the upper layers to use upper-layer security protocols, e.g., TLS (Transport Layer Security). If none of these security measures are used, it is strictly recommended not to use such networks to perform any authentication that involves the use of credentials (e.g., access email account). However, a new alternative consists of using the OWE (Opportunistic Wireless Encryption) to establish an encrypted connection. Even though a password is not shared a priori between a client and an access point, OWE allows them to establish a shared secret key using Diffie-Hellman key establishment protocol.

Network Discovery. In this scenario, an attacker uses a network adapter in "Monitor mode". The attacker utilizes wireless scanning tools to scan all radio channels to detect and discover nearby Wi-Fi networks. If the attacker is interested in a particular network, it can learn a considerable amount of information related to that network. The information may include BSSID, network SSID, associated stations, approximate location, radio channel, security mechanism, and the brand of the used access points. These information can be exploited for more sophisticated attacks.

[4]Wi-Fi frames are network packets generated at the MAC layer. Synchronization frames are commonly known as beacons. They are periodically broadcasted by access points to indicate their presence in the neighborhood.

The network administrator should reduce the power transmission of its access points so that it only covers the operational area. It can also set the network configuration so that its SSID is not broadcasted and it is kept hidden. Finally, the use of a discrete SSID name may reduce the chance for attackers to link a particular SSID to a given organization Wi-Fi network and setting it as a target.

Physical Attack on Access Points. Many wireless access points have their security information (e.g., logname, password, BSSID, SSID, WPA passphrase, or WPS PIN code) printed on the back or front of the device. Thus, if the access point is not kept in a secure location, an attacker can sneak by the access point and read current credentials (if still not changed) to use them later on. The attacker can also steal devices and gain physical access to their memory to extract important information about the whole network.

Network access points must be equipped with physical security. These devices should not carry any indication about the network security settings, such as passwords, usernames or IP addresses. It is also recommended to place access points at places which are not easily accessible. This prevents attackers from reaching the device.

A.3. Integrity-related Attacks on Wi-Fi

This type of attack allows attackers to modify the content of transmitted packets and to adjust their integrity code in such a way so that the packets look as if they were sent from a trusted source. Victim devices receive the packets and process them. Based on the latest research, no attack was reported on modern Wi-Fi devices breaching the data integrity service.

A.4. Availability-related Attacks on Wi-Fi

Wi-Fi was known to be entirely vulnerable to attacks on network availability. Practically, we emphasize on denial of service attacks. We have noticed that almost all attacks on Wi-Fi availability were due to a partial implementation of authentication in Wi-Fi. Nonetheless, after the implementation of PMF (Protected Management Frame) on WPA2 and the emergence of WPA3, most frame-forging-based denial-of-service attacks became unfeasible on these new mechanisms. In what follows, we present some denial-of-service attacks that are still possible on modern Wi-Fi devices.

Device Deauthentication. The IEEE802.11w amendment aimed to provide authentication for some management frames (through Protected Mannagment Frames - PMF). This has made many denial-of-service attacks that are relying on spoofing management frames, e.g. deauthentication attack, to become unfeasible. However, in 2021, Lounis et al., [20], demonstrated that it was still possible to run deauthentication attacks when WPA2 or WPA3 is used with PMF. Also, in 2022, Schepers et al., [21], demonstrated the feasibility of deauthentication attacks when PMF is enabled.

Connection Deprivation on WPA3. It is possible to deprive legitimate Wi-Fi supplicants that attempt to get authenticated and connected to a WPA3-configured access point. As discussed in [22]–[25], an attacker can spoof a legitimate access point and then, in a race condition, reply negatively to any connection attempt from a legitimate supplicant to repeatedly cause an authentication failure. For instance, during a WPA3-SAE (Wi-Fi Protected Access 3-Simultanious Authentication of Equals) authentication, the supplicant proposes to use a Diffie-Hellman group, e.g., Group 19. The access point (authenticator) checks whether the proposed group is supported. If the proposed group is supported, the authentication goes on. However, if it is not supported by the authenticator, the latter replies to the supplicant with a negative message causing the authentication to stop. An attacker can send crafted negative replies each time the supplicant proposes a DH-group. The supplicant will be forced to abort the authentication at each attempt.

As recommended in [22]–[26], future Wi-Fi supplicants and access points must be designed in such a way so that they take decisions based on a group of unauthenticated messages instead of the first unauthenticated message that is received. In this way, supplicants and access points become smarter during an authentication. This would mitigate the discussed connection deprivation attacks.

