Analysis of Evil Twin, Deauthentication, and Disassociation Attacks on Wi-Fi Cameras

Zachary Neal and Kewei Sha
University of Houston-Clear Lake
Houston, United States
{nealz4626, sha}@uhcl.edu

2023 32nd International Conference on Computer Communications and Networks (ICCCN) | 979-8-3503-3618-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCN58024.2023.10230183

***Abstract*—Millions of Wi-Fi cameras have been deployed in businesses and households in the last decade. Most of them are used to provide security surveillance services. It raises new security concerns because these cameras could become the target of various attacks. Among them, Evil Twin, Deauthentication, and Disassociation attacks are well-known, easy-to-launch, and dangerous ones. However, there is a lack of deep understanding and awareness of these attacks, as well as efficient mitigation mechanisms. In this paper, we design a set of experiments to demonstrate how easily and effectively these attacks can be launched from simple computing platforms like Raspberry Pi using publicly available, open-source, and easy-configurable tools toward a set of carefully selected, popular, and highly reputed Wi-Fi cameras. Based on our testing, we report our interesting observations and discuss the mitigation approaches. We believe these attacks are beyond cameras and we hope our work can bring serious attention to the security of Wi-Fi equipped devices.**

***Index Terms*—Evil Twin, Deauthentication, Disassociation, Wi-Fi, Cameras, WPA2/3, Wireless Security**

I. Introduction

Wi-Fi has evolved to be the most pervasive wireless communication technology. According to a report from the Wi-Fi Alliance, 18 billion devices currently are Wi-Fi equipped. [1]. Research published by Maximize Market Research indicates that the wireless security cameras market is valued at 5.25 billion dollars in 2021, and it will reach 13.47 billion dollars in 2029 with an annual growth of 12.5% [2]. The deployment of millions of Wi-Fi cameras for security surveillance raises new security concerns because these cameras can be the target of various attacks.

There are many different kinds of attacks that can be launched against Wi-Fi cameras. For example, a Deauthentication attack can be launched simply by sending Deauthentication frames to a legitimate Wi-Fi access point and the targeted victims [3], [4]. A Disassociation attack is conducted in a similar way. Instead, the attacker sends Disassociation frames [4]. Both attacks result in a disconnection of the victim's device from the legitimate access point. These attacks could be used to stop surveillance services and destroy or prevent the creation of evidence if the camera relies solely on network storage. Evil Twin attacks involve spoofing a legitimate access point and tricking victims into connecting to the attacker's network [5]. This can lead to various Man in the Middle (MITM) attacks [6]. Moreover, Deauthentication/Disassociation attacks can be used in conjunction with Evil Twin attacks to improve effectiveness [7]–[10].

Compared with the pervasive availability of Wi-Fi cameras used in security surveillance, there is not sufficient research that studies the severe risks in Wi-Fi cameras, although several existing efforts discuss Evil Twin attacks and mitigation methods [7]–[9]. In this paper, we investigate the effectiveness of the above attacks on popular Wi-Fi cameras available on the market. We utilize widely used and open-source tools such as Airgeddon [11], Aircrack-ng [12], and MDK4 [13] to demonstrate the easiness and effectiveness of launching these attacks. Moreover, we would like to develop an understanding of the vulnerabilities that can be exploited by these attacks and explore approaches that can mitigate these attacks.

To achieve the above goals, we create a series of experiments. They are designed to test the effectiveness of Evil Twin, Deauthentication, and Disassociation attacks at different distances for different devices, to compare the differences among the attacks, and to check for Evil Twin auto-connection. To show how easily we can launch these attacks, we perform attacks from two types of devices, a regular laptop, and a Raspberry Pi 3B, and we record the time it takes for these attacks to succeed. These attacks target six popular Wi-Fi cameras with various features selected from Amazon.com.

From experiments, we find that two out of six tested cameras auto-connect to the Evil Twin network. This may result in MITM attacks. For these two cameras, the success of the Evil Twin attack requires a Deauthentication or Disassociation attack. Moreover, Evil Twin with Deauthentication attacks is more effective compared with Evil Twin with Disassociation attacks or an Evil Twin by itself. Attacks launched from embedded devices like a Raspberry Pi can be as effective as those launched from a powerful laptop, while distance does not play a significant role in the effectiveness of tested attacks.

This research is beneficial in three ways. First, performing these attacks toward popularly used Wi-Fi cameras can reveal how common the vulnerability exists in these devices and thus bring attention and awareness of their dangers. We hope this will encourage vendors to test their products before releasing them to the market and to develop efficient mechanisms that can efficiently apply patches to stop the attacks if reported. Second, testing these attacks launched in different settings helps us to realize how easily the attacks can be launched. We

also obtain knowledge of the effectiveness of Deauthentication and Disassociation attacks at various distances. As well as how they complement Evil Twin. Third, it implies the need for WPA3 [14] and why vendors need to implement it at a much faster rate. Moreover, we also need to develop other ways to mitigate these attacks where WPA3 might not be an option.

