Scientific Research Publishing

Journal of Information Security, 2024, 15, 63-86
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

# Enhancing Mobile Security through Comprehensive Penetration Testing

**Maryam Roshanaei**

Department of IST, Pennsylvania State University, Abington, USA
Email: mur45@psu.edu

**How to cite this paper:** Roshanaei, M. (2024) Enhancing Mobile Security through Comprehensive Penetration Testing. *Journal of Information Security*, **15**, 63-86.
https://doi.org/10.4236/jis.2024.152006

**Received:** January 20, 2024
**Accepted:** February 24, 2024
**Published:** February 27, 2024



## Abstract

In today's era, where mobile devices have become an integral part of our daily lives, ensuring the security of mobile applications has become increasingly crucial. Mobile penetration testing, a specialized subfield within the realm of cybersecurity, plays a vital role in safeguarding mobile ecosystems against the ever-evolving landscape of threats. The ubiquity of mobile devices has made them a prime target for cybercriminals, and the data and functionality accessed through mobile applications make them valuable assets to protect. Mobile penetration testing is designed to identify vulnerabilities, weaknesses, and potential exploits within mobile applications and the devices themselves. Unlike traditional penetration testing, which often focuses on network and server security, mobile penetration testing zeroes in on the unique challenges posed by mobile platforms. Mobile penetration testing, a specialized field within cybersecurity, is an essential tool in the Cybersecurity specialists' toolkit to protect mobile ecosystems from emerging threats. This article introduces mobile penetration testing, emphasizing its significance, including comprehensive learning labs for Android and iOS platforms, and highlighting how it distinctly differs from traditional penetration testing methodologies.

## Keywords

Mobile Penetration Testing, Cybersecurity, Mobile Security, Vulnerability Assessment

## 1. Introduction

The digital security landscape has undergone a profound transformation in the wake of the mobile technology revolution. Mobile Penetration Testing (Mobile Pen Testing) emerges as a pivotal facet within the realm of cybersecurity, uniquely crafted to confront the distinct challenges inherent to mobile platforms.

Unlike conventional penetration testing that concentrates on assessing network, server, and web application security, Mobile Pen Testing is finely tuned to scrutinize the vulnerabilities specific to mobile applications and devices. Mobile technology's pervasive presence has made mobile devices prime targets for cyber threats, necessitating specialized security measures [1]. Mobile Pen Testing is precisely tailored for this purpose. It delves deep into the intricacies of mobile app security, examining coding, data storage, authentication mechanisms, and communication channels. Furthermore, it dissects the interaction between mobile apps and underlying operating systems, ensuring the detection and mitigation of potential weaknesses [2].

As the use of smartphones and tablets has skyrocketed, so has the potential for security vulnerabilities. Mobile devices [3] often hold a wealth of personal and corporate data, making them attractive targets for cybercriminals. The significance of mobile pen testing lies in its proactive approach to identifying and mitigating potential security breaches before they can be exploited. By simulating real-world attacks, pen testers can uncover vulnerabilities in mobile apps, operating systems, and the devices themselves.

The primary distinction between mobile and traditional pen testing lies in the nature of the targets. While traditional pen testing often focuses on external threats to networks and servers, mobile pen testing explores into the unique environment of mobile operating systems, app ecosystems, and the interplay between hardware and software. This specialization is crucial, as mobile devices present distinct security considerations, such as varied OS configurations, mobile-specific vulnerabilities, and the diverse range of mobile applications. Moreover, mobile pen testing [4] involves different methodologies and tools. While traditional pen testing might leverage network scanning and server vulnerability assessments, mobile pen testing utilizes mobile-specific tools and techniques, such as reverse engineering of apps, analysis of app data storage and transmission, and the testing of mobile APIs.

To illustrate the practical applications of the theoretical concepts discussed in this paper, this article explores into specific case studies centered around the eight comprehensive mobile penetration testing labs dedicated to Android and iOS platforms. These labs represent a tangible bridge between academic knowledge and hands-on application, allowing for a deeper exploration of mobile security's multifaceted challenges. Each lab is meticulously designed to target distinctive yet interconnected aspects of security testing, granting invaluable insights into the platform-specific vulnerabilities and the effective use of open-source tools for penetration testing. By presenting detailed examples of these labs in operation, including the processes undertaken and the results yielded, this article can provide readers with concrete, real-world scenarios. These case studies not only reinforce the foundational theories proposed in the article but also showcase the direct impact of such methodologies in enhancing mobile security measures.

## 2. Mobile Ecosystem Overview

In the context of mobile penetration testing, understanding the mobile ecosystem [5] is vital. This ecosystem is not just diverse but also constantly evolving, encompassing various operating systems, each with its own set of features and security challenges. The two dominant players in this arena are Apple's iOS and Google's Android, though others like Microsoft's Windows for mobile devices also play a role.

### 2.1. Overview of Major Mobile Operating Systems

The landscape of mobile operating systems presents a distinction between Apple's iOS and the Android platform. Understanding the stages [6] of these major mobile operating systems is crucial for effective mobile penetration testing and ensuring robust cybersecurity in an increasingly mobile-centric world. **Table 1** shows the distinction between Apple's iOS [7] and the Android [8] platform.

### 2.2. Unique Security Challenges in the Mobile Ecosystem

The mobile ecosystem [9], due to its varied nature, presents unique challenges for penetration testing. **Table 2** shows the mobile ecosystem's distinctive challenges for penetration testing.

### 2.3. Evolving Threat Landscape

The mobile ecosystem is marked by a constantly shifting threat landscape that demands awareness. Within this landscape [10], new vulnerabilities emerge regularly, affecting both the operating systems and the hardware of mobile devices. These vulnerabilities encompass various aspects, ranging from software bugs to exploitable flaws in processors and even vulnerabilities within communication modules like Bluetooth and Wi-Fi. This persistent evolution of weaknesses in mobile technology poses a significant challenge for security. The latest mobile security threats and trends can be encapsulated by 5G technology, which, while

**Table 1.** Distinction between Apple's iOS and the Android platform.

| Apple iOS | Android |
|---|---|
| • iOS is known for its closed ecosystem, with Apple controlling both hardware and software. This integration creates a consistent and controlled environment.<br>• Vulnerabilities in iOS can have widespread implications due to this closed ecosystem.<br>• iOS devices are prime targets due to their high-value user base. Rigorous security measures are necessary for iOS.<br>• iOS penetration testing primarily addresses app security, data encryption, and defense against jailbreaking exploits. | • Android is characterized by its open-source platform, enabling extensive customization.<br>• This openness brings security variability due to numerous manufacturers and Android version fragmentation.<br>• -Penetration testing in the Android environment frequently tackles challenges related to app permissions, sandboxing, and diverse hardware configurations. |

Table 2. Mobile ecosystem distinctive challenges for penetration testing.

| Mobile Ecosystem | Challenges |
|---|---|
| Diversity of Devices and OS Versions | The numerous devices and OS versions in use complicate the testing process. Each combination can exhibit different vulnerabilities. |
| App Store Security | Both iOS and Android have app stores with different security protocols. Understanding these protocols is essential as they significantly impact app security. |
| Hardware-Related Vulnerabilities | Mobile devices have hardware components like GPS, cameras, and biometric sensors, each introducing unique security considerations. |
| Network Security | Mobile devices frequently switch networks (from cellular to Wi-Fi), raising concerns about the security of data in transit. |
| User Behavior | The way users interact with mobile devices often in a more casual and on-the-go manner can lead to security oversights |

providing faster speeds and reduced latency also brings with it new security challenges. The expansion of the attack surface is one of the primary concerns, as 5G networks create a vast ecosystem of interconnected devices, including IoT sensors and autonomous machinery, in addition to smartphones. This proliferation increases the number of potential entry points for cyber threats, necessitating thorough examination and development of robust mitigation strategies to protect against these emerging vulnerabilities.

The increasing reliance on mobile devices for sensitive transactions [11], including banking, shopping, and various online services, has helped in a new era of convenience and accessibility. Managing finances, making purchases, and accessing confidential information on the go with the tap of a screen is convenient. However, this convenience also comes with significant risks, and cyber criminals are acutely aware of the potential rewards. Mobile devices have become a goldmine of valuable information, and this wealth of data makes them immensely appealing to cybercriminals. As the potential for financial gain from compromising mobile security has never been higher, cybercriminals are actively targeting mobile devices. They employ a variety of tactics, from malware and phishing attacks to social engineering techniques, to exploit vulnerabilities and gain access to sensitive information. Table 3 displays a variety of tactics used to exploit vulnerabilities and gain access to sensitive information.

