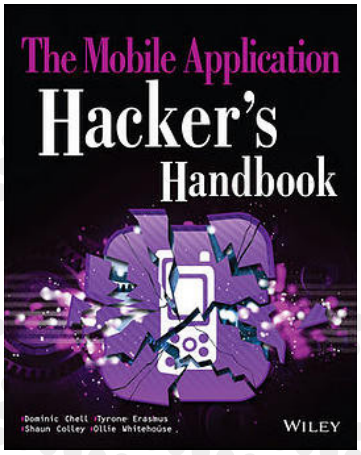
THE MOBILE APPLICATION HACKER'S HANDBOOK - LIVE EDITION

OVERVIEW



MDSec's Mobile Application Hacker's Handbook course is delivered by the lead author of the book. It features all new material and hands-on hacking examples, covering chapters 1-9 of MAHH.

The course follows chapters 1-9 of the Mobile Application Hacker's Handbook, with a strong focus on practical attacks. Over the 2-day training course delivered by the lead author of the book, delegates will learn the tricks and techniques to hack mobile applications on the iOS and Android platforms.

After a short introduction in to the subject, we delve in to the following core modules:

- Introduction to Mobile Application Security Assessment (Chapter 1)
- Analysing iOS applications (Chapter 2)
- How to attack iOS applications (Chapters 3-4)
- Securing iOS applications (Chapter 5)
- Understanding Android applications (Chapter 6)
- Exploiting Android applications (Chapter 7-8)
- Securing Android applications (Chapter 9)

SYLLABUS

Day 1:

The course begins with a brief introduction to mobile application security and the OWASP mobile top ten, following chapter 1 of the book. When delegates are comfortable with general mobile application security practices, we delve in to the security of the iOS platform, including an overview of the platform security features, jailbreaking and approaches to app security assessment. The following modules then review chapters 2, 3 and 4 of the book where common insecurities are covered, including but not limited too:

- Reverse engineering and patching binaries
- Insecure file storage
- Keychain attacks
- Insecure transport security
- Instrumenting the iOS runtime
- Injection attacks
- How to exploit IPC handlers
- How to defeat security controls like jailbreak detection.

Day 2:

Day two of the course picks up at chapter 6, discussing the various attack surfaces for the Android platform and how to approach an app assessment. We then walk through the details the techniques that from chapter 7 and 8 that can be used to attack Android applications, including the following topics:

- Reverse engineering and decompiling Android apps
- Insecure file storage
- Insecure transport security
- Instrumentation of the Dalvik runtime with Frida and Substrate
- Exploitation of insecure IPC endpoints
- Tap jacking.

ABOUT THE TRAINER

Dominic Chell is a director and co-founder of MDSec as well as lead author for the Mobile Application Hacker's Handbook. Dominic has delivered security consultancy and training on mobile security to leading global organisations in the financial, government and retail sectors for the past 9 years. He has previously spoken or provided training at industry leading conferences such as BlackHat, HackInTheBox, 44Con and AppSec.

RECOMMENDATIONS

- A basic knowledge of programming and mobile security concepts
- Administrative access to the laptop and the ability to install a few tools, and disable personal firewalls or virus scanners should they get in the way of the lab exercises
- We strongly recommend a personal laptop – if your corporate laptop build is too restrictive this may affect your ability to participate in the course fully
- A laptop with the capability to connect to wireless and wired networks
- The laptop should be of a reasonable specification, we recommend at least 8GB of RAM with at least 16GB of disk space free
- Students require a player to run VirtualBox images
- All delegates will be provided with a suitable iOS device to perform this section of the labs, it is not necessary to bring your own.

STUDENTS WILL BE PROVIDED WITH

- The training material in electronic format
- A mobile hacking virtual machine, packed with all the tools to perform an assessment
- Downloadable copies of the labs that they can take away and work on in the future.

Trainer	Dominic Chell
Dates	October 20-21, 2016
Level	Introduction

REGISTRATION FEES

Early Bird	$3,020	Ends July 31, 2016
Regular	$3,300	Ends August 31, 2016
Late	$3,630	Starts September 1, 2016

Prices include GST

For more information or to register click here
REGISTRATION WILL CLOSE ON OCTOBER 14, 2016