UNIVERSITY OF WEST LONDON
The Career University

UWL REPOSITORY

repository.uwl.ac.uk

Evil Twin Attacks on Smart Home IoT Devices for Visually Impaired Users

Yeboah-Ofori, Abel ORCID logoORCID: https://orcid.org/0000-0001-8055-9274 and Hawsh, Aden (2023) Evil Twin Attacks on Smart Home IoT Devices for Visually Impaired Users. In: 2023 IEEE International Smart Cities Conference (ISC2), 24-27 September 2023, Bucharest, Romania.

http://dx.doi.org/10.1109/ISC257844.2023.10293225

This is the Accepted Version of the final output.

UWL repository link: https://repository.uwl.ac.uk/id/eprint/10612/

Alternative formats: If you require this document in an alternative format, please contact: open.research@uwl.ac.uk

Copyright: Creative Commons: Attribution 4.0

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy: If you believe that this document breaches copyright, please contact us at open.research@uwl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Rights Retention Statement:

Evil Twin Attacks on Smart Home IoT Devices for Visually Impaired Users

1st Abel Yeboah-Ofori
School of Computing and Engineering
University of West London
United Kingdom
Abel.yeboah-ofori@uwl.ac.uk

1st Aden Hawsh
School of Computing and Engineering
University of West London
United Kingdom
21462142@student.uwl.ac.uk

Abstracts--Securing the Internet of Things (IoT) devices in a smart home has become inevitable due to the recent surge in the use of smart devices by the visually impaired. The visually impaired users rely heavily on these IoT devices and assistive technologies for guidance, medical usage, mobility help, voice recognition, news feeds and emergency communications. However, cyber attackers are deploying Evil Twin and Man-in-the-middle (MITM) attacks, among others, to penetrate the network, establish rogue Wi-Fi access points and trick victims into connecting to it, leading to interceptions, manipulation, exploitation, compromising the smart devices and taking command and control. The paper aims to explore the Evil Twin attack on smart devices and provide mitigating techniques to improve privacy and trust. The novelty contribution of the paper is three-fold: First, we identify the various IoT device vulnerabilities and attacks. We consider the state-of-the-art IoT cyberattacks on Smart TVs, Smart Door Lock, and cameras. Secondly, we created a virtual environment using Kali Linux (Raspberry Pi) and NetGear r7000 as the home router for our testbed. We deployed an Evil Twin attack to penetrate the network to identify the vulnerable spots on the IoT devices. We consider the Kill Chain attack approach for the attack pattern. Finally, we recommend a security mechanism in a table to improve security, privacy and trust. Our results show how vulnerabilities in smart home appliances are susceptible to attacks. We have recommended mitigation techniques to enhance the security for visually impaired users.

Keywords--IoT, Smart Homes, Visually Impaired, Cyber Security, Privacy

I. INTRODUCTION

Providing security in IoT devices in smart homes has become inevitable in improving the quality of life for people with disabilities (PwD) to prevent cyberattacks and ensure privacy and trust, especially with the visually impaired [1]. The proliferation of smart home IoT devices and *the use of technologies in Smart Cities* has ushered in a period of unprecedented domestic connectivity and convenience[2]. Visually impaired users rely on assistive technologies, including Smart home wearable devices such as Blood Pressure Monitors, Smart Watches, Smart Fitness Trackers, and Smart Ear-worn phones to assist them in monitoring their health and working remotely. However, that has led to increased cyberattacks such as the evil twin attack, MITM attack, and DoS, among others [7]. Cyberattacks on smart homes, such as the Evil Twin attack, can devastate visually impaired users who rely heavily on these IoT smart home devices and assistive technologies for guidance, medical usage, mobility help, voice recognition and news and emergency communications [3]. The increased use of IoT devices has also provided cybercriminals with new attack vectors such as ARP spoofing, Evil Maid attacks, DoS attacks, and Remote Access Trojans[7]. Further, smart home doors, navigations and guidance devices, news and information for the visually impaired could be compromised, resulting in the risk of home accidents [8]. Furthermore, a WHO report estimated the Visually impaired users to be about 285 million and rely on assistive technologies[9].

Figure 1 considers how attackers can deploy an Evil Twin attack to penetrate the network, establish a rouge Wi-Fi access point and lure the victim to connect to it, leading to various interceptions, data manipulation, exploitation and compromising of the smart home devices and taking command and control[4].

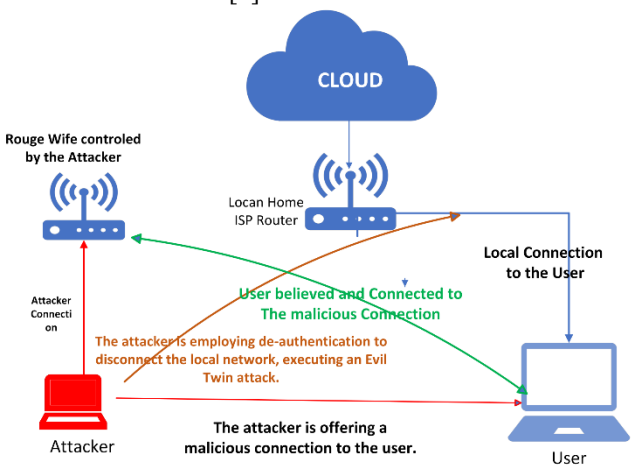

Fig. 1. Evil Twin Attack on Smart Home IoT Devices

A. *State of IoT Devices Connectivity*

Several variables have exacerbated the scale and prevalence of these attacks due to the rapid growth in the IoT industry. A report by IoT Analytics predicts a 9% increase in connected IoT devices worldwide in 2021, bringing the total number of active endpoints to 12.3 billion. More than 27 billion IoT connections are expected by 2025. State of IoT 2023: Number of connected IoT devices growing 16% to 16 billion globally, 2023. The IoT devices growth graph by (State of IoT, 2023) shows that the number of connected IoT devices grew by 16% to 16 billion globally by 2023. shows IoT devices' rapid growth and widespread use in smart homes [5]. The visually impaired experience physiological and psychological impacts during teaching and learning as they are not able to see clearly and concentrate during online learning [6]

