EXPLOITING FLAWS IN A WIFI NETWORK

Agniv Bhaumik
SCOPE
VIT Vellore
Vellore
agniv.bhaumik2020@vitstudent.ac.in

Shreyoshi Kamboj
SCOPE
VIT Vellore
Vellore
shreyoshi.kamboj2020@vitstudent.ac.in

Mrinal Sharma
SCOPE
VIT Vellore
Vellore
mrinal.sharma2020@vitstudent.ac.in

Rohan Gupta
SCOPE
VIT Vellore
Vellore
rohan.gupta2020a@vitstudent.ac.in

Harsh Rajpal
SCOPE
VIT Vellore
Vellore
harsh.rajpal2020@vitstudent.ac.in

***Abstract*—In today's world, cybersecurity is required everywhere. It is a worldwide industry that will face a global shortage of more than 2.2 million information security specialists by 2022. Over the past few decades, almost all our systems have been entirely digitized. Accounting and communications have become almost entirely digital, because of their high speed and accuracy. However, such systems are prone to attacks. Not physical attacks but cyber-attacks. A cyber-attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. If not managed properly, it can cause the loss of critical data and leakage of private information into the public, resulting in losses upwards of billions of dollars. Thus, knowledge and prevention of such attacks are of utmost importance.**

Keywords— ARP Poisoning, DOS, SQL Injection, Exploitation, Mitigation, Kali Linux, Authentication, Middle-man, Packet Tracing.

I. INTRODUCTION

Each year, over 30 million cyberattacks occur. It is expected to cost the world $10.5 Trillion annually by 2025. So, we must understand the techniques used to execute such attacks and what measures can be adopted to prevent it. In this paper, we demonstrate some of the most common types of cyberattacks, such as ARP Poisoning, DOS attacks and SQL Injections.

● ARP Poisoning (also known as ARP Spoofing) is a type of cyber-attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table.

● A Denial-of-Service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

● SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database. In many cases, an attacker can modify or delete this data, causing persistent changes to the application's content or behaviour. We also attempt to develop sound mitigation strategies that can help prevent such attacks

II. PROBLEM STATEMENT:

In the present world, every person uses the internet and is vulnerable to internet-based attacks if certain precautions are not taken. Cyber-attacks can cause immeasurable damages to a company. They can cause tangible damages such as stopping services; they can ruin the public's trust in a company; and they can lead to leaks of important information that may affect corporate survival. Attacks like DOS have become one of the most prominent forms of cybercrime over the last few years. Thus, before finding a solution to these problems, one must be able to perform and understand these attacks.

III. THEORETICAL BACKGROUND:

The WPA2 protocol is hard to hack, but not impossible. A few vulnerabilities had been discovered long back, and since it is a widespread protocol, it has been used by all modern devices for protection as well as hackers for intrusion. This protocol allows disconnecting a device with a single de-auth packet, for which a person does not even need to be connected. This can be misused in many ways, some of which will be demonstrated in our project.

IV. OVERVIEW OF THE PROPOSED SYSTEM

A. *Proposed Methodology*

We will be using different methods to carry out our network-based attacks:

1. DoS attack: We try sending spoofed packets of information that hits every computer in a targeted network, taking advantage of misconfigured network devices.

2. ARP spoofing: We will use Better CAP to perform ARP poisoning in a LAN environment using a VMware workstation in which we have installed Kali Linux and Ettercap tool to sniff the local traffic in LAN.

3. SQL injection: To make an SQL Injection attack, we find vulnerable user inputs within the web page or web application. A web page or web application that has an SQL Injection vulnerability uses such user input directly in an SQL query. We can create input content. Such content is often called a malicious payload and is the key part of the attack. After sending this content, malicious SQL commands are executed in the database.

4. We'll also be using Cisco packet tracer to carry out a visual simulation of how these attacks work.

B. *Algorithm and Steps Explanation:*

1. Denial of Service on a home network

A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users. DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the service or resource they expected. Victims of DoS attacks often target web servers of high-profile organizations such as banking, commerce, and media companies, or government and trade organizations. Though DoS attacks do not typically result in the theft or loss of significant information or other assets, they can cost the victim a great deal of time and money to handle. In this implementation we are trying to implement the DOS attack on a modem of a home-network.