To counter these threats, mobile security measures, including robust penetration testing, play a critical role in identifying and mitigating vulnerabilities [12]. Businesses and individuals alike must remain vigilant and take proactive steps to protect their mobile devices and the valuable data they contain. As the reliance on mobile devices continues to grow, so too does the importance of ensuring their security in an increasingly digital world. In this context, conducting penetration testing in the mobile ecosystem becomes a complex and dynamic struggle. The diversity of devices [13], operating systems, and constant technological

Table 3. Tactics used to exploit vulnerabilities and gain access.

| Tactics | Description |
|---|---|
| Financial Data | Mobile devices often store financial information, such as bank account details, credit card numbers, and payment apps. Gaining access to this data can yield immediate financial gains for cybercriminals. |
| Personal Information | Mobile devices house a wealth of personal information, including contact lists, emails, and social media accounts. Cybercriminals can exploit this information for identity theft or phishing attacks. |
| Authentication Codes | Many online services use mobile devices as a second-factor authentication method. Compromising a mobile device can allow cybercriminals to intercept authentication codes and gain unauthorized access to accounts. |
| Location Data | Mobile devices constantly track their users' locations. This data can be used for various purposes, including targeting users with location-based scams or tracking their movements. |
| App Vulnerabilities | Mobile apps, which are commonly used for transactions, may have vulnerabilities that cybercriminals can exploit to gain unauthorized access or manipulate transactions. |

advancements necessitate a flexible and comprehensive approach to security testing. To stay effective [14], security testing strategies must adapt and evolve alongside the evolving threat landscape. Timely and regular updates to security measures are essential to keep pace with the ever-changing mobile security challenges. This continuous commitment to mobile security is crucial in safeguarding sensitive data and ensuring the integrity of mobile ecosystems.

## 3. Common Vulnerabilities in Mobile Applications

The growing reliance on mobile applications for both personal and professional use has underscored the need to address their security vulnerabilities. In response to threats and to protect the mobile ecosystem in the real world, robust mobile security measures, including comprehensive penetration testing, are imperative. Businesses and individuals must stay vigilant and proactively secure their mobile devices and the sensitive data they hold. The rapid growth in mobile device reliance necessitates an adaptable and thorough approach to security testing. This involves keeping security testing strategies flexible and up-to-date with the latest technological advancements and threat landscape evolutions. Regularly updating security measures is vital to address the ever-changing mobile security challenges. Such an ongoing commitment to mobile security is essential to protect sensitive information and maintain the integrity of mobile ecosystems. [15] Common vulnerabilities found in mobile applications are often the primary focus in mobile penetration testing.

### 3.1. Insecure Data Storage

One of the most prevalent vulnerabilities in mobile applications [16] is insecure

data storage. Sensitive data such as personal information, authentication credentials, and financial details are often stored improperly on the device. This can result from default settings in the development framework, lack of encryption, or flawed data caching strategies. Attackers can exploit these weaknesses to access confidential information, either by physical access to the device or remotely, if the data is transmitted.

### 3.2. Weak Server-Side Controls

Mobile applications [17] frequently interact with servers, and weak server-side controls can lead to significant security breaches. This includes insufficient authentication and authorization checks, vulnerable servers, and insecure APIs. Since mobile apps often act as a front-end to server-side applications, vulnerabilities on the server side can have far-reaching implications, including data breaches and unauthorized access to system resources.

### 3.3. Insufficient Transport Layer Protection

Transport layer protection [18] is critical in safeguarding data during transit between the mobile app and the server. Insufficient protection, such as the use of weak encryption algorithms or incorrect implementation of secure protocols (like SSL/TLS), can leave data exposed to interception and manipulation. This vulnerability is particularly concerning when dealing with unsecured public Wi-Fi networks, where attackers can more easily intercept data.

### 3.4. Client-Side Injection

Client-side injection attacks [19], such as SQL injection, JavaScript injection, and XML injection, occur when an attacker is able to inject malicious code into the app. This can happen due to the app's failure to properly validate input data. Such vulnerabilities can lead to a range of issues including data theft, corruption, and unauthorized access to the device's functionalities.

### 3.5. Other Common Vulnerabilities

Mobile applications can be susceptible to a range of other security issues that pose significant risks. These additional vulnerabilities [20] present serious threats to mobile application security. When exploited, they can allow attackers to bypass security mechanisms, gain unauthorized access to sensitive data, and compromise user privacy. To safeguard mobile applications effectively, it's essential to address not only the well-known vulnerabilities but also these potential issues through comprehensive security assessments and penetration testing. This proactive approach is critical in ensuring that mobile apps remain resilient in the face of evolving threats. Table 4 provides an overview of these additional vulnerabilities.

## 4. Penetration Testing Methodologies for Mobile Apps

The primary methodologies in mobile penetration testing [21] include static

Table 4. Overview of additional vulnerabilities.

| Vulnerabilities | Description |
|---|---|
| Improper Session Handling | Mobile apps may mishandle user sessions, potentially leaving sensitive data exposed or accessible to unauthorized users. Improper session management can lead to session fixation attacks or session hijacking, where attackers take control of active sessions to impersonate users. |
| Broken Cryptography | Insecure encryption or cryptographic implementations can render data protection ineffective. Weak encryption algorithms or improper key management can allow attackers to decrypt sensitive information, exposing user data. |
| Security Misconfigurations | Misconfigurations in the app's settings or server-side components can create vulnerabilities. Common misconfigurations include overly permissive permissions, open ports, or default credentials left unchanged. Cybercriminals can exploit these oversights to gain unauthorized access. |

and dynamic analysis, along with considerations related to emulators versus real devices.

### 4.1. Static Analysis

Static analysis, also known as static application security testing (SAST) [22], involves examining the application's code without executing it. This method is used to identify vulnerabilities that could lead to security breaches, such as insecure code practices, hardcoded sensitive data, and potential backdoors. Tools used in static analysis scan the entire codebase and provide a report highlighting security weaknesses. This analysis is crucial as it helps in identifying vulnerabilities at an early stage of the development lifecycle.

### 4.2. Dynamic Analysis

Dynamic analysis, or dynamic application security testing (DAST) [23], contrasts with static analysis by testing the application during its execution. This method is effective in uncovering runtime issues that static analysis might miss, such as memory leaks, buffer overflows, and issues with data handling. Dynamic analysis often involves interactive testing and simulation of attacks on the application to observe its behavior and response under different scenarios. Tools for dynamic analysis are designed to mimic real-world hacking techniques and can provide insights into how an application would perform under attack.

### 4.3. Use of Emulators versus Real Devices

In mobile penetration testing, testers [24] often face the decision of whether to use emulators or real devices. Table 5 outlines the distinct advantages and limitations associated with each approach.

For comprehensive penetration testing, a combination of these methodologies

Table 5. Advantages and limitations associated with emulators versus real devices.

| Approach | Description |
|---|---|
| Emulators | Emulators are software tools that mimic the hardware and software of mobile devices. They are useful for early-stage testing as they are cost-effective and allow for rapid deployment and testing. However, emulators cannot perfectly replicate the hardware-level interactions and some specific device behaviors, which can lead to an incomplete assessment. |
| Real Devices | Testing on real devices provides a more accurate representation of how an application behaves in the real world. It allows testers to assess hardware-related vulnerabilities, carrier-network dependencies, and other device-specific issues. The downside is the cost and logistics involved in maintaining a diverse set of devices for comprehensive testing. |

[25] is often employed. Static analysis is useful in the early development stages for a quick assessment of the codebase, while dynamic analysis provides a more realistic evaluation of the application's runtime behavior. Testing on both emulators and real devices [26] offers a balanced approach, ensuring broad coverage of potential vulnerabilities. The methodology chosen for mobile penetration testing depends on various factors including the stage of development, specific objectives of the test, available resources, and the nature of the application. A combination of static and dynamic analysis, supplemented by testing on both emulators and real devices, provides a comprehensive approach to uncover and address vulnerabilities in mobile applications.

## 5. Tools and Technologies in Mobile Penetration Testing

The efficacy of mobile penetration testing [27] largely depends on the tools and technologies employed. A wide array of tools is available, each catering to different aspects of mobile security. The landscape of tools and technologies in mobile penetration testing is rich and varied, offering testers a range of options to suit different testing needs. The choice of tools [28] depends on the specific objectives of the test, the stage of the application's development, and the platform it is built for. Understanding and effectively utilizing these tools is key to conducting thorough and successful mobile penetration tests.

### 5.1. Proxy Tools

Proxy tools [29] are essential in mobile penetration testing for intercepting and analyzing traffic between the mobile application and the backend server. Table 6 highlights two widely used proxy tools.

### 5.2. Automated Scanners

Automated scanners [30] simplify the process of identifying vulnerabilities in mobile applications. They scan the app's code or runtime environment and report potential security issues. Table 7 highlights notable automated scanners.

