Detection System for Passive Network Eavesdropping

1st Lukas Kapicak
Department of Telecommunications
VSB–Technical University of Ostrava
Ostrava, Czechia

2nd Jiri Stipal
Department of Telecommunications
VSB–Technical University of Ostrava
Ostrava, Czechia

3rd Kamil Trubak
Department of Telecommunications
VSB–Technical University of Ostrava
Ostrava, Czechia

4th Petr Machnik
Department of Telecommunications
VSB–Technical University of Ostrava
Ostrava, Czechia

5th Phu Le Si
Department of Telecommunications
VSB–Technical University of Ostrava
Ostrava, Czechia

***Abstract*—Eavesdropping on computer networks poses significant risks, including theft of personal data, unauthorized access, and user tracking. Passive eavesdropping is particularly challenging to detect and often becomes evident only after data misuse. This paper highlights the inherent risks of data traffic eavesdropping and introduces a method to detect passive eavesdropping in Wi-Fi networks. The proposed detection method analyzes user behavior through the traffic patterns generated that are integrated into an automatically configured server platform. The server infrastructure was designed to closely mimic real user traffic. Experimental verification demonstrated the system's effectiveness in identifying instances of passive eavesdropping. This significantly improves the security of Wi-Fi networks.**

***Keywords*—Wi-Fi security, passive eavesdropping detection, traffic analysis, user behavior modeling, network traffic simulation, data interception.**

I. Introduction

Today, we can face various security incidents in computer networks. Some of these incidents are of a more serious nature and can result in loss of data, loss of identity, loss of finances, etc. When such a situation occurs, the consequences are only known after the incident, and after a thorough analysis, it is possible to prevent future attacks in some way [1], [2]. This may help a larger number of users, but for an individual or a smaller group of users, such an attack can have a serious impact and affect their daily lives. An attack can be carried out on both a conventional computer network (implemented through a wired connection) and, more importantly, on a Wi-Fi computer network, which by its very nature presents many more potential security threats. Wi-Fi networks are becoming increasingly popular and users use them for all purposes without considering the various security threats and without taking into account the recommendations of Wi-Fi security experts. Based on information from the Journal of Information and Knowledge [3] and CZSO [4], it can be concluded that there is a high risk associated with the use of Wi-Fi networks, especially with the use of public Wi-Fi networks.

Compared to small Wi-Fi providers, mobile operators implement measures to ensure highest security of data transmission in their networks [5]. Today, a typical device is a smartphone and the most common operating systems on these smartphones are Android or iOS. These two operating systems are designed for mobile devices with the widest possible range of users in mind. Mobile devices must offer a wide range of functions and be highly resistant to malfunctions caused by unprofessional handling. Manufacturers of such devices try to remove the user from the technical side of things as much as possible and include complete security management as part of the purchase of such a device. The combination of the above factors creates a real risk of eavesdropping on traffic and also tracking users on wireless networks. The aim was to highlight these risks and propose a solution that could help protect the safety of users in cyberspace.

The structure of this paper is as follows: Section II reviews the current state of the art of Wi-Fi security and eavesdropping detection methods. Section III describes the proposed system architecture for detecting passive eavesdropping. Section IV discusses the methodology for generating data traffic and explains the difference between inserting data traffic and generating all traffic. Section V outlines the experimental tests carried out to verify the proposed methods. Section VI presents the results of the tests, section VII provides a discussion of the findings and suggestions for future research, and finally, section VIII concludes the paper.

978-3-903176-68-3

II. State of the Art

References [6] and [7] outline the potential risks associated with the use of Wi-Fi, particularly in relation to unauthorized tracking. To address this issue, the proposal suggests the implementation of Locally Administered Randomized Addresses (LRA) for wireless local area network (WLAN) MAC addresses of user equipment, instead of using universally administered MAC addresses.

In earlier and current versions of the Android and iOS systems, mobile devices included tracking protection. However, the vulnerabilities in this implementation are examined [8]. The authors address the issue of randomization of MAC addresses and their role in mitigating Wi-Fi-based tracking of mobile devices. Their analysis shows that while MAC address randomization policies exist, they are not consistently applied and often fail to fully address privacy concerns. In [9], the focus shifts to the accuracy of device detection, highlighting its dependence on the specific context of crowd-counting environments.