The rest of the paper is organized as follows. Section II presents the background and motivation of this research. Section III describes the design of the experiments. We discuss the test results and observations in Section IV, followed by a discussion of possible remedies in Section V. Finally, we conclude the paper and discuss future work in Section VI.

II. Background and Motivation

In this section, we first present relevant information about WPA2 and WPA3. Then we briefly introduce the attacks that are of interest, including Deauthentication, Disassociation, and Evil Twin attacks.

A. WPA2 and WPA3

With the widespread of Wi-Fi devices, Wi-Fi security has evolved from WEP, WPA, WPA2 to WPA3 [15]. WPA2 is ratified in 2004 as an improvement over WPA. WPA2 support is required for a product to have a Wi-Fi Alliance certification from March 2006 to June 2020 [16]. Authentication with a WPA2 network relies on the client knowing a passkey. WPA2 is extremely popular, making up 68.75% of all Wi-Fi networks in 2020. One of the main differences between WPA2 and WPA3 is how management frames are handled. In WPA2, management frames are not authenticated so it is easy for an attacker to spoof them. This makes Deauthentication and Disassociation attacks possible [14]. One of the changes WPA3 made is the mandatory implementation of Management Frame Protection (MFP) [14]. This effectively prevents Deauthentication and Disassociation attacks. However, despite the effectiveness of WPA3, its implementation has not been sufficient [16] after its release in June 2018. According to the Wigle.net database, only 0.23% of networks are currently using WPA3 as of March 30th, 2023 [17]. In addition, there are still other security concerns regarding WPA3 such as downgrade attacks, denial-of-service attacks, connection deprivation attacks, active dictionary attacks, etc. [14], [18]–[20].

B. Deauthentication and Disassociation Attacks

Deauthentication and Disassociation attacks are well-known attacks toward 802.11 prior to WPA3. An attacker can create management frames to trick client devices into disconnecting from an AP [8], [10]. Fig. 1 explains how Deauthentication attack works. The attacker needs to obtain the legitimate AP's or victim's Media Access Control (MAC) address by using wireless packet sniffing tools [21]. Then it can send a Deauthentication management frame, i.e., a Deauthentication request, with the spoofed address of the AP or the victim to the other side of the connection. The attack is successful when the AP disconnects the victim after receiving the Deauthentication request from the attacker. Disassociation attacks work in a similar way except that attackers send Disassociation frames instead. Aircrack-ng can be used to send Deauthentication frames [12]. MDK4 sends both Deauthentication and Disassociation frames [13]. These attacks can cause significant problems for Wi-Fi cameras, especially when they are used in security surveillance applications. The success of these attacks will suspend real-time video streaming and disturb security surveillance services, even though some Wi-Fi cameras have the capacity to record surveillance videos using local storage.

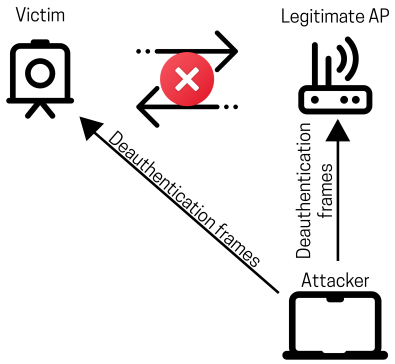

Fig. 1. Concept of the Deauthentication attack.

C. Evil Twin Attacks

An Evil Twin attack happens when an attacker spoofs a legitimate AP by copying its Service Set Identifier (SSID) and MAC address. The attacker can easily find the SSID and MAC address of the legitimate AP by positioning a compatible Wi-Fi adapter and device within the communication range of the AP. Airgeddon [11] is a tool that simplifies the process of creating an Evil Twin and allows us to use Aircrack-ng and MDK4 in conjunction. Once launched, devices could auto-connect to it, or users might manually connect to it thinking it is a legitimate AP. Once accomplished it can lead to various MITM (Man in the Middle) attacks [7]–[9]. An attacker can also sniff packets, which can be very dangerous if sensitive data is not using end-to-end encryption. By combining Evil Twin with a Deauthentication or Disassociation attack, it may significantly improve its effectiveness.

D. Motivation

With a huge amount of Wi-Fi cameras deployed in security surveillance applications [2], they raise serious security concerns about these applications. If these cameras can be easily attacked by the aforementioned attacks, these surveillance applications collapse. Considering the slow deployment of WPA3, this security concern is magnified. However, there still lacks a sufficient understanding or even broad awareness of these attacks. Our research in this paper aims to fill the gap.