### 5.3. Platform-Specific Tools

Different tools are tailored for iOS and Android platforms [31], considering their unique architectures and security models. Table 8 displays iOS and

Table 6. Widely used proxy tools.

| Proxy tool | Description |
|---|---|
| Burp Suite | Burp Suite is a comprehensive solution for web application security. Its proxy tool feature is particularly effective in inspecting and modifying traffic coming from mobile apps. It allows testers to identify vulnerabilities like insecure API calls and data transmission flaws. |
| OWASP ZAP (Zed Attack Proxy | OWASP ZAP is an open-source tool used for finding vulnerabilities in web applications. In the context of mobile apps, ZAP can be used to analyze traffic and test for security weaknesses in the communication with the server. |

Table 7. Automated scanner tools.

| Automated scanner | Description |
|---|---|
| MobSF (Mobile Security Framework) | MobSF is an automated security testing framework for Android, iOS, and Windows platforms. It performs static and dynamic analysis along with web API testing, offering a comprehensive security audit of mobile applications |
| QARK (Quick Android Review Kit) | Specifically designed for Android applications, QARK identifies security vulnerabilities in Android app packages (APKs) and source code. It helps in pinpointing issues like insecure network communications and potential Android-specific vulnerabilities. |

Table 8. iOS and Android tools architectures and security models.

| iOS | Android |
|---|---|
| **iNalyzer**<br>A comprehensive tool for assessing iOS applications, iNalyzer provides a graphical interface for static analysis, highlighting potential security weaknesses in the app's code. | **Drozer**<br>Drozer is a tool for assessing the security of Android apps. It allows testers to interact with the app's components, such as activities, services, and content providers, to identify security gaps. |
| **Frida**<br>Frida is a dynamic instrumentation toolkit used for injecting scripts into iOS apps. It is effective for testing runtime behavior and detecting vulnerabilities like insecure function calls. | **Apktool**<br>Apktool is used for reverse engineering Android applications. It allows testers to decode app resources to understand their functioning and potential vulnerabilities. |
| **Xcode**<br>Xcode is an integrated development environment (IDE) specifically designed for iOS, macOS, watchOS, and tvOS app development. It serves as the primary tool for iOS app development and offers a wide range of features and functionalities. | **ADB (Android Debug Bridge)**<br>ADB is a versatile command-line tool used for various purposes in Android development, testing, and debugging. |

Android tools based on their distinct architectures and security models.

## 6. Mobile Penetration Testing Labs

While the field of cybersecurity has seen significant advancements, a noticeable gap still exists between theoretical knowledge and practical application. Establishing a penetration testing lab [32] involves several crucial steps, including tool installation, configuring the testing environment, and conducting assessments. Within this framework, this article provides a total of eight comprehensive labs dedicated to Android and iOS platforms, each exploring into distinct yet interconnected features of security testing. The subsequent sections introduce Android and iOS penetration testing [32], encompassing fundamental platform insights [33], essential open-source tools [34], and lab setup procedures [35]. **Table 9** provides the eight pen testing labs for Android and iOS platforms.

### 6.1. Android Penetration Testing Labs: Objectives, Structures and Expected Outcomes

**Lab 1: Android Application Static Analysis**

The objective of this lab is to provide participants with the knowledge and hands-on experience to perform static analysis on an Android application. Through this lab, participants will learn to identify potential vulnerabilities and security issues within Android applications [36] and gain the skills to document their findings and propose mitigation strategies. **Figure 1** illustrates the lab 1 structures and expected outcomes.

**Lab 2: Android Application Dynamic Analysis**

The objective of this lab is to conduct dynamic analysis on Android applications. The primary objective is to uncover runtime vulnerabilities and security weaknesses [37], enabling participants to analyze network communication and runtime behavior. **Figure 2** illustrates the lab 2 structures and expected outcomes.

**Lab 3: Android Device Exploitation**

The objective of this lab is to explore common Android device exploitation

**Table 9.** Pen testing labs for Android and iOS platforms.

| Android | iOS |
|---|---|
| **Lab 1**<br>Android Application Static Analysis | **Lab 1**<br>iOS Application Static Analysis |
| **Lab 2**<br>Android Application Dynamic Analysis | **Lab 2**<br>iOS Application Reverse Engineering |
| **Lab 3**<br>Android Device Exploitation | **Lab 3**<br>Network Traffic Analysis and MITM Attacks |
| **Lab 4**<br>Android Reverse Engineering and Malware Analysis | **Lab 4**<br>iOS Application Dynamic Analysis with Frida |

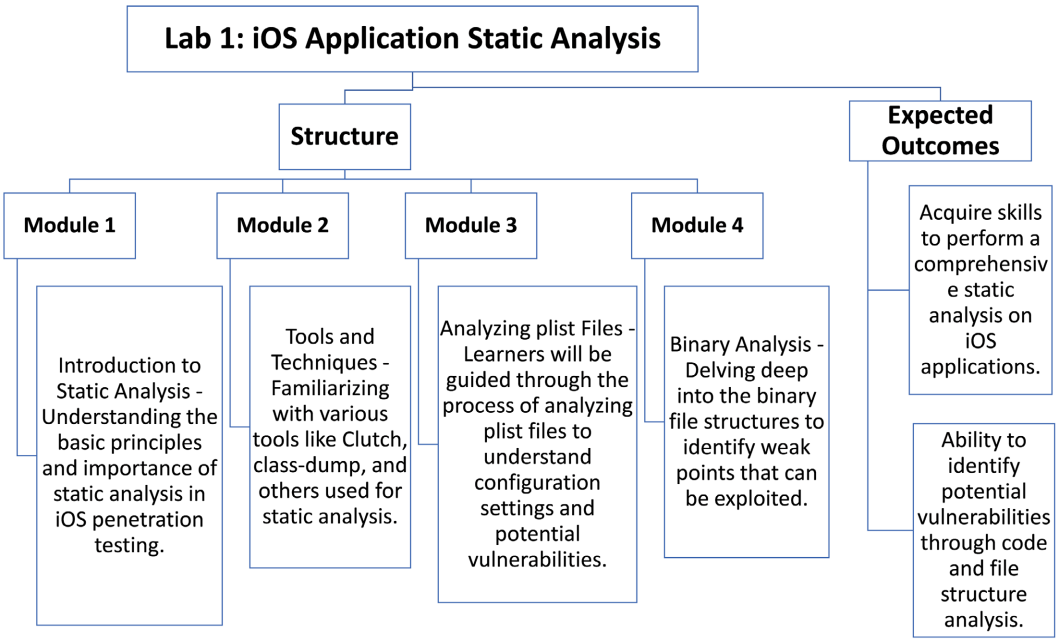


**Figure 1.** Lab 1 structures and expected outcomes.

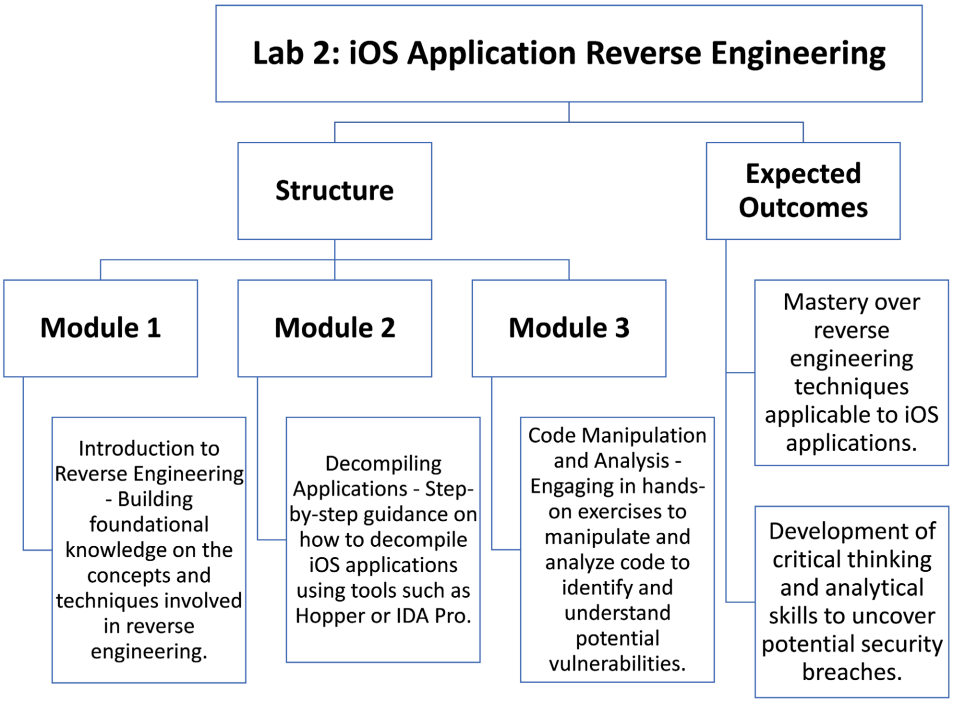


**Figure 2.** Lab 2 structures and expected outcomes.

techniques. The primary objective is to understand the impact of vulnerabilities on Android devices [38] and gain insights into the potential consequences of successful exploitation. **Figure 3** illustrates the lab 3 structures and expected outcomes.

**Lab 4: Android Reverse Engineering and Malware Analysis**

The objective of this lab is to provide the knowledge required to reverse engi-

neer and analyze potentially malicious Android applications. The primary objective is to understand [39] the behavior of suspicious apps, identify indicators of compromise, and assess their impact on Android security. Figure 4 illustrates the lab 4 structures and expected outcomes.