Requirements – A WIFI adapter, Kali Linux, Python

In this attack the WIFI adapter initially scans for various networks in the vicinity when it gets the WIFI address which has to be attacked then it starts scanning which all devices are connected with the particular WIFI and with the help of airplay-ng it finds out the MAC addresses of all the connected devices and the modem. Now it starts sending the DE authentication packets to the modem on behalf of the other connected devices.

2. ARP-Spoofing

An ARP spoofing, also known as ARP poisoning, is a Man in the Middle attack that allows attackers to intercept communication between network devices. The attack works as follows:

● The attacker must have access to the network. They scan the network to determine the IP addresses of at least two devices—let's say these are a workstation and a router.

● The attacker uses a spoofing tool, such as Arp spoof or Driftnet, to send out forged ARP responses.
● The forged responses advertise that the correct MAC address for both IP addresses, belonging to the router and workstation, is the attacker's MAC address. This fools both router and workstation to connect to the attacker's machine, instead of to each other.

● The two devices update their ARP cache entries and from that point onwards, communicate with the attacker instead of directly with each other.

The ARP spoofing attacker pretends to be on both sides of a network communication channel. Once the attacker succeeds in an ARP spoofing attack, they can:

● Continue routing the communications as-is—the attacker can sniff the packets and steal data, except if it is transferred over an encrypted channel like HTTPS.

● Perform session hijacking—if the attacker obtains a session ID, they can gain access to accounts the user is currently logged into.

● Alter communication—for example pushing a malicious file or website to the workstation.

● Distributed Denial of Service (DDoS)—the attackers can provide the MAC address of a server they wish to attack with DDoS, instead of their own machine. If they do this for a large number of IPs, the target server will be bombarded with traffic.

3. SQL Injection

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to affect the execution of predefined SQL commands.

● SQL injection attacks allow attackers to spoof identity, tamper with existing data, cause repudiation issues such as voiding transactions or changing balances, allow the complete disclosure of all data on the system, destroy the data or make it otherwise unavailable, and become administrators of the database server.

● SQL Injection is very common with PHP and ASP applications due to the prevalence of older functional interfaces. Due to the nature of programmatic interfaces available, J2EE and ASP.NET applications are less likely to have easily exploited SQL injections.

● The severity of SQL Injection attacks is limited by the attacker's skill and imagination, and to a lesser extent, defence in depth countermeasures, such as low privilege connections to the database server and so on. In general, consider SQL Injection a high impact severity.

C. *Architecture for the Proposed System*

a) The DOS attack Diagram

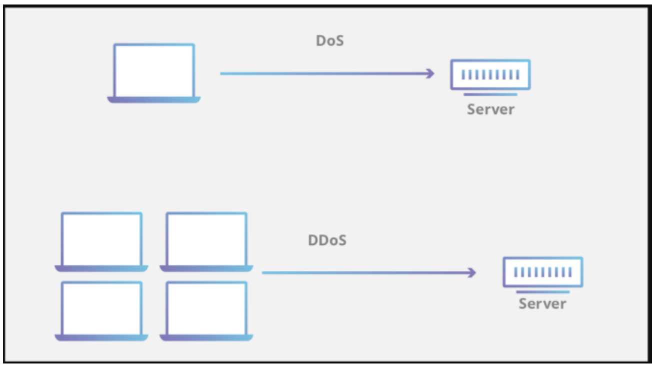

Fig. 1. The DOS – attack diagram

b) ARP Spoofing

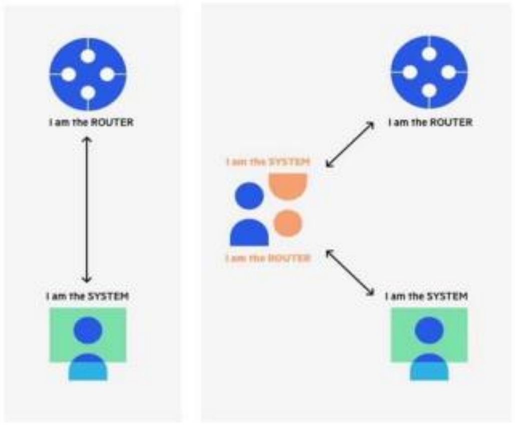

Fig. 2. The ARP spoofing attacker pretends to be both sides of a network communication channel

