iOS Application

Secure Coding

2-day Hands-on Course

Syllabus

iOS Application Secure Coding
2-Day Hands-On Course

Course description

This course will focus on the techniques and tools for testing the security of iOS (iPhone/iPad etc.) mobile applications. During this course the students will learn about important topics such as the iOS Security model, how to perform static analysis, traffic manipulation and dynamic analysis and how to secure the application against those attacks. By taking this course you will be able to analyze their own applications and secure them against malicious attacks.

The objectives of the course are:

- Understand the iOS application threat landscape
- Identify vulnerabilities and exploit them
- Secure the applications against those vulnerabilities

Target audience

Members of the security / software development team:

- iOS developers
- Security penetration testers

Prerequisites

Before attending this course, students should be familiar with:

- Basic knowledge of the iOS development platform

In addition, participants must have mac books with xCode.

Course topics

Day 1

Introduction to iOS Security

- Welcome to iOS
- What makes mobile security so different?
- OWASP Top 10 Mobile
- iOS Device Architecture
- iOS Security Model
- iOS File System isolation
- Build security flags
- Application Sandbox
- The iOS Pen-Testing Environment
- Jailed vs. jailbroken devices
- Cydia Installations
- Laptop Installation
- AppSec-Labs iNalyzer
- **Lab: Exploring the iOS environment**
- **Lab: Secure the build settings**

Application Static Analysis

- The need for Static Analysis
- Sources for Static Analysis
- The IPA file package
- Anti-tampering configuration
- Tampering with IPA Content
- Investigating the Application contents – View Controllers
- Investigating Info.plist file
- Listing all CFUR types on a device
- Investigating Binary – URI Strings
- Investigating Binary – Parameters usage
- Investigating Binary – Encryption
- iOS Binary Application Structure
- Code encryption
- Decrypting Binary - concept
- Static analysis of a decrypted Binary
- Investigating binary content
- Reversing Interfaces
- Using iNalyzer for static analysis
- **Lab: Binary Static Analysis manual and automated**
- **Lab: Secure communication between apps**

Traffic Manipulation

- Traffic Analysis and Manipulation
- Common architecture
- Bad Session Management
- Phone identifiers used in authentication
- Credentials leakage
- Client information sent to advertisement/analytics server
- Server side vulnerabilities
- Sniffing Traffic
- Traffic interception
- Importing SSL certificates & trusted CA's
- SSL Pinning
- **Lab: Implementing SSL pinning**

Day 2

Application Storage Analysis

- Application Storage Analysis
- File System access security
- File System Data Protection Classes
- File System access
- Application storages
- Property list files (.plist)
- Tampering with Property list files (.plist)
- Investigating Plist files – plutil.
- Database files (.db/.sqlite)
- How to prevent snapshots storage
- Persistent Cookies
- Investigating Logs
- Keyboard Cache
- Cryptographic failures
- Keychain access and security
- **Lab: Storing data securely**

Protecting sensitive data

- Introduction to cryptography
- Symmetric Cryptography
- Asymmetric Cryptography
- Hashing
- Digital signatures
- Key derivation function

Temporary runtime manipulation

- Temporary Runtime Manipulation
- Why do we need temporary runtime manipulation?
- Temporary runtime manipulation tools
- Objective-C class interposing
- Runtime manipulation with Cycript
- Cycript as a Tampering tool
- **Lab: Objective-C and runtime manipulation using cycript**