MSc Research Project

Masters in Cyber Security

Krishan Pal

Student ID: 22205713

School of Computing

National College of Ireland

Supervisor: Khadija Hafeez

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Krishan Pal

Student ID: 22205713

Programme: Masters in Cyber Security
Year 2023-2024

Module: Practicum

Supervisor: Khadija Hafeez

Project Title: MALWARE ANALYSIS ON MOBILE PHONE APPS USING KALI LINUX AND ITS MITIGATION SOLUTIONS FROM MAN-IN-THE-MIDDLE ATTACK (MITMMIT)

Word Count: 8122 Page Count: 33

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use another author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Krishan Pal

Date: 14 September 2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on a computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

National College of Ireland

MALWARE ANALYSIS ON MOBILE PHONE APPS USING KALI LINUX AND ITS MITIGATION SOLUTIONS FROM MAN-IN-THE-MIDDLE ATTACK (MITMMIT)

Krishan Pal

Student ID: 22205713

Abstract

MITM attacks are a security threat that deals with threats which involve communication channels between distinct users and permit the opponent to interfere and control the communication flow. These attacks are specific to mobile app frameworks; thus, they regard data relevance and privacy, eradicating confidence in electronic interactions. Here, MITM attacks occur when communication between two parties is intercepted has been shown using the KALI Linux tool. The TCP shell also used to reflect, that the assailant can capture screenshots, viably checking client actions without their information. Furthermore, the compromised gadget can stream live video through the camera, posing serious security and security dangers.

Table of Contents

1. Introduction

1.1 Background of the study

Smartphones are now a necessity in today's society as they enable users banking, communication and entertainment among other services. However, this increased use of mobile apps has been associated with increased cases of mobile app fraud, with programmers acting as middlemen to exploit the gaps and carry out MITM attacks. MITM attacks occur when communication between two parties is intercepted and modified without the involved parties' consent, presenting several risks such as information theft. Thus, the growth of how applications become mobile also changes how hackers try to penetrate them.

Kali Linux, which is widely popular among cybercriminals, stands out with the range of tools developed specifically for penetration testing and security auditing. Frameworks like Burp Suite and Metasploit are useful in determining and preventing dangers in mobile applications (Thankappan *et al*. 2024). These tools help security professionals scrutinize the traffic, perform vulnerability checks and implement countermeasures (Ravindran et al. 2022) successfully.

1.2 Aim

This study aims to analyze and prevent Man-in-the-Middle (MITM) attacks in mobile applications employing Kali Linux tools, improve cybersecurity awareness, and provide recommendations regarding the protection of data during communication.

1.3 Objective

The following objectives to fulfil the aim are

- To determine the effectiveness of the Kali Linux tools, namely Wireshark, Burp Suite, and Metasploit in tracing and diagnosing malware in mobile applications.
- To find out the exposed areas in the mobile app frameworks that can lead to MITM attacks specifically, the security of real-time communications.
- To suggest some actionable measures that need to be interjected to improve the security features to ward off MITM in mobile applications; specifically, certificate pinning.
- To measure the effects of MITM attacks on mobile application's speed and the authenticity of its users' information through the creation of attack scenarios.

- To evaluate the current state of mobile app security and whether they are efficient enough in avoiding MITM vulnerabilities.
- To establish rules and standards followed by developers and security experts to put in place strong security measures against MITM attacks in mobile applications.
- To add concrete data and knowledge to the analyzed area of mobile app security, as well as help develop cybersecurity measures and tools that can help in data protection and increasing user privacy.

These objectives support the fact that this study can employ tools in Kali Linux to analyze all the malware, identifying various vulnerabilities in addition to preventing MITM in the mobile environment through proactive measures.

1.4 Problem Statement

The main security concern under study in this research work is the general menace of Man-in-the-Middle (MITM) attacks on mobile applications (Salem *et al.* 2021). MITM attacks are a security threat that deals with threats which involve communication channels between distinct users and permit the opponent to interfere and control the communication flow. These attacks are specific to mobile app frameworks; thus, they regard data relevance and privacy, as eradicating confidence in electronic interactions.

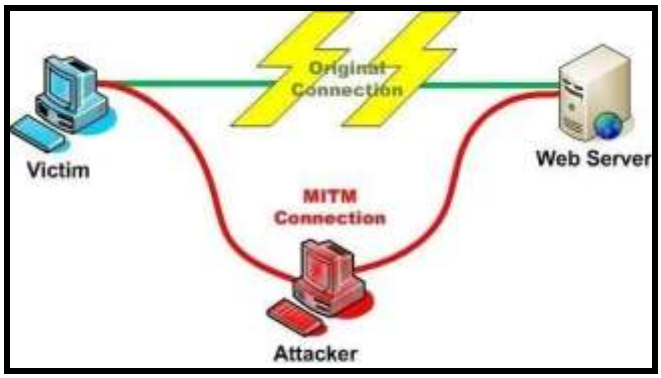

Figure 1.1: MITM Framework to perform an attack in Kali-Linux

(Source**:** Medium.com. 2024,)

The existing prevention methods like encryption and secure socket layers (SSL/TLS) offer some form of security but are usually unable to counter the advanced MITM attacks (Alwazzeh *et al.* 2020). Furthermore, it should also be noted that the dynamics of attacks are developing at a very high speed, and the corresponding security measures and techniques need to be constantly updated.

1.5 Research Significance

This research thus helps in the improvement of mobile application security paradigms through the discovery of associated threats and an outline of measures against Man-in-the-Middle (MITM) threats.

Protection of User Privacy: The security improvements in the analyzed mobile apps are evaluated by the research to prevent attacks on user privacy during communication.

Empowerment of Developers and Security Professionals: The discovery from this research enables developers and security personnel to have knowledge and tools like the Kali Linux utilities in the fight against new-wave mobile application threats.

Contribution to Cybersecurity Knowledge: Thus, the study contributes to the existing literature on cybersecurity by focusing on the specificity of the MITM attack and its countermeasures in the context of mobile apps.

Industry and Policy Implications: The given recommendations can help in proposing changes to the practices of the mobile apps industry as well as policy endeavours in different countries to improve cybersecurity policies for apps.

Trust in Digital Interactions: The research undertakes efforts to lessen MITM risks, the findings ensure improved trust and confidence of the users involved in digital interactions through their portable devices; thereby, encouraging a safer digital sphere.

