Journal of Theoretical and Applied Information Technology
30th June 2023. Vol.101. No 12
© 2023 Little Lion Scientific

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PENETRATION TESTING IN MOBILE DEVICES, VULNERABILITIES AND SOLUTIONS

MARIAM ALHAMED [1]* RAWAN BUKHOWAH [2]*, SARA ALSAHAIM [3] *, AND MOUNIR FRIKHA[4]*

1. Department of Computer Networks and Communications, King Faisal University, Saudi Arabia
2. Department of Computer Networks and Communications, King Faisal University, Saudi Arabia
3. Department of Computer Networks and Communications, King Faisal University, Saudi Arabia
4. Department of Computer Networks and Communications, King Faisal University, Saudi Arabia

E-mail: [1]222402149@student.kfu.edu.sa, [2]222402836@student.kfu.edu.sa,
[3]222401742@student.kfu.edu.sa , [4]mmfrikha@kfu.edu.sa

ABSTRACT

Mobile phones have become an essential thing these days, in education, entertainment, even in the medical field, all these uses for mobile phone led to the fact that mobile phone contains a huge number of data should be protected. Mobile phones with all of its features have also vulnerabilities could anyone exploits, to maintain the security of the mobile phone it has to scan in every specific and regular time to determine vulnerabilities and the security issues to patch and fix by using the penetration testing operation. This paper will represent the OWASP mobile top ten security vulnerabilities, as will identify the different mobile threats and their countermeasures, and the research will review the models for penetration testing threats. This research represents a Mobexler mobile application penetration-testing framework to verify the security vulnerabilities in IOS application, which is LinkedIn application, the methodology divided into seven phases: 1. Planning 2. IPA file and information gathering 3. Selecting application 4. Selection security tools 5. Setup and analysis 6. Manual review of Appxmanifest.xml 7. Dynamic analysis which checks for vulnerabilities and detect security misconfiguration.

Keywords: *Penetration Testing; Mobile Devices, IOS, OWAPS, Threat*

1. INTRODUCTION

Mobile devices are very important today and it is used widely even for personal or business purpose, such of mobile devices are smartphones and tablets. According to a report done by KPBC "the number of smartphone users worldwide has risen above 1.6 billion in 2013" so what about the number of users today! Mobile devices including its applications contain sensitive information of people and sometimes-sensitive information about their work such as user name, password, credit card account number, health state information and contact list and in these days, it becomes an easy target for cyber criminals. Many kinds of attacks that are targeted to the mobile devices and its applications such as malware, sniffing, viruses phishing by attackers and among all threats, malware is the famous one [16]. In addition, the huge concern about mobile applications and their popularity in these days, it is not surprising because now they are not only for calls and for text messages, they used for almost everything.

The crowding of using mobile devices ensure the need of security for these mobile devices. As showing in the figure1 [12] it shows the increase in using mobile devices.

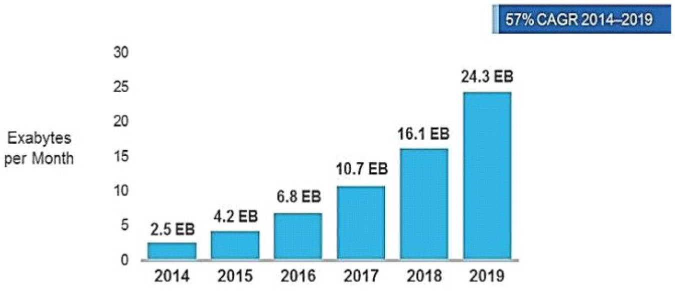


Figure1: Growth of using mobile devices

Penetration testing is used widely with mobile devices such as smartphones and tablet because they are used a lot. Increasing the use of them cases the increase of vulnerabilities and the chance to exploit them by attackers. Penetration testing is used to find weaknesses in the network, so it is very effective tool in helping to solve security issues on the network and applications. Penetration tests are security professionals, there task is to evaluate and hack the enterprise's network, application, system and services for example so then they can fix it before the malicious users do [7].

In mobile app, penetration test process involved by select the testing environment, then lunching testing procedures on the mobile device and analyze results. Wireshark is the most usage penetration testing tools that could be used for monitoring the traffic of network. Other tools are Nmap, Nessus and Metasploit that are included in Kali Linux [16].

The increasing of using mobile devices creates potential threats and many vulnerabilities, so the paper analyzes these threats and vulnerabilities to identify the most previous mobile application testing studies relied on 10 or WAP security vulnerabilities followed by a physical attack. In Android, there was a lot of practicing, unlike the IOS operating system so this paper observes how to develop mitigation techniques upon the IOS operating system specifically.