Battery Exhaustion. In this attack, the attacker sends a flood of encrypted and meaningless traffic to Wi-Fi devices with limited resources (e.g., Wi-Fi sensors). Those devices consume a large amount of energy by processing that network traffic before dropping them off.

This attack is effective when the target device cannot distinguish whether the incoming traffic is bogus or legitimate. Also, if the target device has to perform many cryptographic operations before concluding whether to drop or not a given packet, the attack will have a significant negative impact. If data freshness is considered, an attacker cannot flood old messages or predict future messages by spoofing devices. Moreover, the encryption algorithm should be implemented in such a way so that the target device can perform some lightweight pre-checking on the received packets before performing any expensive cryptographic operation.

RTS Request Misuse. The IEEE 802.11 standard specifies a four-way packet transmission protocol called virtual carrier-sense or RTS/CTS (Request To Send/Clear To Send). This protocol allows a Wi-Fi device to allocate the radio channel to reliably send its packets. In this scenario, an attacker repeatedly sends RTS requests asking to allocate the radio channel for a long period. If the radio channel is granted to the attacker, all connected Wi-Fi devices are then denied from accessing the radio channel to send their packets [27].

The network administrator must ensure that the radio channel is fairly shared and used among the associated Wi-Fi devices. For example, it can configure the access points to accept a limited number of RTS-requests per hour and per Wi-Fi device.

Greedy Behavior. To access the radio channel using the CSMA/CA protocol, all connected Wi-Fi devices sense the radio channel for its availability. If the radio channel is found to be clear, all Wi-Fi devices wait for a certain amount of

time known as DIFS (DCF[5] Interframe Space) before starting the transmission of their packets. If the channel is found to be busy, before or after waiting for DIFS, all Wi-Fi devices wait till the radio channel becomes clear. Once it becomes clear, all Wi-Fi devices wait for another DIFS and compute a random timer (uniformly chosen in between 0 and CW-1, where CW is the contention window, usually set to 15). The timer is then decremented while the radio channel is clear and the timer is greater than 0. The first Wi-Fi device whose timer expires, starts transmitting its packets. Meanwhile, all other Wi-Fi devices abstain from decreasing their timer as long as the channel is busy. Under these circumstances, an attacker violates the rules and starts transmitting before the expiry of the shortest possible timer. This will have two disproportional impacts. First, the data rate of the attacker will increase considerably as it is taking the whole network bandwidth. Second, the data rate of the other devices will slow down and may get nullified [27].

The greedy behavior can be detected using an intrusion detection system. The system monitors how the radio channel is shared and used among a certain number of Wi-Fi devices. If a device unfairly uses the radio channel, the network administrator may suspend that device from the network for sometime or disconnect it. However, such an aggressive countermeasure can be exploited by an attacker to disconnect legitimate devices by spoofing the latter and conducting a greedy behavior attack.

Packets Trashing. In this scenario, the attacker sends random packets exactly at the same time where a legitimate Wi-Fi device is transmitting its packets. This causes a collision of packets which results in a wrong integrity code or FCS (Frame Check Sequence). These corrupted packets are automatically discarded upon their reception due to FCS verification error [4], [28].

Channel Jamming. Usually, in a Wi-Fi network, communications occur on a fixed radio channel on the 2.4 GHz band. In this attack, an attacker generates random signals (noise) on the operational radio channel and causes the connected Wi-Fi devices to believe that the radio channel is busy. This drains the network performance and denies legitimate devices from accessing the radio channel to send their packets.

The above two attacks can be detected by analyzing the radio channels but cannot be mitigated. One of the techniques that can be employed is to automatically switch to another radio channel when the collision or data rate goes down below a certain threshold. Also, the network administrator can set up a mechanism that can localize from where a specific network traffic or radio signal is coming from and hence may try to localize the source, i.e., attacker.

B. Unfeasible Attacks on Wi-Fi

In this subsection, we present various attacks that we believe are no longer feasible on modern Wi-Fi systems that employs the latest version of WPA3 security mechanim.

B.1. Authentication-related Attacks on Wi-Fi

Packet Replay. This attack is related to WEP. In fact, WEP does not guarantee data freshness. This allows an attacker to capture previously exchanged WEP packets and replay them later on to gain some privileges. For instance, if the attacker captures the challenge-response messages during a previous WEP authentication, the attacker can infer the used keystream. By knowing the IV (Initialization Vector) that was used to generate the keystream, the attacker runs multiple association attempts until the access point asks for a response which uses that known IV. In this case, the attacker responds correctly to the challenge and gets successfully authenticated.