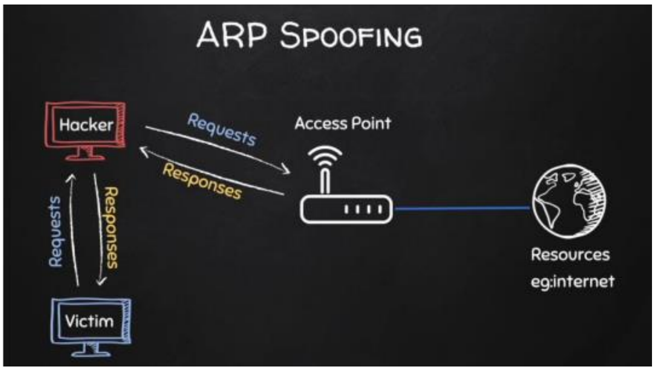

Fig. 3. Pictorial demonstration of ARP spoofing

Conclusions and Future Work

In conclusion, we have demonstrated how we can use better cap on Linux to execute a Man-in-the-Middle attack. Such an attack would allow us to come in the middle of the client and the router and view private data via captured packets. We have also proposed a viable method to prevent and detect it. Then we have also carried out a DoS attack using Kali Linux, a Linux distribution made specifically for pen testing. After launching the attack, we can see the hosts and the clients connected to the network won’t be able to access the internet as it gets disconnected indefinitely. This attack is so powerful that the client won’t be able to connect back to the same network till the time the attack is going on. We have also worked out how an SQL Injection attack can be carried out and have developed an extensive framework to prevent it. For future work, we can include some more common types of network attacks such as Botnets, DNS Spoofing and Packet Sniffers and like this project we can test out methods and protocols to prevent them.

Results and Discussions

Simple actions to minimize security risks and address system vulnerabilities are insufficient; Instead, a seamless policy implementation process supported by solid procedures is required. The security development process necessitates a full awareness of a system's assets, as well as the identification of potential vulnerabilities and threats. Furthermore, knowing about prospective assaults allows system developers to make better decisions about where monies should be invested. It's critical to research the many types of attack actors and figure out which ones are most likely to assault a system. It's easier to see which threat could exploit which system weakness after describing and documenting all threats and their respective actors. To reach their goals or objectives, attackers use a variety of methods, tools, and strategies to exploit vulnerabilities in a system. To avoid potential damage, an organization must first understand the motives and capabilities of the attackers. When a vulnerability impacts the security of a network or a cryptographic system, it puts a large number of devices or services at risk. In situations like these, it's critical that the victim remains calm and assesses the vulnerability's theoretical and practical risks. In order to estimate the vulnerability's possible impact, it's also a good idea to consider the available security measures.

One of the key concerns and challenges raised by any vulnerability is the manufacturers' willingness to respond to such situations, plan, and distribute patches to their products in a timely manner without leaving them vulnerable. Because internet-connected gadgets are becoming more common, it's critical to concentrate on keeping this ecosystem safe, especially since we've already seen security events aimed at jeopardizing cyber security. More research is needed to fill the gaps in information about threats and cybercrime, as well as providing the essential methods to prevent possible attacks, in order to lessen both prospective threats and their repercussions.

