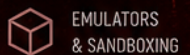
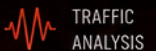
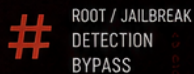
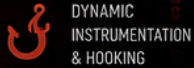
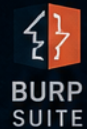


MOBILE APPLICATION SECURITY



THE DEFINITIVE GUIDE TO PROTECTING
ANDROID, iOS, AND CROSS-PLATFORM APPLICATIONS



THREAT MODELING
& RISK ASSESSMENT



SECURE CODING
& ARCHITECTURE



CRYPTOGRAPHY
& DATA PROTECTION



REVERSE ENGINEERING
& ANALYSIS



PENETRATION TESTING
& EXPLOITATION



INCIDENT RESPONSE
& RECOVERY

STEVE T.

Mobile Application Security

The Definitive Guide to Protecting Android, iOS, and Cross-Platform Applications

Steve T.

This book is available at <https://leanpub.com/mobileapplicationsecurity>

This version was published on 2026-06-19



This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2026 Steve T.

Contents

Mobile Application Security	1
The Definitive Guide to Protecting Android, iOS, and Cross-Platform Applications	1
Table of Contents	2
Introduction: The Mobile Security Landscape	6
Chapter 1: Foundations of Mobile Architecture	8
Chapter 2: Threat Modeling and Risk Assessment	9
Chapter 3: Secure Coding and Development Practices	10
Chapter 4: Authentication and Authorization on Mobile	11
Chapter 5: Cryptography and Secure Storage	12
Chapter 6: Network Security and API Protection	13
Chapter 7: The OWASP Mobile Top 10 (2024)	14
Chapter 8: Reverse Engineering Android Applications	16
Chapter 9: Reverse Engineering iOS Applications	17
Chapter 10: Mobile Penetration Testing Methodology	18
Chapter 11: Runtime Manipulation and Bypass Techniques	19
Chapter 12: Code Obfuscation and Anti-Tampering	20
Chapter 13: CI/CD Security and Secure DevOps for Mobile	21
Chapter 14: Cloud Backend and API Security for Mobile	22
Chapter 15: Malware Analysis and Incident Response	23
Chapter 16: Compliance, Regulations, and Governance	24
Conclusion: The Future of Mobile Security	25
References	26

Mobile Application Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

The Definitive Guide to Protecting Android, iOS, and Cross-Platform Applications

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Table of Contents

Introduction: The Mobile Security Landscape

- 1 - Why Mobile Is Uniquely Vulnerable
- 2 - The Scope of the Attack Surface
- 3 - How to Use This Book
- 4 - Conventions and Notation

Chapter 1: Foundations of Mobile Architecture

- 1 - Android App Components and Lifecycle
- 2 - iOS App Layers and the Sandbox Model
- 3 - Cross-Platform Frameworks: Flutter and React Native
- 4 - Application Packaging and Distribution
- 5 - The OS Security Model: Sandboxing, Code Signing, and Privilege Separation

Chapter 2: Threat Modeling and Risk Assessment

- 1 - STRIDE **for** Mobile Applications
- 2 - Data Flow Diagrams and Asset Identification
- 3 - Attack Tree Methodology
- 4 - Risk Scoring with CVSS and DREAD
- 5 - Worked Example: Threat Modeling a Banking App

Chapter 3: Secure Coding and Development Practices

- 1 - Input Validation and Output Encoding
- 2 - Secure Memory Management
- 3 - Error Handling, Logging, and Crash Reporting
- 4 - Secure Configuration: AndroidManifest.xml and Info.plist
- 5 - Third-Party Dependency Security
- 6 - Secure Coding Patterns **for** Native and Cross-Platform

Chapter 4: Authentication and Authorization on Mobile

- 1 - Biometric Authentication on Android and iOS
- 2 - Password and Passcode Security
- 3 - Multi-Factor Authentication
- 4 - Session Management and Token Security (JWT, OAuth 2.0, OIDC)
- 5 - Role-Based and Attribute-Based Access Control
- 6 - Secure Implementation Patterns and Pitfalls

Chapter 5: Cryptography and Secure Storage

- 1 - Symmetric Encryption: AES-GCM and ChaCha20
- 2 - Asymmetric Encryption and Key Exchange
- 3 - Hashing and Password Storage (SHA-256, Argon2)
- 4 - Android Keystore System
- 5 - iOS Keychain and CryptoKit
- 6 - Secure Storage Patterns **for** Databases and Preferences
- 7 - Cryptographic Pitfalls and Common Mistakes

Chapter 6: Network Security and API Protection

- 1 - TLS Configuration and Best Practices
- 2 - Certificate Pinning: Theory and Implementation
- 3 - Man-in-the-Middle Attack Prevention
- 4 - Mobile API Architecture (REST, GraphQL, gRPC)
- 5 - OWASP API Security Top 10 **for** Mobile
- 6 - Intercepting Proxy Setup: Burp Suite, mitmproxy, Charles

Chapter 7: The OWASP Mobile Top 10 (2024)