In environments such as universities and shopping malls, detecting devices connected to Wi-Fi networks is a challenge, unless the proposed Protected Mode Monitoring (PMM) method is used. Reference [10] emphasizes that MAC address randomization alone does not sufficiently protect users from being tracked.

Reference [11] deals with the location of smartphones in indoor environments. The authors present a novel hybrid tracking algorithm that combines Pedestrian Dead Reckoning (PDR) with features extracted from Wi-Fi/iBeacon signals.

The publication [12] focuses on the analysis of data transmitted by mobile devices over networks. With a particular focus on Wi-Fi networks, the paper highlights the prevalence of user data transmission via this interface and underlines the ease with which such transmissions can be intercepted. The authors emphasize that there are significant security concerns with respect to data transmitted over Wi-Fi networks.

Additional research underscores the limitations of existing encryption protocols. For example, while WPA2 has been a standard for securing Wi-Fi networks, its vulnerabilities, such as those exposed by the KRACK attack, highlight significant security flaws that attackers can exploit to decrypt traffic and inject malicious data [13]. Moreover, recent studies have shown that even the latest WPA3 protocol is not immune to security threats, as Dragonblood vulnerabilities demonstrated potential weaknesses in the Dragonfly handshake, leading to possible password theft and user impersonation [14].

Furthermore, it has been noted that WPA2's personal mode, which uses a Pre-Shared Key (PSK), is particularly susceptible to brute-force attacks due to its reliance on a shared key among all users. This shared key approach makes it easier for attackers to decrypt all traffic on a network once the key is compromised [14]. In contrast, WPA2-Enterprise offers better security by using a RADIUS server for authentication, which provides unique keys for each session and mitigates the risk of key exposure [15].

The evolution of encryption protocols from WEP to WPA3 illustrates ongoing efforts to enhance Wi-Fi security. However, the continuous discovery of new vulnerabilities indicates that securing wireless communications remains a complex and evolving challenge [15]. As a result the technical advances in security is necessary to address persistent threats to Wi-Fi security in a comprehensive way. Additionally, regulatory measures are crucial to ensure the uniform implementation of security protocols, enforce compliance across different manufacturers and service providers, and protect consumers from the potential fallout of security breaches, as highlighted by the vulnerabilities exposed in the WPA2 protocol through key reinstallation attacks (KRACK).

III. System Architecture

The experiment tests a new method to detect passive eavesdropping in Wi-Fi networks. It was carried out using a complex set-up that included servers and routers configured to mimic typical network traffic and user behavior. The main focus was to inject and then detect unusual traffic patterns that would indicate eavesdropping activity. Throughout the experiment, data was meticulously collected and analyzed to determine the effectiveness of the detection method. The results were intended to confirm that the system could successfully detect and alert to instances of passive eavesdropping, thus improving network security.

A model diagram of the server infrastructure is shown in Figure 1. The diagram consists of several functional blocks. The main part is a block that contains application containers that authenticate user logs and a logging server. The test device (tester) communicates with the server platform over a separate secure channel via VPN. User authentication takes place on the Active Directory server. Based on this infrastructure, a test infrastructure was built.

The main test measurement took place on the university campus for 14 days, and then the data was used to analyze the number of connected clients and the data content transmitted. During this time, a total of 630 unique MAC addresses were connected to the test Wi-Fi network. Most of the clients were on Android and iOS mobile devices. From this number of connected clients, it is clear that users do not consider network security and manually connect to the public Wi-Fi network as soon as they discover its availability in the vicinity.

When a mobile device connects to such a network, it transmits a lot of sensitive information to the network that a potential attacker can exploit. This includes information such as websites visited, network services used, and, not least, usernames and passwords. During testing, access data in unencrypted form to various servers, such as a mail server, a web server, and a FTP server, was intercepted from four users.

IV. Data Traffic Generation and Insertion

Based on observed measurements under laboratory conditions, as described in section III, network traffic was generated using data captured from real user activity. This traffic is

978-3-903176-68-3 ©IFIP 2024

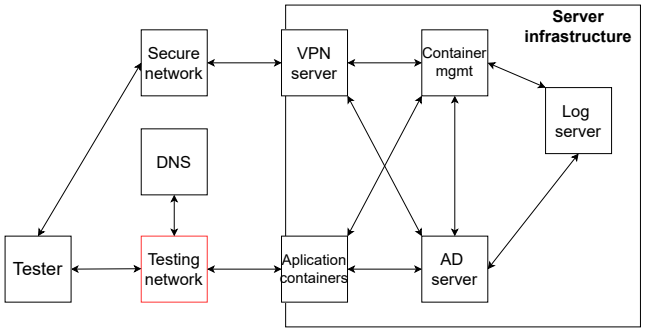

Fig. 1: System Architecture

categorized into automatic and manual. The selection depends on the protocol used and its use by real users. The test scenario and the type of generated network traffic are chosen by the tester during the test methodology setup. Network traffic can be generated through a specially adapted device or merged with real user activity.