The paper is organized as follows: Section 2 present background that since 2000 and 2001 the research work on mobile operating systems was began, outline the research objectives and the scope of the paper, what the motivations and the paper determines its expected outcomes. Section 3 presents various penetration testing threat models such as security development lifecycle (SDL) model, threat model and Open Web Application Security Project (OWASP) model. Section 4 present related works. Section 5 present methodology. Section 6 present results and discussions. Section 7 limitation followed by section 8 conclude the paper and section 9 future work.

2. BACKGROUND

Mobile devices that know like smartphones, laptops and PDA become the first important thing on the word, for every moment in the person life and for daily activates even though for work. So, since the time has changed. Web applications are mostly converted into mobile apps. Furthermore, the paper focused on mobile penetration testing even for operating systems like Android and mobile applications and mobile cloud computing.

In these days, the worker works outside the working hours and outside the office, so he needs mobile device to complete his tasks and enter to the enterprise data from not just private network of enterprise he also enters from many public networks. One survey found that 81% of global executives use a mobile device and analyst estimates that 1 billion mobile workers that mean most people need to use their phone or laptop to do their job by 2011 and this for every one's benefits. In other hands, their device may not secure enough against any malicious apps or attacks form hackers [1]. Mobile devices users and mobile applications increase substantially so enhance the level of security and applied penetration testing is sufficiently important to finding the hidden vulnerabilities. Some of serious threats of mobile devices are malwares, viruses, man-in-the-middle (MitM) attacks that cusses loose of sensitive information, Penetration testing is gaining important from long time because of increasing use of mobile devices. Penetration testing known as Pen-test or white hat which used to identifying vulnerabilities in any application and using test scenarios to uncover issues that can allow an intruder to gain access to a data/system. In addition, penetration testing helps in gathering information of mobile application, analysis all exist vulnerabilities of mobile application and it is important to mention that penetration testing differ from vulnerabilities assessments [2]. The big concern is the security of mobile applications and studies since 2012 showing that weaknesses include 63% of insecure data storage, 57% of insecure trans-mission of data, 40% of lack of protection, 40% client-side injection and 69% leakage of sensitive data [3]. OWASP stands for Open Web Application Security Project provide a product called OWASP Mobile Top Ten that is for mobile application security and it is as documentation of the 10 weaknesses that exist in mobile applications, including the above weaknesses [3]. Since 2000 and 2001 the research work on mobile operating systems was began [4]. With using Android OS growing up a lot of attack vectors and vulnerabilities which are detected in 2018 and 2019 showing that major vulnerabilities which hackers exploit them are DoS, gain privileges, file injection, SQL injection, Http response splitting and more [2]. Android is an open-source that has its own security mechanism. In addition, along with the penetration testing, the analyzing of the security mechanisms of the

Android OS is important. Therefore, this study aimed:

- OWASP Mobile Top 10 Security Vulnerabilities.
- Threats in different types of operating system in mobile devices.
- Penetration tests in the IOS mobile application.
- Identifying the suggested countermeasures

As smartphones are integral part of our daily lives based on the Internet. Smartphones make it easy for their users to perform activities online. Although smartphones provide many conveniences and facilities, such as the ability to hold a meeting at the level of countries in the world through online meetings application. Therefore, attackers are trying to find a way to exploit the vulnerabilities in smartphones. This project focuses on IOS operating systems in smartphones. The results of this study will help to identify the vulnerabilities and the techniques used to find a vulnerability in different types of operating systems such as IOS application.

Due to the rapid development in the technical transformation, where technology began with large personal commuters and developed to what we see today in the small de-vices such as mobile phones in the present time, therefore mobile phones has become a substitute for using the computers or laptops in the daily life such as medical procedures, work, education and entertainment. However, with the tremendous development in mobile phone technology, there is also a development in threats facing it. Which might threaten the security of the data. There are several types of threats in mobile phones such as physical threats, social engineering threats, malware and threats could be different based on the operating system.

In order to solve the problem of technical threats, there is what is known by penetration testing, which is intended to do a test to find out what penetrations might be in the mobile phone, then based on the result it is processed and updated to patch these holes, as the researchers define it “a security-oriented systemic probing of the system from inside or out-side to seek out vulnerabilities that an attacker could exploit”. [1]

The necessity of the mobile phone in the daily life and the importance of the penetration testing to protect it, this was the motive for choosing the topic of this research. Finally, the results of this study will be vulnerabilities of IOS. The technique to exploit the vulnerabilities. In addition, the types of attacks for different operating systems in mobile devices and techniques of penetration testing in the different operating systems will be identified.

