Mobile Security Course Syllabus

Course Overview:

This course provides an in-depth exploration of mobile application security, with a primary focus on the Android ecosystem. Through this course, students will develop a solid understanding of the Android security model, identify and assess potential vulnerabilities, and practice secure coding and reverse engineering techniques. By the end of this course, participants will be equipped to perform penetration testing, secure sensitive data, and strengthen the overall resilience of mobile applications.

Module 1: Introduction to Mobile Security

This introductory module presents a broad view of the mobile security landscape, covering essential threats and vulnerabilities that can affect mobile applications. Students will also be introduced to foundational security concepts to establish a strong base for future modules.

- Overview of Mobile Security Landscape
- Threats and Vulnerabilities in Mobile Applications
- Basic Security Principles: Confidentiality, Integrity, Availability (CIA)

Module 2: Setting Up the Environment

Setting up an efficient environment is essential for mobile security testing. In this module, students will configure research devices, emulators, and development tools to simulate real-world Android environments.

- Research Device & Emulator Setup
- Overview of Android Studio and Development Tools
- Introduction to Android Application Structure

Module 3: Basics of Android Security

This module covers the Android operating system's unique security model, permissions, and core security components. Students will understand how Android’s architecture impacts security and how to navigate its permissions system securely.

- Android OS Security Model
- Android Permission Model
- Key Security Components: Activities, Services, Broadcast Receivers, and Content Providers

---

Module 4: Network Security and Interception

As mobile applications often communicate over networks, understanding network security is critical. In this module, students will learn to intercept network traffic and recognize common vulnerabilities within mobile networking, such as SSL pinning bypass and unencrypted communications.

- Network Communication Basics in Android
- Network Interception Techniques
- Common Vulnerabilities in Mobile Networking (e.g., SSL Pinning, Unencrypted Communications)

Module 5: Reverse Engineering Fundamentals

Reverse engineering is crucial for understanding how mobile applications function at the code level. This module provides hands-on experience with reverse engineering Android applications and using tools to analyze app structure and behavior.

- Reverse Engineering Android Applications
- Essential Tools for Android Reverse Engineering (APKTool, JADX)

Module 6: Dynamic Instrumentation and Testing

This module introduces dynamic instrumentation, a technique used to analyze and manipulate running applications. Students will explore tools like Frida and Xposed for in-depth vulnerability testing.

- Introduction to Dynamic Instrumentation
- Tools: Frida, Xposed Framework
- Testing Applications for Vulnerabilities Using Dynamic Instrumentation

---

Module 7: Android Components and Security Issues

This module focuses on the unique security considerations for Android components such as services, broadcast receivers, and content providers. Students will examine security risks associated with each component and discuss best practices to mitigate these risks.

- Android Services: Security Risks and Best Practices
- Broadcast Receivers: Intent Attack Surface
- Content Providers and File Providers: Security Implications

Module 8: Storage and Data Protection

Data security is critical for any application. This module covers insecure storage mechanisms in Android and demonstrates best practices for protecting sensitive information, including encryption and secure data storage techniques.

- Android (Insecure) Storage Mechanisms
- Best Practices for Secure Storage
- Data Encryption and Decryption on Android Devices

Module 9: Securing Android WebViews

WebViews are a common source of vulnerabilities in Android applications. This module focuses on securing WebView implementations to prevent attacks such as Cross-Site Scripting (XSS), emphasizing best practices and content security policies.

- WebViews and Common Vulnerabilities
- Secure WebView Implementation
- Cross-Site Scripting (XSS) and Content Security Policies in WebViews

---

Module 10: Advanced Android Security Topics

This module dives into advanced security topics, including dynamic analysis and malware detection. Students will engage in a case study on reverse engineering malware

- Dynamic Analysis of Android Apps
- Malware Analysis and Detection
- Case Study: Reverse Engineering

Module 11: Project and Hands-On Labs

In this final module, students apply what they've learned through practical labs and a comprehensive project. They will conduct a security assessment on an Android application, practicing skills in network interception, reverse engineering, and dynamic testing.

- Practical Labs on Network Interception, Reverse Engineering, and Dynamic Testing
- Final Project: Security Assessment of an Android Application
- **Course Wrap-Up**

The course concludes with key takeaways, best practices, and resources for continued growth in mobile security. Students will leave with the skills to protect Android applications against evolving threats and to pursue further specialization in mobile security.

- Key Takeaways and Industry Best Practices
- Future Directions in Mobile Security
- Resources for Further Study and Professional Growth

Note: Each module includes practical labs, quizzes, and assignments designed to reinforce key concepts and provide real-world application. The course culminates in a hands-on project, offering students the opportunity to showcase their skills in a real-world scenario.

The **Mobile Security** course is designed for:

1. **Aspiring Mobile Security Professionals**: Individuals aiming to specialize in securing mobile applications, particularly those with an interest in the Android ecosystem and its security challenges.
2. **Penetration Testers**: Cybersecurity professionals who want to expand their skill set to include mobile application security, focusing on penetration testing techniques tailored to Android apps.
3. **Mobile Application Developers**: Developers looking to enhance their understanding of secure coding practices and integrate security measures into their mobile applications.
4. **Security Analysts and Consultants**: Professionals who assess mobile security within organizations and wish to build their expertise in identifying and mitigating vulnerabilities in mobile apps.
5. **Cybersecurity Enthusiasts**: Individuals passionate about cybersecurity who want to delve into the specifics of mobile security, including reverse engineering, data protection, and network vulnerabilities.
6. **Ethical Hackers**: Ethical hackers or individuals preparing for certifications in mobile security, who need hands-on experience with mobile app testing and security best practices.
7. **Students in Cybersecurity or IT**: College students pursuing degrees in cybersecurity or IT who want to develop practical skills in mobile security and penetration testing.
8. **Malware Researchers and Forensics Experts**: Professionals working in malware analysis or digital forensics, particularly in the context of mobile apps, looking to understand malware behavior and mobile threat analysis.