- 1 - M1: Improper Credential Usage
- 2 - M2: Inadequate Supply Chain Security
- 3 - M3: Insecure Authentication/Authorization
- 4 - M4: Insufficient Input/Output Validation
- 5 - M5: Insecure Communication
- 6 - M6: Inadequate Privacy Controls
- 7 - M7: Insufficient Binary Protections
- 8 - M8: Security Misconfiguration
- 9 - M9: Insecure Data Storage
- 10 - M10: Insufficient Cryptography

Chapter 8: Reverse Engineering Android Applications

- 1 - APK Anatomy **and** Deconstruction
- 2 - Static Analysis with JADX, APKTool, **and** MobSF
- 3 - Decompilation **and** Smali Disassembly
- 4 - Native Code Analysis with Ghidra
- 5 - Dynamic Instrumentation with Frida
- 6 - Hands-On Lab: Analyzing a Vulnerable Android App

Chapter 9: Reverse Engineering iOS Applications

- 1 - IPA Anatomy and Mach-O Binary Analysis
- 2 - Static Analysis with Hopper, IDA Pro, and Ghidra
- 3 - Swift and Objective-C Runtime Introspection
- 4 - Dynamic Instrumentation and Debugging
- 5 - Flutter App Reverse Engineering with reFlutter and Blutter
- 6 - Hands-On Lab: Analyzing a Vulnerable iOS App

Chapter 10: Mobile Penetration Testing Methodology

- 1 - Pre-engagement Planning and Reconnaissance
- 2 - Device Setup: ADB, Emulators, and Jailbreaking
- 3 - Static Analysis Phase
- 4 - Dynamic Analysis Phase
- 5 - Network Traffic Interception
- 6 - Reporting and Remediation Guidance
- 7 - Tool Arsenal: MobSF, Drozer, Burp Suite, Needle

Chapter 11: Runtime Manipulation and Bypass Techniques

- 1 - Frida Fundamentals: Scripts, Hooks, and RPC
- 2 - SSL Pinning Bypass (Android and iOS)
- 3 - Jailbreak and Root Detection Bypass
- 4 - Anti-Tampering and Integrity Check Evasion
- 5 - Memory Manipulation and Runtime Patching
- 6 - Cycript and Objective-C Runtime Hacking
- 7 - Hands-On Lab: Bypassing Security Controls

Chapter 12: Code Obfuscation and Anti-Tampering

- 1 - ProGuard and R8 for Android
- 2 - Swift and Objective-C Obfuscation
- 3 - Native Code Protection
- 4 - Control Flow Obfuscation
- 5 - String Encryption and Resource Protection
- 6 - Integrity Verification and Anti-Tampering Architectures
- 7 - Evaluating Obfuscation Effectiveness

Chapter 13: CI/CD Security and Secure DevOps for Mobile

- 1 - SAST and DAST in CI/CD Pipelines
- 2 - Dependency Scanning (SCA) and Secret Detection
- 3 - Automated Penetration Testing Integration
- 4 - Secure Build Environments
- 5 - Infrastructure as Code Security
- 6 - Tool Integrations: GitHub Actions, Jenkins, CircleCI

Chapter 14: Cloud Backend and API Security for Mobile

- 1 - Cloud Architecture **for** Mobile Backends
- 2 - Server-Side Authentication and Authorization
- 3 - Data Validation and Sanitization
- 4 - Rate Limiting and Abuse Prevention
- 5 - Database Security
- 6 - WebSocket and Real-Time Communication Security
- 7 - Microservices Security Patterns

Chapter 15: Malware Analysis and Incident Response

- 1 - Mobile Malware Taxonomy
- 2 - Static and Dynamic Malware Analysis Techniques
- 3 - Sandboxing and Automated Analysis
- 4 - Behavioral Analysis and Indicators of Compromise
- 5 - Incident Response **for** Mobile Applications
- 6 - Forensic Investigation on Mobile Devices
- 7 - Real-World Case Studies

Chapter 16: Compliance, Regulations, and Governance

- 1 - GDPR and Data Privacy **for** Mobile Apps
- 2 - HIPAA **for** Health Data
- 3 - PCI-DSS **for** Payment Security
- 4 - CCPA/CPRA
- 5 - ISO 27001/27017/27018
- 6 - NIST Mobile Security Guidelines
- 7 - App Store Review Policies and Compliance

Conclusion: The Future of Mobile Security

- 1 - Emerging Threats and Trends
- 2 - AI-Powered Attacks and Defenses
- 3 - 5G, IoT Convergence, and the Expanding Surface
- 4 - A **Call for** Continuous Vigilance

References

Introduction: The Mobile Security Landscape

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Why Mobile Is Uniquely Vulnerable

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

The Scope of the Attack Surface

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

How to Use This Book

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Conventions and Notation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 1: Foundations of Mobile Architecture

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Android App Components and Lifecycle

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

iOS App Layers and the Sandbox Model

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Cross-Platform Frameworks: Flutter and React Native

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Application Packaging and Distribution

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

The OS Security Model: Sandboxing, Code Signing, and Privilege Separation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 2: Threat Modeling and Risk Assessment