Literature Surveys:

S.No.	Title of the paper	Authors	Summary
1.	A Comprehensive Taxonomy of Wi-Fi Attacks.	Mark Vink	This paper aims to provide an overview of the available research and create an in-depth taxonomy of attacks against Wi-Fi networks.
2.	Detecting and Localizing Identity-Based Attacks in Wireless Networks.	Yingying Chen, Jie Yang, Wade Trappe, and Richard P. Martin.	In this paper, a method is proposed for detecting both spoofing and Sybil attacks by using the same set of techniques.
3.	Preserving Privacy in WIFI Localization with Plausible Dummy Locations	Ping Zhao, Wuwu Liu, Guanglin Zhang, Zongpeng Li and Lin Wang	To design an effective yet lightweight WIFI localization privacy algorithm, this paper proposes to reinforce dummy techniques with plausible dummy locations to resist the attacks.
4.	EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WIFI	Pragati Shrivastava , Mohd Saalim Jamal ,Kotaro Kataoka	In this paper, “EvilScout,” is proposed, an evil twin detection and mitigation framework that utilizes the information of the IP-prefix distribution by the Legitimate Access Point.
5.	Revealing Your Mobile Password via WIFI Signals: Attacks and Countermeasures	Yan Meng, Jinlei Li, Haojin Zhu, Xiaohui Liang, Yao Liu, and Na Ruan	In this study, a novel and practical keystroke inference framework, WindTalker is introduced, that can be used to infer the sensitive keystrokes on a mobile device through WIFI-based side-channel information.
6.	WIFI Attack Vectors	Hal Berghel and Jacob Uecker	The article here discusses different attack vectors of Wi-Fi networks and how they can be exploited.

7.	A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3	Christopher P. Kohlios, Thaier Hayajneh	The main contribution of this article is to analyze the technology offered in the new Wi-Fi Protected Access III (WPA3) security scheme and provide the first comprehensive security analysis and discussion to determine whether it has addressed the vulnerabilities of its predecessor.
8.	WIFI networks and malware epidemiology	Hao Hua,b, Steven Myersb, Vittoria Colizzac, Alessandro Vespignani	This article discusses how technology like the 802.11n standard with flaws is helping in spreading malware as the same exploit can be used on a wide array of devices using the same standards.
9.	Research of WIFI Systems Protection Efficiency	K. Brima, I. Opurum, R. Zolotyi	This article goes beyond Wi-Fi networks and showcases weaknesses in radios, potential attacks over Internet, etc.
10.	Device-Free Secure Interaction With Hand Gestures in WIFI-Enabled IoT Environment	Y. Zhao	In this study, we have studied and tested the application of secure interaction over WIFI signals and we have tested how various factors can be merged together to make the system more secure.
11.	A Quantitative Study of DDoS and E-DDoS Attacks on WIFI Smart Home Devices	B. Tushir, Y. Dalal, B. Dezfouli and Y. Liu	In this paper, We have studied the impact of DDoS and EDDoS on WIFI smart home devices.It focuses on the connection and energy consumption of IoT devices when they are under attack. There are three major conclusions that were drawn.

12.	Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux	E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N. Al Hashimi, M. Qbea'H, and S. Alrabaee	In this research, we have learned how to protect data in open WIFI as it can be easily accessed by anyone on the network.
13.	Survey on Wireless Network Security	Nazir, Rashid & Laghari, Asif & Kumar, Kamlesh & David, Shibin & Ali, Munwar.	In this study, we looked at wireless communication designs and protocols, security challenges, and the types of threats utilized to launch an assault, as well as their answers.
14.	Vulnerability Analysis of an Automotive Infotainment System's WIFI Capability	E. F. M. Josephlal and S. Adepu	This study focuses on conducting organized vulnerability testing on the WIFI capabilities of a vehicle infotainment system in order to determine the weaknesses of the automotive infotainment system.
15.	Research on WIFI Penetration Testing with Kali Linux	He-Jun Lu, Yang Yu	This article brings to attention the various methods of penetration testing Kali Linux offers. We can explore all kinds of vulnerabilities in it to 4 provide the best defense against hackers.
16.	Discovering and exploiting 802.11 wireless driver vulnerabilities	Laurent Butti, Julien Tinnès	This article follows up on a previous article on vulnerabilities in standards and further explains how they can be exploited.
17.	Denial of Service Attacks in Wireless Networks: The case of Jammers	Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy	This article showcases various methods of jamming strategies by exploiting flaws in the widespread protocols distributed in wireless systems all over the world.
18.	How Vulnerable Is the Public WIFI AP You Are Using?	Ruming Tang, Haibin Li, Kaixin Sui, Zihao	In this article, an app SAVY is created to measure how