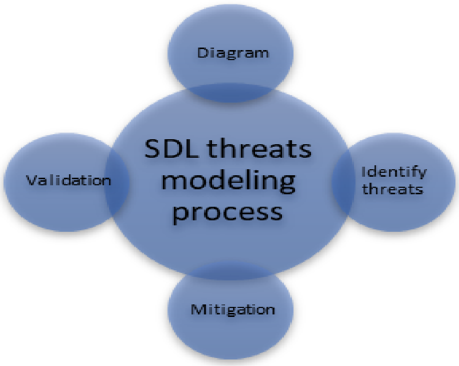
3. MODELLING PENETRATION TESTING THREATS

3.1 Security Development Lifecycle (SDL) Model

This model is used to analysis and assessment threats that related to mobile devices, so this tool helps developers and penetration testers to identify, mitigate and validate these threats. For implementing, in the model there are three important steps must be carried out:

3.1.1 Decompose the Application

In the stage, the penetration testers must deal with data, through identify the relationship between that the application has in inside and outside with the environment. Therefore, the information that found from outside and inside, the type of these data founded and know the information and storage management process will give several security threats it should be categorized for the next step.



3.1.2 Give Hierarchy to Threats

This stage can be done by using different models such as STRIDE tool (spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege). This model helps to act as the attacker through identifying threats from the system and its components. In addition, there are other tools could be used for the hierarchy.

3.1.3 Mitigate the Threats

In this stage, a mitigation map is made where the threat could be assigned and then the action taken to mitigate it. In the figure 2 below, the process of SDL threat modelling is showing [12].

Figure2: SDL threat modelling process

3.2 Threat Model

This model is focus in identifying and determining vulnerabilities in mobile devices and its applications. In addition, the model helps in understanding an attack surface and by which vulnerability can attacker expose the device or even the users' sensitive information. There are many threats, which are categorized by this model:

3.2.1 Insecure Data Storage

Mobile device's file system that is not encrypted, it may expose by a malicious user and absolutely these files are store have sensitive information.

3.2.2 Lack of Binary Protection

Binary protection is not secure enough, with binary protection, information in mobile devices can be easily modified, changed, and reverse-engineered and analyzed by attackers.

3.2.3 Unintended Data Leakage

It happens by stored sensitive information in an unsecure location inside the mobile devices; this information becomes simply accessed by malicious users.

3.2.4 Malware in Applications

It is the most usage way that done by attackers and it is popular. Attacker’s goal is to exploit the threats of mobile devices and its applications. Such kinds of malware are worms, virus, Trojan horses and adware.

3.2.5 Weak Cryptography

Weak cryptography algorithms in the encryption process causes of returns encrypted code or confidential information to its original unencrypted form by attackers.

3.2.6 Insufficient Transport Layer Protection

During transmission between mobile devices, attackers may traverse the network to gain sensitive information.

These vulnerabilities lead to these types of attack, MitM attack, replay attack, phishing attack, session hijacking, masquerade, traffic analysis and Wi-Fi sniffing, account lockout attack and privilege escalation attack [10].

3.3 OWASP

This model is known as Open Web Application Security Project (OWASP), it is focus on how to understand, develop, obtain, operate and maintain mobile devices and its applications to be trusted by users. One of OWASP tools are used specifically on mobile application security and this model document top ten weaknesses that could be exposit in mobile applications. The top ten mobile applications vulnerabilities are clarifying in table 1 with its description and the table shows if the risk level is high, medium or Tinggi (Parah) [10].

4. RELATED WORK

Many research papers on Android and IOS application security focus on permissions, Android malware, and other security issues. In this section, we discuss the previous studies on Android and IOS security.

In the study of Palak Ar et al. [1] (2017) the researchers illustrated and defined penetration testing and the role of it in the security assessment as the study divided the testers into groups back box, white box and Gary box each of them has level in the knowledge of the tested system, as the study illustrated the penetration testing tools such as port scanning. While, in the study of Ioan Adascalitel [2](2019), the author performed a review on smart phones and IOT security, the study illustrated the increasing of using smart phones and the different potential threats, the study analyzed threats into two categories the first physical threats and vulnerabilities such as lost device or damage device, the second one software-based threats and vulnerabilities such as threats on the network level when the device is connected to unsecure network.

In the study of Alin Zamfiroiu et al. [3], the researcher reviewed an article on mobile data vulnerabilities; the researchers illustrated the hardware threats such as cold boot at-tack and the software threats such as malware attack.

In this study of Martin butler et al. [4], the authors performed A review on the influence of mobile operating systems on user security behavior, the study threats detection based on behavioral studies focusing on different aspects of smartphone user behavior, because the user behavior is affecting on the security aspects in his device.

The study by Alshehri et al. [5] discussed that in 2017 there are more than 700,000 applications removed from the Google Store because of malicious applications. Therefore, the authors proposed a tool for Android operating system (DOPA) to perform penetration tests in Android smartphones and control the user's device without permission. They found that with the proposed tool, the user can monitor the ports and take the best measures to solve the open ports problem.