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

STRIDE for Mobile Applications

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Data Flow Diagrams and Asset Identification

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Attack Tree Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Risk Scoring with CVSS and DREAD

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Worked Example: Threat Modeling a Banking App

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 3: Secure Coding and Development Practices

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Input Validation and Output Encoding

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secure Memory Management

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Error Handling, Logging, and Crash Reporting

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secure Configuration: AndroidManifest.xml and Info.plist

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Third-Party Dependency Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 4: Authentication and Authorization on Mobile

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Biometric Authentication on Android and iOS

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Password and Passcode Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Multi-Factor Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Session Management and Token Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Role-Based and Attribute-Based Access Control

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secure Implementation Patterns and Pitfalls

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 5: Cryptography and Secure Storage

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Symmetric Encryption: AES-GCM and ChaCha20

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Asymmetric Encryption and Key Exchange

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Hashing and Message Authentication (SHA-256, HMAC, Argon2)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Android Keystore System

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

iOS Keychain and CryptoKit

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secure Storage Patterns for Databases and Preferences

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Cryptographic Pitfalls and Common Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 6: Network Security and API Protection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

TLS Configuration and Best Practices

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Certificate Pinning: Theory and Implementation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Man-in-the-Middle Attack Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Mobile API Architecture (REST, GraphQL, gRPC)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

OWASP API Security Top 10 for Mobile

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Intercepting Proxy Setup: Burp Suite, mitmproxy, Charles

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 7: The OWASP Mobile Top 10 (2024)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M1: Improper Credential Usage

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M2: Inadequate Supply Chain Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M3: Insecure Authentication/Authorization

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M4: Insufficient Input/Output Validation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M5: Insecure Communication

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M6: Inadequate Privacy Controls

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M7: Insufficient Binary Protections

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M8: Security Misconfiguration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M9: Insecure Data Storage

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

M10: Insufficient Cryptography

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 8: Reverse Engineering Android Applications

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

APK Anatomy and Deconstruction

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Static Analysis with JADX, APKTool, and MobSF

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Decompilation and Smali Disassembly

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Native Code Analysis with Ghidra

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Dynamic Instrumentation with Frida

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Hands-On Lab: Analyzing a Vulnerable Android App

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 9: Reverse Engineering iOS Applications

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

IPA Anatomy and Mach-O Binary Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Static Analysis with Hopper, IDA Pro, and Ghidra

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Swift and Objective-C Runtime Introspection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Dynamic Instrumentation and Debugging

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Flutter App Reverse Engineering with reFlutter and Blutter

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Hands-On Lab: Analyzing a Vulnerable iOS App

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 10: Mobile Penetration Testing Methodology

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Pre-engagement Planning and Reconnaissance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Device Setup and Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Static Analysis Phase

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Dynamic Analysis Phase

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Network Traffic Interception

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Reporting and Remediation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Tool Arsenal: MobSF, Drozer, Burp Suite, Needle

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 11: Runtime Manipulation and Bypass Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Frida Fundamentals: Scripts, Hooks, and RPC

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

SSL Pinning Bypass (Android and iOS)

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Jailbreak and Root Detection Bypass

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Anti-Tampering and Integrity Check Evasion

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Memory Manipulation and Runtime Patching

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Cycript and Objective-C Runtime Hacking

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Hands-On Lab: Bypassing Security Controls

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 12: Code Obfuscation and Anti-Tampering

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

ProGuard and R8 for Android

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Swift and Objective-C Obfuscation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Native Code Protection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Control Flow Obfuscation

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

String Encryption and Resource Protection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Integrity Verification and Anti-Tampering

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Evaluating Obfuscation Effectiveness

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 13: CI/CD Security and Secure DevOps for Mobile

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

SAST and DAST in CI/CD Pipelines

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Dependency Scanning (SCA) and Secret Detection

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Automated Penetration Testing Integration

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secure Build Environments

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Infrastructure as Code Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Tool Integrations: GitHub Actions, Jenkins, CircleCI

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Secret Management

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 14: Cloud Backend and API Security for Mobile

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Cloud Architecture for Mobile Backends

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Server-Side Authentication and Authorization

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Data Validation and Sanitization

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Rate Limiting and Abuse Prevention

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Database Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

WebSocket and Real-Time Communication Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Microservices Security Patterns

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 15: Malware Analysis and Incident Response

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Mobile Malware Taxonomy

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Static and Dynamic Malware Analysis Techniques

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Sandboxing and Automated Analysis

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Behavioral Analysis and Indicators of Compromise

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Incident Response for Mobile Applications

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Forensic Investigation on Mobile Devices

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Real-World Case Studies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Chapter 16: Compliance, Regulations, and Governance

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

GDPR and Data Privacy for Mobile Apps

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

HIPAA for Health Data

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

PCI-DSS for Payment Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

CCPA/CPRA

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

ISO 27001/27017/27018

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

NIST Mobile Security Guidelines

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

App Store Review Policies

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

Conclusion: The Future of Mobile Security

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.

References

This content is not available in the sample book. The book can be purchased on Leanpub at <https://leanpub.com/mobileapplicationsecurity>.