B. *Attacks on IoT Devices for the Visually Impaired*

IoT device attacks take various forms, including botnet commandeering connected devices to initiate distributed denial of service (DDoS) attacks or malware designed to extract sensitive data or exploit inherent vulnerabilities in smart home devices or networks. DoS, Evil Twin, MITM attacks, and phishing attempts can have devastating consequences, including financial loss, data theft, and even physical injury [7].

Additionally, smart home mobility devices such as smart canes and walking aids use GPS, AI-generated algorithms, accelerometer, magnetometer, and gyroscope

technologies to monitor and assist the visually impaired user with positioning, orientation, speed and directions. Attackers could remotely compromise, manipulate, and prevent the visually impaired from moving around securely. Furthermore, attackers could use the Evil Twin attack to intercept, manipulate, exploit, and compromise smart medical devices, resulting in severe medical service disruptions and emergency services in critical situations [10]. Examining network segmentation, firewalls, and encryption to reduce the risks associated with IoT devices is relevant in improving IoT security. However, these devices come with inherent vulnerabilities that make securing them challenging. This requires the implementation of secure authentication protocols, encryption, and network segmentation. One of the critical challenges for visually impaired users is their inability to apply timely software and firmware updates to mitigate vulnerabilities.

The paper aims to explore the Evil Twin attack on IoT smart home devices and provide mitigating techniques to ensure privacy and trust. The novelty contribution of the paper is three-fold: First, we identify the various IoT device vulnerabilities and attacks. We consider the state-of-the-art IoT cyberattacks on appliances such as Smart TVs, Smart Door Lock, and cameras, among others. Secondly, we created a virtual environment using Kali Linux (Raspberry Pi) and NetGear r7000 as the home router for our testbed. We deployed an Evil Twin attack to penetrate the network to identify the vulnerable spots on the IoT devices. We consider the Kill Chain attack approach for the attack pattern. Finally, we recommend a security mechanism to improve security, privacy and trust for the visually impaired. Our results show how vulnerabilities in smart home appliances are susceptible to attacks and recommended mitigation techniques to enhance the security for visually impaired users.

II. STATE OF THE ART

This section discusses existing literature and the state of the art regarding smart home (IoT) devices, technologies, attacks, vulnerabilities, and their subsequent impact on visually impaired users. Yet, the increased connectivity also provides cybercriminals with new opportunities to exploit security vulnerabilities, potentially compromising the safety and privacy of homeowners [11]. Regarding smart home devices, Karie et al. (2020) reviewed IoT threat detection, challenges, and future directions by emphasizing the security risks and identifying the lack of standardization in device production as a critical contributor to security risks. [12], explored the vulnerability of low-power IoT devices to cyber-attacks, citing their limited computational capabilities and minimal power consumption as contributing factors. The authors proposed a power-efficient intrusion detection system (IDS) to monitor networks for malevolent activity[13]. However, there are challenges related to the security of the firmware update procedure in IoT devices. [14] discussed the benefits of smart homes and the significant security and privacy risks they pose. The authors elucidate the concept of a smart home environment, its vulnerabilities, and the current security measures to counter such threats. However, attacks from open places such as airports, hotels, and internet cafes on IoT devices require further research. Smart Homes and explored the detecting mechanisms for Evil-twin Attacks in Smart Homes using the Received Signal Strength Indicator by highlighting current approaches, such as detecting attacks on SSIDs, MAC addresses and network traffic patterns. The approach used a multipath effect of WiFi signal to detect the identity of the connected Access Points. However, the paper focuses on weak network exploits, not IoT device attacks. [15] implemented an Evil Twin Attack using discrete event systems in IEEE 802.11 Wi-Fi networks to detect intrusions on the web during a rogue attack on the access points during handshake. However, the paper did not focus on any specific attack on IoT devices in the smart none environment. Most literature on protecting smart homes from IoT-based cyber threats concentrates on standalone security techniques. [16] highlighted common attacks on smart homes, not on devices like Access control, robust encryption systems, demanding authentication processes, advanced anomaly detection mechanisms, and anticipatory threat intelligence approaches.

Some challenges include inadequate standardisation in security protocols, limited user behaviour, and insufficient understanding of user behaviour in smart homes. Integration of legacy systems in smart homes can lead to vulnerabilities that might be exploited. Adequate stakeholder collaboration among manufacturers, service providers, and users is required due to the complexity of smart homes. Finally, a lack of coordination among various entities, resulting in possible security holes and limited emerging technology, including AI, is essential to assess security implications.

III. APPROACH

This section presents an overview of the approach used for the paper, focusing on assessing the security of IoT devices, testing their security postures, and analysing the attack tactics, techniques and procedures attackers use to penetrate IoT devices. Our approach considers the Kill Chain attack model for the attack pattern. To address cybersecurity issues on smart home IoT devices, the paper employs a research technique that combines a qualitative approach by implementing attack methods to identify vulnerabilities to comprehend better complex phenomena such as user behaviour or social norms to understand the threat landscape.