In the study of Al-Ahmad. A et al [6] proposed requirements for penetration testing for MCC, namely offloading and mobile state management. These are two new and important requirements that were not considered in penetration testing for previous technologies. The model serves to uncover hidden vulnerabilities, facilitates mutual trust, provides security guarantees, enables developers to build more secure mobile cloud applications, and finally provides recommendations to avoid vulnerabilities. While, in the study of Alanda. A et al [7] conducted penetration testing of mobile cloud computing applications to identify the vulnerability and techniques used to find a vulnerability in Android operating systems and Android applications. The authors tested five Android applications from the Play Store and found vulnerabilities based on OWASP's top ten mobile device documentation. The authors found that 80% of the vulnerabilities are the same as in OWASP Mobile 10. Jon et al. [8] provide an overview of threats to mobile devise and specifically for data and what are possible defenses, which consider as penetration testing practices. Furthermore, the paper demonstrates threats into seven categories that are described deeply, and then the paper discusses every threat that in return has its defense/s, in penetration testing knowing threats is the first step so this paper is very important. Some of these threats are malware, social engineering and malicious insider actions etc., and defense actions like data encryption, firewalls, anti-virus and virtual private networks etc. At the end of the paper, it assesses priorities among the different threats and defenses and some suggestions for further research. While in the study of Naresh et al., [9] present and describes the Android OS and its architecture and types of operating systems. In addition, the paper present security mechanisms in the Android OS with valuates and discovering security issues with the help of penetration testing. The paper focused on WLAN network security issues while preforming penetration tests. In the study of Sriramulu et al. [10] focused on analyzing mobile banking applications for both Android and IOS to determine related security threats then the paper pro-posed threat model. This model helps in determining possible vulnerabilities and appropriate penetration tests. Therefore, the paper presents a detailed analysis of the security mechanisms of mobile banking applications, which helps developers, security tester, researchers and bankers and bank customers to increase their awareness. As showing in the paper, according to recent report 95% of the top 200 free IOS and Android apps exhibit at least one risky behavior another report shows that 91% of IOS apps and 85% of Android apps are face threats on such parts like on location tracking, enable address. The paper also suggests a security-testing framework for mobile applications. At the end it analyzes these mobile banking applications to the OWASP listed of mobile security risks and the paper give its observation.

Acheampong.E et al [11] used the Android security framework Mobexler for automated security testing, while source code review was performed manually. Therefore, the implemented Android penetration tests used seven common open-source mobile application security tools, namely MobSF, APKTool, Drozer, Frida, Burpsuite, Logcat, and Inspeckage. The authors tried to check the vulnerabilities when the application is running in real time. In conclusion, they recommended that companies adopt a hybrid approach to penetration testing.

Celio et al [12] used software methodologies for highlighting the importance of impalement guidelines in the development of OWASP for the mobile applications and then link these founded guidelines with the related top ten security vulnerabilities that associated from the OWASP. Furthermore, the paper discuses and describe the most functionalities that effect on implementation such as authentication and password management, communication security, payment control, information storage and data protection, session management and the obfuscation of code. In addition, the paper carried out the steps of SDL threat model. Steffen et al [13] proposed a model-driven development to support mobile applications that face challenges and under this model the paper present, others model such as a modeling language and an infrastructure for native apps in Android and IOS. In addition, the paper provides case studies for several apps to enhance the security. While the study of UL HAQ et al [14] addressed the difficulties, Android developers face in creating a secure application for android using the software quality model ISO /IEC 25010. By including all vulnerabilities during the design process using an Android vulnerability repository, they were able to identify the issues and gaps that could help developers create a mobile application that is secure. In conclusion, they noted that while these frameworks provide recommendations, strategies and tools for effective penetration testing, the methods used are generic and mostly focused on web-based applications. Without the experience and knowledge of the impact of change, developers and testers cannot use them.

In this study of Syed Farhan Alam Zaidi et al. [15], the authors performed a survey on A Survey on Security for Smartphone Device; the study illustrated the Structure of Smartphones Operating System and the vulnerabilities such as System Fault / Defects, Insufficient Management of Apps, Unsecure Wireless Network, Lack of User Awareness.