By utilizing publicly available, open-source tools such as Airgeddon, Aircrack-ng, and MDK4, We first plan to perform attacks and conduct an in-depth analysis of Evil Twin, Deauthentication, and Disassociation attacks when applied to attack Wi-Fi cameras. This allows us to demonstrate the danger, effectiveness, and easiness of these attacks. In addition,

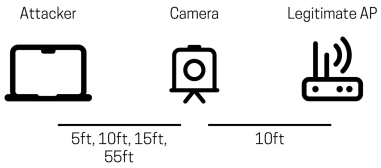

Fig. 2. Experiment setup.

we want to study the differences and effectiveness between Deauthentication and Disassociation attacks, as well as investigate how they can be more dangerous when we couple them with Evil Twin attacks. Furthermore, we want to test the possibility of a Wi-Fi camera auto-connecting itself to an Evil Twin network because this can raise serious security and privacy concerns. When the results of this research are shared with Wi-Fi camera users and vendors, we hope this can raise awareness and education about Wi-Fi camera security to the public. Besides, we hope that vendors can apply more security controls before they release products to the market, or they can take quick actions to patch the Wi-Fi cameras if a vulnerability is reported. Finally, we would like to not only urge the deployment of WPA3 but also boost research in mitigation approaches that complement WPA2.

III. Design of the Experiment

In alignment with the goals of the proposed research, this section describes the design of the experiments, the choices of tools, the data to collect, and the selection of cameras.

A. Experiment Setup

In the experiment, we use three devices as shown in Fig. 2, including a legitimate router/access point (the AP), a Wi-Fi camera (the victim), and a device that simulates an attacker (the attacker). The victim is located within the communication range of both the AP and the attacker. Before the attack, the victim connects to the legitimate AP. After the attacker launches different attacks targeting the victims, We observe the behaviour of the victim and record the data that helps us to indicate the status of attacks. This simulates a very similar environment where these attacks may be deployed in real life.

We use a TP-Link AC1200 (Archer A54) as the legitimate AP. This is a popular router for family Wi-Fi networks and receives a 4.3 review score with over 25,000 reviews on Amazon.com. For the attacker, we use two types of devices, a Kali Linux virtual machine (VM) hosted on a MacBook Pro 2018 and a Raspberry Pi 3B running the ARM version of Kali Linux [22]. The virtual machine was configured with 4GB of RAM, 4 processor cores (from a 2.3 GHz Quad-Core Intel Core i5), and USB 2.0. Both devices use an Alfa AWUS036NHA Wireless Adaptor attached via USB. These two devices represent a powerful, full-feathered, general-purpose computer and a less powerful, portable, embedded computing device. We want to test if such an embedded device is sufficient to launch the attack. Additionally, in the Evil Twin attack simulation, the attacker will set up an open, unencrypted network, while the legitimate network uses WPA2-PSK, with AES encryption, in 11bgn mixed mode for all cameras except the Google Nest. The Google Nest supports WPA3 so the legitimate router used WPA3-SAE for that camera. The attacker can set up this attack without knowing the password of the legitimate network. The choice of cameras is detailed in Section III-B.

Besides testing Deauthentication and disassociation attacks, we also test three different styles of Evil Twin attack, i.e., Evil Twin by itself, Evil Twin with Deauthentication, and Evil Twin with Disassociation. The Evil Twin by itself attack involves only setting up a spoofed AP and observing the behaviors of victims. The Evil Twin with Deauthentication attack involves setting up a spoofed AP and sending Deauthentication frames targeting the AP and/or the victim. The Evil Twin with Disassociation attack also creates a spoofed AP, but it sends both Deauthentication and Disassociation frames targeting the AP and/or the victim. We chose Deauthentication and Disassociation attacks due to their popularity, ease of use and strong effectiveness against WPA2 networks. There are other denial of service attacks supported by Airgeddon [11] but they are outdated and not as effective. The Evil Twin attack by itself is designed to test how the camera's firmware responds to two identical networks with different security settings.

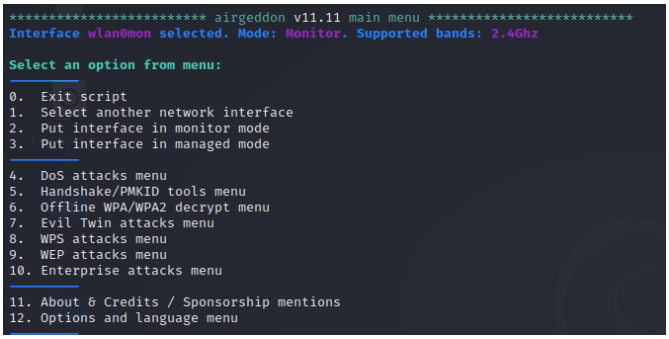

Fig. 3. A snapshot of Airgeddon.

The selected tools to launch attacks are all open-source, easy-to-use, and compatible with Kali Linux [22]. Table I indicates the tools for specific attacks. For the Evil Twin with Deauthentication/Disassociation attack, we use Airgeddon [11] since it supports these attacks naturally through a user-friendly and intuitive interface. A screenshot of Airgeddon is shown in Fig. 3. The Deauthentication attacks are powered by Aircrack-ng [12] that only sends Deauthentication frames, while the Disassociation attacks are powered by MDK4 [13] that sends both Deauthentication and Disassociation frames at the same time. As shown in Fig. 4, a command from the Aircrack-ng suite is used to launch Evil Twin by itself.