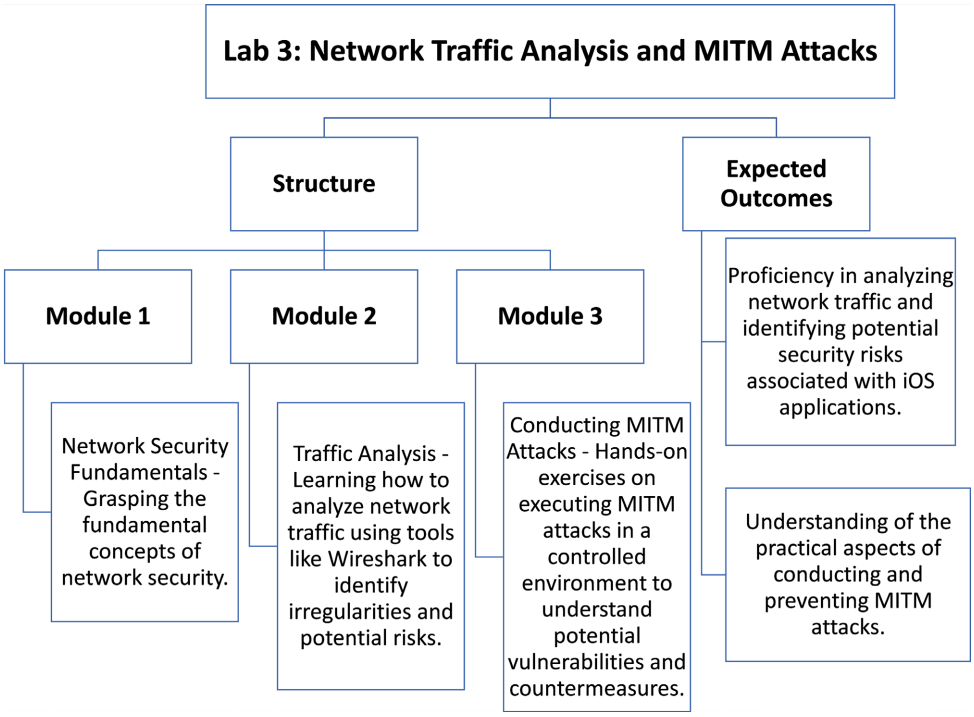


Figure 3. Lab 3 structures and expected outcomes.

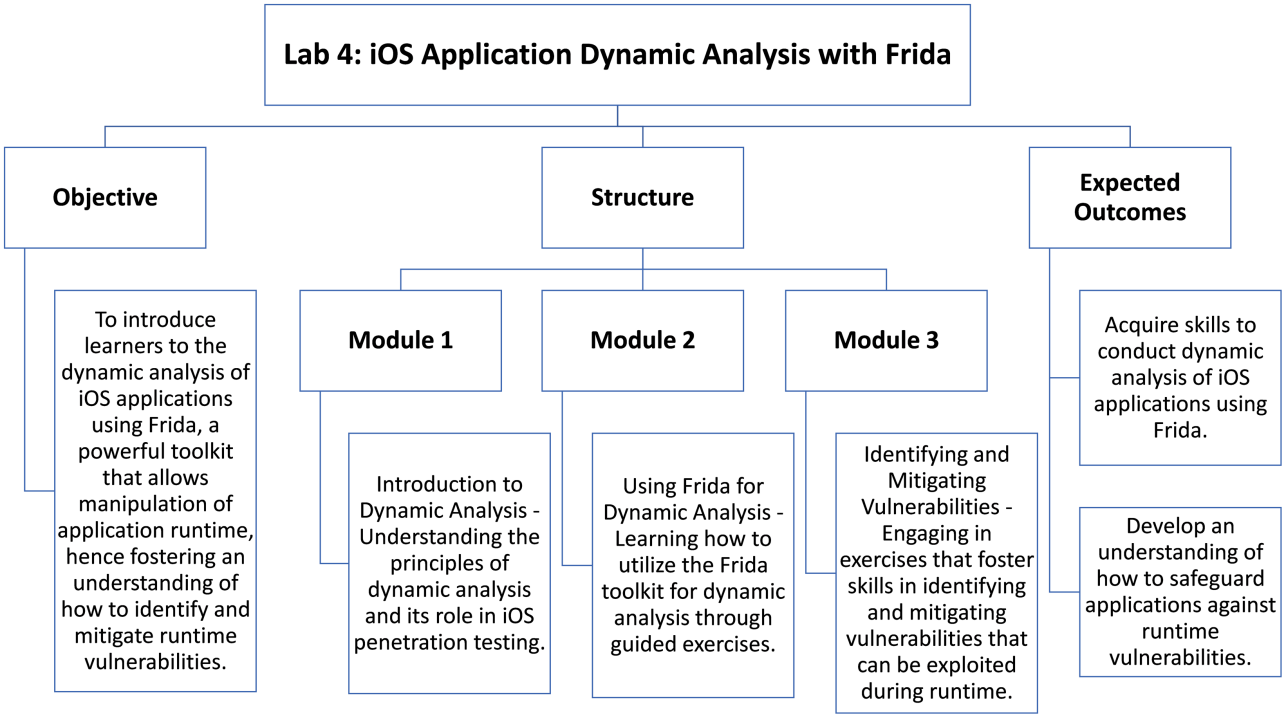


Figure 4. Lab 4 structures and expected outcomes

### 6.2. iOS Penetration Testing Labs: Objectives, Structures and Expected Outcomes

**Lab 1: iOS Application Static Analysis**

The objective of this lab is to provide learners with a foundational understanding of static analysis and its importance in iOS penetration testing. This lab will help learners develop skills to analyze the structure and components of iOS applications [40] without executing them. Figure 5 illustrates the lab 1 structures and expected outcomes.

**Lab 2: iOS Application Reverse Engineering**

The objective of this lab is to immerse learners into the complex yet fascinating world of reverse engineering where they will acquire skills to decompile and manipulate iOS application [41] code, uncovering underlying vulnerabilities and potential security breaches. Figure 6 illustrates the lab 2 structures and expected outcomes.

**Lab 3: iOS Network Traffic Analysis and MITM Attacks**

The objective of this lab is to foster an understanding of network security concepts within the context of iOS applications, enabling learners to analyze network traffic and conduct MITM attacks ethically [42] to uncover security risks and data leaks. Figure 7 illustrates the lab 3 structures and expected outcomes.

**Lab 4: iOS Application Dynamic Analysis with Frida**

The objective of this lab is to introduce learners to the dynamic analysis of iOS applications using Frida [43], a powerful toolkit that allows manipulation of application runtime, hence fostering an understanding of how to identify and mitigate runtime vulnerabilities. Figure 8 illustrates the lab 4 structures and

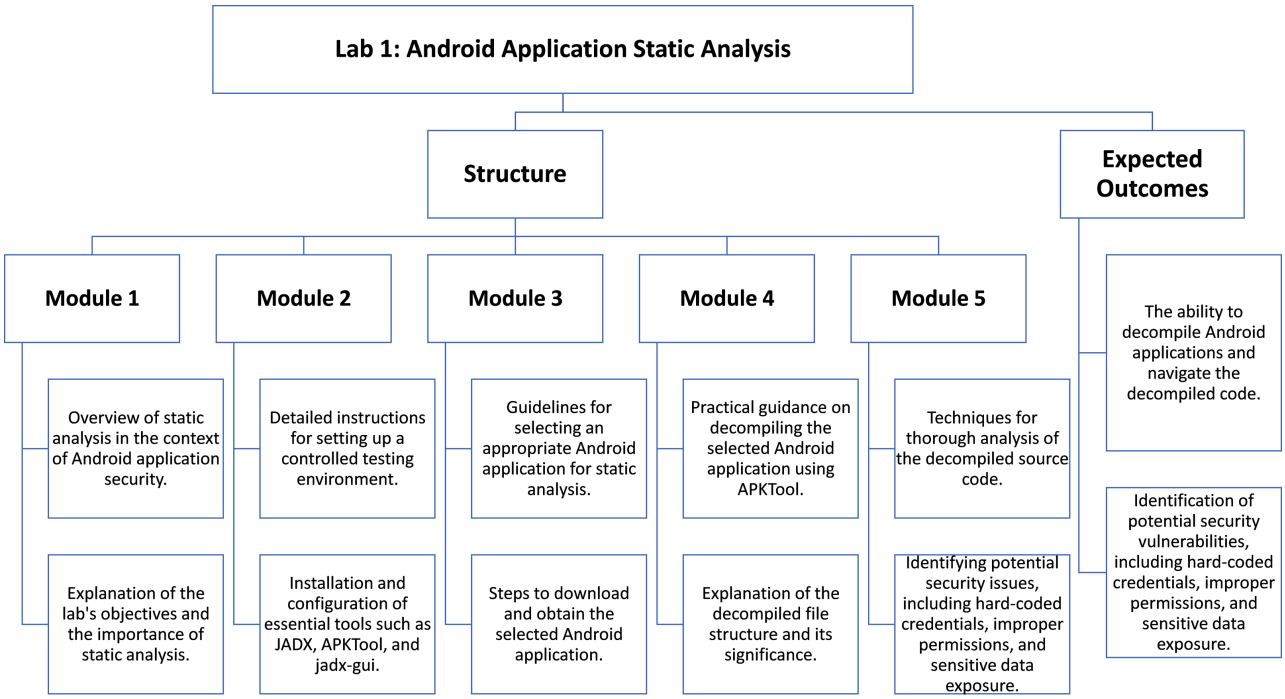


Figure 5. Lab 1structures and expected outcomes.

