Course Introduction

Mobile security has become increasingly important with the deployment of mobile devices and applications in the enterprise—from small businesses to Fortune 100 companies. Mobile devices have greatly advanced from a mere device for communication to an extent that they have become replacements for cameras, music players, game consoles, and even computers. With the advancement in mobile technology is a growing concern on the sensitive information being collected and processed on these devices that must be secured in order to protect the privacy of the users and the intellectual property of the company.
This course provides in-depth knowledge of Mobile Device and Application Security—highlighting and analysing the latest mobile threats and mitigations. It explains the differences between the security models used by iOS, Android, Windows Phone, and Blackberry, and how to evaluate the security of mobile devices and applications by means of reverse engineering, network activity analysis, and penetration testing.

Course Objectives

- To understand the differences between iOS, Android, Windows Phone, and Blackberry
- To understand how to exploit the vulnerabilities in the cellular network and wireless network infrastructure
- To understand how to evaluate the security of mobile devices and applications for enterprise deployment
- To understand how to conduct a mobile application penetration test
- To understand how to discover and exploit mobile application vulnerabilities
- To understand the impact of a successful exploit and how to protect against these threats

Learning Level

- Intermediate

Course Duration

- 5 Days

Course Prerequisite

- None

Target Group

- Mobile Application Developers

For More Information & Registration, Please Contact Training Division
Tel:(66) 2253-4736, Fax:(66) 2253-4737, Hotline:(66) 86-325-7129, E-mail: registration@acisonline.net

System/Network Administrators

IT Auditors

Information Security Professionals

Anyone interested in learning about Mobile Device and Application Security

Course Outline

Day 1

- The Evolution of Mobile Devices and Applications
- Mobile Threats and Mitigations
- iOS Security Model
- Windows Phone Security Model
- Blackberry Security Model

Day 2

- Enterprise Mobile Device Policy and Management
- Mobile Device Management Frameworks
- Bypassing Mobile Device Management
- Introduction to Cellular Network Security
- Introduction to Wireless Network Security

Day 3

- Static Application Analysis
- Reverse Engineering iOS Binaries

Reverse Engineering Android Binaries

Dynamic Application Analysis

iOS Runtime Analysis and Manipulation

Android Runtime Analysis and Manipulation

Day 4

- Network Activity Analysis
- Automated Application Analysis
- Mobile Application Penetration Testing Methodology
- OWASP Mobile Security Project

Day 5

- Mobile Application Penetration Testing

Official Training Partner