8KSEC

COURSE INFORMATION

iOS Internals and Application Security

Course Overview:

This course is designed to provide a comprehensive understanding of the internals of iOS and its security features. The course will cover topics such as the iOS operating system architecture, memory management, application sandboxing. Students will learn the fundamental concepts and tools used in reverse engineering, including static and dynamic analysis techniques, as well as various debugging and disassembly tools. Additionally, the course will delve into iOS application security, including topics such as code signing, encryption, and secure communication. Students will learn how to use Frida, a dynamic instrumentation framework, for reverse engineering and dynamic analysis of mobile applications. We will also discuss advanced topics such as hooking, memory manipulation, and instrumenting network communication. This course will also discuss the tools and techniques used for analyzing iOS malware. The course will also cover the different stages of iOS malware analysis, including static, dynamic, and behavioral analysis. Additionally, the course will delve into the different methods of mitigating and preventing iOS malware.

We are bringing an updated version of the course with the latest tools & techniques. The training will be based on exploiting the Damn Vulnerable iOS app, and a wide range of real-world application vulnerabilities in order to give in-depth knowledge about the different kinds of vulnerabilities in Mobile applications.

This course will be a mix of lectures, practical labs, and projects designed to give students hands-on experience with iOS internals and application security. Students will gain the skills needed to reverse engineer, design, develop, and secure iOS applications. Slides, Custom scripts, Videos, VM, and detailed documentation on the labs will be provided to the students for practice after the class. Corellium access will also be provided to students during the duration of the training course. Students will also be provided access to Slack/Discord channel where the trainers will help prepare them for the class, and the students can retain access to it for the foreseeable future.

Key learning objectives:

- Reverse engineering iOS binaries (Apps and system binaries)
- Get PoC applications to perform 1 click exploits on Mobile apps
- Get an intro to common bug various bug categories on iOS
- Learn to audit iOS apps for security vulnerabilities
- Understand and bypass anti-debugging and obfuscation techniques
- Learn manual and automated ways of bypassing exploit mitigations
- Get a detailed walkthrough on using Ghidra, Hopper, Frida, etc

Why should you take this course?

This is a completely hands-on course designed for beginners and intermediate 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 exercises without the need to carry physical phones. Slack/Discord 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.

Both the trainers have exceptional background in Mobile Security, IoT and Devops having tested wide range of public facing consumer applications, social media giants, hardware vendors and financial institutions. The trainers have taught sold-out classes on Mobile, IoT and Kernel Security for the last few years around the globe for multiple conferences and privately held organizations. The attacks taught in the class are completely hands-on and based on the learnings from this experience and personal research.

Who Should Attend?

This course is for vulnerability researchers, penetration testers, mobile developers, or anyone keen to learn more about the iOS operating system.

Prerequisite Knowledge:

The course covers topics ranging from beginners to advanced topics. Basic Linux skills are the only requirement for the course. Some basic vulnerability research experience is a bonus, but not necessarily required for this course.

Hardware/Software requirement:

- Laptop with: 8+ GB RAM and 20 GB hard disk space
- 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 and Slack/Discord access will be sent a few weeks prior to the class

What will the students get:

- Huge list of good reads and articles for learning mobile application security
- Source code for vulnerable applications
- Source code for Exploit PoCs' that can be used for Bug Bounties
- 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
- Students will be provided access to cloud instances for the duration of the course
- Slack/Discord access for the class and after for regular mobile security discussions

Who are the Trainers:

Prateek Gianchandani is currently working as the Head of Product & Application Security at Careem - An Uber Company. He 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 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