		Jin,Xiao Yang, Dan Pei, Beichuan Zhang	vulnerable a public Wi-Fi AP is and create awareness on the potential threats it poses, along with a report to the developers.
19.	Research of WIFI Systems Protection Efficiency	K. Brima, I. Opurum, R. Zolotyi	This article goes beyond Wi-Fi networks and showcases weaknesses in radios, potential attacks over Internet, etc.
20.	A Comprehensive Attack Flow Model and Security Analysis for WIFI and WPA-3	Christopher C Kohlios, Thaier Hayajneh	Surveys all available attacks on a WIFI network using WPA-2 in an organized manner based on timing.
21.	Wireless Network Attack: Raising the Awareness of Kampung WIFI residents	Syahrul Fahmy, Akhyari Nasir, Nooraida Shamsuddin	Different wireless configurations are used to replicate the different wireless settings in the region using commercial broadband connections.
22.	The Untold Secrets of WIFI-Calling Services: Vulnerabilities, Attacks, and Countermeasures.	T. Xie et al.	They conducted the first security investigation utilizing commodity devices on operational Wi-Fi calling services in three major US operators' networks. They reveal that present Wi-Fi calling security isn't foolproof and point out three flaws.
23.	The Dark Side of Operational Wi-Fi Calling Services.	T. Xie, G. -H. Tu, C. -Y. Li, C. Peng, J. Li and M. Zhang	They create two proof-of-concept attacks by exploiting them: user privacy leakage and telephone harassment or denial of voice service (THDoS), bypassing the security defenses placed on mobile devices and network infrastructure.
24.	Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities.	M. Mendonca and N. F. Neves	Wdev-Fuzzer is a fuzzer that may be used to find security flaws in

			Wi-Fi device drivers, according to this study. Their preliminary tests with a Windows Mobile 5 device driver show that Wdev-Fuzzer can detect previously undetected issues.
25.	Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks.	A. Hussain, N. A. Saqib, U. Qamar, M. Zia and H. Mahmood	They suggest two efficient jamming techniques: low-data-rate random jamming and protocol-aware RF jamming based on shot-noise. They also came up with a tight upper bound for the duration and number of shot-noise pulses in Wi-Fi, GSM, and WiMax networks.
26.	Security Aspects and Vulnerabilities in Authentication Process WIFI Calling – RF measurements.	C. Capota, S. Halunga, O. Fratu, S. Eugen and P. Mădălin	This work investigates the Wi-Fi calling security requirements that an attacker can utilise to reveal users' locations, device technical details, access to sensitive data, and DoS attacks. They put the protocol to the test for various DoS assaults before coming up with some effective remedies to avoid or mitigate the effects of the attacks.
27.	WIFI Dimensioning to offload LTE in 5G Networks 2019	D. Saliba, R. Imad, S. Houcke and B. E. Hassan	They investigated the remaining available capacity in terms of available WIFI throughput that could be distributed over the transferred LTE users using this approach, and then the minimum required number of WIFI APs that will be supporting the LTE network for efficient traffic offloading using

			this approach.
28.	On the Use of Wide Channels in WIFI Networks 2020.	S. Malekmohammadi, C. Rosenberg and R. Stanica	They look into the joint channel, power, and carrier sense threshold allocation problem in IEEE 802.11ac networks, demonstrating that the current practise of using narrower channels at maximum power when the deployment is dense yields significantly worse performance than a solution using the widest possible channel at much lower power.
29.	A WIFI-Based Smart Home Fall Detection System Using Recurrent Neural Network 2020	J. Ding and Y. Wang	This article describes a passive device-free FDS for smart homes based on a commodity WIFI framework, which is primarily made up of two hardware platforms and client applications.
30.	6G, LIFI and WIFI Wireless Systems: Challenges, Development and Prospects 2022	C. Zeyu	To provide users with a ubiquitous wireless network connection, an integrated network system of space and earth is proposed. Three communication methods' technologies and obstacles are sorted out, and the ways they might be integrated and utilised are evaluated through significant research and analysis.
31.	Single-Target Real-Time Passive WIFI Tracking 2022	Z. Wang, J. A. Zhang, M. Xu and J. Guo	They described a system called WIFI Doppler Frequency Shift (WiDFS) in this paper, which uses channel state information (CSI) acquired from commercial-off-the-