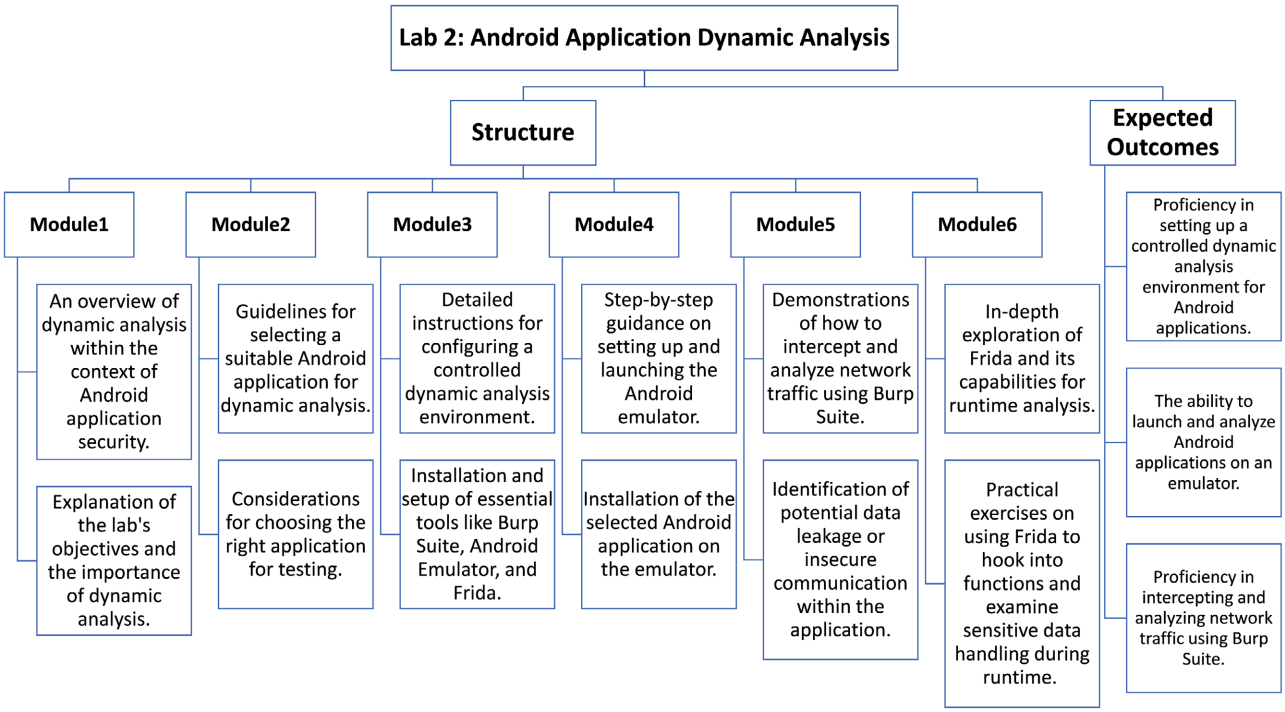


**Figure 6.** Lab 2 structures and expected outcomes.

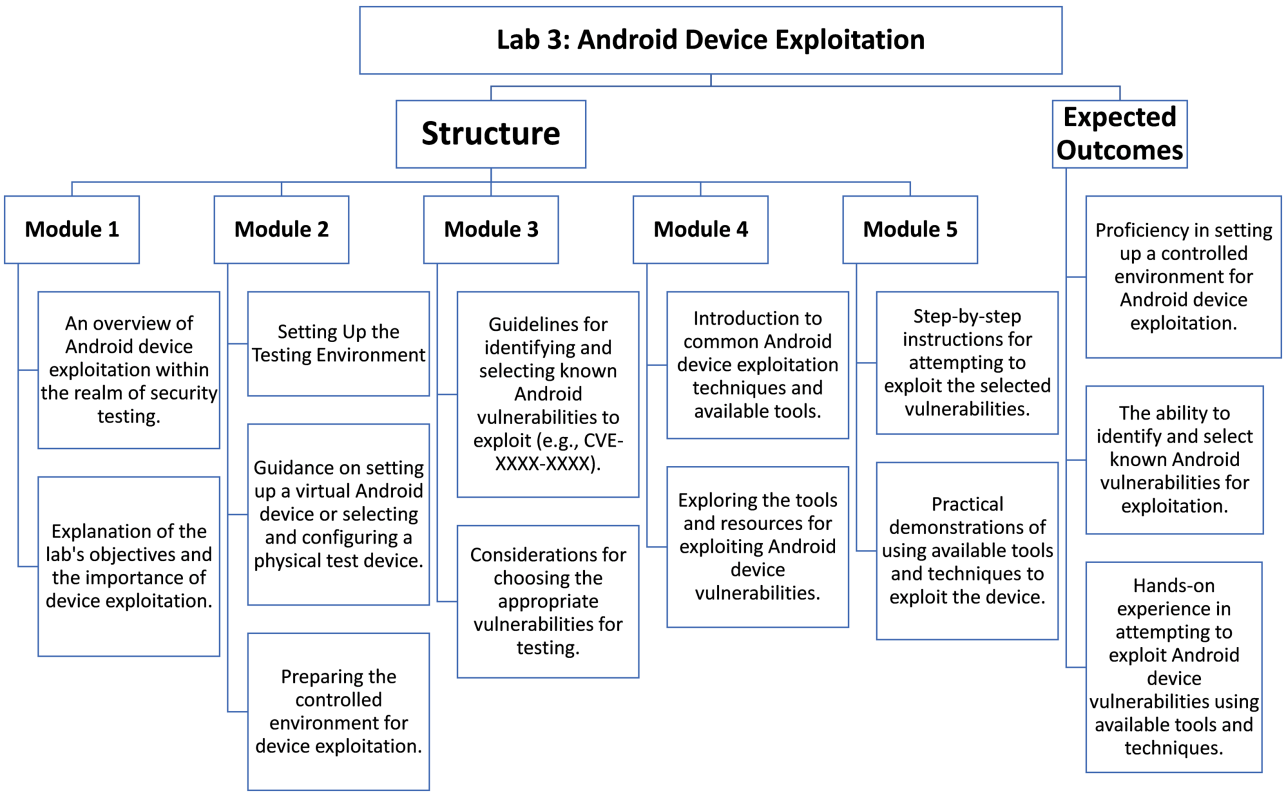


**Figure 7.** Lab 3 structures and expected outcomes.

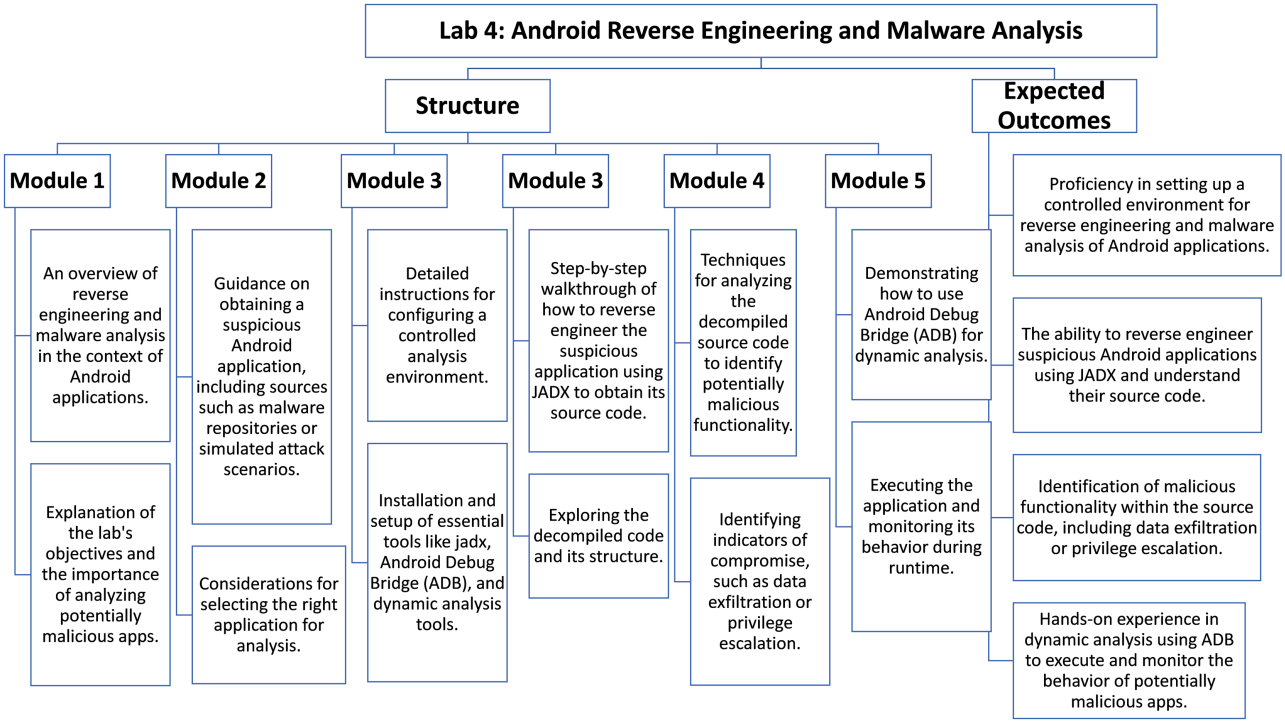


**Figure 8.** Lab 4 structures and expected outcomes.

expected outcomes.

