Android Security

Course Summary

Description

Android Security is a three-day course focusing specifically on the various security concerns of the Android platform.

We explore the Android architecture and security model, permission system and enforcement, encryption, known exploits, memory protections, data protection, device management, SELinux, as well as tools security researchers use to find Android vulnerabilities. We also focus on best practices for coding and deploying secure Android apps. Learn what to do - and what not to do - to keep your apps, your business, and your customers secure.

Objectives

By the end of this course, students will be able to:

- Describe how the Android platform security model works
- Explain the steps involved in rooting an Android device
- Perform static analysis on application resources and executable code
- Discover vulnerabilities using penetration testing
- Apply best practices to secure exposed application interfaces
- Implement secured networking with limited trust exposure risk
- Protect sensitive persisted application data
- Integrate and manage secured work profiles

Topics

- Android Stack Overview
- Android Platform Security
- Android Rooting
- Reverse-Engineering Applications
- Android Penetration Testing
- Securing Application Code
- Secure Network Communications
- Securing Persisted Application Data
- Mobile Device Administration (Android for Work)

Audience

The Android Security course is designed for security-conscious application developers and system integrators looking to tighten the security of both their devices as well as the applications running on them.

Prerequisites

Before taking this course, Android Overview training or any other Android class that contains Android Overview module is required. It is highly recommended that participants be familiar with basics of Java, C/C++, and Linux administration to fully take advantage of this course. Additionally, "bootcamp-level" knowledge of Android Studio and the Gradle build system is required.

Duration

Three days

Android Security

Course Outline

I. Android Stack Overview

This module introduces you to the Android operating system to ensure a basic familiarity with the Android architecture, background, and terminology. You will also learn about the design philosophy of Android and the considerations involved with its open source licensing.

A. Linux Kernel Layer
B. Native User Space Layer
    1. Application Runtime
C. Application Frameworks Layer
D. Applications Layer
E. Application (APK) Structure

II. Android Platform Security

Android extends standard Linux security to control access to device features like network interfaces, cameras, and stored personal information. In this module you learn how Android's permission model interacts with standard Linux security and how to define and enforce custom permissions to restrict access to system extensions.

A. Application sandbox
B. SELinux Policies in Android
C. Full Disk Encryption
D. Verified Booting
E. Application (APK) Signing
F. File system access permissions
G. Application Permissions Model
    1. Using permissions
    2. Declaring custom permissions
H. Vulnerabilities and Exploits
I. Android Malware Scanning

III. Android Rooting

Rooting circumvents portions of the platform security model to achieve various ends. You will learn about common exploits used to achieve root, and walk through the rooting process.

A. Reasons for rooting devices
B. Device rooting process
C. Common root exploits
D. Rooting under SELinux

IV. Reverse-Engineering Applications

Performing static analysis on application binaries can provide a lot of useful information…to a tester or an attacker. You will learn how to reverse-engineer the contents of an APK to better understand what contents of an application are easily exposed.

A. Android bytecode structure
B. Unpacking APK resources
C. Disassembling APK executable code
D. Modifying and repackaging APK contents
E. Common disassembly tools

V. Android Penetration Testing

Dynamic analysis allows us to test an applications ability to process input. You will use common penetration testing tools to discover the attack surface an application presents. Using "fuzzing" and other data injection techniques, you learn how to find vulnerabilities in an Android application's exposed attack surface.

VI. Securing Application Code

This module introduces coding practices you can use to harden your application code and patch potential vulnerabilities.

A. Obfuscation
B. Validating input on exposed components
C. Protecting exposed IPC endpoints
D. Commonly missed side-channel leaks

VII. Secure Network Communications

This module introduces coding practices for securing the network traffic your application generates. You will learn proper techniques for minimizing risk when handling web-based content in an application.

A. Exposing network-related vulnerabilities
B. Encryption with SSL/TLS
C. Certificate pinning
D. Virtual Private Networks (VPNs)
E. Protecting WebView code

Android Security

Course Outline (cont'd)

VIII. Securing Persisted Application Data

This module introduces coding practices for securing the data your application persists on disk.

A. Storage APIs
B. User authentication credentials
   1. Avoiding leaks
   2. Alternatives to storing
C. Storing sensitive data
D. Encrypting persisted data

IX. Mobile Device Administration (Android for Work)

Keeping enterprise applications secure if a big concern on Android devices. In this module, you will learn to use the device administration framework to create applications that enforce enterprise policies on controlled devices. You will also learn considerations for coding applications that need to execute inside of a secured work profile.

A. Device administration APIs
B. Application restrictions
C. Device provisioning and profile management
D. Integrating with Google's Android for Work program