Academic and Practical Applications: Thus, the study contributes to the existing scholarly literature by enhancing theoretical understanding in the area of mobile security while also providing practical beneficial suggestions for enhancing real-life security measures in the creation of and distribution of mobile applications into the market.

1.6 Research Rationale

The motivation for this research comes from the fact that mobile applications are still under the threat of MITM attacks and this threat is continuously being developed. Since mobile devices are becoming more and more the centre of our communication or transaction, and a host of other facets of our lives, including sharing sensitive data, it becomes pertinent to protect them from MITM attacks.

Thus, using tools available in Kali Linux, such as Wireshark, Burp Suite, and Metasploit, the work of this study can perform detailed malware analysis and vulnerability penetration testing (Alhamed *et al.* 2023). These tools help researchers do virtually what is feasible in

production, expose insecure points of mobile applications, and investigate current mechanisms of securing mobile apps.

2 Related Work

2.1 Introduction

Smartphones are rapidly becoming the most widely spread device which has dramatically changed people's interactions with digital technologies and made the main types of activities like banking, communication, and entertainment possible. While the app store is rapidly growing, this sad reality is the fact that it is deemed vulnerable to mobile application fraud, especially through Man-in-the-Middle (MITM) attacks.

2.2 Thematic Discussion

2.2.1 MITM Attacks on Mobile Applications

MITM attacks pose a major threat to mobile applications because such attacks enable the attacker to intercept and alter messages exchanged between the users and servers.

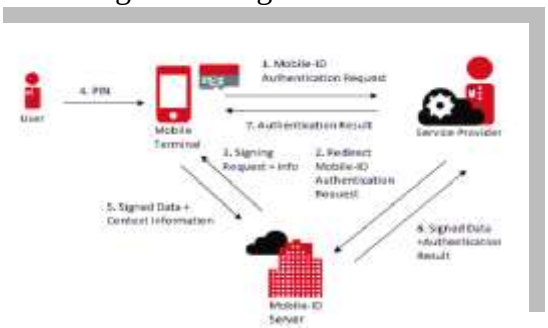

Figure 2.1: MAN in the Middle Attack on Mobile

(Source: Researchgate.net 2024)

These assaults capitalize on flaws in application layout and development, communicational security, and protection mechanisms, and provide transgressing access to private data, fiscal information, and authentication credentials (Reece *et al.* 2024). The literature stresses that MITM attacks are dynamic and are continuously evolving; thus, people must review their security strategies to combat them.

2.2.2 Kali Linux Tools for Malware Analysis and Penetration Testing

Kali Linux, which is among the most used platforms in cybersecurity today, comes with several tools that focus on penetration testing and security auditing. These are Wireshark, Burp Suite, and Metasploit, which are important tools used in the analysis of security threats as well as in the prevention of such threats. Wireshark is a free packet analyzer tool that

captures ‘‘live’’, that is, while the packets are being transmitted in the network (Sinnaiya *et al.* 2024).

2.2.3 Risks Linked to Mobile App Frameworks

Despite improving the UX and establishing connectivity, mobile app frameworks add certain vulnerabilities that can be used by MITM attackers (Bhardwaj *et al.* 2024). Many of these threats originate from insecure communication channels, wrong algorithm usage in applying encryption, and weak forms of authentication. Research shows that real-time communication especially is insecure and easily compromised thus the need for heightened security.

2.2.4 Certificate Pinning as a Mitigation Strategy

The literature designates certificate pinning as a viable solution to the problem of MITM attacks (Sutter *et al.* 2024). To accomplish this goal, certificate pinning ties a specific certificate to an application; this makes it possible for the app to only connect to trusted servers in a bid to exclude the acting of forged certificates by attackers.

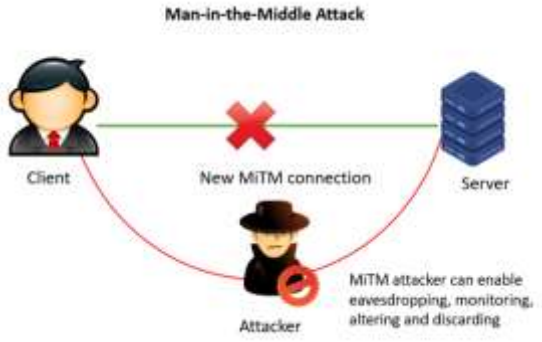

Figure 2.2: Man-in-the-Middle Attack a Mitigation Strategy

(Source: Google.com. 2024)

Several analyses reveal that the integration of certificate pinning brings a high level of protection in mobile applications where a secure connection path is developed.

2.2.5 Current State of Mobile App Security

The literature review sums up the current trends in mobile app security, pointing out that besides encryption and SSL/TLS, people are not sufficiently protected from such perished MITM attacks. It means that the effectiveness of security measures in the context of constantly evolving cyber threats has to be regularly evaluated and improved.

2.2.6 Consequences of MITM attacks on mobile applications

Analyzing the implications of MITM attacks on mobile applications, one has to say that they significantly impact the overall effectiveness of the software, as well as the level of users’ trust in the program’s functions. Harmful consequences regarded by the literature include the negative effect on application speed, data and user’s privacy.

2.3 Research Gap

There is a wealth of literature regarding the nature of MITM attacks and their countermeasures, especially in the context of mobile applications but the following research issues remain unaddressed.

2.3.1 Real-world assessment of Kali Linux utilities

Software like Wireshark, Burp Suite, and Metasploit are popular for penetration testing and even security auditing. Still, there is a lack of experimental work that measures the results of detection in the real world in the designed tools (El-Taj *et al.* 2024).

2.3.2 Consequence of the Implementation of Strategies for Mitigation

It is for this reason that certificate pinning among other measures has been recommended to help as a defence against MITM attacks.

2.3.3 Standard Operating Procedures for Maintenance of Continuity of the Security Updates

The fact that the threats which exist in the digital world are constantly changing means that evaluation and improvement of safety usually becomes a never-ending process. However, the literature on security is scanty in providing a clear methodological framework for normal security sweeps and threat and risk assessment.

As for present research, the following 4 weaknesses of mobile application frameworks are considered to be exploitable by MITM attackers: But a review that systematically organizes and evaluates these risks has not been performed.