When data freshness is correctly implemented in an authentication protocol, an attacker will not be able to replay old messages. This countermeasure has been implemented in WPA and WPA2, which aim to replace WEP. Although WPA and WPA2 are relatively more secure than WEP, it is highly recommended to switch to WPA3, which is more secure than WEP, WPA, and WPA2 mechanisms.

Wi-Fi Backdoor. Most access points and routers, with wireless capabilities, either bought from a retail shop or offered by an ISP (Internet Service Provider), come with default security settings (e.g., logname=admin, password=admin or logname=“ ” and password=admin). It is the responsibility of the subscriber to change the default settings. An attacker, who is subscribed to an ISP, tests the connectivity with all possible IP addresses that are in its network subnet. For example, if its IP address is 105.101.80.125, the attacker pings all IP addresses from 105.101.80.01 to 105.101.80.254. If an IP address replies to the ping, the attacker web-browses the IP address for the login page of the remote router. If the credentials of that router are left to default and that device allows connections from outside (i.e., Internet), the attacker will be able to login into the subscriber's router and learn a number of sensitive information related to the subscriber's itself or the Wi-Fi network, such as WEP/WPA key, SSID, connected clients, phone number, email address, subscriber's address, and subscriber's name.

Modern Wi-Fi access point comes with a reasonably secure configuration. Also, the ability to connect to the access point from the Internet is disabled by default. In the worst case, the network administrator has to change the default network and security configurations, such as the network SSID (changed to a discrete name), the IP address range, user names and passwords. It should also disable non secure mechanisms, such as WEP and WPS, on both frequency bands, i.e., 2.4GH and 5Ghz.

Online WEP Key Cracking. In 2001, the key scheduling algorithm of RC4 used in the WEP mechanism was shown to contain severe design flaws [4]–[8], [18], [29]–[31]. These flaws can be exploited by attackers to recover the WEP key and decrypt all network communications. Few years later, in 2004, researchers [30] demonstrated that an attacker equipped with an ordinary computer can gradually reconstruct the WEP key in less than 2 hours. If an attacker passively eavesdrops

[5]DCF (Distributed Coordination Function) is a concurrent-based access mode where all Wi-Fi devices have the same chance to access the radio channel. The other mode is PCF (Point Coordination Function), where the access to the radio channel is controlled by the access point.

a large number of WEP-encrypted packets (around 4,000,000 to 6,000,000 packets), it will be able to perform a byte by byte keystream recovery till recovering the whole WEP key. Interestingly, in the same year, a person under the pseudonym KoreK [32] posted on the NetStumbler forum an improved version of the technique [30]. Its technique reduces the required number of packets for cracking the WEP key to 700,000 packets [5] (500,000 packets [31]). Three years later (2007), researchers [31] demonstrated that a 104-bit WEP key can be cracked in 60 seconds using 35,000 to 40,000 packets (with 0.5 probability of success) and using 85,000 packets (with 0.95 probability of success). Once the key is disclosed, the attacker can fabricate, decrypt, and/or modify the content of Wi-Fi packets.

The user should not use WEP security mechanism as well as the devices that only support WEP. The WEP key can be cracked easily using modern computers. As Wi-Fi Alliance recommends, we also suggest the use of WPA2-PSK or WPA3-SAE instead of WEP.

Offline WPA Key Cracking. This attack aims to find the WPA password of a given Wi-Fi network. An attacker starts by eavesdropping a communication between a Wi-Fi station and an access point and tries to capture the four-way-handshake messages (by forcing a re-authentication). This handshake consists of four EAPoL[6] messages containing values generated by both parties to prove to each other the knowledge of the correct password. Upon capturing the four EAPoL messages, the attacker operates a brute force procedure or uses a dictionary of words to find out the right password that was used during the four-way-handshake. This attack may take decades to succeed on ordinary computers if the password is strong enough. However, it may also take less than a second if the password is in the attacker's dictionary. There are some cheap online cloud services, such as WPACracker.com [33], that can be used to crack a WPA key in a shorter time. The attacker just has to capture the handshake and upload it to the cloud service.

The network administrator has to make sure that the used WPA passwords in its Wi-Fi network fulfill certain password security patterns. These patterns include the length of the password (e.g., must be at least 6 characters) and the used letters (e.g., mixture of uppercase, lowercase, special characters, and numbers). The password should also be updated regularly and kept secret.