Table 1: Top 10 Vulnerabilities

Table 2: Summary Of The Suggested Methodology For Protecting Mobile Application Against Vulnerabilities

Numbers	vulnerabilities	Description	Risk level
1	Improper platform usage	It happens by improper use for platforms and security controls. Other reasons like non-use of touchID, keyChain IOS.	High
2	Unsafe data storage	It happens by emerge unsafe data storage and unsafe authentication.	High
3	Insecure Communication	It happens by poor link protocols, unencrypted communication for sensitive information and weak negotiation.	High
4	Unsafe Authentication	Authentication process may failure	High
5	Insufficient cryptography	Cryptography is happen specifically to a sensitive information assets. It is related to TLS and SSL goas on insecure communication.	High
6	Insecure Authorization	It happens via authorization process failure such as authorization decisions on the client side and forced navigation.	High
7	Quality of the customer code	This category includes all problems and issues at the code level in the mobile client. This would capture things like buffer overflows, format string vulnerabilities.	Medium
8	Code adulteration	It happens by binary patches, modification of local resources, method hooks, method swizzling and dynamic memory modification. In addition, an attacker can directly modify the code.	Tinggi (Parah)
9	Reverse Engineering	It happens by software such as tools, IDA Pro, Hopper and other tools that help the attacker to check the application's internal operation.	Medium
10	Strange Functionality	Such as hidden backdoor functionality done by an attacker and other internal security controls that outside production environment.	High

Authors	**The name of the paper**	**Publication year**	**Methodology**	**Methodology Advantage**	**Methodology Disadvantage**
Palak Ar et al. [1]	Analysis of Penetration Testing Tools	2017	An overview	The study illustrated and defined penetration testing and the role of it in the	There is no disadvantage.

				security assessment as the study divided the testers into groups black box, white box and Gary box each of them has level in the knowledge of the tested system.	
Ioan Adascalitel[2]	Smartphones and IOT security	2019	An overview	The study illustrated the several mobile phones threats as the mitigation for these threats.	There is no disadvantage.
Alin Zamfiroiu et al. [3]	Mobile data vulnerabilities	2019	An overview	The study discusses threats such as hardware threats such as cold boot attack and the software threats such as malware attack, as the study recommend some mitigation actions such as updating OS and encryption.	There is no disadvantage.
Martin butler et al. [4]	The influence of mobile operating systems on user security behavior	2021	An overview	The study illustrated Threats in the operating system, as the study discussed behavioral studies focusing on different aspects of smartphone user behavior.	The study did not present several mitigations.
Alshehri et al [5]	DOPA: Detecting Open Ports in OS	2018	Qualitative	Detect open ports in Android and inform users.	The conclusion does not discuss future work.
Al-Ahmad. A et al [6]	Android Systematic Literature Review on Penetration Testing for Mobile Cloud Computing Applications	2020	Qualitative	Provides chance the developers to build more secure mobile cloud application.	There is no limitation.
Alanda.A et al[7]	Mobile Application Security Penetration Testing Based on OWASP	2019	Qualitative	The authors tested five Android applications from the Play Store and found that 80% of the vulnerabilities were common.	The recommendations are not clear and there is no future work.

Jon et al. [8]	Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses.	2020	An overview	The paper observes all possible threats that related to mobile devices and its applications in an organized manner and discusses security technologies for these threats.	The paper only focused in threats and defenses and ignored such important parts of what the paper should include.
Naresh et al. [9]	Penetration Testing of Android-based Smartphones	2011	Methodology by NIST	It's clear paper that cover all paper's objectives in good way.	There is no disadvantage.
Sriramulu et al. [10]	VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps	2017	Case study and survey	The paper supports it ideas with case study and show valuable results of security and reputation of such mobile banking applications.	Even the paper focus on developing a security framework, there are a lot of unneeded information.
Acheampong.E et al [11]	Automatic and manual discovery of vulnerabilities in selected Android Mobile applications.	2022	Qualitative	The authors used hybrid Android penetration testing to identify the possible attacks.	There is no limitation.
Celio et al [12]	A Conceptual Exploration for the Safe Development of Mobile Devices Software Based on	2018	Qualitative	The paper focus on safe software development methodologies and such of these software are security development lifecycle (SDL) and the paper applied this model in detail, correctness by construction (CbyC), cigital	High degree of security for mobile devices is needed.

	OWASP			touchpoints and TSP-Secure. These methodologies are very useful in improving software quality and reducing the number of defects and complying with the specified functionality.	
Steffen et al [13]	Model-driven development of mobile applications for Android and iOS supporting role-based app variability	2018	Descriptive	The paper proposed Model-driven development.	The paper does not mention to penetration test techniques.
UL HAQ et al [14]	Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review	2021	Qualitative	The authors used ISO /IES 25010 to identify the security issues developers face when building applications in Android.	The paper did not perform penetration testing.
Syed Farhan Alam Zaidi et al. [15]	A Survey on Security for Smartphone Device	2016	Survey	The Authors discuss several threats such as physical attacks and relay attack.	There is no disadvantage.

The main goal for most of these related studies is to find vulnerabilities like OWASP list of vulnerabilities and suggested technologies such as applied threat analysis model. Table 3 shows a summary of the vulnerability and solutions that related to mobile penetration testing.