TABLE I
List of Attacks and Used Tools

Attack	Tool
Evil Twin by itself	Aircrack-ng
Evil Twin with Deauthentication/Disassociation	Airgeddon
Deauthentication Attack	Aircrack-ng
Disassociation Attack	MDK4

```
┌──(kali㉿kali)-[~]
└─$ sudo airbase-ng -a 54:AF:97:06:05:5D -e Test -c 10 wlan0mon
16:15:36  Created tap interface at0
16:15:36  Trying to set MTU on at0 to 1500
16:15:36  Trying to set MTU on wlan0mon to 1800
16:15:36  Access Point with BSSID 54:AF:97:06:05:5D started.
```

Fig. 4. A snapshot of using Aircrack-ng command to launch Evil Twin by itself attack.

To investigate the impact of distance between the attacker and the victim, we set the distance between them to be 5ft, 10ft, 15ft, and 55ft respectively in different tests, while the distance between the victim and the legitimate AP is fixed to 10ft, a reasonable distance in a common Wi-Fi network. We try 55ft as a long distance to find an upper limit where Evil Twin attacks start to lose effectiveness. All attacks are tested at each distance for each camera.

TABLE II
MEASURED SIGNAL STRENGTH (SS)

Description	Result
SS Between the AP and the Camera (10ft)	-34 dBm
SS Between the attacker and the Camera (5ft)	-31 dBm
SS Between the attacker and the Camera (10ft)	-32 dBm
SS Between the attacker and the Camera (15ft)	-44 dBm
SS Between the attacker and the Camera (55ft)	-70 dBm

We collect several types of data to support attack analysis. First, we measure the signal strength of the AP and the attacker at each distance. This provides additional information beyond the impact of the distance. Table II records the measured signal strength of both devices at different distances. The attacker has a similar level of signal strength compared with the AP when it sits 5 or 10ft away from the victim. Its signal strength degrades and becomes weaker than the AP's when the attacker moves to a location over 15ft away from the victim. Second, we measure the time for the victim to connect to our Evil Twin. A timer is set when the attack starts, and it stops when the camera appears under the Control window in Airgeddon. We use the camera's associated mobile app to record the time that the victim loses connection to the legitimate AP after the attack. A timer starts when the attack launches, and it stops when the app shows a disconnection from the camera's live feed. This method obtains an approximate time that is close enough to be used as an estimation. Third, we sniff the attack traffic using Wireshark [23] for further analysis. Fig. 5 shows sample information from a captured Deauthentication frame.

Source Address	54:af:97:06:05:5d
Destination Address	ff:ff:ff:ff:ff:ff (Broadcast)
Reason Code	0x0007

Fig. 5. Information contained in a sample Deauthentication frame.

B. Selection of Cameras

We select six cameras from Amazon.com for our test. When we select these cameras, we consider multiple factors as listed in Table III-B, aiming to select a set of popular cameras with various features and good reviews (4.0+). For example, we select cameras with and without WPA3 support. As we cannot find a lot of popular cameras with WPA3 support, five out of six cameras only support WPA2. Half of these cameras have an SD slot. It allows them to record videos locally. Next, we chose these cameras based on their popularity and affordability. Half of these cameras receive more than $17,000$ reviews. One is extremely popular with over $240,000$ reviews. The price of these cameras ranges from $30 to $200, covering low-end to high-end options available on the market. Finally, we also want a camera aimed at commercial use, so we selected the Alivision PTZ Camera.

IV. Results and Observations

This section discusses our observations from the experiments. The results are displayed in Fig. 6-10. In each figure, each bar indicates a time in seconds related to a specific attack with the specification of the attacking device, the camera, and the distance between them. For example, in Fig. 6, the leftmost blue bar indicates that the Evin Twin by itself attack launched by a virtual machine located 5ft away from the Kasa camera successfully disconnects the camera from the legitimate AP in 54 seconds. If a camera is not listed in a figure, it means the attack does not work for it at any distance. If the attack does not work on a camera for a specific distance, the bar is marked with a red "X". Also, in some cases when the camera auto-connects to an Evil Twin almost no time after it loses connection to the legitimate AP, the bar is marked with a blue "X". Please also note that, in the figure, VM stands for Virtual Machine, and RP stands for Raspberry Pi 3B.

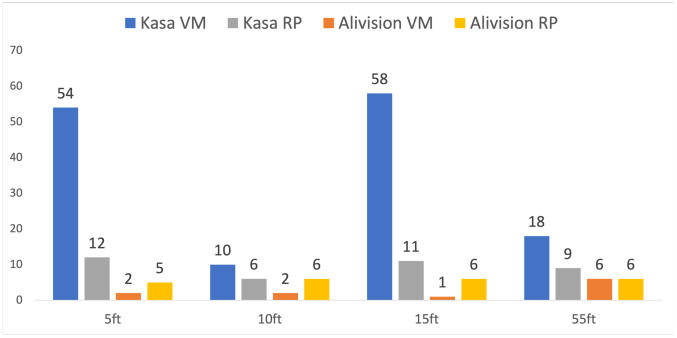

Fig. 6. Disconnection time of Evil Twin by itself.