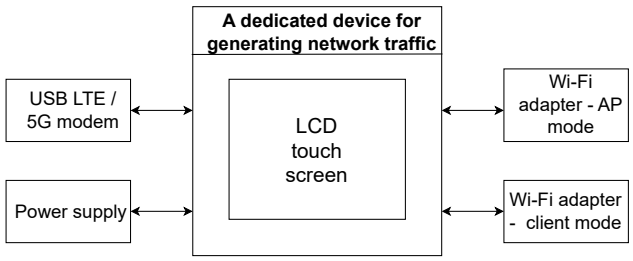

Fig. 2: Dedicated device for generating network traffic.

This device can be any system running software designed to generate network traffic. A diagram of the operation of this device is shown in Figure 2. Such a device is equipped with an external modem and a pre-installed operating system. Network protocols with automatic and manual traffic include IMAP, POP, HTTP, and SIP. The mobile device first generates a query for the domain name of the test server against the DNS server (assigned by the DHCP server on the network under test). The test device then begins to generate network traffic. When generating network traffic, the network identity must also be ensured. Each application client on the network generates a unique fingerprint and this fingerprint must be preserved.

Network traffic injection means using an existing mobile device equipped with an application to generate network traffic. This traffic is then inserted into the actual end-user traffic. This functionality has been implemented in the form of a network traffic generation application. To generate actual network traffic, it is necessary to rely on the properties of the individual protocols under test. For example, the approach to generating network traffic is different for the IMAP protocol and the HTTP protocol.

$$
\begin{aligned}
APPdataA_{T\langle 0;M\rangle} = \\
& TRAFFIC_{T>0\wedge T\leq M} \\
& + DNS \\
& + GENdata\,(1)_{T>2\wedge T\leq 10} \\
& + GENdata\,(N)_{(T+X)<M}
\end{aligned}
\tag{1}
$$

The Eq. 1 describes the generation of automatic and manual network traffic. *APPdataA* is the data generated in time (T) from the start of the connection to the maximum test time (M). *TRAFFIC* or normal network traffic starts when the user connects to the Wi-Fi network (test network) and ends when the test ends. *GENdata* is the test data.

Initial data is generated from the 2nd second after connection to the network (due to the normal latency of the client application) and continues until the 10th second. Thereafter, data are generated continuously (checking the data on the server) and at random intervals until the test is complete. The amount of data generated *(N)* depends on the duration of the test and the set interval for data transfer. The test is estimated to last 120 seconds, based on real user behavior observed on the test Wi-Fi network.

The software part of RaspberyPI is designed so that the traffic generated matches the real traffic. This includes:

- Identification of devices in the network.
- Preserving the identity of software tools such as web browser, mail client, etc.
- Interface for setting up network traffic generation.
- Network traffic generation applications.

V. Experimental Testing

In order to experimentally confirm the functionality of the proposed model of user behaviour and consequently the detection of passive eavesdropping, it is necessary to provide verification in the following points:

- The structure of generated data traffic is similar to real user traffic in data networks.
- The generated data traffic is similar in time component to the real user traffic.
- The test infrastructure must be indistinguishable from the real server infrastructure.

In the experimental Wi-Fi network, a time comparison was made between the user's real traffic and the user's test traffic. The comparison is based on the packet sequence time histories of the same services, and correlation of measured data for experimental and real user traffic was also performed.

Real data flow was represented by a mobile device with client applications installed for the respective services tested (IMAP, HTTP and FTP) to compare test and commercial server scenarios. Traffic was captured directly at the Wi-Fi access point. All traffic was sent to the monitoring device. The test flowchart is shown in Figure 3. The Mikrotik router acts as the Wi-Fi access point and all traffic is sent to the logging device, which stores all transmitted traffic.