2.4 Summary

According to the above perspective, it is evident that there is a need to fight MITM attacks in mobile applications because people are using smartphones to communicate, bank, and in almost all aspects of life. MITM attacks are dangerous because they intercept the communication and change the content by either stealing information or altering data. As will be observed from the tools available in Kali Linux, penetration testing and security auditing tools can prove useful for deploying solutions to such vulnerabilities.

3 Research Methodology

3.1 Introduction

This research work adopts the systematic research methodology to assess and mitigate Man-in-the-Middle (MITM) attacks, where Kali Linux tools are used for mobile applications. The methodology includes the use of Wireshark, the Burp Suite instrument, and Metasploit for tracing and diagnosing malware. Thus, in the framework of this work, the disclosed areas of mobile applications that can be unsafe for MITM attacks on real-time communication are determined. Some recommended changes are as follows: certificate pinning is proposed to improve the security parameters. Specific attack scenarios are designed to identify the impacts that MITM attacks have on the speed and authenticity of the information belonging to a user in the context of an MLSA mobile application. The state of mobile app security in the current world is assessed to identify how the various approaches prevent cases of MITM. This methodology also involves formulating guidelines and best practices that the developers and security specialists can apply in designing good security systems.

3.2 Research Approach

This study adopts a research design to analyze and prevent Man-in-the-Middle (MITM) attacks on Mobile applications using tools from Kali Linux. The extent to which such measures can be assured in excluding MITM attacks are evaluated by comparing best practices with recorded results in similar contexts. This evaluation establishes if these measures are enough to eliminate MITM vulnerabilities. In the course of the study, qualitative data gathered from secondary sources forms the basis of a lit review within the framework of the study (Singh *et al.* 2020). Through this approach, the study provides clear insights into MITM attacks on mobile applications and provides practical interventions for improving the security of mobile applications, to safeguard user's information, all of which are significant to the field of mobile application security.

3.3 Research Design

This research work, therefore, adopts a mixed-methods approach in the study and the prevention of Man-in-the-Middle (MITM) attacks in mobile applications using different tools in Kali Linux. The research integrates primary and secondary data to provide insightful information regarding the threats and protection measures concerning MITM attacks. Regarding the quantitative dimension of the study, MITM attacks on mobile phones are

performed using Kali Linux which consists of, Wireshark, Burp Suite, and Metasploit (Dwivedi *et al.* 2022). These tools are used for the capturing of packets in the network, as well as the discoverability of openings that may be exploited, and auditing the efficiency of various security measures including the certificate pinning. On the qualitative side, the data collection is primarily based on secondary research including journals, reports and cybersecurity databanks. This entails a literature review on the nature of mobile app security threats, types of attacks, and existing protective measures. Thus, based on the analysis of the prior works, case studies, and related instances of MITM attacks, the study offers a clear understanding of the offender's profile, vulnerabilities in mobile application architectures, and the efficacy of the countermeasures.

Secondly, the work entails a survey to determine the security threats of real-time communication in mobile applications. This aspect should assess the susceptibility of the targeted websites to MITM attacks and the results of attempts to bypass the existing security measures such as certificate pinning. The gathered information is processed to determine the common practices, optimum security strategies, and challenges related to mobile applications. Given this dynamic, the present mixed-methods study provides a comprehensive view of the problems and their remedies in relation to MITM attacks in mobile apps. This paper is of great value for identifying modern trends in the protection of applications and offers recommendations for safeguarding the data of mobile users. Such findings would be valuable for advancing further research on strengthening the protective systems against various malicious threats from the perspective of the constantly expanding mobile technologies sector.

3.4 Tools and techniques

Various instruments and methods have to be employed in this research to properly analyse and address the threat of Man-in-the-Middle (MITM) attacks on mobile applications. The main instruments used within this work are Wireshark, Burp Suite, and Metasploit, which are vital tools of the Kali Linux system.

Wireshark

Of protocol analysis tools, Wireshark can capture and display live packets for analysis.

Network traffic. It is applied to listen to network traffic between mobile applications and/or their back ends. Servers to clarify what specific actions are evil or may contain defects

(Blancaflor *et al.* 2023). Wireshark has an outstanding filtration system by which the user can decide to capture only a particular type of traffic
which is extremely useful for tracking the viral and analyzing the security issues.

Burp Suite

The scanner that is used to test mobile applications for their vulnerabilities is Burp Suite which can be described as a versatile web vulnerability scanner. It is for the analysis of HTTP/HTTPS connections, security tests, and various vulnerabilities that are exploitable during MITM attacks. The proxy server, intruder and repeater sub-sections of Burp Suite are useful in mimicking different attacks and putting mobile applications to the test as far as such threats are concerned.

Metasploit

Metasploit is a commonly used penetration testing software that enables emulation of different cyber-attacks of which MITM is included (Mirza *et al.* 2021). It is employed to take advantage of the stated weak points in the mobile applications in a bid to show the effects of these attacks. Metasploit has a vast repertoire of exploits and payloads that can be useful in investigating the organization comprehensively, and in confirming the efficiency of the countermeasures to be taken.

Controlled Lab Environment

In their natural environment, these tests may pose a significant risk to those conducting or executing them; that is why a controlled lab setting is crucial for experiments' safety and efficacy (Sandhu *et al.* 2021). Such items include mobile devices, networks, and virtual machines running Kali Linux OS. It enables one to make isolations of the test scenarios, in a way that; the actual effects of the model will not be profound, providing at the same time a real-world test environment.

3.5 Ethical consideration

The research also makes sure that all the experiments including the MITM attacks are carried out in the lab. This precaution eliminates unnecessary exposure of physical systems and, where possible, people to harm. All the Kali Linux tools including Wireshark, Burp Suite, and Metasploit are only used within the legal and ethical realm of the research and are solely limited to the research goals and do not lead to any sort of interference and unwanted system breakdown. The study abides by various institutional and legal requirements that are associated with researching cybersecurity (Özdemir *et al.* 2021). The ethical clearance committees give the green light on the research activities in a bid to portray all the activities

as ethically acceptable. Scientists are bound by professionalism and most are ready to surrender the facts accurately and clearly; no tampering in research data is entertained.

3.6 Summary

The methodology chapter explains in detail how the research is going to be conducted to address MITM attacks on mobile apps using the tools of Kali Linux. Selecting the framework is based on the study of real-time communication within mobile applications, the evaluation of the existing protection tools, and the integration of the certificate pinning approach. The study assesses the current position of mobile app security, surveys the optimal strategies, and sets a benchmark for developers and security analysts. Ethical concerns are used in determining the proper way to handle data and meeting set legal requirements.