Table 3:Summery of the vulnerability and solution

Author	Vulnerabilities	Solutions
Ioan Adascalitel [2]	**1.** Physical threats (stolen, damaged, and lost devices) **2.** Software-based threats (network	**1.** Connect to a trusted network **2.** Encryption **3.** -Educate the user

	level man in the middle, phishing)	
Alin Zamfiroiu et al. [3]	Hardware threats such as cold boot attack. software threats such as malware attack.	**1.** Updating operating system **2.** encryption **3.** Password
Martin butler et al. [4]	Threats in the operating system	Behavioral studies focusing on different aspects of smartphone user behavior.
Alshehri et al[5]	Open port SSH to browse the user files.	Detect open ports in Android and inform users by using DOPA: Detecting Open Ports in Android OS.
Alanda et al[7]	OWASP vulnerabilities: 1-Improper Platform Usage 2-Insecure Data Storage 3-Insecure Communication 4-Insecure Authentication 5-Insufficient Cryptography 6-Insecure Authorization 7-Client Code Quality 8- Code Tampering 9-Reverse Engineering 10-Extraneous Functionality	1- Implement secure coding. 2- Use strong encryption for data storage. 3- Use last version in SSL / TLS in communication between server and client. 4- The authentication must be done on the server side. 5- Use a strong cryptographic algorithm. 6- Every request that comes in must be able to be verified by the backend system. 7- Pay attention to the permissions of the application being used. 8- Using anti-tampering. 9- Use obfuscation tool.
Jon et al. [8]	Different types of attacks, virus, worms, targeted attacks, phishing, spoofing and SSL MitM attack.	Some tools like antivirus, anti-spyware packages, SSL encryption firewalls, software life cycle management, configuration management, inputs encryption, password encryption, VPN and backup.
Sriramulu et al. [10]	OWASP vulnerabilities: 1-Improper Platform Usage 2-Insecure Data Storage 3-Insecure Communication 4-Insecure Authentication 5-Insufficient Cryptography 6-Insecure Authorization 7-Client Code Quality 8- Code Tampering 9-Reverse Engineering 10-Extraneous Functionality	It is used primarily with the permission to test cryptography properties as authentication, confidentiality, non-repudiation, also Static and Dynamic analysis helps to detect vulnerabilities by performing vetting (testing) of the mobile apps.
Acheampong etal[11]	Dangerous permission	Performed automated and manual penetration testing for application.
Celio et al [12]	Types of malware on mobile devices and penetration and security threats. OWASP vulnerabilities: 1-Improper Platform Usage 2-Insecure Data Storage 3-Insecure Communication 4-Insecure Authentication 5-Insufficient Cryptography 6-Insecure Authorization 7-Client Code Quality 8- Code Tampering 9-Reverse Engineering 10-Extraneous Functionality	Security Development Lifecycle (SDL) is one of great tools. SDL threat modeling used to analysis and assessment threats like malware. OWASP top ten vulnerabilities can be avoided by its guidelines and its OWASP threat analysis model that is applied throughout the life cycle of application development. Other methodologies are proposed as solutions to increase level of security software that able to resist attacks.
UL HAQ et al [14]	OWASP vulnerabilities: 1-Improper Platform Usage	The OWAPS identified the top 10

	2-Insecure Data Storage 3-Insecure Communication 4-Insecure Authentication 5-Insufficient Cryptography 6-Insecure Authorization 7-Client Code Quality 8- Code Tampering 9-Reverse Engineering 10-Extraneous Functionality	vulnerabilities in mobile application as well as it provides methods to deal with these security risks such as MASVS-R which used to handle sensitive data and MASVS-L1 to cover standard security.
Syed Farhan Alam Zaidi et al. [15]	**1.** Physical Attack **2.** Virus **3.** Relay Attack	**1.** Re-manufacturing whether is software or hardware. **2.** Install update Antivirus in your system. **3.** Use secure network and trusted proxy application.

5. METHODOLOGY

In this work, we will use Mobexler Mobile Application Penetration Testing Framework for verifying exploitable security vulnerability in one selected IOS mobile application. The phases performed in this research are as follows:

5.1 Planning

In the initial phase of this work, we select the IOS application for penetration testing as part of the project. In order to narrow down our analysis and penetration testing, a scoping exercise was conducted to formulate the type of penetration testing to be performed. Our testing was conducted in a "black box" approach, meaning that there was no collaboration with the owners prior to testing.

5.2 IPA Files and Information Gathering

In the information-gathering phase, we will obtain data from IPA files. The IPA files of the selected IOS application will be downloaded from the app store. The app backup recovery program will then be used to extract the IPA files from the application. The files are then set up on the Genymotion IOS emulator.