Impact of Distance and Signal Strength. Distance does not seem to be an important impact on the effectiveness of most tested attacks. Only in the Evil Twin with Deauthentication attack, the attack starts to fail on one camera (Blink mini) when the attacker is 15ft or more away from the victim. The reason could be SS fading with the distance. This observation surprises us as launching successful attacks from a device far away from the victim can make the attacks more dangerous and difficult to detect and locate the attacker.

Disconnection in Evil Twin by Itself. Another interesting finding is that two out of six cameras, specifically Kasa and

TABLE III
LIST OF SELECTED CAMERAS

Name	WPA3 Support	SD Card Support	Average Review Score	Number of Reviews	Price
Ring Stick Up Camera 3rd generation [24]	No	No	4.7	54,914	$99.99
Kasa Indoor Pan EC70 [25]	No	Yes	4.4	17,629	$29.99
Blink Mini (Wired) [26]	No	No	4.4	240,934	$34.99
Reolink Argus Eco [27]	No	Yes	4.1	1,381	$59.99
Alivision PTZ IP Camera [28]	No	Yes	4	86	$198.90
Google Indoor Nest Wired (2nd generation) [29]	Yes	No	4.3	1,411	$89.95

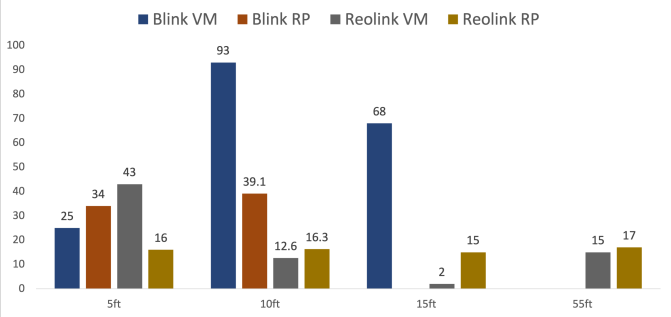

Fig. 7. Disconnection time of Evil Twin with Deauthentication.

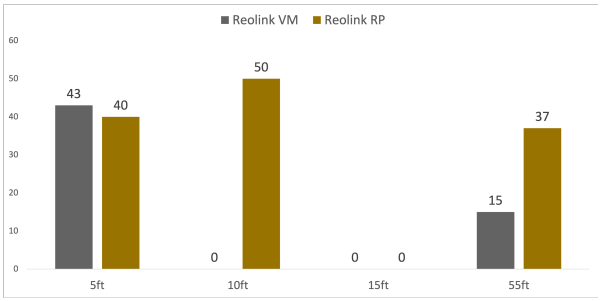

Fig. 8. Disconnection time of Evil Twin with Disassociation.

the expensive Alivision, will lose connection to the legitimate AP as soon as an Evil Twin is set up by using Aircrack-ng command as shown in Fig. 4. The time it takes for the camera to lose connection to the legitimate AP is shown in Fig. 6. No Deauthentication or Disassociation frames are needed. This attack could potentially work even toward some WPA3-supported cameras since it does not require sending management frames [14], although it does not work on the only WPA3-supported camera in our list, Google Nest.

Evil Twin Auto-Connection. Two out of six cameras, specifically the Blink Mini (the most popular one in our list with over 240k reviews) and Reolink Argus Eco are vulnerable to Evil Twin auto-connection, as shown in Fig. 7 and 8. Fig. 11 shows a snapshot captured from Airgeddon when the Blink Mini successfully auto-connects to the Evil Twin. Cameras auto-connecting to an Evil Twin is a big concern because it is an easy-to-launch attack but can potentially lead to dangerous MITM attacks. We are astonished to find this simple attack can be so effective toward such a popular top-seller and Amazon choice product.

Deauthentication vs. Disassociation Effectiveness. Deauthentication and Disassociation attacks are both effective and have a similar efficiency toward all five WPA2-supported cameras, including the expensive and business-level Alivision PTZ IP Camera, as shown in Fig. 9 and 10. Moreover, the Evil Twin auto-connection attacks are more successful with Deauthentication than with Disassociation as shown in Fig. 7 and 8, i.e., Evil Twin auto-connection with Deauthentication succeeds in two cameras, while Evil Twin auto-connection with Disassociation only succeeds in one camera.

Unusual Response to Disassociation Attack. Another interesting finding is that the Ring Stick Up camera would sometimes become completely unresponsive after an Evil Twin with Disassociation attack. It would never reconnect to the legitimate AP even after the attack is turned off. Making it restore the connection to the AP requires rebooting the camera by reconnecting the battery. This only occurs with Disassociation attacks, but not Deauthentication attacks.