4 Design Specification

4.1 Introduction

The following is a presentation of the research carried out on the Protection against Man-in-the-Middle MITM attacks on mobile applications using Kali Linux tools. The findings of the study are based on secondary data collected through the survey of literature materials, such as case and industry studies, and documented experiments with tools like Wireshark, Burp Suite, and Metasploit. These tools' efficiency regarding the detection and real diagnosis of malware is assessed, as well as given unsuccessful attempts to expose the different levels of vulnerabilities in the mobile app framework, primarily for real-time communications. The chapter also evaluates the effectiveness of some of the security measures like certificate pinning on the prevention of MITM attacks. Also, the current status of security for mobile apps is discussed to establish if it is sufficient to address these threats.

4.2 Design

Figure 4.1: The Host machine- IP address

(Source: Generated from Linux)

The above figure outlines the IP address allotted to the facilitating machine. This particular IP address is utilized to get to and explore the test site that has been made for show purposes. The figure highlights the IP address related to the eth0 interface, which serves as the essential interface for facilitating the site. This address is significant for coordinating activity to the server, permitting clients to connect with the test location. By utilizing the IP address of eth0, the facilitating machine can viably oversee and show the site substance to clients getting to it for the show.

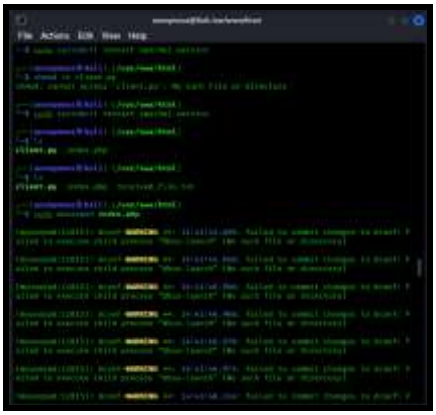

Figure 4.2: Creating a demonstration website and hosting it using the Apache server

(Source: Generated from terminal)

The following step includes making an `index.php` record within the root catalogue of `/var/www/html`. This registry is critical since Apache servers are ordinarily designed to utilize it as the essential area for facilitating web substance. By setting the `index.php` record in this registry, the Apache server will recognize and serve this record as the default page for the site. This step is significant for setting up a web application, as the `index.php` file often

acts as the most passage point for the application's usefulness, taking care of demands and directing activity to the suitable assets inside the net server.

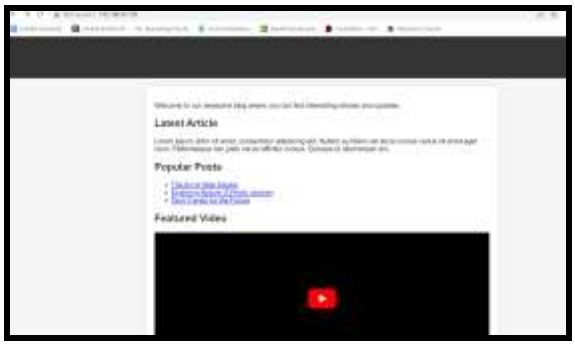

Figure 4.3: User interface of the website

(Source: Generated from Linux)

The over figure outlines the client interface of the demo site made for consideration. This site is facilitated on the neighbourhood IP address of a Linux machine, utilizing an Apache server for arrangement. The demo site is outlined to mimic an ordinary portable application environment, permitting the testing and investigation of Man-in-the-Middle (MITM) assault scenarios. By facilitating it locally, analysts can closely screen and control the arrange activity and security conventions input. This setup guarantees a secure and reasonable environment to viably illustrate and analyze the effect of MITM assaults and the adequacy of different relief measures.

Figure 4.4: Code of the demo spam website

(Source: Generated from Linux)

The figure shows the code for a demo site, exhibiting a fundamental system that consolidates HTML, CSS, and JavaScript. This code structure is outlined to form a utilitarian and outwardly engaging web page. A key highlight of this demo location is a notice that shows up upon floating, which is modified to enact after a delay of five seconds. This promotion is deliberately connected to a malevolent app, encouraging its download by clueless clients. This setup outlines potential security powerlessness, illustrating how pernicious performing artists can abuse such components to convey destructive programs to users' gadgets.

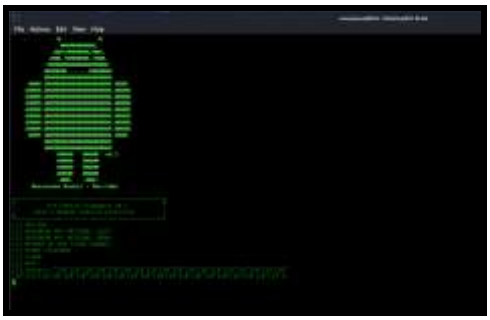

Figure 4.5: Using an evil droid tool to create a malicious app

(Source: Generated from Linux)

The figure outlines the Command Line Interface (CLI) of the Fiendish Droid instrument. This device is based on Perl and is created utilizing different Linux instruments, counting Force, Metasploit, and Apktool. It gives an extension of choices for creating malevolent APK records. On this occasion, Alternative One is chosen to produce an APK record inserted with a multi-handler payload.

Figure 4.6: Setting up the listening host

(Source: Generated from Linux)

After choosing the primary choice, a graphical client interface (GUI) window pops up, inciting the client to characterize the IP address of the Linux machine. This IP address is pivotal because it will be utilized to begin a turnaround shell audience utilizing the Metasploit system. The turnaround shell audience permits the Linux machine to tune in for approaching associations from compromised gadgets, encouraging inaccessible get to and control. By indicating the IP address, the client guarantees that the Metasploit system can set up a communication channel, empowering the execution of encouraged infiltration testing exercises and malware examination focused on versatile applications.

Figure 4.7: Choosing the reverse TCP meterpreter shell

(Source: Generated from Linux)

These payloads are particularly outlined based on the Android system, empowering compelling entrance testing on Android gadgets. Among the diverse choices, the Meterpreter turn-around TCP shell is chosen for this show. This specific shell is chosen due to its vigorous capabilities, which incorporate executing commands, capturing screenshots, and extricating touchy data from the target gadget. The Meterpreter switch TCP shell gives a comprehensive toolkit for checking and controlling the compromised gadget, making it a perfect choice for illustrating the misuse handle in this ponder.