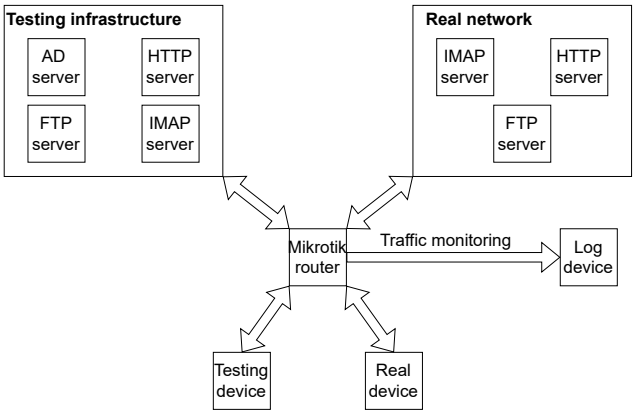

Fig. 3: Experimental verification scheme.

Unlike, for example, honeypots where all attacks on the server platform are monitored, our server infrastructure focuses primarily on credibility. All web service security methods (firewall, fail2ban, IDS and IPS systems) can be applied to the server infrastructure. A server platform secured in this way must appear to be a real platform. The LDAP server log can be used to monitor positive logins, or if the container is not directly connected to the LDAP server, the system log for Docker containers can be used, or syslog can be used to monitor user logins to the platform.

VI. Test Results

The comparison of the structure of the transmitted data for the tested network services is based on captured traffic. The aim was to ensure that the traffic generated within its own infrastructure matched the real traffic within the commercial infrastructure. Of course, it is not possible to ensure that the traffic is the same, there will always be differences in destination IP addresses and DNS names. For experimental validation of the proposed methods, traffic can be easily captured and presented under laboratory conditions, simulating to some extent the behavior of an attacker. A schematic of the test is shown in Figure 3.

The IMAP traffic represents mail downloads by the client application on the tested Wi-Fi network. To test the real server, we choose a public solution that allows the use of an unsecured login to the IMAP server on port 143. The email service provider does not recommend this method of logging into email services. A potential attacker can easily capture the user's password. A sample login from the Android application is shown in the Figure 4. The IMAP connection was in what is known as automatic mode.

As part of the test infrastructure, a Docker container with a mail server was created. This mail server was configured to log in only with a single account created on the LDAP server. The network traffic was then generated within the test application using the mobile application with the user created for this particular network (see Figure 5).

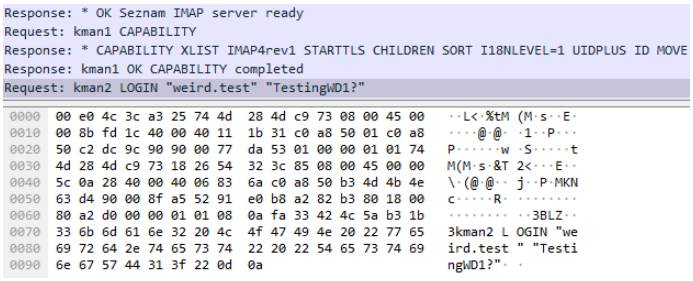

Fig. 4: Sample IMAP server login - public e-mail server.

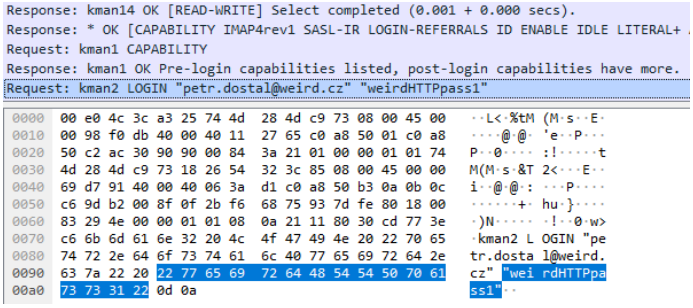

Fig. 5: Sample IMAP server login - test e-mail server.

This positive login was then reported to the Active Directory (LDAP) server (see table I). Based on this positive user login it can be concluded that the tester has generated traffic. All positive logins during the test are considered as test logins. The username/password combination will never be used again after the test is completed. Further positive logins may be considered as eavesdropping detection.