Virtual Machine vs. Raspberry Pi 3B. From Fig. 9 and 10, there is no significant difference if the attack is launched from the virtual machine or Raspberry Pi 3B. This implies that the attacker can launch the attack using small-size and portable embedded devices. It increases the danger of attacks.

Packet Analysis. We sniff packets using Wireshark when attacks make the Blink Mini and Reolink Argus Eco connect to an Evil Twin. Packet analysis for the Blink Mini shows the camera uses TCP with TLS 1.2, and its source port is 52117 with a destination port of 443, a common port for HTTPS. Reolink Argus Eco uses UDP with a source port of 53546 and a destination port of 13783. Due to the encryption, the video data could not be reassembled or accessed at both cameras.

V. POSSIBLE MITIGATION APPROACHES

Currently, we believe the best method of defense against Deauthentication and Disassociation attacks is probably WPA3. Based on the packet analysis, Deauthentication and Disassociation attacks rely on management frames not being validated, so protecting management frames can mostly prevent these attacks [14]. According to our tests, if we disable Deauthentication or Disassociation attacks, it will be difficult for attacks to make a camera auto-connect to an Evil Twin. Unfortunately, implementation and deployment of WPA3 have been very slow [16], [17]. If WPA3 cannot be available, we need to seek solutions that build on top of WPA2. Below are some potential directions that we can explore.

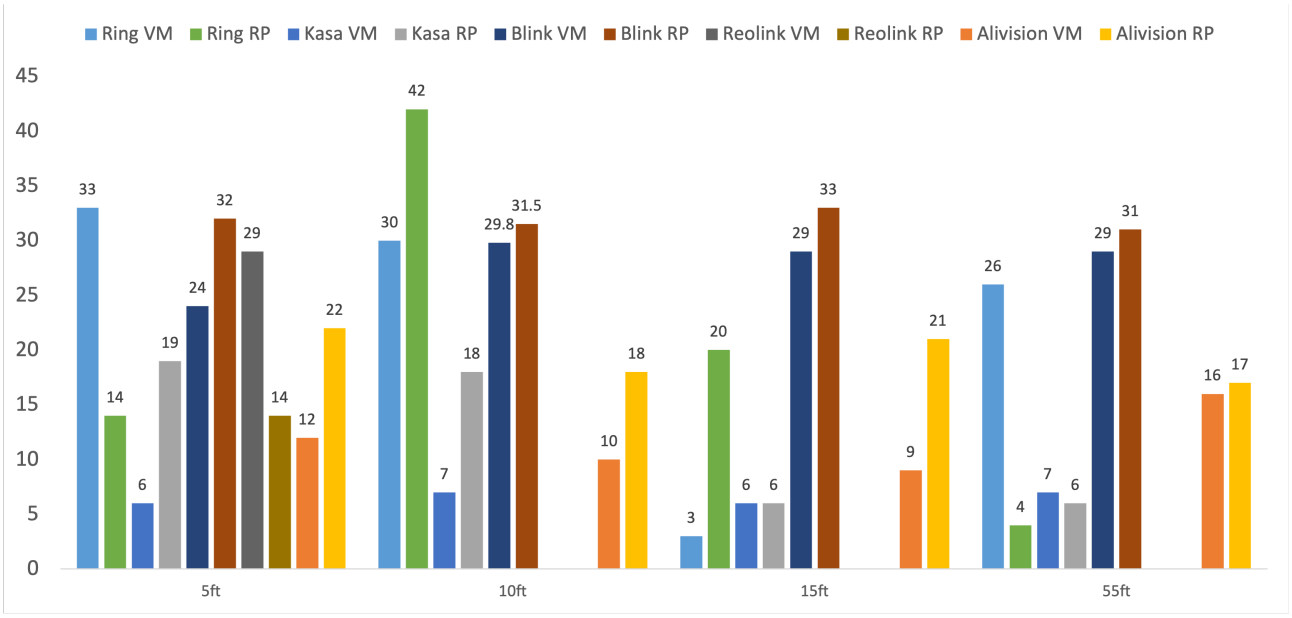

Fig. 9. Disconnection time of Deauthentication.