The approach aims to test and evaluate Evil Twin attacks in smart homes. We used a Foscam 5MP Wi-Fi Camera, an ALFA Network AWUS036ACH, a laptop running Kali Linux as a hacking tool, and five IoT devices for our implementation. The design for the home IoT devices will serve as a testbed for the implementation and how to mitigate, fulfilling the goal of the article and casting light on the implementation process. The process involves setting up the environment for all connected IoT devices, implementing attacks and recommending mitigations.

IV. IMPLEMENTATION

This section discusses the implementation processes and the step-by-step methods used for the Smart Home IoT device attack mitigations. The implementation considers the following phases in achieving the attack goals.

A. Phase 1: Setting Up the Lab Environment for the Smart Home IoT Device Attach Implementation

The initial setup of home IoT devices testing consists of a Camera and an ALFA Network AWUS036ACH adapter, home computers, Laptops, and Notepads. Install Kali Linux as a Virtual box on a Windows laptop for the attacks. The following is the home Network equipment as indicated in Figure 3. List of Connected devices in the testing home. BT Smart Hub is my Internet gateway, and NetGear r7000 is our home router. ZyXEL GS1200-5 5-Port Web Managed Desktop Gigabit Switch, OKdo ROCK 4 Model C+ 4GB

(Raspberry Pi), Home Laptops, Foscam IP Camera, Home Smart Door Lock, Home Pcs 9, Smartphones, Smart TV, Amazon Echo speaker and Tablets. We consider the list of Software and tools used in the Lab.

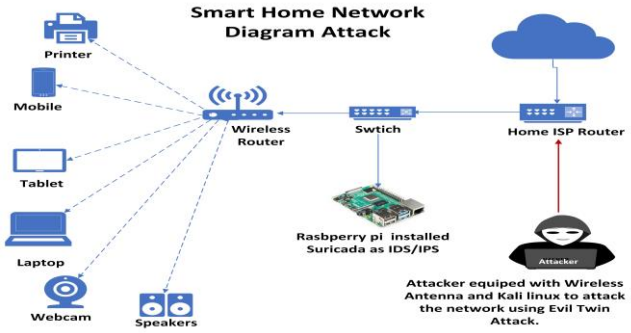

Fig. 2. Home Network with NIDS Installed

Figure 2 depicts the outline of the home smart home environment we are testing and how all deviate interconnectedness—Windows computer with Virtual Box. Kali Linux is installed in the virtual box. rock-4c-plus_debian_bullseye_kde_b55, Wireless software attack Nmap, Airgeddon, Aircrack-ng, Airodump-ng,bettercap, Ettercap, Hping3 and Wireshark. NIDS (Network Intrusion Detection System) Suricata and Snort. Figure 4 shows a graphical representation of the design. Figure 5 shows four equipment: the BT ISP home router, the internet gateway, and the NETGEAR R 7000 router, the primary home router linking all the equipment. Figure 3 shows the logically connected devices for testing the home network, IPS and address.

192.168.1.0/24 > 192.168.1.153 » net.show

IP	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.1.153	08:00:27:3c:b8:ce	eth0	PCS Computer Systems GmbH	0 B	0 B	02:50:01
192.168.1.254	a4:ce:da:0c:e7:19	gateway	Arcadyan Corporation	2.0 MB	1.3 MB	02:50:01
192.168.1.3	98:0d:67:fd:23:72		Zyxel Communications Corporation	0 B	38 kB	02:52:29
192.168.1.73	d4:3b:04:cd:23:6e	DESKTOP-K827OVG.local	Intel Corporate	24 kB	22 kB	04:49:05
192.168.1.74	9c:b6:d0:3e:7e:2c	ADEN_DELL	Rivet Networks	243 kB	135 kB	04:49:05
192.168.1.103	74:c1:4f:7b:72:68		Huawei Technologies Co.,Ltd	5.2 kB	38 kB	02:52:30
192.168.1.139	18:48:be:b6:f7:92	Android.local		223 kB	38 kB	04:49:06
192.168.1.143	74:d4:23:b7:9b:94			49 kB	38 kB	04:49:07
192.168.1.165	0a:db:34:f4:f6:6a			44 kB	36 kB	04:49:07
192.168.1.172	62:a5:f3:19:5e:b7			49 kB	38 kB	04:49:06
192.168.1.213	50:6a:03:ab:93:8c		Netgear	58 kB	40 kB	04:49:07
192.168.1.236	bc:d0:74:25:0a:68	ADENs-MacBook-Pro.local		48 kB	39 kB	04:49:09

Fig. 3. Logically Connected Home Network Devices

B. *Phase 2: Implementing Attack Scenarios*

There is a growing need to learn how cyberattacks affect IoT devices in smart homes [17]. Cyberattacks can result in everything from a breach of personal privacy to devastating financial losses. For instance, hackers can exploit holes in IoT devices to acquire private information, financials, and even behaviour patterns. They can take over gadgets and utilise them to disrupt security protocols, influence home automation systems, or even inflict physical harm through overloading, causing considerable financial and emotional loss due to disrupting their daily lives.

C. *Deploying The Evil Twin Attack*

The Evil Twin Attack is a wireless network attack in which the attacker mimics a wireless access point with a malicious one.