5.3 Selecting Application

When selecting an application, we only considered those that would satisfy the user base. The app's popularity in the IOS store, the presence of functions for processing sensitive data, preferably login functions, and other features. Thus, we have selected LinkedIn application in IOS version, which is a social media platform for business, and employment that works as a website and mobile application. The reasons for choosing this app be-cause it asks to use location, and contain personal information about the members. In addition, there are more than 875 million members use it. The login method of this application by Google or Password.

5.4 Selection Security Tools

We will use open source security tools for mobile applications to perform effective analysis. These tools work very well with IPA files. We have selected four tools, namely Burpsuite, MobSF, Drozer and Logcat. These tools were chosen for mobile penetration testing because they are widely available and effective. In addition to the accessibility of the tools, the selection criteria also considered community support. Regular updates. The selected tools are listed in the table below:

Table 4: Different open-source security tools for testing IOS applications

Tool	Purpose
Burpsuite	Manual and automated penetration testing tool
MobSF	All-in-one automated tool for static, dynamic and malware analysis.
Drozer	Mobile application dynamic analysis security tool
Logcat	Application package log analysis tool

5.5 Setup and Analysis

The IPA package file contains the code for the application. (It is similar to a zip file). Therefore, we will convert the file to a zip file so that we can unzip it later and view the contents. After that, we download the IPATool to convert AppxManifest.xml to a readable format. After we get the Java source code, it is manually examined for confidential information such as passwords, API keys, etc., which are hardcoded into the code. To speed up the process, MobSF is also used for static analysis.

5.6 Manual Review of Appxmanifest.Xml

The manifest file provides important information about the program to the IOS operating system, App Store, and build tools. The following must be declared in the manifest file:

1. The components of the app, which include all of its functions, services, sender recipients, and content providers.

2. The permissions that the app needs to access the secure areas of the system or other apps. It also specifies the permissions that must be granted to other apps in order for them to access content from this app. Which devices can download the app from the App Store depends on the hardware and software requirements. We will use manual verification to check the status and permissions specified in the file. Some components that will be checked are:

3. Typos when using custom permissions that do not match the declared custom permissions.

4. Test for exported activity.

5.7 Dynamic Analysis

To check for vulnerabilities, we will perform dynamic analysis when the application is running in real time. In addition, in this approach, we will detect security misconfiguration. Some of the components we will be looking for are;

Table 5: IOS mobile application dynamic analysis test components

Analyzing app logs with the tool pidcat	**Test for Intent Sniffing**
Check common settings for permanent login	Test for local encryption issues

6. RESULTS AND DISCUSSION

After analyzing the previous studies, we found that the most previous mobile application penetration testing studies relied on 10 or WAP security vulnerabilities followed by a physical attack. The top ten or OWASP security vulnerabilities which are 1. Improper platform usage, 2. Insecure data storage, 3. Insecure communication, 4. Insecure authentication, 5. Insufficient cryptography, 6. Insecure authorization, 7. Client code Quality, 8. Code tampering, 9. Reverse engineering, 10. Extraneous functionality followed by physical attacks. According to our findings, there are many solutions to mitigate cell phone vulnerabilities, such as performing cell phone penetration tests based on OWASP vulnerabilities, which is the most common solution. It also performs automated and manual penetration testing for applications, the penetration testing will identify the security issues and the vulnerabilities which help to fix these security issues and avoid any possible risk SDL threat modelling, test cryptography, anti-virus and anti-spyware packages, SSL encryption, firewalls, software lifecycle management, configuration management, inbound encryption, password encryption, VPN and backup. In this study, we conducted an intensive literature review and analysis of mobile application penetration testing. Then, we explored the related issues in mobile applications and their OS. We found the following issues as per the literature review in section 4:

1.Sensitive information may store in an unsecured location that is easy to be accessed by hackers.

2.Weak Cryptography is easy to detect by malicious users

3.malware such as worms, viruses, Trojan horses and adware are a big issue.

4.OWASP top 10 vulnerabilities.

5. Physical (hardware) threats.

7. LIMITATION

Although IOS applications use strong authentication mechanisms and store sensitive data securely to keep your mobile applications safe, we need to perform IOS application penetration testing to check all possible vulnerabilities that can be exploited by attackers. In this paper, we propose only one method for penetration testing of IOS applications. Due to lack of time, we have not increased the number of studies and realistic experiences that support penetration testing for IOS applications. In addition, we have not performed the proposed method.

8. CONCLUSIONS

Vulnerabilities in any system make it vulnerable to exploits, this research discusses several models to discover vulnerabilities such as threat model, security development life cycle model, and OWASP. This paper mentioned some threats and their solutions, based on the data analysis the most threats happen is the OWASP security vulnerabilities followed by physical attacks. The research represents a method to verify exploitable security vulnerability which is Mobexler mobile application penetration testing frame work and with all the phases, while the chosen mobile application was linked in application in IOS, the reason of chosen it because it asked to use sensitive information such as location and contain personal information about the members.