Figure 4.8: Successfully generated a malicious app

(Source: Generated from Linux)

The figure outlines the fruitful creation of a malevolent APK record. This application is hence exchanged to the root catalogue of the apparatus, guaranteeing it is situated for assist control and examination. Amid this handle, a payload is produced and can be clearly distinguished through a compilation window that shows up, giving real-time criticism and affirmation of the payload's creation. This step is vital within the workflow because it illustrates the capability of the instrument to insert noxious code inside a portable application, setting the arrangement for consequent testing and examination of potential vulnerabilities and security measures.

Figure 4.9: Opening the Metasploit framework for reverse shell connection

(Source: Generated from Linux)

The over figure outlines the Force terminal working inside Kali Linux, exhibiting the turn around TCP audience effectively running. This setup is designed to catch and set up an association from an Android phone. The turnaround TCP audience may be a vital component in infiltration testing and cybersecurity examination, empowering the location and observing of approaching associations from focused on gadgets.

5 Implementation

The chapter focuses on the client side of an Android phone operating in a virtual machine environment focusing on x64 architecture and Android Nougat. This setup also increases security as well as flexibility since one can carry out the testing of applications without affecting hardware. All the figures in the chapter concern several characteristics of the network: The network communication IP address, application download, permission, and system information. The chapter is focused on the unsupervised applications that are warning against the risks related to them including unauthorized access, control over devices, and privacy invasion. It also outlines the utilization of Kali Linux tools including Wireshark, Burp Suite, as well as Metasploit in countering Man-in-the-Middle (MITM) attacks. It is suggested to use encryption protocols and MFA when it comes to the protection of mobile applications and with a preference towards improving user experience. Further, the chapter explicates the ways Intrusion Detection Systems (IDS) as well as securitization practices can strengthen the security of the mobile app.

Figure 5.1: The IP address of the Host machine

(Source: Generated from Linux)

The figure shows the client interface of the Android phone, which works inside a virtual machine environment. This setup is based on the x64 design and utilizes the Android Nougat working framework. By running in a virtualized setting, the framework permits improved security and adaptability, empowering clients to test applications and conduct investigations without compromising the basic equipment.

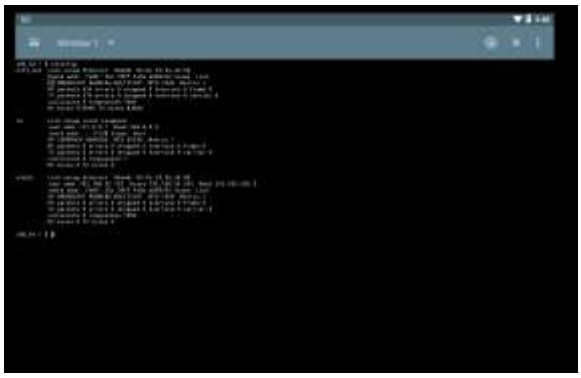

Figure 5.2: The IP address of the Android phone

(Source: Generated from Linux)

The figure shows the IP address of an Android phone, which is significant for organising communications. The Android environment, built on the Linux part, gives a vigorous environment that incorporates a terminal for executing different commands. This usefulness permits clients and security experts to perform progressed operations and troubleshoot and organize issues specifically on the gadget. Checking the IP address is basic within the context of security testing because it affirms the target's arranged identity and approves fruitful abuse endeavours.

Figure 5.3: Accessing the website from an Android phone

(Source: Generated from Linux)

The figure outlines the site interface obtained through a web browser, highlighting the client encounter while exploring the location. Outstandingly, it shows an unmistakable pop-up promotion that shows up as a meddlesome component, compelling clients to download a particular APK record. This promotion regularly utilizes powerful dialect and eye-catching visuals to pull into consideration, making a sense of direness. Such strategies can lead to clients accidentally downloading possibly destructive applications, which may contain malware or other security dangers.

5.1 Evaluation

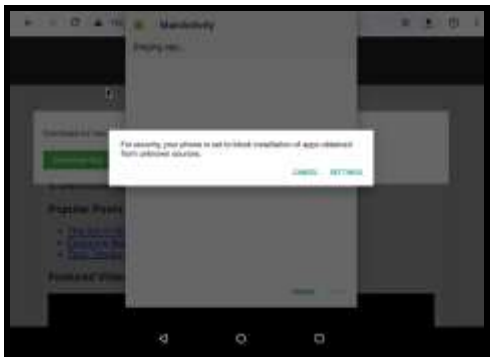

Figure 6.1: Downloading the application on the phone

(Source: Generated from Linux)

The figure shows the download and establishment preparation of the Android application. They note that Android gadgets frequently do not permit consent for putting in APK records from places other than well-known application stores like the Google Play Store. The method also underlines the importance of those authorizations and ensures that only applications are downloaded to maintain the keenness of gadgets.

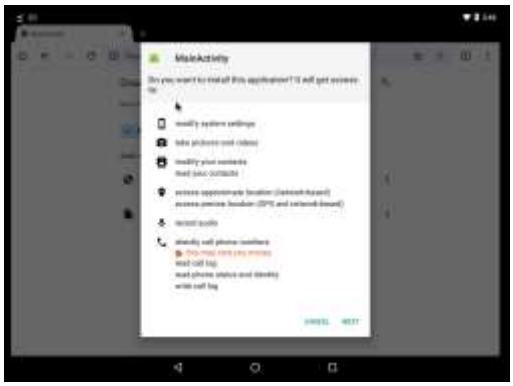

Figure 6.2: Graning all the permissions

(Source: Generated from Linux)

The over figure displays the establishments and required authorizations window which bifurcates the preamble of the application strategy and stresses the critical consents for presentation. Specifically, it underlines the get-to permissions requested by the app, including the get-to the camera, mouthpiece, and contacts. These consents are necessary for the applicability of the application, but simultaneously cause doubts regarding the protection of the clients and protection of their information. Clients must pay due attention to such suggestions and possibly get them because the latter may result in unauthorized data gathering and potentially malicious activity of vengeful performing artists.