## 7. Legal and Ethical Considerations in Mobile Penetration Testing

While the technical aspects of mobile penetration testing are critical for ensuring security, equally important are the legal and ethical considerations. The legal and ethical considerations [44] are fundamental to responsible mobile penetration testing. Obtaining proper authorization, respecting privacy and data integrity, complying with relevant laws, and practicing responsible disclosure are all critical components of a lawful and ethical penetration testing process. Following these principles not only protects the tester legally but also upholds the integrity and trustworthiness of the penetration testing profession.

The foremost legal consideration in penetration testing is obtaining proper authorization. Testing without explicit permission can be considered illegal and lead to severe legal consequences, including criminal charges. Authorization [45] should be in writing and clearly define the scope of the testing, including the systems to be tested, the methods to be used, and any limitations or constraints. Table 10 highlights the importance of obtaining proper Authorization.

### 7.2. Ethical Considerations

Ethical considerations [46] in penetration testing center on preserving privacy, maintaining data integrity, and assessing the broader impact of testing on both the system and its users. Table 11 presents a detailed breakdown of these ethical

considerations in the context of penetration testing.

### 7.3. Legal Compliance

Penetration testers [47] must also be aware of and comply with relevant laws and regulations, which can vary by region and industry. This includes laws related to data protection, cybercrime, and privacy. Table 12 summarizes key data protection acts in the USA [48] and EU [49], along with relevant cybercrime laws [49].

In the event that vulnerabilities are discovered, responsible disclosure is an ethical imperative. This involves notifying the organization about the vulnerabilities in a confidential manner and giving them sufficient time to address the issues before any public disclosure.

Table 10. Importance of obtaining proper authorization.

| Authorization | Description |
|---|---|
| Written Consent | Written consent should be obtained from the organization or individual who owns the system or application being tested. This consent protects the penetration tester and ensures that all parties are aware of the testing activities. |
| Scope of Authorization | The authorization should explicitly state the extent and limitations of the testing. It should detail what is permitted, such as the types of attacks, the time frame for testing, and any specific areas that are off-limits. |

Table 11. Ethical Considerations in penetration testing.

| Ethical Consideration | Description |
|---|---|
| **Privacy** | Testers should respect the privacy of the organization and its users. Any sensitive data encountered during testing must be handled confidentially and securely. |
| **Data Integrity** | Ensuring data integrity is crucial. Testers should avoid any actions that could potentially damage the system or lead to data loss. Any changes made to the system should be reversible. |
| **Non-Disclosure Agreements (NDAs)** | Testers often sign NDAs to protect the confidentiality of the information they access during testing. This agreement ensures that sensitive information about the system's vulnerabilities is not disclosed to unauthorized parties. |

Table 12. Legal Compliance in pen testing.

| Act | Descriptions |
|---|---|
| Data Protection Laws | Compliance with data protection laws such as GDPR (General Data Protection Regulation) in Europe or HIPAA (Health Insurance Portability and Accountability Act) in the United States is essential when handling personal data during testing. |
| Cybercrime Laws | Awareness of cybercrime laws is crucial to ensure that the testing activities are not misinterpreted as malicious attacks. |

## 8. Future Trends in Mobile Security

The deployment of 5G technology [50] marks a significant milestone in the realm of mobile communications, promising faster speeds and reduced latency. However, this technological advancement comes hand in hand with an array of fresh security challenges that require meticulous examination and mitigation strategies.

One of the foremost challenges posed by 5G [51] is the substantial expansion of the attack surface. With the advent of 5G networks, an extensive ecosystem of connected devices emerges, encompassing not only smartphones but also a multitude of IoT sensors, autonomous machinery, and more. The proliferation of these endpoints multiplies the potential entry points for cyber threats exponentially. Consequently, penetration testers must undertake a holistic approach, scrutinizing the entire spectrum of connected devices and the integrity of the underlying network infrastructure to identify vulnerabilities effectively.

The introduction of network slicing [52], a prominent feature of 5G, adds another layer of complexity to security testing. Network slicing involves the creation of multiple virtual networks within a single physical network infrastructure. Each network slice [53] may cater to specific applications or services with distinct security requirements. This dynamic environment complicates the testing process, demanding tailored assessments for each network slice to ensure the isolation and security of each segment. Furthermore, 5G's support for edge computing [54] introduces a paradigm shift in data processing. Data is now processed closer to its source, reducing latency and enhancing real-time capabilities. However, this architectural change also raises novel security concerns, as securing these edge nodes and safeguarding the data they handle becomes paramount. Ensuring data integrity, confidentiality, and resilience against potential attacks are critical aspects of mobile penetration testing in the 5G era [55].

Moving beyond 5G, the increasing utilization of biometric [56] security measures, such as fingerprint and facial recognition, in mobile devices brings its own set of challenges. While these methods offer convenience, they introduce the need for robust security measures to safeguard biometric data against unauthorized access and misuse. This necessitates comprehensive evaluations of how this sensitive data is securely stored, processed, and transmitted. Additionally, the risk of spoofing attacks, where attackers mimic biometric traits to gain unauthorized access, requires focused testing for vulnerabilities. Ensuring the accuracy and reliability of biometric authentication methods becomes a key objective in mobile penetration testing.

The integration of artificial intelligence (AI) and machine learning (ML) into mobile security solutions [57] for threat detection and response is on the rise. Penetration testers must acquaint themselves with these technologies to effectively assess their effectiveness and pinpoint potential vulnerabilities. AI-driven security systems exhibit adaptability to new threats at an unprecedented pace, necessitating the development of effective testing strategies to assess these adap-

tive systems thoroughly. On the flip side, the rise of AI also equips attackers [58] with the capability to employ these technologies for more sophisticated attack methods. Thus, mobile penetration testers must employ advanced testing methodologies to stay ahead of evolving threats. Moreover, the integration of IoT devices with mobile technology adds another layer of complexity to security assessments. Mobile apps that control IoT devices can serve as vectors for attacks if not adequately secured. This necessitates an expansion of the penetration tester's focus to include the security of IoT devices and their interactions with mobile apps. The interconnected nature of mobile devices and IoT gadgets means that vulnerabilities in one domain can potentially impact the other, underlining the need for a comprehensive testing approach.

In response to heightened concerns [59] about user privacy, mobile applications are increasingly incorporating privacy-enhancing technologies such as zero-knowledge proofs and secure multi-party computation. Understanding and effectively testing these privacy-enhancing technologies represent uncharted territories for mobile penetration testers. This emerging field demands a thorough understanding of how these technologies preserve user privacy while upholding the functionality and security of mobile apps in an ever-evolving digital landscape. The evolving landscape of mobile technology presents an ever-expanding set of security challenges for penetration testers. From the complexities of 5G to biometric security, AI integration, IoT integration, and privacy-enhancing technologies, testers must adapt their methodologies, strategies, and skillsets to ensure the security and resilience of mobile ecosystems against an ever-evolving threat landscape.

The future of mobile penetration testing [60] is expected to be shaped by a number of emerging trends. Rapid technological advancements and the evolution of cyber threats necessitate a forward-thinking approach to security testing. In the evolving landscape of mobile penetration testing, several key trends are anticipated to define the future of the field. One significant trend is the increased use of artificial intelligence and machine learning algorithms, which are expected to automate many aspects of penetration testing. This automation could lead to more efficient vulnerability assessments and the capability for continuous, large-scale testing. Another area of expansion is in the testing of Internet of Things (IoT) devices. As the IoT continues to grow, the attack surface widens correspondingly. Penetration testing will need to evolve to cover a broader range of IoT devices, addressing their complexity and diversity to ensure comprehensive security. The deployment of 5G networks introduces new protocols and network configurations, requiring penetration testing to adapt accordingly. This includes addressing the security concerns associated with ultra-dense networks and the edge computing paradigm. As mobile services become increasingly reliant on cloud computing, penetration testing must also shift focus to the security of cloud-based mobile services. This includes ensuring the security of data storage and processing within the cloud. The rise in the use of biometric authen-

tication on mobile devices brings the need for advanced biometric security testing. Penetration testers will need to develop new methods to test these systems against spoofing and evasion techniques. An enhanced focus on supply chain security is also anticipated. Penetration testing will likely expand to assess the security of third-party services and libraries that are integral to mobile ecosystems, addressing supply chain risks. Lastly, the development of mobile threat intelligence capabilities will become crucial. These capabilities will play a significant role in identifying and understanding emerging threats, thereby aiding penetration testers in anticipating and preparing for new attack vectors.

