Offensive Mobile Reversing and Exploitation

1. Abstract

This course is designed to introduce beginners as well as advanced security enthusiasts to the world of mobile security using a fast-paced learning approach through intensive hands-on labs. The class starts with a basic introduction to the ARM instruction set and an intro to reverse engineering before moving on to the internals of iOS and Android. We then discuss some of the latest exploitation techniques using real-world bugs (e.g., voucher_swap for iOS 12) followed by a walkthrough of how jailbreaks are written. We also discuss some of the common vulnerability types (Heap Overflows, Use-after-free, Uninitialized Stack variable, Race conditions).

The training then moves on to application security and is based on exploiting Damn Vulnerable iOS app, Android-InsecureBankv2 written by the authors of this course and a broad range of other real-world applications. Slides and detailed documentation on the labs will be provided to the students for practice after the class.

After the training, the attendees will:
- Get an understanding of ARM64 instruction set (including ARM 8.3)
- Learn the fundamentals of iOS IPC (XPC, Mach)
- Get an intro to some common bug categories UaF, Heap overflow, etc
- Understand how jailbreaks and exploits are written (including iOS 12)
- Reverse engineer iOS and Android binaries (Apps and system binaries)
- Be able to audit iOS and Android apps for security vulnerabilities
- Understand some of the latest bugs and mitigations (PAC, CoreTrust, Code Signing)
- Understand and bypass anti-debugging and obfuscation techniques
- Get a quick walkthrough on using IDA Pro, Hopper, Frida, etc

2. Course Outline

Part 1 - iOS Exploitation

Module 1: Getting Started with iOS Pentesting
- iOS security model
- App Signing, Sandboxing, and Provisioning
- Setting up XCode 9
- Changes in iOS 12
- Primer to iOS 12 security
- Exploring the iOS filesystem

- Intro to Objective-C and Swift4
- What's new in Swift 4?
- Setting up the Pentesting environment
- Jailbreaking your device
- Cydia, Mobile Substrate
- Getting started with Damn Vulnerable iOS app
- Binary analysis
- Finding shared libraries
- Checking for PIE, ARC
- Decrypting IPA files
- Self-signing IPA files

Module 2: iOS exploitation basics

- How are jailbreak exploits written?
- Diffing for Patches
- Intro to ARM assembly
- ARM Pointer authentication
- ROP, KASLR, and KPP
- Use after free, Heap overflow basics
- Reversing the Kernel
- Code signing bypass techniques
- Sandbox bypass techniques
- Exploiting Mach Ports
- Chaining exploits
- Patching the Kernel
- Achieving persistence

Module 3: Static and Dynamic Analysis of iOS Apps

- Static Analysis of iOS applications
- Dumping class information
- Insecure local data storage
- Dumping Keychain
- Finding URL schemes
- Dynamic Analysis of iOS applications
- Cycript basics
- Advanced Runtime Manipulation using Cycript
- Method Swizzling
- GDB basic usage
- Modifying ARM registers
- Basic App Exploitation techniques using Frida
- Advance App Exploitation techniques using Frida

Module 4: iOS application vulnerabilities

- Exploiting iOS applications
- Broken Cryptography
- Side channel data leakage
- Sensitive information disclosure
- Exploiting URL schemes
- Client-side injection
- Bypassing jailbreak, piracy checks
- Inspecting Network traffic
- Traffic interception over HTTP, HTTPs
- Manipulating network traffic
- Bypassing SSL pinning

Module 5: Reversing iOS Apps

- Introduction to Hopper
- Disassembling methods
- Modifying assembly instructions
- Patching App Binary
- Logify

Module 6: Securing iOS Apps

- Securing iOS applications
- Where to look for vulnerabilities in code?
- Code obfuscation techniques
- Piracy/Jailbreak checks
- iMAS, Encrypted Core Data

Part 2 - Android Exploitation

Module 1

- Why Android
- Intro to Android
- Android Security Architecture
- Android application structure
- Signing Android applications
- ADB – Non-Root
- Rooting Android devices
- ADB – Rooted

- Understanding the Android file system
- Permission Model Flaws
- Attack Surfaces for Android applications

Module 2

- Understanding Android Components
- Introducing Android Emulator
- Introducing Android AVD

Module 3

- Proxying Android Traffic
- Reverse Engineering for Android Apps
- Smali Learning Labs
- Smali vs Java
- Dex Analysis and Obfuscation
- Android App Hooking

Module 4

- Exploiting Local Storage
- Exploiting Weak Cryptography
- Exploiting Side Channel Data Leakage
- Manual and Automated Root Detection and Bypass
- Exploiting Weak Authorization mechanism
- Identifying and Exploiting flawed Broadcast Receivers
- Identifying and Exploiting flawed Intents
- Identifying and Exploiting Vulnerable Activity Components
- Exploiting Backup and Debuggable apps
- Analysing Proguard, DexGuard, and other Obfuscation Techniques
- Exploiting Android NDK
- Manual and Automated SSL Pinning Bypass techniques

Module 5

- App Exploitation using Drozer
- Basic App Exploitation techniques using Frida
- Advance App Exploitation techniques using Frida
- App Exploitation using AppMon
- Automated source code analysis
- Detecting Leaks in Android Apps

3. Bio

Prateek Gianchandani is currently working as a Security Researcher at DarkMatter. He has more than 7 years of experience in security research and penetration testing. His core focus area is mobile exploitation,reversing engineering and embedded device secuirty. He is also the author of the open source vulnerable application named Damn Vulnerable iOS app. He has presented and trained at many international conferences including Defcon, Blackhat USA, Brucon, Hack in paris, Phdays, Appsec USA etc. In his free time, he blogs at http://highaltitudehacks.com

Dinesh leads the Mobile Security Testing Center of Excellence at Security Innovation. His core area of expertise is Mobile and Embedded application pentesting and exploitation. He has spoken at conferences like Black Hat, Bsides, Def Con, BruCon, AppsecUSA, AppsecEU, HackFest and many more. He maintains an open source intentionally vulnerable Android application named InsecureBankv2 for use by developers and security enthusiasts. He has also authored the guide to Mitigating Risk in IoT systems that covers techniques on security IoT devices and Hacking iOS Applications that covers all of the known techniques of exploiting iOS applications. Twitter: https://twitter.com/din3zh
LinkedIn: https://www.linkedin.com/in/dineshshetty1