TABLE I: EXAMPLE OF A POSITIVE USER LOGIN TO AN IMAP SERVER VIA ACTIVE DIRECTORY LOG

Authenticated DC	:	weirdserver.weird.cz
LoggedOn Time	:	22. 1. 2024 11:25:25
User	:	DostalP
User Location	:	services
Workstation	:	mailserver3
IP Address	:	10.11.12.99
Computer Location	:	Domain Controllers/WEIRDSERVER

The validation of IMAP traffic between the dedicated solution and the public solution is represented by the graph in Figure 6. The histogram shows the number of packets as a function of time.

All data were generated by the test application and Figure 6 shows a comparison of IMAP connections from the dedicated server infrastructure and the public server infrastructure. The histogram shows that the traffic was also in automatic mode, where communication started immediately after connecting to the tested network. The analysis of both graphs shows that the communication through both servers was similar.

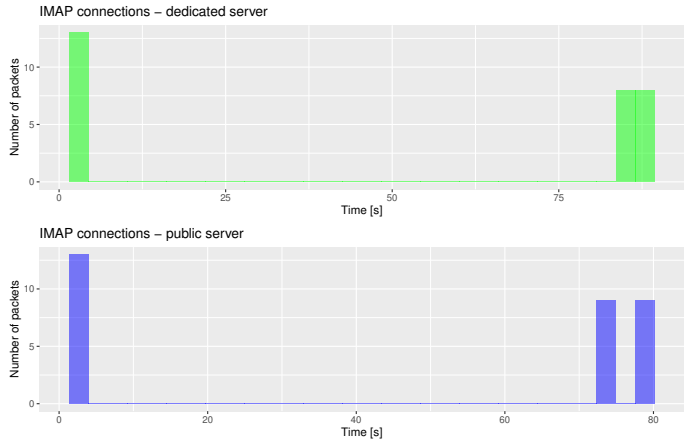

Fig. 6: Histogram of IMAP connections - the dedicated and public server.

One of the steps is to test the correlation between these data streams. The RStudio tool was used to compare real and test traffic, in terms of the time component of the transmitted data. There is a positive correlation between test and real traffic.

```
Pearson's product-moment correlation
sample estimates: 0.9995664
```

From the scatter plot Figure 7, we can see that the traffic for both tests is similar in terms of the time component and the content transmitted.

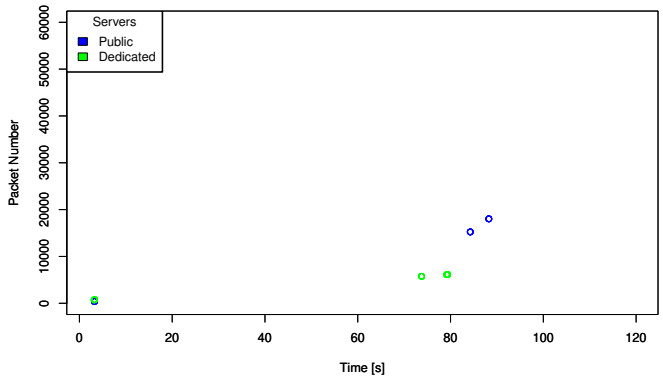

Fig. 7: IMAP server traffic comparison.

VII. Further Discussion

The data indicates that several key conclusions can be drawn from the detected positive logins:

- It can be reasonably assumed that the specific network under test is being eavesdropped upon.
- From a successful login, the public IP address can be determined.
- From the public IP address, it is possible to ascertain the geographical location of the attacker's login. This may be the network under test or another network.
- It is possible to ascertain whether the attack is carried out by an automated system or a human from the behaviour observed after login.
- It is possible to subsequently trace falsely generated user data equipped with a steganographic element, thereby enabling the intent of the attacker to be tracked.
- It is not possible to determine at which point in the transmission chain the eavesdropping occurred. Whether the attack occurred directly within the network under test or further down the transmission path. It can be stated that the network under test is untrusted.

It has been observed that a significant number of users treat untrusted Wi-Fi networks as if they were their home network, attempting to access data or intercept content. In order to allow this content to be used by the attacker and to create a record of the use of this content, a server platform was created for these purposes based on recent trends in network services, as previously mentioned. In order to optimize the use of system resources, technologies such as virtualization, containerization, and virtual networks were implemented. The deployment of this solution on a large scale requires the use of multiple domains and public IP addresses. In order to provide experimental validation, a custom domain and a server platform were used and the proposed solution was demonstrated to provide the expected functionality.