WPA3 Key Cracking. In April 2019, researchers [34] discovered a set of vulnerabilities named Dragonblood. These vulnerabilities were discovered in the SAE (Simultaneous Authentication of Equals) handshake (a.k.a., dragonfly) used in WPA3-SAE. They demonstrated that by abusing timing or cache-based side-channel leaks (from the password encoding method[7]), it is possible to recover the WPA3 password using password partitioning attacks. The same work showed that it is possible to trick a Wi-Fi client into downgrading from WPA3-SAE to WPA2-PSK. This would allow an attacker perform offline WPA2 key cracking attack.

It is recommended [34] not to use a set of multiplicative groups such as group 22, 23, and 24. Also, it is recommended to use ECC DH-groups over MODP and exclude MAC addresses during password encoding. This would decrease side-channel leaks. Furthermore, to mitigate the downgrading attack, Wi-Fi clients should remember if a network supports WPA3-SAE. Wi-Fi clients should not connect to a Wi-Fi access point that indicates the support of only WPA2-PSK if the same access point has been previously saved as a WPA3-capable access point.

Key Re-Installation. This set of attacks were introduced in 2017 under the name of KRACKs (Key Reinstallation Attacks) [35]. It exploits the fact that some WPA implementations allow the retransmission of the third EAPoL message of the WPA four-way-handshake if an acknowledgment is not received. By doing so, the receiver reinstalls a previously installed keychain each time it receives this third EAPoL message. In addition to that, it resets the transmit packet counter as well as the receive replay counter. This forces the receiver (usually the supplicant) to reuse the same key twice (i.e., data is encrypted using the same key twice). The attacker exploits this to generate multiple attacks. To that end, the attacker first sets up a man-in-the middle scenario between the supplicant and the access point during a four-way-handshake and prevents the supplicant acknowledgment message (i.e., the fourth EAPoL message) from reaching the access point. This consequently induces the access point to resend the third EAPoL message again to the supplicant. The latter reinstalls the derived PTK keychain and resets the nonces used by the encryption mechanism. This allows the attacker to replay and decrypt certain messages (in case of TKIP, CCMP, and GCMP) and/or forge packets (in case of TKIP and GCMP). Furthermore, if the packets can be decrypted, the attacker can perform higher level attacks.

The network administrator must ensure that the WPA implementation used in its network meets the following criteria: (1) Does not allow the retransmission of the third EAPoL message during the four-way-handshake. (2) Does not reset the nonce if the key is reinstalled [35].

WPS Online Cracking. In 2011, WPS (Wi-Fi Protected Setup) was discovered to have a serious design flaw which can easily be exploited to brute force the PIN code and retrieve the WPA passphrase. Tools, such as pixiewps [36] and Reaver [37], can be used for this purpose.

To mitigate this attack, the administrator can perform one of the following: (1) Disable the WPS mechanism on both radio bands, the 2.4 GHz and the 5GHz. (2) Restrict the number of WPS PIN code failure attempts to 3 and delay the next attempt by 30 minutes.

B.2. Confidentiality-related Attacks on Wi-Fi

The following attacks are no longer possible on modern Wi-Fi systems. They are related to vulnerabilities in WEP

[6]EAPoL: Extensible Authentication Protocol over LAN.

[7]WPA3 applies two password encoding methods: (1) hash-to-curve is used when ECC (Elliptic Curve Cryptography) is adopted to encode the password into an elliptic curve point. (2) hash-to-element is used when MODP (Multiplicative groups modulo a prime) is adopted to encode the password into a group element.

and WPA-TKIP mechanisms. These vulnerabilities are not available in WPA2-AES and WPA3. Also, modern Wi-Fi systems do not provide the use of WEP and WPA-TKIP.

Wardriving. In this attack, attackers collaborate by driving around cities, neighborhoods, and villages, to scan for Wi-Fi networks that use open access mechanism or WEP. They use dedicated tools and cheap devices along with a GPS (Global Positioning System) device to record or tag the locations of the discovered insecure Wi-Fi networks in a map. The map is then shared among the attackers for future attacks. Other variants of this attack are warcycling or warbiking (using bicycle), wartraining (while inside trains), warwalking, warjogging, and wardroning or warflying (using drones).

The Wi-Fi network administrator should avoid using the broken security mechanisms such as WEP, or leave the network insecure. This prevents the attackers (wardrivers) from selecting the network as a good target network. Hiding the network SSID is also a good initiative.