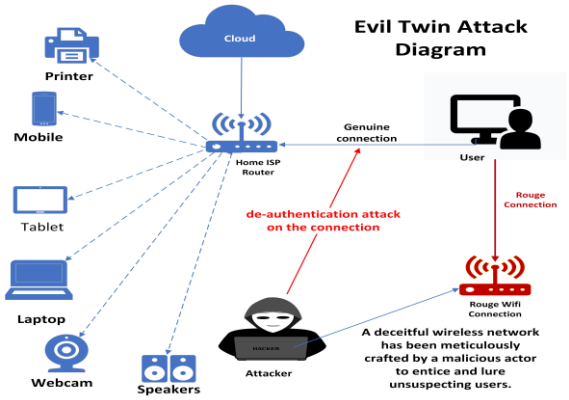

Figure 4. The Evil Twin Attack on Wireless Network

. Once a user joins a hostile network, the attacker can intercept and manipulate their communication, steal sensitive data, and execute other harmful acts. Figure 4 demonstrates how attackers obtain access to home routers using an Evil twin attack. For the implementation, we demonstrate the step-by-step attack using the screenshots below for the implementation process. We set up how a USB wi-fi adopter *iKalili* in Linux machine wireless antenna.

D. *Implementing the Attack Steps*

The following attack steps are used for the implementation**:**

Step 1: Select a wireless antenna for the Kali Linux system, as shown in Figure 4.

Step 2: On the Kali Linux machine, check if the antenna drivers are installed and selected by typing *iwconfig,* as shown below in the screenshot. Figure 5. shows the wlan0 interface in our machine we will be using to retest the demonstration. We type the *iwconfig* command to display the connected wireless adapters.

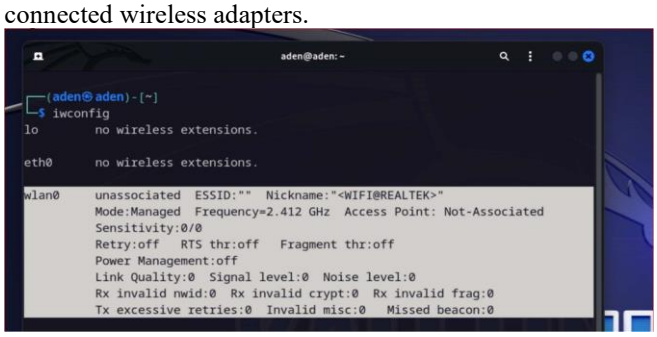

Fig. 5. Checking the available wireless adapter on my machine using the *iwconfig* command.

Step3. We type the *airgeddon* into Kali to call the command.

Kali will check that all the necessary repositories are installed and mark them with an "OK" sign by bringing up airgeddon. Once this is confirmed, we can proceed to use *airgeddon* script. Figure 7 shows how we used the *airgeddon* command to display wlan0 and the Kali interfaces, as mentioned in Figure 6. Further, we will choose the wlan0 interface as it is the alfa USB wireless capable of putting on monitor mode with 2.4GHz and 5.0GHz.

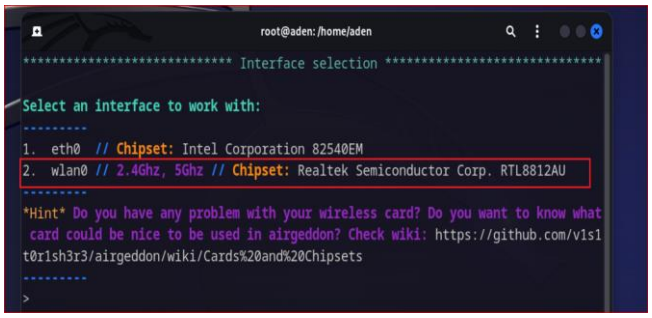

Fig. 7. Airgeddon Interface Installed in Kali Machine

Step 4: In Figure 8, We choose number 2 for wlan0 to be selected as the tool to demonstrate the evil twin attack on my home wireless router to obtain the password.

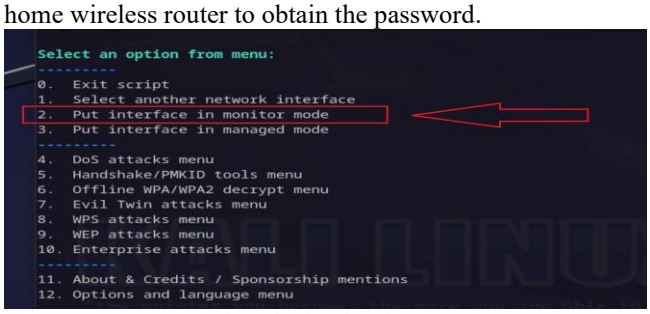

Fig. 8. *airgeddon* Menu after selecting the wlan0

Figure 9 shows how we switch the wlan0 interface from managed to monitoring mode, enabling us to listen to all nearby Wi-Fi networks.

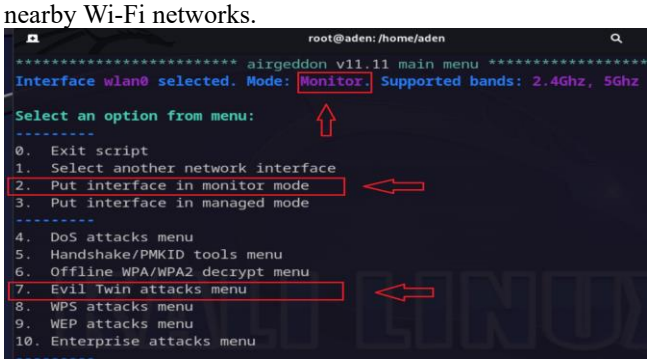

Fig. 9. Wlan on Monitor Mode

Step 5: We selected option 7, Evil Twin Attack, from the menu as indicated in Figure 10, then we were presented with a submenu as shown in Figure 10, marking the fields for BSSID, ESSID, and Channel empty since we have not yet captured any wireless network information. We will select option 9, corresponding to the Evil Twin Access Point (AP) attack with a captive portal.