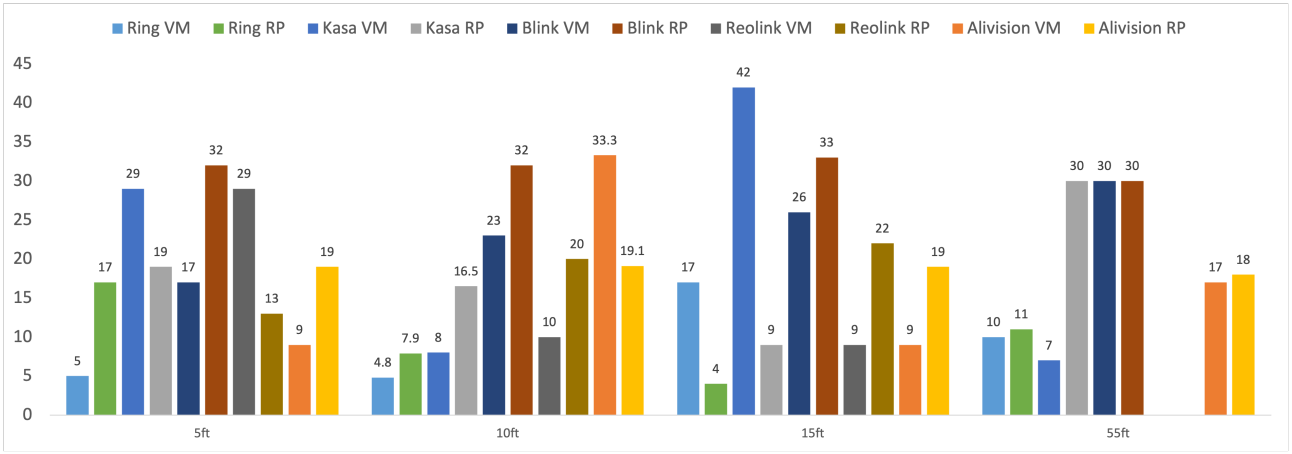

Fig. 10. Disconnection time of Disassociation.

First, Virtual Private Network (VPN) technologies are under consideration to mitigate some MITM attacks [8]. By using a VPN, the attacker may not be able to read any data from packets that are sniffed. It is also important to use protocols with end-to-end encryption whenever possible. A company policy could require all employees to always be using a VPN even when connected to the company's own Wi-Fi networks. Second, systems can be set up to monitor for Evil Twin networks [8]. A whitelist could be created containing known BSSIDs or MAC addresses that belong to the organization. If an AP is using an SSID but it has a BSSID that is not part of the whitelist, that likely means an Evil Twin is set up. Or if an AP has no encryption when it should be but is using your SSID and one of your BSSIDs, it is a good indicator that an Evil Twin is present. An incident response team could then try to locate the source of the Evil Twin and respond to the threat accordingly. Third, using cameras that have local storage, such as an SD card, to ensure the footage is not lost even if it is disconnected from the network. Wired cameras could also be used in conjunction with Wi-Fi cameras if possible.

Fourth, it is also imperative that vendors test their products for various types of common attacks. They also need to keep alert to new attacks and take action quickly when successful attacks are reported. For example, after our tests, we have reported the vulnerability of Evil Twin auto-connection to both Blink and Reolink. Reolink has taken quick action by issuing a firmware update through its app. Blink has responded and said the issue was sent to their security team. Fifth, security algorithms can be deployed locally in cameras to detect and stop known attacks. For example, cameras should be programmed to check if the network security configuration or MAC address has changed before auto-connection. Cameras

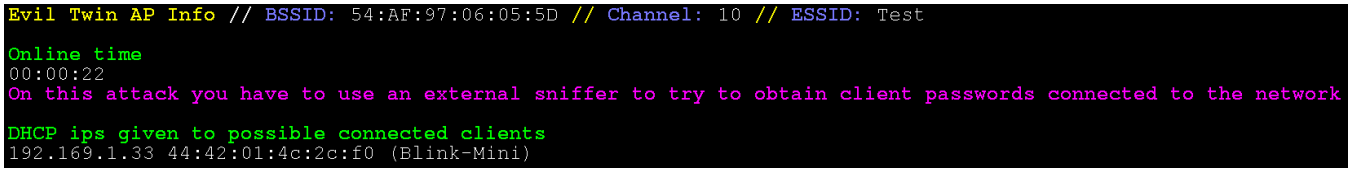

Fig. 11. Screenshot of Blink Mini auto-connecting to Evil Twin.

might want to make sure that they do not lose connection when an Evil Twin network is started. However, losing connection might be preferable to connecting to an Evil Twin network. Finally, it is essential to promote Wi-Fi security awareness education. This can make the attacks much more difficult.

VI. Conclusion and Future Work

Evil Twin, Deauthentication, and Disassociation attacks are serious security issues for Wi-Fi cameras, especially when considering the lack of WPA3 support in most popular Wi-Fi cameras. These attacks require no user interaction or prior authentication and can be easily performed using popular open-source software [11]–[13], [22]. Of the 6 cameras we test, two of them auto-connect to our Evil Twin. The results have been reported to the respective vendors. Also, two different cameras lose connection just because an Evil Twin network is set up. This can potentially be an attack that continues to work even with WPA3 since it does not require sending management frames. We also observe that Deauthentication attacks tend to be more successful in getting a device to auto-connect to an Evil Twin than Disassociation attacks. Finally, we discuss several possible mitigation approaches.

We plan to extend this work from three perspectives. First, we would like to test possible attacks aimed at Wi-Fi devices that have WPA3 support. Second, with the popularity of connected autonomous vehicles (CAV), we want to analyze the security risks of wireless components in CAVs. Finally, we intend to study novel security protection algorithms and protocols, as well as innovative device security administration mechanisms that can be applied in extremely large-scale applications like Internet of Everything.