Keystream Reuse Attack. In RC4, the keystream is the concatenation of a 40-bit to 104-bit WEP-key along with an IV (Initialization Vector). The IV changes randomly or incrementally for each packet depending on the implementation. This provides a unique keystream for each packet. Nonetheless, because of the small size of the IV (24-bit), all IV possible combinations (i.e., 2^{24}) are rapidly consumed (few seconds at 5Mbps) [4]. This allows an attacker who eavesdrops an ongoing communication for some time to be able to capture packets encrypted with the same keystream. By having two ciphertexts encrypted with the same keystream, the attacker can compute the xor of the plaintext of the two packets. If the attacker manages to guess at least one plaintext, it will be able to decrypt the remaining plaintexts [38].

The size of the IV has been increased to 48 bits in TKIP (Temporal Key Integrity Protocol). Also, the way the IV is used in TKIP is more secure than it used to be in WEP. However, it is recommended to use CCMP (Counter Mode CBC-MAC Protocol) encryption mechanism rather than TKIP to avoid dealing with keystream reuse.

WEP Packet Decryption. In this attack, an attacker starts by eavesdropping a WEP authentication and tries to capture the challenge (sent in plaintext) as well as its response. Then, it xors them together to obtain the used keystream. By knowing the IV (sent unencrypted) that was used for generating the keystream, the attacker would be able to decrypt all packets that were encrypted using the same keystream.

WEP mechanism does not provide forward secrecy. Encryption algorithms that are based on xoring the plaintext by a keystream (e.g., RC4) should not apply the same keystream twice. This provides forward secrecy.

ChopChop Attack on RC4. This attack was posted in the NetStumbler forum by a person under the pseudonym KoreK in 2004 [32]. It allows an attacker to interactively decrypt the last m bytes of an RC4 encrypted packet by sending $m \times 128$ packets to the network. It exploits the linear property of the XOR logical operator used by the RC4 algorithm for encryption, and by the CRC32 algorithm to compute the ICV code for data integrity. The attacker intercepts a target encrypted packet and chops off the last byte which invalidates the ICV code of the packet. Then by assuming the plaintext value of the chopped byte, the attacker adjusts the ICV code so that it becomes valid. Indeed, when the attacker assumes the correct byte, it receives a response from the access point. This response indirectly indicates that the assumption on the last byte was correct. The attacker repeats this process to guess all remaining bytes of the packet.

RC4 and CRC32 algorithms have serious flaws due to some properties such as the linearity of the XOR logical operator. Algorithms that have this kind of property must be implemented in a very careful manner so that attackers cannot decrypt messages or tamper with messages and adjust their integrity code by flipping some bits. The AES symmetric cipher can be used along with different operational modes to mitigate this attack. This requires the use of WPA2 or WPA3 mechanisms. Nevertheless, the network administrator has to make sure that its Wi-Fi device network cards do not contain the KrØØk vulnerability[8] which allows attackers to decrypt some WPA2 (AES-CCMP) packets.

ChopChop Attack on TKIP. This attack [5] allows the attacker to decrypt packets when TKIP is used with a long TKIP re-keying interval. In particular, when the range of IPv4 addresses used in a Wi-Fi network are known and the access point is operating the IEEE 802.11e, the attack becomes easier. The attacker captures encrypted ARP-requests[9] or responses and replays them a number of times in a ChopChop style on different QoS (Quality of Service) channels that still have a lower TSC (TKIP sequence counter). If the access point replies, then the guess was successful and the attacker manages to read the encrypted bytes. More sophisticated variants of this attack were reported in [6] and [19].

Considering the network configurations that are exploited by this attack, an obvious solution consists of using a shorter TKIP re-keying interval.

B.3. Integrity-related Attacks on Wi-Fi

Fortunately, these attacks exploited vulnerabilities in WEP mechanism, which is no longer used by modern devices.

ICV Tampering. WEP mechanism adopts the CRC32 algorithm to generate an ICV (Integrity Check Value) to guarantee data integrity. It has been demonstrated in [18] that an attacker can modify the content of a message and adjust the IVC value accordingly to make it valid. The CRC method used to compute the ICV is called a linear method (or affine) in which an attacker can predict which bits in the ICV will be flipped if the attacker changes a single bit in the message.