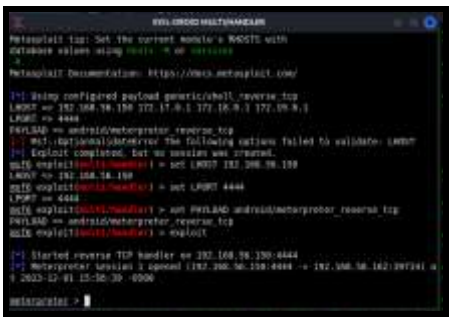

Figure 6.3: Getting the reverse shell connection from an Android phone

(Source: Generated from Linux)

This association is accomplished through the establishment of a noxious application, which misuses vulnerabilities inside the versatile working framework. Once introduced, the application empowers inaccessible get-to, permitting an aggressor to execute commands and control the gadget from a remove. This handle highlights the noteworthy security dangers related to unsubstantiated applications and the significance of strong security measures. By picking up unauthorized get to, assailants can compromise delicate information and control the gadget, underscoring the requirement for viable techniques to relieve such dangers in portable situations.

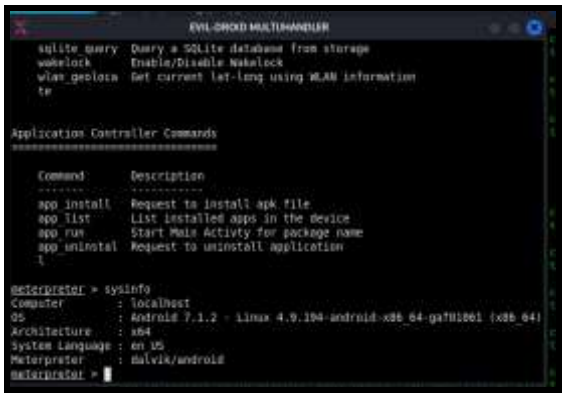

Figure 6.4: Ensuring the connection by system information

(Source: Generated from Linux)

The over figure illustrates the benefits set up after effectively interfacing to the Android phone through an invert TCP association. This sort of association permits the analyst to pick up farther to get to the device's working framework. The execution of the sysinfo command affirms the dynamic association by showing point-by-point framework arrangement data around the Android gadget, counting its show, form, and equipment determinations. This affirmation not as it were approve the keenness of the association but moreover gives basic experiences into the target devices environment, which is pivotal for advanced examination and potential misuse amid the inquiry about handle.

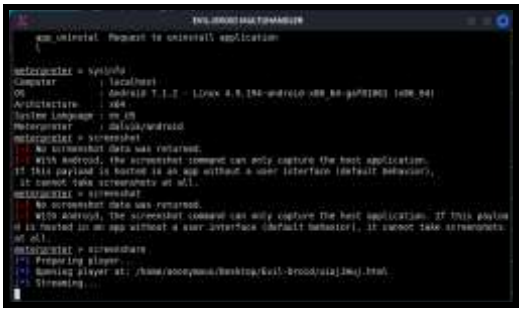

Figure 6.5: Accessing camera and screenshot features of Android phone

(Source: Generated from Linux)

The over figure outlines the unauthorized manhandling of consents by getting to the mouthpiece and camera of the portable phone. This abuse empowers the assailant to set up a switch TCP shell, allowing them further control over the gadget. Through this shell, the assailant can capture screenshots, viably checking client actions without their information. Furthermore, the compromised gadget can stream live video through the camera, posing serious security and security dangers. This level of interruption illustrates how malevolent

applications can use authorizations to attack individual protection and assemble delicate data, emphasizing the requirement for strong security measures in versatile app advancement.

5.2 Discussion

The success of these measures, together with the application of Kali Linux tools, high-encryption schemes, as well as the utilisation of SDDPs, is examined further in the following subsections.

Assessment of Kali Linux Tools

Some of the Kali Linux tools that can be used to identify and prevent MITM attacks include; Wireshark, Burp Suite, and Metasploit. Burp Suite has the feature to intercept and analyse the HTTP/HTTPS traffic making it easier to discover the flaws in the mobile application, and, Metasploit has exploited libraries that allow for the full-penetration test (Arnaldy & Perdana, 2019). All these tools are a strong base for cybersecurity specialists to detect, analyse, and mitigate the threats concerning mobile applications.

Importance of Encryption Protocols

In avoiding MITM attacks, there is a need to ensure compliance with advanced encryption protocols like Transport Layer Security (TLS). The use of reliable encryption mechanisms in the reaction to MITM attacks is crucial bearing in mind that it renders it hectic for the attacker to decode the intercepted information (Gong, Ochiai, & Esaki, 2020).

Function and purpose of Multi-Factor Authentication (MFA)

The probability of the unauthorized use of the mobile application is reduced by incorporating MFA, which demands the use of several identification methods to gain access. MFA can be useful in defending against MITM attacks in cases where the attacker can obtain the users' initial credentials due to the enhancement of security it brings according to Albalawi & Almaiah (2022). Nevertheless, for most of the applications, MFA provides benefits but at the same time, it enlarges the user interface leading to a possible restrained user experience. Thus, paradoxes must be found between the concepts of security and usability.

A study on the effect of IDS on computer security Systems.

AIDS is widely used in networks to detect anomalous activities such as MITM; therefore, the use of IDS is very important in preventing MITM attacks. IDS is capable of recognizing certain characteristics of data traffic such as consistent high traffic or newly discovered routes which are behavioural measures of MITM attacks (Niboucha et al. , 2022).

Secure Development Practices

These practices mandate that security becomes a part of the development cycle to ensure that as much as possible no introduction of the vulnerabilities takes place. The chapter provides a recap of the findings that pertain to the efficacy of countermeasures against Man-in-the-Middle attacks on Android applications. It emphasizes the use of the tools in Kali Linux such as Wireshark, Burp Suite, and Metasploit in identifying and fixing the flaws. The use of HTTPS, SMIA, and different SSL cyphers is proven to be effective in avoiding MITM attacks, along with practising security in software development. Further, intrusion detection systems client-side Anomaly detection and secure channels of communication can be regarded as some other security parameters. Using machine learning for the constant check of anomalies and performing security check-ups increases the effectiveness of threat identification, adding to mobile application security.

6 Conclusion and Future Work

This dissertation aims to explore different measures/tactics as well as utilities in preventing Man-in-the-Middle (MITM) attacks on mobile applications. By implementing sophisticated cybersecurity tools and tactics, namely, Kali Linux, Wireshark, Burp Suite, and Metasploit to determine and rectify the loophole in mobile applications. The results underpin optimal protocols like Transport Layer Security (TLS), which are central to data protection against interception by attackers. Also, studies indicate that establishing MFA significantly decreases the probability of attacks, thus improving security overall. Principles like maintaining security through development, security evaluations, code reviews, and vulnerability assessments are important due to the reason that they help to identify security holes before they can be exploited.

