++

Offensive iOS Exploitation

Course Info

MWR INFOSECURITY

Contents page

1. Abstract

This is an exercise-driven training course that uses detailed tutorials to guide the attendee through all the steps necessary to exploit a real iOS application, and in the process, provide an understanding of the modern attacker's mind-set and capabilities. This course will cover iOS hacking, from the basics of vulnerability hunting on the platform to advanced exploitation techniques. At its conclusion, the course will have imparted the information necessary to develop secure and robust applications.

This is a technical course suitable for those interested in mobile application security. The training does not require any prior security knowledge in order to benefit fully from the course, as the content covers all of the basics necessary to understand advanced concepts. However, a working knowledge of iOS is a prerequisite and it is recommended that attendees are familiar with the syntax and structure of an iOS application.

In addition, this workshop will use MWR's newly released tool "Needle" to identify and exploit common mobile application security flaws, over and above the OWASP Mobile Top Ten. Needle is an open source modular framework which aims to streamline the entire process of conducting security assessments of iOS applications, and acts as a central point from which to do so. Needle is intended to be useful not only for security professionals, but also for developers looking to secure their code. A few examples of testing areas covered by Needle include: data storage, inter-process communication, network communications, static code analysis, hooking and binary protections.

Other take-aways will include how to develop secure mobile applications that can withstand advanced attacks, how hackers attack mobile applications and iOS devices, and the most up to date and effective secure coding practices.

Even if a device isn't essential, as practical examples will be delivered by the Instructors, delegates are however suggested to bring their own jailbroken iOS device (running iOS >= 8.4) to fully enjoy the course, as these won't be provided.

The following are the modules composing the training:

- The iOS Security Model and the iOS ecosystem
- How to setup an iOS testing environment
- The process of analysing an iOS application
- Data Security
  - Coverage of the available mechanisms for protecting application data in iOS
  - How to test for data security
- Runtime and Binary Protections
  - Understanding the security relevance of running an application in a jailbroken device
  - Understanding the concept of Instrumentation
  - Understanding how to protect applications with binary protections
  - How to test for and bypass binary protections

- Transport Security
  - Network communications in iOS
  - Securing iOS applications' communications
  - How to test for and bypass transport security

2. Detailed Syllabus

Analysing iOS Applications

- Overview of the iOS ecosystem
  - File system structure
  - Configuration profiles
  - Application distribution (App store, Ad-hoc, Enterprise)
- iOS testing environment
  - Testing tools
  - iOS App Store Package (IPA)
  - Installing iOS applications
- Analysing iOS Applications
  - iOS assessments (what pentesters are looking for)

iOS Development

- Development environment (XCode & Licenses)
- Objective-C overview

iOS Security Model

- Secure boot chain
- Application code signing
- Application sandbox (Seatbelt profiles, Entitlements)
- Anti-exploitation mechanisms (ASLR, W^X, Canaries)

Data Security

- Data-at-rest encryption
- Data protection API
- Storage types (Keychain, NSUserDefaults, other data storages)
- Caching (Application Backgrounding, Keyboard Caching, HTTP Response Caching)
- Keybags
- System Log
- Inter-Process Communication (IPC)

Runtime and Binary Protections

- Understanding the security relevance of running an application in a jailbroken device
- Understanding the concept of Instrumentation
- Understanding how to protect applications with binary protections
  - Binary protections
  - Detecting jailbroken devices
  - Bypassing jailbreak detection
  - Other Security Controls (securing the Runtime, tamperproofing, anti-debugging protections)

Transport Security

- Network Communications in iOS
- Securing iOS applications' communications
  - Different ways to man-in-the-middle iOS connections
  - SSL/TLS
    - NSURL / CFNetwork / Secure Transport API Coverage
    - Certificate validation (with examples of some bad practices)
    - TLS session security (with examples of some bad practices)
  - Intercepting communications (HTTP/S)
  - TLS certificate pinning
    - Different ways to pin
    - Certificate pinning bypass
- Javascript to Objective-C bridging in UIWebView
  - WebViews
  - Javascript bridges

3. Who Should Take This Course

- Security professionals who wants to get a deeper understanding of the security implications of the iOS platform and of the techniques that can be used to perform security assessments of iOS applications
- Developers who want to write better (secure) code
- Anyone who wants to learn to use Needle proficiently

4. What Students Should Bring

- 1 jailbroken iOS device running iOS >= 8.0 (8.X preferred)
- 1 USB Lightning cable
- Laptop running Linux or OSX (With 20 GB minimum free space)
- Virtualization software capable of running VMDKs (.ova)
- A text editor you are comfortable writing in (instructors recommend Sublime Text 2 or Vim)
- Setup instructions will be sent to the student prior to the class