The CRC algorithm is usually used for error detection and correction. It is not an adequate algorithm for integrity protection, in particular, to protect against intentional tampering. We highly recommend to use WPA2 or WPA3 where

[8] KrØØk (CVE-2019-15126), discovered in 2019, is a hardware vulnerability residing in many Wi-Fi chips manufactured by Broadcom and Cypress.

[9] ARP (Address Resolution Protocol) is a link layer protocol that translates a logical 32-bit IPv4 address of a connected device into its physical 48-bit MAC address.

data integrity codes are generated using AES-Cipher Bloc Chaining-Message Authentication Code.

Micheal Algorithm Attack. This attack is a consequence of the ChopChop attack on TKIP described in Section V.B.2. When the ChopChop attack is performed on TKIP, an attacker manages to get a plaintext along with its corresponding MIC (Message Integrity Check) code. The attacker would be able to reverse the Micheal algorithm (as it is not a one way function [39]) and recover the MIC key that was used to compute the MIC. This allows the attacker to modify the contents and regenerate the MIC using the disclosed key.

The Micheal algorithm has been shown to contain many security flaws [39], [40]. It is not a one way function and hence can be reversed. Thus, data integrity functions that do have such properties should not be used to preserve data integrity. WPA2 or WPA3 would be a better alternative as data integrity codes are generated using AES-CBC-MAC, which is thus far considered secure.

B.4. Availability-related Attacks on Wi-Fi

In the following paragraphs, we present some denial-of-service attacks that were feasible on WEP, WPA, and WPA2 with PMF (Protected Management Frames) disabled. That is to say, if a Wi-Fi system still uses WPA2 with PMF disabled, the attacks remain feasible. Nevertheless, in this paper, we consider these attacks to be unfeasible on modern Wi-Fi systems under the assumption that these systems would at least run the latest version of WPA3, or WPA2 with the latest version of PMF.

Device Deauthentication. The IEEE 802.11 management frames (e.g., disassociation request/response and deauthentication request/response frames) are not authenticated when WEP, WPA-PSK, and WPA2-PSK mechanisms are used. This allows an attacker to spoof any Wi-Fi device and send forged frames over the network. In the deauthentication attack, the attacker spoofs the access point and repeatedly sends forged deauthentication frames to connected devices and cause their permanent disconnection [27]. Another way of performing this attack on certain access points was discussed in [22]. It consists of establishing a connection using OSA (Open System Authentication) with an access point using the access point's MAC address (self-connection). As a consequence, certain access points react to such authentication attempt by sending a deauthentication frame to the entire network. This would deauthenticate all connected stations.

Device Disassociation. Similar to the deauthentication attack, an attacker spoofs the access point and sends forged disassociation requests to connected Wi-Fi devices and causes their disassociation from the network. The target devices get disassociated but not deauthenticated. They just have to reassociate to join the network again [27].

Device Reassociation. In this scenario, the attacker spoofs a legitimate Wi-Fi device which is associated with a given BSS and tries to reassociate it with a second BSS without any disassociation from the first one. In this way, the attacker creates inconsistencies in the network configuration causing several network protocol execution failures [4].

Packet Wasting. The IEEE 802.11 defines a power saving mode that allows Wi-Fi devices with limited power supply to switch into sleep mode to save some energy. During the power saving period, the access point buffers all packets destined to devices in sleep mode. This requires all Wi-Fi devices to be synchronized with the access point to wake up at the right time to retrieve their respective buffered packets. The key synchronization information are periodically broadcasted by the access point using the TIM (Traffic Indication Map) field of the beacon management frame. When a Wi-Fi device wakes up from the power saving mode, it requests its buffered packets if there are any from the access point. The access point delivers the packets to its destination and cleans its buffer to save memory space. In such circumstances, an attacker spoofs a legitimate Wi-Fi device while it is sleeping and causes the access point to deliver the packets and clean its buffer. Thus, when the legitimate Wi-Fi device wakes up and requests for its packets, the access point informs that device that there is nothing buffered for it [27].

Device Desynchronization. This attack scenario aims to cause disturbance on the power saving mode. The attacker spoofs the access point and sends forged beacon management frames that contain wrong synchronization information. This would cause Wi-Fi stations to wake up from the power saving mode at the wrong time [27].

Traffic Freezing. In this scenario, the attacker spoofs a legitimate Wi-Fi device and sends forged management frames informing the access point that the device is switching into power saving mode. This will considerably drain real-time traffic sent to the legitimate Wi-Fi device [4].