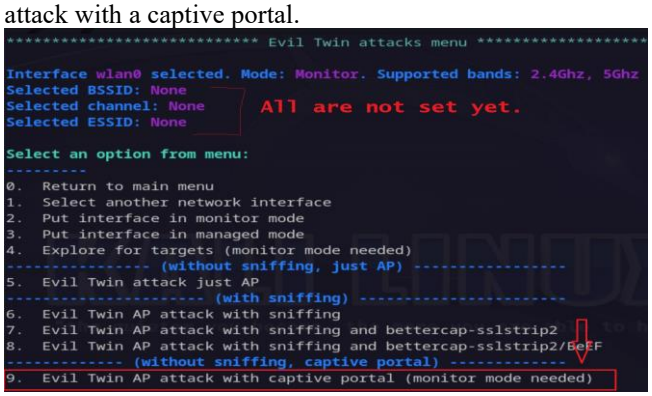

Fig. 10. Selecting the Evil Twin Attack to Deploy

Step 6: Capturing the intended wireless SSD, SSE and channel name. We have chosen 9, as highlighted in Figure 10 on our menu as we have mentioned earlier; after clicking those steps and a couple of Yes or No on the Kali terminal,*airgeddon* starts capturing SSID and channel names of neighbouring wirelesses. After approximately 30 seconds, we used the control + C command to halt the wireless network capture process and import the captured list of wireless networks into the *airgeddon* terminal. Figure 11 shows the *Airgeddon* command capturing mode after selecting the number 9 evil twin attack sub-menu.

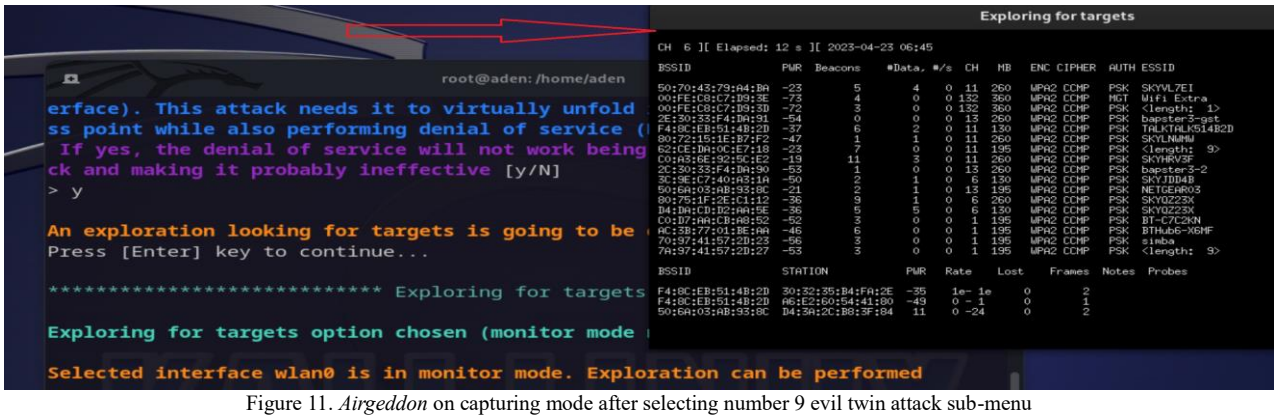

Figure 11. *Airgeddon* on capturing mode after selecting number 9 evil twin attack sub-menu

For privacy reasons, we concealed the ESSID and BSSID of the neighbouring networks in Figure 11 while retaining the details of the network being used for demonstration purposes and the network. Figure 12 shows how we have successfully imported the captured wireless channels by identifying the network router with ESSID=NETGEAR03 and BSSID=50:6A:03:AB:93:8C.

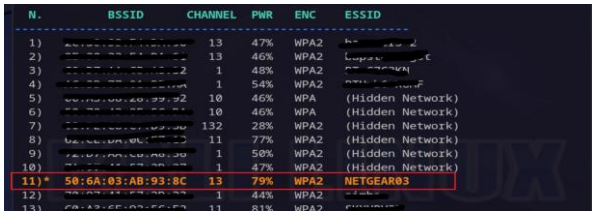

Fig. 12. Wireless Network Capture Process

Next, we will select option 11 from the list indicated by the arrow, enabling us to import the network ESSID

and BSSID into the *airgeddon* terminal. Figure 13 provides a visual representation of the process.

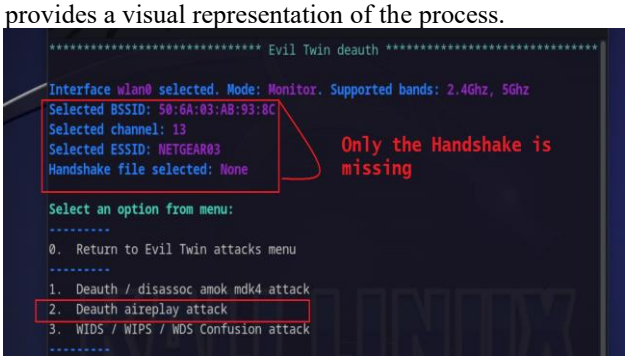

Fig. 13. Network information imported BSSID, ESSID and Channel.

Step 7: We choose our attack method after successfully capturing the ESSID and BSSID of our network, NETGEAR03. Further, we select option number 2 from the menu, which is the *Deauth AirPlay* attack. This is a powerful tool available within *Airgeddon* that sends a Deauth frame. The first step is capturing the handshake file, as shown in Figure 13, and then sending Deauth frames to our network. This attack can disrupt the network connectivity during capturing The Handshake After the De-Authentication Attack.