			shelf (COTS) WIFI devices to enable single-target real-time passive tracking. They consider a typical system design that includes a single-antenna transmitter and a three-antenna receiver, but their technique can be easily adapted to various configurations.
32.	Has your WIFI left you wide open to cybercrime?	Greig Schofield, Netmetix	Know your company WIFI. Seek out the padlock. Know your network
33.	Smartphone Location Spoofing Attack in Wireless Networks	Chengbin Hu	The WIFI based localization and navigation are vulnerable to external signal attacks.
34.	Defending wireless communication against eavesdropping attacks using secret spreading codes and artificial interference	Qinghua Wang	Theoretical analysis on the potential performance degradation at the eavesdropper and at the legitimate receiver for a point-to-point wireless communication system using direct-sequence spread spectrum (DSSS) with coherent phase-shift keying (PSK) modulation
35.	Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks	Yingying Chen; Jie Yang; Wade Trappe; Richard P. Martin	A method for detecting both spoofing and Sybil attacks by using the same set of techniques. First propose a generalized attack-detection model that utilizes the spatial correlation of received signal strength (RSS) inherited from wireless nodes.
36.	Revealing Your Mobile Password via WIFI Signals: Attacks and Countermeasures	Qinghua Wang	Theoretical analysis on the potential performance degradation at the

			eavesdropper and at the legitimate receiver for a point-to-point wireless communication system using direct-sequence spread spectrum (DSSS) with coherent phase-shift keying (PSK) modulation.
37.	A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3	Christopher P. Kohlios, Thaier Hayajneh	The main contribution of this article is to analyze the technology offered in the new Wi-Fi Protected Access III (WPA3) security scheme and provide the first comprehensive security analysis and discussion to determine whether it has addressed the vulnerabilities of its predecessor.
38.	Research Of Wifi Systems Protection Efficiency	K. Brima, I. Opurum, R. Zolotyi	This article showcases weaknesses in radios, potential attacks over Internet and also goes beyond Wi-Fi networks.
39.	Secure WiFi Fingerprinting-based Localization	Mona A. Aboelnaga; M. Watheq El-Kharashi; Ashraf Salem	This article develops novel algorithms to identify attacked access points and make accurate localization in the presence of attacks. We evaluate the performance of our developed algorithms using different WiFi fingerprinting datasets under different attack models.

REFERENCES

[1] Mark Vink, A Comprehensive Taxonomy of Wi-Fi Attacks, Master Thesis Cyber Security, Radboud University Nijmegen

[2] Yan Meng, Jinlei Li, Haojin Zhu, Senior Member, IEEE, Xiaohui Liang, Member, IEEE, Yao Liu, Member, IEEE, and Na Ruan, Member, IEEE, Revealing Your Mobile Password via WIFI Signals: Attacks and Countermeasures, IEEE transactions on mobile computing, Vol. 14, No. 8, August 2015.

[3] Ping Zhao, Member, IEEE, Wuwu Liu, Guanglin Zhang, Member, IEEE, Zongpeng Li, Senior Member, IEEE, and Lin Wang, Senior Member, IEEE, Preserving Privacy in WIFI Localization with Plausible Dummy Locations, IEEE Transactions On Vehicular Technology.

[4] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and Richard P. Martin, Member, IEEE, Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks, IEEE Transactions On Vehicular Technology, Vol. 59, No. 5, June 2010.

[5] Pragati Shrivastava , Mohd Saalim Jamal , and Kotaro Kataoka, EvilScout: Detection and Mitigation of Evil Twin Attack in SDN Enabled WIFI, IEEE Transactions On Network And Service Management, Vol. 17, No. 1, March 2020.

