Training: Capstone Courseware

256 Securing Android Applications

TRAINING GOALS:

This informative one-day course offers a fresh look at the Android operating system from the perspectives of both user and enterprise security, and gives the Android developer a clear sense of best practices and pitfalls in application development.

The course moves from an overview of the operating system and its security features through high-level considerations, "do's and don'ts," and offers hands-on exercises in securing existing Android applications against possible hacks -- which hacks they can carry out using prepared, simulated malware operating on the Android device or emulator. In this way students get a concrete understanding of concerns and techniques including:

- File-system security
- Injection and cross-site attacks
- Inter-process attacks
- Custom permissions
- Login practices
- Cryptography and network communications

Learning Objectives

- Understand the security characteristics of mobile computing, and the Android OS in particular.
- Manage application data in a secure fashion.
- Apply appropriate safeguards over entry points to applications, including intent filters, bound services, and broadcast receivers.
- Use cryptography as appropriate, especially in remote communications.
- Manage user credentials, including passwords and issued tokens.

CONSPECT:

- Mobile OS Security
  - Vulnerabilities of Mobile Systems
  - Security Overview of Android
  - For Comparison: iOS
  - Analysis and Areas of Concern

  - Digital Signature of Applications
  - Rooted Devices
  - Clickjacking
  - Best Practices
  - The OWASP Mobile Top 10
- Application Security
  - Permissions
  - Custom Permissions
  - Security Configuration
  - Storage Models
  - Internal Storage
  - USB, Bluetooth, WiFi, and External Media
  - File System Security
  - Encrypted File Systems
  - Injection Vulnerabilities
  - Inter-Process Communication
  - Guarding IPC Entrances
  - Services and Broadcast Receivers
  - Logging
- Remote Connectivity
  - Remote Connections from Mobile Devices
  - The INTERNET Permission
  - HTTP and HTTPS Communication
  - Keystores and Cryptography
  - Username/Password Login
  - Managing Credentials
  - HMACs
  - Managing Token Pairs

REQUIREMENTS:

- **Java programming** experience is required - Course 103 is excellent preparation.
- Introductory knowledge of **Android programming** is required - Course 251 or similar.
- We recommend **intermediate Android programming** in advance of this course - Course 252.
- Intermediate Android Development would be ideal, but this is not required.

Difficulty level

■■■□□□

CERTIFICATE:

The participants will obtain certificates signed by Capstone Courseware.

TRAINER:

Authorized Capstone Courseware Trainer.

ADDITIONAL INFORMATION:

IDE Support: Eclipse Juno

In addition to the primary lab files, an optional overlay is available that adds support for Eclipse Juno. Students can code, build, deploy, and test all exercises from within the IDE. We make full use of the Android SDK and its Eclipse plugin and device emulators.