9. FUTURE DIRECTION

There are many studies that discuss many tools and frameworks for mobile penetration testing, especially Android application penetration testing, and a little bit about IOS applications penetration testing. We need to be aware that as technology advances, so does the cyberattack, and for that reason, all security vulnerabilities need to be reviewed, because it is not static, and with each advance, the level of security needs to be compared to the existing and new features that will be part of the application. [12] In this paper, we proposed to perform penetration testing in LinkedIn application in IOS version. Based on the research objectives, we will perform the proposed methodology in the future. In addition, we will make the following contribution to help developers build secure applications which is a vulnerability repository that can be updated to provide guidance in designing the IOS applications.

FUNDING:

This work was funded by King
Faisal University, Saudi Arabia [Project No.
GRANT2,967].

ACKNOWLEDGMENTS:

This work was supported through the Annual Funding track by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Project No. GRANT2,967].

REFERENCES

[1] Aar, P., & Sharma, A. K. (2017). Analysis of penetration testing tools. International Journal of Advanced Research in Com-puter Science and Software Engineering (IJARCSSE), 7(9), 36.

[2] Adăscăliţei, I. (2019). Smartphones and IoT Security. Informatica Economica, 23(2), 63-75.

[3] ZAMFIROIU, A., POCATILU, P., & CAPISIZU, S. (2019, May). Mobile data vulnerabilities. In Proceedings of the IE 2019 In-ternational Conference (pp. 407-412).

[4] Butler, M., & Butler, R. (2021, January). The Influence of Mobile Operating Systems on User Security Behavior. In 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP) (pp. 134-138). IEEE.

[5] Alshehri, A., Alshahrani, H., Alzahrani, A., Alharthi, R., Fu, H., Liu, A., & Zhu, Y. (2018, May). Dopa: Detecting open ports in android OS. In 2018 IEEE Conference on Communications and Network Security (CNS) (pp. 1-2). IEEE.

[6] Al-Ahmad, A. S., Kahtan, H., Hujainah, F., & Jalab, H. A. (2019). Systematic literature review on penetration testing for mo-bile cloud computing applications. IEEE Access, 7, 173524-173540.

[7] Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020, May). Mobile application security penetration testing based on OWASP. In IOP Conference Series: Materials Science and Engineering (Vol. 846, No. 1, p. 012036). IOP Publishing.

[8] Friedman, J., & Hoffman, D. J. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile compu-ting and review of applicable defenses. Information-Knowledge-Systems Management Archive, 7(1), 159–180. https://doi.org/10.5555/1402701.1402714.

[9] Naresh, K., & Muhammad, E. U. H. (2011). Penetration Testing of Android-based Smartphones. University of Gothen-burg/Department of Computer Science and Engineering.

[10] Bojjagani, S., & Sastry, V. (2017). VAPTAi: A Threat Model for Vulnerability Assessment and Penetration Testing of Android and iOS Mobile Banking Apps. 2017 IEEE 3rd International Conference on Collaboration and Internet Computing (CIC). https://doi.org/10.1109/cic.2017.00022.

[11] Acheampong, E. O., & Kaur, E. D. AUTOMATIC AND MANUAL DISCOVERY OF VULNERABILITIES IN SELECTED AN-DROID MOBILE APPLICATIONS (PENETRATION TESTING APPROACH).

[12] Gil, C., Baquero, L. E., & Hernandez, M. T. (2014). A Conceptual Exploration for the Safe Development of Mobile Devices Software Based on OWASP. International Journal of Applied Engineering Research, 13(18), 13603–13609.

[13] Vaupel, S., Taentzer, G., Gerlach, R., & Guckert, M. (2016). Model-driven development of mobile applications for Android and iOS supporting role-based app variability. Software &Amp; Systems Modeling, 17(1), 35–63. https://doi.org/10.1007/s10270-016-0559-4.

[14] Haq, I. U., & Khan, T. A. (2021). Penetration frameworks and development issues in secure mobile application development: A Systematic Literature Review. IEEE Access, 9, 87806-87825.

[15] Zaidi, S. F. A., Shah, M. A., Kamran, M., Javaid, Q., & Zhang, S. (2016). A survey on security for smartphone de-vice. International journal of advanced computer science and applications, 7(4).

[16] Wang, Y., & Alshboul, Y. (2015). Mobile security testing approaches and challenges. 2015 First Conference on Mobile and Secure Services (MOBISECSERV). https://doi.org/10.1109/mobisecserv.2015.7072880.