Acknowledgement

This paper is partially supported by the National Science Foundation (NSF) HSI program under grant no. 1928622 and CISE-MSI program under grant no. 2240513.

References

[1] W.-F. Alliance, "Wi-fi alliance® 2022 wi-fi® trends," 2022. [Online]. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-2022-wi-fi-trends

[2] M. M. Research, "Wireless security camera market: Global industry analysis and forecast (2021-2029) trends, statistics, dynamics, segment analysis," *Globe Newswire*, 2021.

[3] A. Amoordon, V. Deniau, A. Fleury, and C. Gransart, "A single supervised learning model to detect fake access points, frequency sweeping jamming and deauthentication attacks in ieee 802.11 networks," *Machine Learning with Applications*, vol. 10, p. 100389, 2022.

[4] N. Baharudin, F. H. M. Ali, M. Y. Darus, and N. Awang, "Wireless intruder detection system (wids) in detecting de-authentication and dis-association attacks in ieee 802.11," in *2015 5th International Conference on IT Convergence and Security (ICITCS)*. IEEE, 2015, pp. 1–5.

[5] A. Bartoli, E. Medvet, and F. Onesti, "Evil twins and wpa2 enterprise: A coming security disaster?" *Computers & Security*, vol. 74, pp. 1–11, 2018.

[6] M. Ahmad, S. Lutfi, and S. Abdullah, "Extended generic process model for analysis mitm attack based on evil twin," in *Journal of Physics: Conference Series*, vol. 1569, no. 2. IOP Publishing, 2020, p. 022031.

[7] F. Lanze, A. Panchenko, I. Ponce-Alcaide, and T. Engel, "Undesired relatives: Protection mechanisms against the evil twin attack in ieee 802.11," in *Proceedings of the 10th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 2014, p. 87–94.

[8] R. Muthalagu and S. Sanjay, "Evil twin attack mitigation techniques in 802.11 networks," *International Journal of Advanced Computer Science and Applications*, vol. 12, 06 2021.

[9] V. Roth, W. Polak, E. Rieffel, and T. Turner, "Simple and effective defense against evil twin access points," in *Proceedings of the first ACM conference on Wireless network security*, 2008, pp. 220–235.

[10] P. Bahl, R. Chandra, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "Enhancing the security of corporate wi-fi networks using dair," in *Proceedings of the 4th International Conference on Mobile Systems, Applications and Services*, 2006, p. 1–14.

[11] Airgeddon, https://github.com/v1s1t0r1sh3r3/airgeddon, 2022.

[12] Aircrack-ng, https://github.com/aircrack-ng/aircrack-ng, 2022.

[13] MDK4, https://github.com/aircrack-ng/mdk4, 2022.

[14] M. Appel and I. S. Guenther, "Wpa 3-improvements over wpa 2 or broken again?" *Network*, vol. 7, 2020.

[15] S. Kwon and H.-K. Choi, "Evolution of wi-fi protected access: security challenges," *IEEE Consumer Electronics Magazine*, vol. 10, no. 1, pp. 74–81, 2020.

[16] G. Sagers, "Wpa3: The greatest security protocol that may never be," in *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2021, pp. 1360–1364.

[17] "Wigle stats," 2023. [Online]. Available: https://wigle.net/stats

[18] K. Lounis and M. Zulkernine, "Wpa3 connection deprivation attacks," in *Risks and Security of Internet and Systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29–31, 2019, Proceedings 14*. Springer, 2020, pp. 164–176.

[19] E. Chatzoglou, G. Kambourakis, and C. Kolias, "How is your wi-fi connection today? dos attacks on wpa3-sae," *Journal of Information Security and Applications*, vol. 64, p. 103058, 2022.

[20] M. Patel, P. Amritha, and R. Sam jasper, "Active dictionary attack on wpa3-sae," in *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1*. Springer, 2021, pp. 633–641.

[21] P. Asrodia and H. Patel, "Analysis of various packet sniffing tools for network monitoring and analysis," *International Journal of Electrical, Electronics and Computer Engineering*, vol. 1, no. 1, pp. 55–58, 2012.

[22] O. Security, "Kali linux," https://www.kali.org, 2022.

[23] Wireshark, "Wireshark," https://github.com/wireshark/wireshark, 2022.

[24] "Ring stick up cam battery," 2022. [Online]. Available: https://a.co/d/6nh48lP

[25] "Kasa indoor pan/tilt," 2022. [Online]. Available: https://a.co/d/39RESRQ

[26] "Blink mini," 2022. [Online]. Available: https://a.co/d/98bVZm7

[27] "Reolink argus eco," 2022. [Online]. Available: https://a.co/d/bPLQfZ2

[28] "Alivision ptz ip camera," 2022. [Online]. Available: https://a.co/d/a67RFJ7

[29] "Google nest cam (indoor, wired)," 2022. [Online]. Available: https://store.google.com/product/nest_cam_indoor_specs