## 9. Conclusion

The importance of mobile penetration testing cannot be understated. In an era where mobile devices play an integral role in daily lives, securing these devices and their applications is of utmost importance. Mobile penetration testing serves as a critical defense against the ever-growing sophistication of cyber threats. By identifying and mitigating vulnerabilities before they can be exploited by malicious actors, mobile penetration testers fulfill an indispensable role in the cybersecurity ecosystem. Their work not only protects sensitive data and user privacy but also upholds the integrity and trustworthiness of mobile technology. As mobile technology continues to evolve and integrate more deeply into personal and professional lives, the field of mobile penetration testing must evolve in tandem. Importantly, the relevance of mobile penetration testing isn't confined to the present moment. Mobile technology is on an inexorable trajectory of innovation and integration into various aspects of our daily lives. This evolution introduces exciting opportunities and, simultaneously, new challenges. Technologies like 5G, biometrics, artificial intelligence, and the Internet of Things (IoT) are at the forefront of these developments. Staying ahead of emerging threats, adapting to new technologies, and adhering to legal and ethical standards are essential for maintaining the security and resilience of the mobile world. The future of mobile security relies on the dedication, expertise, and innovation within the mobile penetration testing community.

## Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

## References

[1] Alhamed, M. and Rahman, M.H. (2023) A Systematic Literature Review on Penetration Testing in Networks: Future Research Directions. *Applied Sciences*, **13**, Article 6986. https://doi.org/10.3390/app13126986

[2] Falade, P.V. and Ogundele, G.B. (2023) Vulnerability Analysis of Digital Banks' Mobile Applications. arXiv: 2302.07586.

[3] Parveen, M. and Shaik, M.A. (2023) Review on Penetration Testing Techniques in Cyber Security. 2023 *Second International Conference on Augmented Intelligence*

*and Sustainable Systems* (*ICAISS*), Trichy, 23-25 August 2023, 1265-1270. https://doi.org/10.1109/ICAISS58487.2023.10250659

[4] Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2022) Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, **62**, 82-97. https://doi.org/10.1080/08874417.2020.1712269

[5] Zhang, K., Wang, J., Xin, X., Li, X., Sun, C., Huang, J. and Kong, W. (2022) A Survey on Learning-Based Model Predictive Control: Toward Path Tracking Control of Mobile Platforms. *Applied Sciences*, **12**, Article 1995. https://doi.org/10.3390/app12041995

[6] Eshnazarova, M.Y. and Katayeva, M.M. (2021) Theoretical Basis of Mobile Learning and Use of Mobile Platforms. *International Journal on Integrated Education*, **4**, 184-187.

[7] Kollnig, K., Shuba, A., Binns, R., Van Kleek, M. and Shadbolt, N. (2022) Are iPhones Really Better for Privacy? A Comparative Study of IOS and Android Apps. *Proceedings on Privacy Enhancing Technologies*, **2022**, 6-24. https://doi.org/10.2478/popets-2022-0033

[8] Tewari, A. and Singh, P. (2021) Android App Development: A Review. *Journal of Management and Service Science*, **1**, 1-6. https://doi.org/10.54060/JMSS/001.02.006

[9] Mustapha, I., Vaicondam, Y., Jahanzeb, A., Usmanovich, B.A. and Yusof, S.H.B. (2023) Cybersecurity Challenges and Solutions in the Fintech Mobile App Ecosystem. *International Journal of Interactive Mobile Technologies*, **17**, 100-116. https://doi.org/10.3991/ijim.v17i22.45261

[10] Sarieddine, K., Sayed, M.A., Torabi, S., Atallah, R. and Assi, C. (2023) Investigating the Security of EV Charging Mobile Applications as an Attack Surface. *ACM Transactions on Cyber-Physical Systems*, **7**, 1-28. https://doi.org/10.1145/3609508

[11] Zhou, K.Q. (2022) Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security. *Mesopotamian Journal of CyberSecurity*, **2022**, 57-64. https://doi.org/10.58496/MJCS/2022/007

[12] Garg, S. and Baliyan, N. (2023) Mobile OS Vulnerabilities: Quantitative and Qualitative Analysis. CRC Press, Boca Raton. https://doi.org/10.1201/9781003354574

[13] Wong, A.Y., Chekole, E.G., Ochoa, M. and Zhou, J. (2023) On the Security of Containers: Threat Modeling, Attack Analysis, and Mitigation Strategies. *Computers & Security*, **128**, Article ID: 103140. https://doi.org/10.1016/j.cose.2023.103140

[14] Pour, M.S., Nader, C., Friday, K. and Bou-Harb, E. (2023) A Comprehensive Survey of Recent Internet Measurement Techniques for Cyber Security. *Computers & Security*, **128**, Article ID: 103123. https://doi.org/10.1016/j.cose.2023.103123

[15] Senanayake, J., Kalutarage, H., Al-Kadri, M.O., Petrovski, A. and Piras, L. (2023) Android Source Code Vulnerability Detection: A Systematic Literature Review. *ACM Computing Surveys*, **55**, 1-37. https://doi.org/10.1145/3556974

[16] Cinar, A.C. and Kara, T.B. (2023) The Current State and Future of Mobile Security in the Light of the Recent Mobile Security Threat Reports. *Multimedia Tools and Applications*, **82**, 20269-20281. https://doi.org/10.1007/s11042-023-14400-6

[17] Haris, N., Chen, K., Song, A. and Pou, B. (2023) Finding Vulnerabilities in Mobile Application APIs: A Modular Programmatic Approach. arXiv: 2310.14137.

[18] Chimuco, F.T., Sequeiros, J.B., Lopes, C.G., Simões, T.M., Freire, M.M. and Inácio,

P.R. (2023) Secure Cloud-Based Mobile Apps: Attack Taxonomy, Requirements, Mechanisms, Tests and Automation. *International Journal of Information Security*, **22**, 833-867. https://doi.org/10.1007/s10207-023-00669-z

[19] Zhang, X., Ye, H., Huang, Z., Ye, X., Cao, Y., Zhang, Y. and Yang, M. (2023) Understanding the (In) Security of Cross-Side Face Verification Systems in Mobile Apps: A System Perspective. 2023 *IEEE Symposium on Security and Privacy* (*SP*), San Francisco, 21-25 May 2023, 934-950. https://doi.org/10.1109/SP46215.2023.10179474

[20] Acharya, S., Rawat, U. and Bhatnagar, R. (2022) A Comprehensive Review of Android Security: Threats, Vulnerabilities, Malware Detection, and Analysis. *Security and Communication Networks*.

[21] Heiding, F., Süren, E., Olegård, J. and Lagerström, R. (2023) Penetration Testing of Connected Households. *Computers & Security*, **126**, Article ID: 103067. https://doi.org/10.1016/j.cose.2022.103067

[22] Molina-Coronado, B., Mori, U., Mendiburu, A. and Miguel-Alonso, J. (2023) Towards a Fair Comparison and Realistic Evaluation Framework of Android Malware Detectors Based on Static Analysis and Machine Learning. *Computers & Security*, **124**, Article ID: 102996. https://doi.org/10.1016/j.cose.2022.102996

[23] Nie, L., Said, K.S., Ma, L., Zheng, Y. and Zhao, Y. (2023) A Systematic Mapping Study for Graphical User Interface Testing on Mobile Apps. *IET Software*, **17**, 249-267. https://doi.org/10.1049/sfw2.12123

[24] Gomez, J., Kfoury, E.F., Crichigno, J. and Srivastava, G. (2023) A Survey on Network Simulators, Emulators, and Testbeds Used for Research and Education. *Computer Networks*, **237**, Article ID: 110054. https://doi.org/10.1016/j.comnet.2023.110054

[25] Kamal, K.K., Joshi, P., Bang, A. and Bhatia, K. (2023) Effective Security Testing of Mobile Applications for Building Trust in the Digital World. 2023 7*th International Conference on Trends in Electronics and Informatics* (*ICOEI*), 11-13 April 2023, Tirunelveli, 550-556.

[26] Wang, J., Hu, P., Zhang, Y. and Wang, J. (2022) A Comparison of Discrete Event Simulator and Real-Time Emulator for Mobile Ad Hoc Network. In: Jiang, X., ed., *MLICOM* 2022: *Machine Learning and Intelligent Communication*, Springer, Cham, 63-74. https://doi.org/10.1007/978-3-031-30237-4_6

[27] Yamin, M.M., Katt, B. and Gkioulos, V. (2020) Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*, **88**, Article ID: 101636. https://doi.org/10.1016/j.cose.2019.101636

[28] Putra, R.S., Aulia, M.F., Maulana, S.A. and Jusia, P.A. (2024) Android Security: Malware Detection with Convolutional Neural Network and Feature Analysis. *Media Journal of General Computer Science*, **1**, 7-13. https://doi.org/10.62205/mjgcs.v1i1.7

[29] Vats, P., Mandot, M. and Gosain, A. (2020) A Comprehensive Literature Review of Penetration Testing & Its Applications. 2020 8*th International Conference on Reliability*, *Infocom Technologies and Optimization* (*Trends and Future Directions*) (*ICRITO*), Noida, 4-5 June 2020, 674-680. https://doi.org/10.1109/ICRITO48877.2020.9197961

[30] Fatima, A., Khan, T.A., Abdellatif, T.M., Zulfiqar, S., Asif, M., Safi, W., Al Hamadi, H. and Al-Kassem, A.H. (2023) Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat. 2023 *International Conference on Business Analytics for Technology and Security* (*ICBATS*), Dubai, 7-8

March 2023, 1-8. https://doi.org/10.1109/ICBATS57792.2023.10111168

[31] Haq, I.U. and Khan, T.A. (2021) Penetration Frameworks and Development Issues in Secure Mobile Application Development: A Systematic Literature Review. *IEEE Access*, **9**, 87806-87825. https://doi.org/10.1109/ACCESS.2021.3088229

[32] Oconnor, T.J. and Stricklan, C. (2021) Teaching a Hands-On Mobile and Wireless Cybersecurity Course. *Proceedings of the* 26*th ACM Conference on Innovation and Technology in Computer Science Education*, 26 June-1 July 2021, 296-302. https://doi.org/10.1145/3430665.3456346

[33] Singh, G.D. (2022) The Ultimate Kali Linux Book: Perform Advanced Penetration Testing Using Nmap, Metasploit, Aircrack-ng, and Empire. Packt Publishing Ltd, Birmingham.