Step 8: We captured the handshake file that will be used for the attack. Figure 16 indicates that the handshake has been successfully captured. The system prompts us to select a path to save the file. We choose to keep it manually on /home/aden/Desktop. By hitting the Enter button, the system initiates multiple parallel de-authentication windows. We created a Folder and File Path to Save the PASSWORD.

E. Creating De-authentication Frames

Figure 14 shows how the attacker creates de-authentication frames to capture the devices by initiating a command between two devices that enables the interfaces to connect. That forces the client to disconnect from the network by sending several de-authentication frames to the victim. When the victim tries to reconnect to the system, create a rogue site and ask the victim to connect unaware.

Step 9: We have captured a screen capture from the phone, as shown in Figure 14, by combining three images. The first image shows the attacker disconnecting us from our network and creating a rogue network with the same name. The second image, marked with the number 2, displays the AP screen that appeared when we tried to connect to the network.

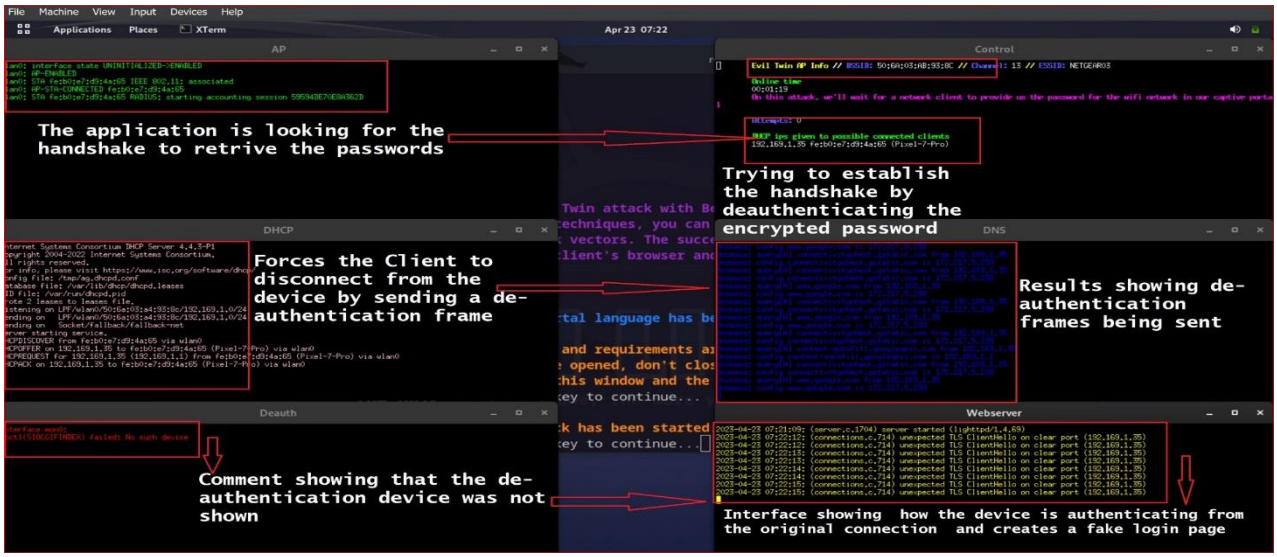

Fig. 14. De-authentication of Several Parallel Windows

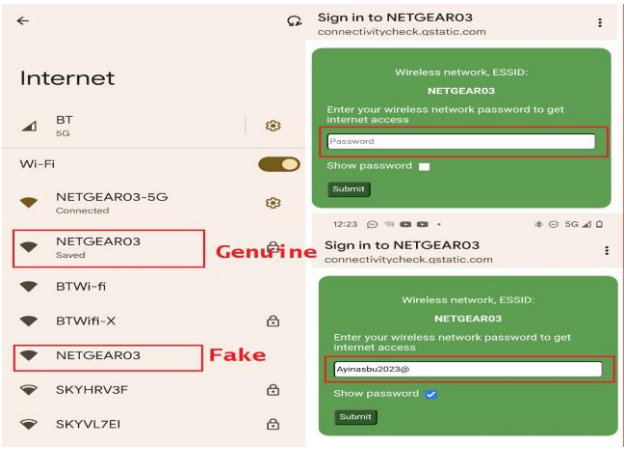

Fig. 15. The Rouge Wireless Name Created by the Attacker to Capture the Password

Figure 15 shows what happened when we entered the password in clear text, and upon hitting the submit button, the Kali Linux *airgeddon* terminal captured our wireless network password. The attacker now has access to our network and all connected IoT devices. When we tried joining the network, we received an image, as in Figure 18, asking us to input our password with the same Wi-Fi name, but we were unaware it was a phoney network.

F. Results of the Evil Twin Attack in Victim Network

Finally, it stores the captured password in the previously selected folder. When we open that file, Figure 16 shows what appears on the attacking system (Kali Linux), which offers my network password in plain text.

Fig. 16. Password Captured in Clear Text in the Victim Smart Network

V. RESULTS

The paper has explored how Evil Twin attacks are deployed on smart home IoT devices to exploit vulnerabilities. We discuss how exploited vulnerabilities could impact visually impaired users due to their reliance on assistive technologies and accessible designs.

A. Vulnerabilities that Could Impact on Visually Impaired

The following are some of the vulnerabilities.