6.1 Linking with Objectives

Objective 1: This research work aims to assess the efficiency of Kali Linux tools the study effectively employs the tools including Wireshark, Burp Suite, and Metasploit in tracing and diagnosing malware in mobile applications. The demonstration of these tools' capability which involves setting up a reverse shell and capturing information supports the fact that these tools are effective in identifying and investigating the vulnerability of the mobile applications**.** Wireshark, Burp Suite, and Metasploit – for tracing and diagnosing malware problems in mobile applications. The study implies that the tools are successful in the detection of the weakness and diagnosis of the malware. Another feature regarding the acquisition of packets with the help of Wireshark is that all the data packets can be analysed

which might help identify irregularities that signify MITM attacks. One advantage of using Burp Suite is the HTTP/HTTPS traffic intercepting and analysing which allows for discovering the security issues in mobile applications, another advantage of Penetration testing is Metasploit's exploit database that contains a wide range of exploits. Altogether, these tools develop a strong background to check, analyse, and fix the risks in mobile applications to improve their security for cybersecurity specialists.

Objective 2: Vulnerabilities of exposed areas in Mobile Application Frameworks

To this end, the study develops a demo website and hosts it on an Apache server to demonstrate some of the possibly exploitable vulnerabilities in the mobile app frameworks. The presence of a fake malicious app and then its execution, as well as the MITM attack scenarios, indicate the extent of risks in real-time communication; risks are associated with unverified APK downloads and the absence of effective security measures.

Objective 3: Implementable Protection Steps

This section will focus on proposing the measures that should be taken to enhance security.

Certificate pinning is agreed to be a key countermeasure in the research towards improving security in mobile applications. This showcases the vulnerability of some devices' features like the cameras and microphones to unauthorized access, thus the necessity to enhance security. To reduce the possibility of MITM attacks, the study suggests using certificate pinning and other measures.

Objective 4: Consequence of MITM Attacks

The assessment in the study focuses on the effects of MITM attacks on the functionality and security of mobile applications used for users' data. In the contexts of the attacks analysed by the research, it shows how an adversary can interrupt the application speed and corrupt the data, making known the high impacts in such cases.

Objective 5: To assess the level of security used in the Mobile App.

Another important aim is assessing the state of protection in modern mobile applications and its effectiveness in preventing MITM threats. It becomes imperative to conduct periodic security assessments and full vulnerability tests and follow secure development standards regarding mobile applications. This evaluation suggests that the issues of protection of the user data and integrity of the application require constant enhancement of the security measures.

Objective 6: This shall entail the formulation of security standards.

Some of the prominent recommendations made by the study of secure coding are: validation of the inputs; handling of errors; and security audits carried out at fixed intervals. Thus,

following the standards mentioned above, developers will be able to reduce the number of potential vulnerabilities that can be utilized in MITM attacks.

Objective 7: Impact towards Knowledge Enhancement of Mobile App Security

Last but not least, the study is going to contribute to the noted area of mobile app security with actual data and acquire the knowledge that can potentially assist with the emergence of cybersecurity and tools for enhancing the protection of data and user privacy. The significance of the research is in the wealth of information it provides on the level of efficiency of various security measures as well as gaps existing in mobile applications.

6.2 Recommendations

The following recommendations are the focus on improving security for mobile application against threats such as Man-in-the-Middle (MITM).

- Implement Advanced Encryption: These developers must also ensure that they implement strict measures of security on data transfer such as Transport Layer Security (TLS). This assist in filtering out all the malicious interferences from attackers hence making sure that all sensitive information is out of bounds to anyone who wants access in for the purpose of carrying out MITM attacks.
- Adopt Multi-Factor Authentication (MFA): Implementing MFA enhance the security of mobile applications because one has to enter multiple authentication factor credentials to access the system. This added layer of security makes it a lot harder for the attackers to get into the system and hence decreasing the chances of success.
- Conduct Regular Security Audits: It is required to perform security audit and vulnerability scans – the last ones will help to define possible security flaws. This is because a consistent monitoring enables developers to work on the flaws and release updates that mitigate threats before the attackers exploit the gaps and make mobile applications susceptible to various threats.
- Use Certificate Pinning: Incorporation of the certificate pinning should be done by developers for purposes of ensuring that only mobile applications communicates with trusted servers only. This means that even if an attacker tries to intercept communication, he cannot reroute traffic to the bad guys' abode.
- Leverage Kali Linux Tools: Open source tools like Wireshark, Burp Suite and Metasploit are very useful for surveillance, analysis and controlling of security vulnerability. These tools help developers as well as security personnel for properly identifying and handling vulnerabilities.

- Deploy Intrusion Detection Systems (IDS): IDS must be installed to ensure that traffic flow in the network is observed and any suspicious traffic that is indicative of the MITM attack is noted for action to be taken.
- Educate Developers: Ongoing training in secure coding is quite important since it prepares developers for the ever changing security challenges that are a reality in mobile application development in the current world.

6.3 Future Studies

Further work should be directed towards the identification of enhanced prevention methods of MITM attacks that would be relevant in the new era of actualisation of 5G networks and IoT devices. Due to the growing integration and interconnection of these systems, the researchers are left with no choice other than to innovate scientific methods for handling these systems' security.

- To support the effectiveness and practicality of machine learning as well as artificial intelligence algorithms in MITM attack detection, further research and studies are required. AI can help future research come up with smart and self-learning security systems to counter the ever-changing risks (Greenwood et al. 2014). This approach could greatly improve how secure those mobile applications and other venues of digital interaction are.
- The behavioural aspect of users represents yet another avenue for the subsequent research concerning the vulnerability to MITM attacks. Research could explore how levels of users' awareness and usage impact the application's effectiveness which could inform how educational and policy measures could strengthen cybersecurity practices.

7 References

Albalawi, A.M. and Almaiah, M.A., 2022. Assessing and reviewing of cyber-security threats, attacks, and mitigation techniques in IoT environment. *J. Theor. Appl. Inf. Technol*, *100*, pp.2988-3011.

