COURSE INFORMATION

Mobile Security Masterclass: Platform Internals and InSecurity

Course Overview:

This in-depth and immersive three-day course offers participants an opportunity to gain a deep understanding of iOS and Android platform internals, application security, and exploitation. The course is fast-paced and covers a wide range of topics, including reverse engineering, exploitation techniques, vulnerability analysis, kernel internals, and mitigation strategies.

The masterclass features real-world case studies on exploits, malware, and vulnerability analysis. Participants will learn about the mobile OS security model and exploit mitigations available on these platforms. There will be an in-depth discussion and hands-on labs for ARM64 instruction set, code signing, sandboxing, inter-process communication mechanisms, and advanced techniques to bypass anti-debugging and obfuscation.

This masterclass is designed for security professionals and software engineers who wish to enhance their expertise in mobile security and acquire practical skills to assess, secure, and analyze both iOS and Android platforms.

Slides, and detailed documentation on the labs will be provided to the students for practice after the class. Corellium access will be provided to students during the duration of the training course.

Key learning objectives:

- Get an understanding of latest ARM64 instruction set
- Introduction to Ghidra along with scripting
- Introduction to different exploitation categories (UaF, Heap Overflow etc)
- Exploit Mitigations (ASLR, PAN, PAC, Stack Canaries etc)
- Understand some common vulnerabilities and mitigations in Mobile Browsers
- Reverse engineering iOS binaries (Apps and system binaries)
- Symbolicate the kernel and reverse engineer Kernel extensions
- Learn about the different security mitigations in Userland and the XNU Kernel
- Learn how code signing and sandboxing works in iOS
- Learn about the different IPC mechanisms in iOS (Mach, XPC etc)
- Exploiting URL Schemes and Deep Links
- Learn the internals of iOS/Android Kernel along with several Kernel security mitigations
- Understand some of the latest bugs and mitigations (PAC, CoreTrust, PPL, etc)
- Reverse engineer iOS and Android binaries (Apps and system binaries)
- Learn how to audit iOS and Android apps for security vulnerabilities
- Understand and bypass anti-debugging and obfuscation techniques

- Understand the Android System Architecture and AOSP source code
- Learn how to customize and build Android Kernel for Vulnerability Research
- Gain knowledge about Android Internals and Security Model
- Learn about Android RunTime and Binder Internals
- Grasp Android Boot, Recovery, and Rooting processes
- Gain knowledge about Android Platform Permission, DAC, CAP, SECCOMP, and SELinux
- Overview of Kernel protections and bypasses
- Real-World Case Study of Android Exploit
- Real-World Case Study of Android Malware
- Learn how to exploit Mobile Games and Billing
- Learn advanced Frida scripting and Application instrumentation

Why should you take this course?

This course provides content for intermediate as well as advanced students. Instead of just slides, attendees will get a chance to exploit all of the vulnerabilities taught by the instructors. The attendees will be provided with Cloud-based Corellium labs for performing the hands-on iOS and Android exercises without the need to carry physical phones. The slack channel is created before the course for the students so that they can be adequately prepped in terms of hardware and software before the class. The attacks taught in the class are completely hands-on and based on the learnings from the trainers' experience and personal research.

Who Should Attend?

This course is for penetration testers, mobile developers, security researchers, security engineers, or anyone keen to learn mobile security and wants to get started in OS exploitation.

Prerequisite Knowledge:

The course covers topics ranging from intermediate to advanced topics. Basic Linux skills is the only requirement for the course. The Mobile OS and kernel exploitation modules will require basic exploit development background.

Hardware/Software requirement:

Laptop with:

- 8+ GB RAM
- Students will be provided with access to Linux cloud instances
- Students will be provided with access to Corellium for iOS hands-on and as such do not need to carry iOS devices
- Administrative access on the system

Detailed Course Setup instructions will be sent a few weeks prior to the class.

What will the students get:

- Cloud Access for attendees
- Videos for the vulnerabilities shared in the class
- Huge list of good reads and articles for learning mobile security
- Source code for vulnerable applications
- Take home Custom VM for hands-on pentesting after the class
- Students will be provided with access to Corellium for iOS hands-on for the duration of the course
- Slack access for the class and after for regular mobile security discussions

Who are the Trainers:

Prateek Gianchandani has more than 10 years of experience in security research and penetration testing. His core focus area is mobile exploitation, reverse engineering, and embedded device security. 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, POC, TyphoonCon, Blackhat USA, Brucon, Hack in Paris, Phdays, Appsec USA, etc. In his free time, he blogs at https://highaltitudehacks.com.
Twitter: https://twitter.com/prateekg147
LinkedIn: https://www.linkedin.com/in/prateekgianchandani

Dinesh's core area of expertise is Mobile and Embedded application pen-testing and exploitation. He has spoken at conferences like Black Hat, Bsides, DefCon, 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 which covers techniques on security IoT devices and Hacking iOS Applications which covers all of the known techniques of exploiting iOS applications.
Twitter: https://twitter.com/din3zh
LinkedIn: https://www.linkedin.com/in/dineshshetty1

8ksec is a foremost cyber security research company offering exceptional training and consulting services to aid clients in enhancing their security stance. Our experts possess extensive experience in delivering specialized cybersecurity training and consulting to several commercial and defense organizations across the United States, Europe, and the Middle East and North Africa region