- Inaccessible websites and applications: can prevent the visually impaired from accessing crucial information and services on their smartphones, such as banking applications and paying bills. That could result in financial difficulties, missed payments and psychological impact.
- Malware and Phishing Attacks: The visually impaired rely heavily on screen readers, voice assistants, and biometric authentication to navigate the digital devices during login. Suppose a malware or phishing attack to compromise IoT devices; the victims will unknowingly disclose passwords, sensitive information, and ID, leading to ID theft, financial loss and emotional distress.
- Social Engineering Exploits: The visually impaired user might expose themselves to social engineering attacks as they may experience shoulder surfing attacks, and their biometric data and voice recognition can be exposed to cyber attackers. That could impact the smart cane's walking aids and disrupt their movements.
- Smart Devices and Assistive Technologies: Visually impaired individuals use smart devices and assistive technologies to enhance their daily lives, and disruption of such devices will disrupt their routines and could result in inaccessible smart lighting, smart cameras, temperature controls and smart door locks.
- Online Shopping and E-Commerce: Visually impaired users depend on screen readers and touch screens to navigate commercial platforms to browse through online products, read reviews and complete online purchases. Cyber attackers could exploit the online apps using Evil twin attacks to gain access to the network, exploit the smart devices and redirect purchases.
- Medical and Services: Attackers could exploit vulnerabilities on medical devices such as smart blood pressure monitor kits, Smartwatches, Smart fitness trackers, and Smart Ear-worn/headsets, leading to inaccessible vulnerabilities in healthcare portals. That could prevent visually impaired users from accessing medical records, scheduling appointments, and communicating with healthcare providers.
- Educational Resources: The visually impaired students use digital educational resources, including virtual reality devices. Attackers could exploit the smart devices, learning management systems and educational content, preventing victims from assignment submission and participating in virtual classrooms.
- Medical Emergency Alerts and Notifications: Smart home IoT devices such as smartphones and smart alarms could be tempered with, leading to non-functional devices and could cause significant problems in the event of major natural disasters, emergencies, and timely and accessible information.

The vulnerabilities in smart devices have the potential to significantly impact the daily lives of visually impaired users, leading to missed opportunities, depression, compromised health management and safety risks.

B. Contribution to the Body of Knowledge

Our work has contributed to the body of knowledge by identifying challenges that visually impaired users are experiencing when using smart home devices. The vulnerabilities that could be exploited and types of attacks that could be deployed. The psychological, physiological and societal impact that the visually impaired users experience daily. For our novelty contributions, Table 1 shows how smart home appliances are susceptible to attacks. We have recommended mitigation techniques to improve security for developers, designers and organisations to consider by prioritising accessibility and safety to improve smart home IoT devices for visually impaired users.

VI. CONCLUSION AND RECOMMENDATIONS

The consequences of Evil Twin attacks on smart home devices for visually impaired users are devastating and life-changing due to the impact on the mobility support, smart canes or walking aids that control their impairment of the user's ability to move around securely. The paper has discussed privacy and safety concerns to the victims' health, psychological well-being, and independence from compromised smart medical devices and guidance systems that disrupt their daily routines and emergency communication. The paper examined the threat landscape of smart home security and discussed the vulnerabilities and potential repercussions of cyberattacks on smart homes. We set up a lab and testbed for IoT devices and implemented the Evil Twin Attack to compromise the network.

The results show that the visually impaired user could experience ID theft, inaccessible networks, disruptions of services, compromised wearable devices, impact on their educational systems and social engineering exploits. The paper has discussed security mechanisms that provide privacy and security controls and raise awareness about potential risks to visually impaired users.

The paper contributes to safer smart home environments and preventing potential security breaches by focusing on increasing awareness and proposing solutions for securing smart home IoT systems, thus protecting users' privacy and safety.

Future works will focus on research into emerging technologies in artificial intelligence (AI) and machine learning (ML) algorithms to detect anomalies, attack patterns, and threat predict for future trends in IoT device usage to improve the security and trust for disabled users considering the invincibility nature of cyberattacks.

TABLE 1: RECOMMENDED MITIGATION TECHNIQUES

IoT Devices	Attack Methods	Impact	Mitigation
Smart TV	Deploy Brute Force attack, WiFi compromise to penetrate the network to Exploit Default Password.	Attacker gains unauthorised access to the security settings and takes command & control. Remotely spy on the victim,	Change the default password setting upon installation. Use mixed character passwords, upper case, lower case and symbols.
Smart Phone	Deploy malicious Phone jacking apps, Phishing, Session hijacking, keylogger, Shoulder surfing, and cookies interception.	Username and password theft, ID theft, Personal Bank details theft, Impersonations, Redirections, Manipulation,	Password authentication mechanisms such as MFA, Voice, and fingerprint updates, Modify Web Catches and tighten Security Using HTTP headers. Prevent HTTP Redirects.
Smart Camera	Deploy remote access trojan, brute force, and Spoofing to penetrate	Spying, Loss of real-time, Camera Jamming and legal monitoring capabilities	Install Firewalls, IDS/IPS. Use frequency-hopping spread spectrum (FHSS) technology to counter eavesdropping.
Smart Door Lock	Deploy Bluetooth sniffer attack to gain access and use the Wireshark tool to capture packets—physical manipulation.	Compromise mobile phone app. user privacy, Bluetooth Connection, unauthorised lock control, Wi-Fi breach, compromised lock firmware.	Implement AES Encrypt and update lock firmware. Turn off Bluetooth when not in use. Install firewall. Implement Multifactor Authentication, Install Security cameras and smart alarms.
Wearable Devices: Blood Pressure Monitors, Smart Watch, Smart fitness trackers, Smart Ear-worn/headset	Deploy RAT DoS on WiFi network Access Points to gain access and data Interceptions—false data injection attack.	Unauthorized access to sensitive health data. False Diabetic readings, Corrupt device functionality, Blood Pressure manipulation, Diminished device usage. Compromise User the tracker	Secure RFID, Update Firmware, Hide Barcodes, Change Passwords regularly. Update Apps regularly, Implement a Zero Trust mechanism, and Encrypt data during transmission and storage.
Smart Canes and Walking Aids	Deploy GPS Spoofing attack to compromise vibration sensors, voice instruction guides, cameras, and computer vision software.	Misleading location tracking accidents, Physiological and Psychological impact on the visually impaired.	Validate GPS data from multiple sources. Regular Software Updates, Use Strong Passwords, and Disable GPS and tracking location when not used.
Smart Medical Service	Deploy RAT, Evil Twin attack to compromise Smart medical systems, leading to exploitation and manipulation of emergency service disruptions and appointments.	Health data tampering: medical and emergency services disruptions, compromised patient monitoring records, Reputation Damage, and Lack of Trust.	Use secure communication protocols, SSL, TLS, Firewalls, and IDS/IPS to monitor traffic, Apply Regular updates and Install anti-malware software. Authenticate Users, Update the Access Control List and Apply Zero-trust policies.