[34] Ravindran, U. and Potukuchi, R.V. (2022) A Review on Web Application Vulnerability Assessment and Penetration Testing. *Review of Computer Engineering Studies*, **9**, 1-22. https://doi.org/10.18280/rces.090101

[35] James, P., Powell, L., O'reilly, L. and Moller, F. (2020) Hands-On Security Testing in a University Lab Environment. *Proceedings of the* 2020 *ACM Conference on Innovation and Technology in Computer Science Education*, 68-74. https://doi.org/10.1145/3341525.3387366

[36] Bayazit, E.C., Sahingoz, O.K. and Dogan, B. (2022) A Deep Learning Based Android Malware Detection System with Static Analysis. 2022 *International Congress on Human-Computer Interaction, Optimization and Robotic Applications* (*HORA*), Ankara, 9-11 June 2022, 1-6. https://doi.org/10.1109/HORA55278.2022.9800057

[37] Tossou, S. and Kacem, T. (2023) Mobile Threat Detection System: A Deep Learning Approach. 2023 13*th International Conference on Information Science and Technology* (*ICIST*), Cairo, 8-14 December 2023, 323-332. https://doi.org/10.1109/ICIST59754.2023.10367120

[38] Blancaflor, E., Billo, H.K.S., Saunar, B.Y.P., Dignadice, J.M.P. and Domondon, P.T. (2023) Penetration Assessment and Ways to Combat Attack on Android Devices through StormBreaker—A Social Engineering Tool. 2023 6*th International Conference on Information and Computer Technologies* (*ICICT*), Raleigh, 24-26 March 2023, 220-225. https://doi.org/10.1109/ICICT58900.2023.00043

[39] Gyunka, B.A., Oladele, A.T. and Adegoke, O. (2023) Adaptive Android APKs Reverse Engineering for Features Processing in Machine Learning Malware Detection. *International Journal of Data Science*, **4**, 10-25. https://doi.org/10.18517/ijods.4.1.10-25.2023

[40] Shimmi, S.S., Dorai, G., Karabiyik, U. and Aggarwal, S. (2020) Analysis of iOS SQLite Schema Evolution for Updating Forensic Data Extraction Tools. 2020 8*th International Symposium on Digital Forensics and Security* (*ISDFS*), Beirut, 1-2 June 2020, 1-7. https://doi.org/10.1109/ISDFS49300.2020.9116208

[41] Asher, S.W., Jan, S., Tsaramirsis, G., Khan, F.Q., Khalil, A. and Obaidullah, M. (2021) Reverse Engineering of Mobile Banking Applications. *Computer Systems Science and Engineering*, **38**, 265-278. https://doi.org/10.32604/csse.2021.016787

[42] Afzal, A., Hussain, M., Saleem, S., Shahzad, M.K., Ho, A.T. and Jung, K.H. (2021) Encrypted Network Traffic Analysis of Secure Instant Messaging Application: A Case Study of Signal Messenger App. *Applied Sciences*, **11**, Article 7789. https://doi.org/10.3390/app11177789

[43] Soriano-Salvador, E. and Guardiola-Múzquiz, G. (2023) Detecting and Bypassing Frida Dynamic Function Call Tracing: Exploitation and Mitigation. *Journal of Computer Virology and Hacking Techniques*, **19**, 503-513.

https://doi.org/10.1007/s11416-022-00458-7

[44] Gogolin, G. (2021) Digital Forensics Explained. CRC Press, Boca Raton. https://doi.org/10.1201/9781003049357

[45] Omolara, A.E., Alabdulatif, A., Abiodun, O.I., Alawida, M., Alabdulatif, A. and Arshad, H. (2022) The Internet of Things Security: A Survey Encompassing Unexplored Areas and New Insights. *Computers & Security*, **112**, Article ID: 102494. https://doi.org/10.1016/j.cose.2021.102494

[46] Schmeelk, S.E. and Dragos, D.M. (2023) Penetration Testing and Ethical Hacking: Risk Assessments and Student Learning. 2023 *IEEE Frontiers in Education Conference* (*FIE*), College Station, 18-21 October 2023, 1-6. https://doi.org/10.1109/FIE58773.2023.10342914

[47] Ke, T.T. and Sudhir, K. (2023) Privacy Rights and Data Security: GDPR and Personal Data Markets. *Management Science*, **69**, 4389-4412. https://doi.org/10.1287/mnsc.2022.4614

[48] Bharti, S.S. and Aryal, S.K. (2023) The Right to Privacy and an Implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the Companies. *Journal of Contemporary European Studies*, **31**, 1391-1402. https://doi.org/10.1080/14782804.2022.2130193

[49] Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q. and Gao, C. (2023) Exploring the Global Geography of Cybercrime and Its Driving Forces. *Humanities and Social Sciences Communications*, **10**, Article No. 71. https://doi.org/10.1057/s41599-023-01560-x

[50] Shobowale, K.O., Mukhtar, Z., Yahaya, B., Ibrahim, Y. and Momoh, M.O. (2023) Latest Advances on Security Architecture for 5G Technology and Services. *International Journal of Software Engineering and Computer Systems*, **9**, 27-38. https://doi.org/10.15282/ijsecs.9.1.2023.3.0107

[51] Rath, K.C., Khang, A. and Roy, D. (2024) The Role of Internet of Things (IoT) Technology in Industry 4.0 Economy. CRC Press, Boca Raton. https://doi.org/10.1201/9781003434269-1

[52] Liu, L., Lu, S., Zhong, R., Wu, B., Yao, Y., Zhang, Q. and Shi, W. (2020) Computing Systems for Autonomous Driving: State of the Art and Challenges. *IEEE Internet of Things Journal*, **8**, 6469-6486. https://doi.org/10.1109/JIOT.2020.3043716

[53] Wijethilaka, S. and Liyanage, M. (2021) Survey on Network Slicing for Internet of Things Realization in 5G Networks. *IEEE Communications Surveys & Tutorials*, **23**, 957-994. https://doi.org/10.1109/COMST.2021.3067807

[54] Olimid, R.F. and Nencioni, G. (2020) 5G Network Slicing: A Security Overview. *IEEE Access*, **8**, 99999-100009. https://doi.org/10.1109/ACCESS.2020.2997702

[55] Debbabi, F., Jmal, R., Fourati, L.C. and Ksentini, A. (2020) Algorithmics and Modeling Aspects of Network Slicing in 5G and beyonds Network: Survey. *IEEE Access*, **8**, 162748-162762. https://doi.org/10.1109/ACCESS.2020.3022162

[56] Yang, W., Wang, S., Sahri, N.M., Karie, N.M., Ahmed, M. and Valli, C. (2021) Biometrics for Internet-of-Things Security: A Review. *Sensors*, **21**, Article 6163. https://doi.org/10.3390/s21186163

[57] Schmitt, M. (2023) Securing the Digital World: Protecting Smart Infrastructures and Digital Industries with Artificial Intelligence (AI)-Enabled Malware and Intrusion Detection. *Journal of Industrial Information Integration*, **36**, Article ID: 100520. https://doi.org/10.1016/j.jii.2023.100520

[58] Waqas, M., Tu, S., Halim, Z., Rehman, S.U., Abbas, G. and Abbas, Z.H. (2022) The

Role of Artificial Intelligence and Machine Learning in Wireless Networks Security: Principle, Practice and Challenges. *Artificial Intelligence Review*, **55**, 5215-5261. https://doi.org/10.1007/s10462-022-10143-2

[59] Gupta, C., Johri, I., Srinivasan, K., Hu, Y.C., Qaisar, S.M. and Huang, K.Y. (2022) A Systematic Review on Machine Learning and Deep Learning Models for Electronic Information Security in Mobile Networks. *Sensors*, **22**, Article 2017. https://doi.org/10.3390/s22052017

[60] Samet, D., Ktata, F.B. and Ghedira, K. (2024) A Security Framework for Mobile Agent Systems. *Automated Software Engineering*, **31**, Article No. 12. https://doi.org/10.1007/s10515-023-00408-7