Alhamed, M. and Rahman, M.H., 2023. A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, *13*(12), p.6986.

Alwazzeh, M., Karaman, S. and Shamma, M.N., 2020. Man-in-the-middle attacks against SSL/TLS: Mitigation and defeat. *Journal of Cyber Security and Mobility*, pp.449-468.

Arnaldy, D. and Perdana, A.R., 2019, September. Implementation and analysis of penetration techniques using the man-in-the-middle attack. In *2019 2nd International Conference of Computer and Informatics Engineering (IC2IE)* (pp. 188-192). IEEE.

Bhardwaj, A., Bharany, S., Abulfaraj, A.W., Ibrahim, A.O. and Nagmeldin, W., 2024. Fortifying home IoT security: A framework for a comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities. Egyptian Informatics Journal, 25, p.100443.

Blancaflor, E., Pastrana, R.L.P.J., Sheng, M.J.C., Tamayo, J.R.D. and Umali, J.A.M., 2023, March. A Security and Vulnerability Assessment on Android Gambling Applications. In the International Conference on Computer and Communication Engineering (pp. 106-115). Cham: Springer Nature Switzerland.

Cherian, M.M. and Varma, S.L., 2022. Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks. *International Journal of Computer Network and Information Security*, *14*(1), p.52.

Dwivedi, A., 2022. LAUNCHING AN ATTACK AND EXPLOITING THE ANDROID USING METASPLOIT FRAMEWORK. International Journal of Scientific Research in Modern Science and Technology, 1(4), pp.19-32.

El-Taj, H. and Miralam, L., 2024. Network sniffing and its consequences: a comprehensive survey. International Journal of Computer Science and Information Security (IJCSIS), 22(3).

Gong, S., Ochiai, H. and Esaki, H., 2020, July. Scan-based self anomaly detection: client-side mitigation of channel-based man-in-the-middle attacks against Wi-Fi. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1498-1503). IEEE.

Greenwood, D.S.J.S.G. and Khan, Z.L.L., 2014, February. Smv-hunter: Large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps. In *Network and Distributed System Security Symposium (NDSS). Internet Society, San Diego, CA* (pp. 1-14).

Hwang, H., Jung, G., Sohn, K. and Park, S., 2008, January. A study on MITM (Man in the Middle) vulnerability in wireless network using 802.1 X and EAP. In *2008 International Conference on Information Science and Security (ICISS 2008)* (pp. 164-170). IEEE.

Mallik, A., 2019. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, *2*(2), pp.109-134.

Meyer, U. and Wetzel, S., 2004, October. A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 90-97).

Michelena, Á., Aveleira-Mata, J., Jove, E., Bayón-Gutiérrez, M., Novais, P., Romero, O.F., Calvo-Rolle, J.L. and Aláiz-Moretón, H., 2024. A novel intelligent approach for man-in-the-middle attacks detection over internet of things environments based on message queuing telemetry transport. Expert Systems, 41(2), p.e13263.

Mirza, S., Abbas, H., Shahid, W.B., Shafqat, N., Fugini, M., Iqbal, Z. and Muhammad, Z., 2021, October. A malware evasion technique for auditing android anti-malware solutions. In 2021 IEEE 30th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE) (pp. 125-130). IEEE.

Mohd Saudi, M., Husainiamer, M.A., Ahmad, A. and Idris, M.Y.I., 2023. iOS mobile malware analysis: a state-of-the-art. Journal of Computer Virology and Hacking Techniques, pp.1-30.

Muzammil, M.B., Bilal, M., Ajmal, S., Shongwe, S.C. and Ghadi, Y.Y., 2024. Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. IEEE Access.

Muzammil, M.B., Bilal, M., Ajmal, S., Shongwe, S.C. and Ghadi, Y.Y., 2024. Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. *IEEE Access*.

Niboucha, R., Saad, S.B., Ksentini, A. and Challal, Y., 2022. Zero-touch security management for mMTC network slices: DDoS attack detection and mitigation. *IEEE Internet of Things Journal*, *10*(9), pp.7800-7812.

Özdemir, D. and Zaim, H.Ç., 2021. Investigation of Attack Types in Android Operating System. Journal of Scientific Reports-A, (046), pp.34-58.

Ravindran, U. and Potukuchi, R.V., 2022. A Review on Web Application Vulnerability Assessment and Penetration Testing. *Review of Computer Engineering Studies*, *9*(1).

Reece, M., Rastogi, N., Lander, T., Dykstra, J., Mittal, S. and Sampson, A., 2024, June. Defending Multi-Cloud Applications Against Man-in-the-Middle Attacks. In Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (pp. 47-52).

Salem, O., Alsubhi, K., Shaafi, A., Gheryani, M., Mehaoua, A. and Boutaba, R., 2021. Man-in-the-Middle attack mitigation in internet of medical things. *IEEE Transactions on Industrial Informatics*, *18*(3), pp.2053-2062.

Sandhu, G.S., 2021. Implementation of Portable Security Analysis Tool.

Singh, V.R., Sharmila, S.P. and Chaudhari, N.S., A Study on Analysis of Malware in Android Applications.

Sinnaiya, C.R.R.M.M., Al-Mahri, M.M.B., Veerasamy, D. and Karickom, S.T., 2024. Comprehensive Analysis of the Current State of Cyber Security Measures for IoT Devices. Southeast Europe Journal of Soft Computing, 13(1), pp.69-78.

Stricot-Tarboton, S., Chaisiri, S. and Ko, R.K., 2016, August. Taxonomy of Man-in-the-Middle Attacks on HTTPS. In *2016 Ieee Trustcom/Bigdatase/Ispa* (pp. 527-534). IEEE.

Sutter, T., Kehrer, T., Rennhard, M., Tellenbach, B. and Klein, J., 2024. Dynamic Security Analysis on Android: A Systematic Literature Review. IEEE Access.

Thankappan, M., Rifà-Pous, H. and Garrigues, C., 2024. A signature-based wireless intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks. *IEEE Access*.

Toutsop, O.M., 2022. *Internet of Things Platform Security and Countermeasures* (Doctoral dissertation, Morgan State University).

Yang, Y., McLaughlin, K., Littler, T., Sezer, S., Im, E.G., Yao, Z.Q., Pranggono, B. and Wang, H.F., 2012. Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems.

Χρόνης, Α., 2023. Malware Analysis and Reverse Engineering.