REFERENCES

[1] K. Murugesan, K. K. Thangadorai, and V. N. Muralidhara, "PoEx: Proof of Existence for Evil Twin Attack Prevention in Wi-Fi Personal Networks," in *2021 8th International Conference on Future Internet of Things and Cloud (FiCloud)*, Aug. 2021, pp. 92–98. doi: 10.1109/FiCloud49777.2021.00021.

[2] L. Ayavaca-Vallejo and D. Avila-Pesantez, "Smart Home IoT Cybersecurity Survey: A Systematic Mapping," in *2023 Conference on Information Communications Technology and Society (ICTAS)*, Mar. 2023, pp. 1–6. doi: 10.1109/ICTAS56421.2023.10082751.

[3] K. Bauer, H. Gonzales, and D. McCoy, "Mitigating Evil Twin Attacks in 802.11," in *2008 IEEE International Performance, Computing and Communications Conference*, Dec. 2008, pp. 513–516. doi: 10.1109/PCCC.2008.4745081.

[4] P. Bhatia, C. Laurendeau, and M. Barbeau, "Solution to the wireless evil-twin transmitter attack," in *2010 Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Oct. 2010, pp. 1–7. doi: 10.1109/CRISIS.2010.5764921.

[5] "State of IoT 2023: Number of connected IoT devices growing 16% to 16 billion globally," *IoT Analytics*, May 24, 2023. https://iot-analytics.com/number-connected-iot-devices/ (accessed May 25, 2023).

[6] N. Nazar, I. Darvishi, and A. Yeboah-Ofori, "Cyber Threat Analysis on Online Learning and Its Mitigation Techniques Amid Covid-19," in *2022 IEEE International Smart Cities Conference (ISC2)*, Sep. 2022, pp. 1–7. doi: 10.1109/ISC255366.2022.9922102.

[7] A. A. Olazabal, J. Kaur, and A. Yeboah-Ofori, "Deploying Man-In-the-Middle Attack on IoT Devices Connected to Long Range Wide Area Networks (LoRaWAN)," in *2022 IEEE International Smart Cities Conference (ISC2)*, Sep. 2022, pp. 1–7. doi: 10.1109/ISC255366.2022.9922377.

[8] Md. A. Rahman, K. Abualsaud, S. Barnes, M. Rashid, and S. M. Abdullah, "A Natural User Interface and Blockchain-Based In-Home Smart Health Monitoring System," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*, Feb. 2020, pp. 262–266. doi: 10.1109/ICIoT48696.2020.9089613.

[9] W. Elmannai and K. Elleithy, "Sensor-Based Assistive Devices for Visually-Impaired People: Current Status, Challenges, and Future Directions," *Sensors*, vol. 17, no. 3, p. 565, Mar. 2017, doi: 10.3390/s17030565.

[10] A. M. Mosadeghrad, "Factors Affecting Medical Service Quality," vol. 43, 2014.

[11] J. Deogirikar and A. Vidhate, "Security attacks in IoT: A survey," in *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Feb. 2017, pp. 32–37. doi: 10.1109/I-SMAC.2017.8058363.

[12] A. Bandekar and A. Y. Javaid, "Cyber-attack Mitigation and Impact Analysis for Low-power IoT Devices," in *2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, Honolulu, HI: IEEE, Jul. 2017, pp. 1631–1636. doi: 10.1109/CYBER.2017.8446380.

[13] S. S. Swarna Sugi and S. R. Ratna, "Investigation of Machine Learning Techniques in Intrusion Detection System for IoT Network," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, Dec. 2020, pp. 1164–1167. doi: 10.1109/ICISS49785.2020.9315900.

[14] S. Nagarkar, "Evaluating Privacy and Security Threats in IoT- based Smart Home Environment," vol. 14, no. 7, 2019.

[15] A. D. Seth, S. Biswas, and A. K. Dhar, "De-Authentication Attack Detection using Discrete Event Systems in 802.11 Wi-Fi Networks," in *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Dec. 2019, pp. 1–6. doi: 10.1109/ANTS47819.2019.9118100.

[16] T. A. A. Abdullah, W. Ali, S. Malebary, and A. A. Ahmed, "A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home," 2019.

[17] W. Zhou *et al.*, "Discovering and Understanding the Security Hazards in the Interactions between IoT Devices, Mobile Apps, and Clouds on Smart Home Platforms." arXiv, Jun. 26, 2019. Accessed: May 25, 2023. [Online]. Available: http://arxiv.org/abs/1811.03241