Options to improve user security include the following points:

- Do not use public Wi-Fi networks.
- Be aware of the transmitted content.
- Use VPN networks.

VIII. Conclusion

Based on experimental verification, it can be concluded that the proposed method is functional. The first verification consisted of analyzing the data of the transmitted content and comparing the time component. All transmitted data content was captured in a manner similar to how a potential attacker could capture and analyze traffic. This was achieved by port mirroring on the router.

The server platform that provides the environment to test the proposed method was also verified. All server services were found to be fully functional. From a design perspective, the services must be automatically executable and match the real traffic as well. The proposed system detects positive eavesdropping only in the case of positive logins to the infrastructure. Otherwise, (standard attacks, password testing, etc.) must be filtered.

References

[1] A. F. Gentile, P. Fazio, G. Miceli. "A Survey on the Implementation and Management of Secure Virtual Private Networks (VPNs) and Virtual LANs (VLANs) in Static and Mobile Scenarios," *MDPI Telecom,* 2021, 2, pp. 430-445, doi: 10.3390/telecom2040025

[2] F. De Rango, M. Tropea, P. Fazio. "Mitigating DoS attacks in IoT EDGE Layer to preserve QoS topics and nodes' energy," *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops,* 2020, pp. 842-847, doi: 10.1109/INFOCOMWKSHPS50562.2020.9162902

[3] S. R. Shimray, C. K. Ramaiah. "Use of Internet through Mobile Devices: A Survey," *SRELS Journal of Information Management,* 2019, 56.2, pp. 100-105, doi: 10.17821/srels/2019/v56i2/141631

[4] Czech Statistical Office. "Sample Survey on ICT Usage in Households and by Individuals," 2024. Available at: https://www.czso.cz/csu/vykazy/sample-survey-on-ict-usage-in-households-and-by-individuals

[5] M. Mehic et al. "Quantum Cryptography in 5G Networks: A Comprehensive Overview," *in IEEE Communications Surveys and Tutorials*, 2024, 26 (1), pp. 302-346, doi: 10.1109/COMST.2023.3309051

[6] H. J. Lu, Y. Yu. "Research on WiFi Penetration Testing with Kali Linux," *Complexity*, 2021, doi: 10.1155/2021/5570001

[7] R. Rajavelsamy, D. Das, M. Choudhary. "Privacy Protection and Mitigation of Unauthorized Tracking in 3GPP-WiFi Interworking Networks," *2018 IEEE Wireless Communications and Networking Conference (WCNC)*, 2018. pp. 1-6, doi: 10.1109/WCNC.2018.8377154

[8] M. Vanhoef et al. "Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms," *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security,* 2016. pp. 413-424. doi: 10.1145/2897845.2897883

[9] T. Rütermann, A. Benabbas and D. Nicklas. "Know Thy Quality: Assessment of Device Detection by WiFi Signals," *2019 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops),* 2019, pp. 639-644, doi: 10.1109/PERCOMW.2019.8730828

[10] O. Nakhila, A. Attiah, Y. Jin and C. Zou. "Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks," *MILCOM 2015 - 2015 IEEE Military Communications Conference,* 2015, pp. 665-670, doi: 10.1109/MILCOM.2015.7357520

[11] T. D. Vy, T. L. N. Nguyen and Y. Shin. "A Precise Tracking Algorithm Using PDR and Wi-Fi/iBeacon Corrections for Smartphones," *in IEEE Access,* 2021, 9, pp. 49522-49536, doi: 10.1109/ACCESS.2021.3069261

[12] J. Freudiger. "How Talkative is your Mobile Device? An Experimental Study of Wi-Fi Probe Requests," *2015 Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks,* 2015, pp. 1-6, doi: 10.1145/2766498.2766517

[13] Y. Liu. "Security in Wireless Networks: Analysis of Wi-Fi Security and Attack Cases Study,"*2022 International Conference on Artificial Intelligence in Everything (AIE),* 2022, doi: 10.1109/AIE57029.2022.00097

[14] K. Moissinac et al. "Wireless Encryption and WPA2 Weaknesses," *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC),* 2021, doi: 10.1109/CCWC51732.2021.9376023

[15] M. Vanhoef and F. Piessens. "Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2," *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security,* 2017, doi: 10.1145/3133956.3134027

978-3-903176-68-3 ©IFIP 2024