[6] Hal Berghel and Jacob Uecker, WIFI Attack Vectors, Digital Village.

[7] Christopher P. Kohlios, Thaier Hayajneh, A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3, Fordham Center for Cybersecurity, Fordham University, New York, NY 10023, USA.

[8] Hao Hu, Steven Myers, Vittoria Colizza, and Alessandro Vespignani, WIFI networks and malware epidemiology, February 3, 2009.

[9] K. Brima, I. Opurum, R. Zolotyi (Ternopil Ivan Puluj National Technical University), Research of Wi-Fi systems protection efficiency.

[10] E. F. M. Josephlal and S. Adepu, "Vulnerability Analysis of an Automotive InfotainmentSystem's WIFI Capability," 2019 IEEE 19th International Symposium on High AssuranceSystems Engineering (HASE).

[11] B. Tushir, Y. Dalal, B. Dezfouli and Y. Liu, "A Quantitative Study of DDoS and E-DDoSAttacks on WIFI Smart Home Devices," in IEEE Internet of Things Journal, vol. 8, no. 8,pp. 6282-6292, 15 April15, 2021.

[12] E. Al Neyadi, S. Al Shehhi, A. Al Shehhi, N.Al Hashimi, M. Qbea'H and S. Alrabaee,"Discovering Public Wi-Fi Vulnerabilities Using Raspberry pi and Kali Linux," 2020 12thAnnual Undergraduate Research Conference on Applied Computing (URC), 2020.

[13] Nazir, Rashid & Laghari, Asif & Kumar, Kamlesh & David, Shibin & Ali, Munwar.(2021). Survey on Wireless Network Security. Archives of Computational Methods in Engineering.

[14] Y. Zhao et al., "Device-Free Secure Interaction With Hand Gestures in WIFI-Enabled IoTEnvironment," in IEEE Internet of Things Journal.

[15] Lu, He-Jun, and Yang Yu. "Research on WIFI Penetration Testing with Kali Linux."Complexity 2021.

[16] Brima, K., I. Opurum, and R. Zolotyi. "Research of WIFI systems protection efficiency."Матеріали VІнауково-технічної конференції „Інформаційні моделі, системи татехнології " (2018).

[17] T. Xie et al., "The Untold Secrets of WIFI-Calling Services: Vulnerabilities, Attacks, and Countermeasures," in IEEE Transactions on Mobile Computing.

[18] T. Xie, G. -H. Tu, C. -Y. Li, C. Peng, J. Li and M. Zhang, "The Dark Side of Operational Wi-Fi Calling Services," 2018 IEEE Conference on Communications and Network Security (CNS), 2018.

[19] M. Mendonca and N. F. Neves, "Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities," 10th IEEE High Assurance Systems Engineering Symposium.

[20] A. Hussain, N. A. Saqib, U. Qamar, M. Zia and H. Mahmood, "Protocol-aware radio frequency jamming in Wi-Fi and commercial wireless networks," in Journal of Communications and Networks.

[21] C. Capota, S. Halunga, O. Fratu, S. Eugen and P. Mădălin, "Security Aspects and Vulnerabilities in Authentication Process WIFI Calling – RF measurements," 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2021.

[22] D. Saliba, R. Imad, S. Houcke and B. E. Hassan, "WIFI Dimensioning to offload LTE in 5G Networks," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), 2019.

[23] S. Malekmohammadi, C. Rosenberg and R. Stanica, "On the Use of Wide Channels in WIFI Networks," 2019 IEEE 44th Conference on Local Computer Networks (LCN), 2019.

[24] J. Ding and Y. Wang, "A WIFI-Based Smart Home Fall Detection System Using Recurrent Neural Network," in IEEE Transactions on Consumer Electronics.

[25] C. Zeyu, "6G, LIFI and WIFI Wireless Systems: Challenges, Development and Prospects," 2021 18th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2021.

[26] Z. Wang, J. A. Zhang, M. Xu and J. Guo, "Single-Target Real-Time Passive WIFI Tracking," in IEEE Transactions on Mobile Computing.