Sleep Deprivation. In this scenario, the attacker spoofs the access point and sends forged beacon frames containing information that indicates the presence of buffered packets for devices in power saving mode. The devices in the power saving mode send a request to retrieve their packets and stay awake for the entire beacon interval if a response is not received. By repeating this process, the attacker prevents the legitimate Wi-Fi devices from using the power saving mode and thereby drains their batteries [4], [27].

To mitigate the previous attacks, the 802.11 management frames must be authenticated. Originally, WEP and WPA-PSK did not provide any authentication for management frames. However, since the IEEE 802.11w amendment, it has become possible to use the PMF (Protected Management Frame) and mitigate all previous attacks. Nevertheless, as mentioned earlier, some recent research [20], [21] have shown that some of these attacks (e.g., deauthentication attacks) were still possible even when PMF is enabled. The latest version of PMF should fix this issue.

IV. Conclusion

Wi-Fi is a wireless communication technology that has been around since the late nineties. Nowadays, it is the most adopted wireless short-range communication technology in various IoT

(Internet of Things) applications and on many wireless AI (Artificial Intelligent) systems. Although Wi-Fi security has significantly improved throughout the past years, it is still lagging behind. Many vulnerabilities still exist allowing attackers to generate different types of attacks. These attacks can breach the authentication, confidentiality, and data integrity of Wi-Fi networks. At the same time, many vulnerabilities have been fixed or patched, and the attacks that were relying on those vulnerabilities would fail on modern Wi-Fi devices.

We believe that it is important for young security engineers, in general, and for wireless intelligent system designers, in particular, to be aware of the existing vulnerabilities and possible attacks on modern Wi-Fi systems and their respective countermeasures. That would also help them to not have to look back and care about attacks that can no longer be generated on today's Wi-Fi systems.

In this paper, we have extensively reviewed the attacks on Wi-Fi technology. We have classified these attacks as feasible and unfeasible on nowadays modern Wi-Fi systems. Also, for each attack, we have discuss the possible countermeasures to mitigate it.

REFERENCES

[1] IEEE, "IEEE Std 802.11ac," *Amendment 4: Enhancement for Very High Throughput for Operation in Bands bellow 6GHz*, 2013.

[2] E. Pietrosemoli, "Long Distance Wifi Trial," *International Summit for Community Wireless Networks*, 2007.

[3] Wi-Fi-Alliance, "Wi-Fi Specifications." https://www.wi-fi.org/discover-wi-fi/specifications, 2018. Accessed: 2020-01-19.

[4] B. Jerman-Blažič and W. S. Schneider, *Security and Privacy in Advanced Networking Technologies*. NATO science series: Computer and systems sciences, IOS Press, 2004.

[5] E. Tews and M. Beck, "Practical Attacks Against WEP and WPA," in *Proceedings of the Second ACM Conference on Wireless Network Security*, pp. 79–86, ACM, 2009.

[6] N. AlFardan and D. J. Bernstein and K. G. Paterson and B. Poettering and J. C. N. Schuldt, "On the Security of RC4 in TLS," in *Presented as part of the 22nd USENIX Security Symposium*, pp. 305–320, USENIX, 2013.

[7] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP," in *Proceedings of the Network and Distributed System Security Symposium*, 2002.

[8] S. R. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in The Key Scheduling Algorithm of RC4," in *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, pp. 1–24, Springer-Verlag, 2001.

[9] IEEE, "IEEE Std 802.11i," *Amendment 6: Medium Access Control Security Enhancement*, 2004.

[10] IEEE, "IEEE Std 802.11," *Wireless LAN Medium Access Control and Physical Layer Spec*, 2016.

[11] IEEE, "IEEE Std 802.11ad," *Amendment 3: Enhancement for Very High Troughput in the 60GHz band*, 2012.

[12] NIST, "Advanced Encryption Standard (AES)." http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001. Accessed: 2020-01-19.

[13] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Transaction Information Theory*, vol. 22 (6), pp. 644–654, 1976.

[14] Wi-Fi-Alliance, "WPA3 Specification Version 1.0." https://www.wi-fi.org, 2018. Accessed: 2020-01-19.

[15] D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," in *Second International Conference on Sensor Technologies and Applications*, pp. 839–844, 2008.

[16] M. Kershaw, "Kismet: A Wireless Network and Device Detector, Sniffer, Wardriving Tool, and WIDS (Wireless Intrusion Detection) Framework." https://www.kismetwireless.net/, 2008. Accessed: 2020-01-19.

