¡capacitación es ... crecer!
¡capacitación es ... seguridad!
¡capacitación es ... desarrollo!
¡capacitación es ... profesionalismo!

Android Security Essentials

ATC AUTHORIZED Training Center

Datos Importantes

Duración:
12 horas

Formato:
Presencial

Materiales:
Material impreso por participante

Equipo:
Un equipo por participante

Nivel:
Básico-Intermedio

Servicio de cafetería

Descripción del Curso

Este curso de 12 hrs. cubre el modelo de seguridad para Android a nivel del desarrollador y del usuario final.

Objetivos

- Entender la arquitectura de Android.
- Entender el modelo de seguridad de Android
- Construir las aplicaciones de Android con las mejores prácticas de seguridad en mente
- Construir aplicaciones más seguras y más robustas.

Audiencia

Este curso se recomienda a programadores sobre Android.

Prerrequisitos

Para lograr el máximo aprovechamiento del curso, los alumnos necesitan:

- Tener conocimientos de programación en Java.

Cursos Asociados

- Android Application Development

Android Security Essentials

Temario

Lesson 1: Introduction and Android Security Architecture
- Android Security Program Overview and Architecture.
- Kernel level security (Linux), and rooting Android.
- Android Application Components.
- The Application Sandbox.
- Managers and Services
  - Activity Manager Service.
  - Package Manager Service.
  - Notification Manager Service.
  - Search Manager Service.
  - Connectivity, Telephony, and Wi-Fi Manager Services.
  - Download and Storage Manager Services.
  - Window Manager Service.

Lesson 2: Android Permission Model and third party applications
- Android Application Framework Layer.
- Third party application permissions.
- Using Protected APIs.
- Custom Permissions.
- Android Malware: Prevention, Detection, and Removal.
- Security Enhanced Android (SE Android).

Lesson 3: Component Security and Protecting data storage
- How Android achieves Inter-process communication.
- Restricting access to Android components.
- Vulnerabilities of Stored Data.
- Cryptography and Encryption.
- Signing your application

Lesson 4: Client-Server communication security.
- Threats Facing Devices Transferring Data.
- Protecting web transferred data.
- Input Validation.
- Prevent Command Injection.