[17] K. Lounis, A. Babakhouya, and N. Taboudjemat, "Setting up a Wireless Intrusion Detection Solution based on Kismet," *Technical report CERIST-DTISI/RT-11-000000023-dz*, 2011.

[18] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, pp. 180–189, ACM, 2001.

[19] K. G. Paterson and B. Poettering and J. C. N Schuldt, "Plaintext Recovery Attacks Against WPA/TKIP," in *Fast Software Encryption*, pp. 325–349, Springer, 2015.

[20] K. Lounis, S. H. H. Ding, and M. Zulkernine, "Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3," vol. 13291 of *International Symposium on Foundations and Practice of Security*, 2022.

[21] A. R. Domien Schepers and M. Vanhoef, "On the Robustness of Wi-Fi Deauthentication Countermeasures," Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks, 2022.

[22] K. Lounis and M. Zulkernine, "Bad-token: Denial of Service Attacks on WPA3," vol. 15 of *ACM Proceedings of the 12th International Conference on Security of Information and Networks*, 2019.

[23] K. Lounis and M. Zulkernine, "Connection Deprivation Attacks on WPA3," vol. 12026 of *Proceedings of the 14th International Conference on Risks and Security of Internet and Systems*, 2019.

[24] K. Lounis, "Security of wireless short-range technologies and an authentication protocol for IoT," Ph.D. Thesis, School of Computing, Queen's University, 2020.

[25] K. Lounis and M. Zulkernine, "Attacks and Defenses in Short-Range Wireless Technologies for IoT," *IEEE Access*, vol. 8, pp. 88892–88932, 2020.

[26] K. Lounis and M. Zulkernine, "Exploiting Race Condition for Wi-Fi Denial of Service Attacks," 13th International Conference on Security of Information and Networks (SIN'20), 2020.

[27] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *Proceedings of the 12th Conference on USENIX Security Symposium*, vol. 12, pp. 15–27, USENIX Association, 2003.

[28] G. Lin and N. Guevara, "On Link Layer Denial of Service in Data Wireless LANs: Research Articles," *Wirel. Commun. Mob. Comput.*, vol. 5 (3), pp. 273–284, 2005.

[29] W. A. Arbaugh, N. Shankar, Y. C. J. Wan, and K. Zhang, "Your 80211 Wireless Network Has No Clothes," *IEEE Wireless Communications*, vol. 9 (6), pp. 44–51, 2002.

[30] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "A Key Recovery Attack on The 802.11b Wired Equivalent Privacy Protocol WEP," in *ACM transaction on Information and System Security*, vol. 7 (2), pp. 319–332, ACM, 2004.

[31] E. Tews, R.-P. Weinmann, and A. Pyshkin, "Breaking 104 Bit WEP in Less Than 60 Seconds," in *Information Security Applications*, pp. 188–202, Springer Berlin Heidelberg, 2007.

[32] KoreK, "Next Generation of WEP Attacks?." http://www.netstumbler.org/news/next-generation-of-wep-attacks-t12277.html, 2004. Accessed: 2020-01-19.

[33] WPACracker, "WPACracker.net." http://www.wpacrack.net/index.html, 2009. Accessed: 2020-01-19.

[34] M. Vanhoef and E. Ronen, "Dragonblood: A Security Analysis of WPA3's SAE Handshake." https://papers.mathyvanhoef.com/dragonblood.pdf, 2019. Accessed: 2019-04-29.

[35] M. Vanhoef and F. Piessens, "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," in *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 1313–1328, 2017.

[36] Pixiewps, "An Offline Wi-Fi Protected Setup Brute-Force Utility." https://github.com/wiire-a/pixiewps, 2014. Accessed: 2020-01-19.

[37] Reaver, "Brute Force Attack Utility Against Wifi Protected Setup Registrar PINs." https://github.com/t6x/reaver-wps-fork-t6x, 2011. Accessed: 2020-01-19.

[38] E. Dawson and L. Nielsen, "Automated Cryptanalysis of XOR Plaintext Strings," in *Cryptologia*, vol. 20 (2), pp. 165–184, USENIX Association, 1996.

[39] A. Wool, "A Note on The Fragility of The Michael Message Integrity Code," *IEEE Transactions on Wireless Communications*, vol. 3 (5), pp. 1459–1462, 2004.

[40] N. Ferguson, "Michael: An Improved MIC for 802.11 WEP." http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/2-020.zip, 2002. Accessed: 2020-01-19.