SECURE MOBILE APPLICATION DEVELOPMENT

A 2-day Black Hat USA workshop with Sense of Security

August 4-5 & August 6-7
Mandalay Bay | Las Vegas

OVERVIEW

Mobile applications are not new and are entering a state of maturity in the market and development cycles. As users shift their usage patterns towards mobile devices, it is clear that all applications developed and deployed will include a version targeting the major mobile operating systems.

With most of the logic and all controls being on the client side, they represent a shift in paradigms when it comes to security features. Where all security controls in web applications are handled and implemented on the application server and the server-side code, the mobile applications behave more like the thick clients of yore and put them in the hands of the user.

Even within mobile application development, there is significant differentiation between platforms, development toolchains, practises, security controls and features. Even the available programming languages has surged as the platforms mature. From Objective-C and Java, to native C++, Swift and Kotlin that run on the metal, to middleware layers and C#, JavaScript and Angular, development practises vary wildly.

Focusing on the logistics of development, the two major operating systems (Android and iOS) require vastly different knowledge from the developers, resulting usually in completely separate teams handling the project from end-to-end. It is not uncommon to look at the same application over different platforms and find different GUI, different features, different capabilities and different levels of maturity.

During our security reviews, we keep finding the same issues that by the time they are identified in a pen-test cost time and resources for developers to remediate or implement and code for:

- No jailbreak/root detection or weak implementation
- No SSL pinning or flawed implementation
- Local security controls bypass
- Local storage of sensitive data
- Flawed or weak crypto features

This workshop is created by pen-testers but aimed at developers who would like to learn what an attacker looks for in their application, what the usual pitfalls are, and how to create layers of controls to compensate for their code being in the public domain and in hands of the enemy. Common attacks will be demonstrated to highlight the impact, and then the participants will work together with the trainers to understand remediation options, evaluate them and improve upon them. These controls are inspired on each platform's best practice standards and by the trainers' extensive experience from pen-testing and participating in CTFs.

PRICING

EARLY

$3,600

Ends May 25

REGULAR

$3,900

Ends July 13

LATE

$4,100

Ends August 3

ON-SITE

$4,200

Ends August 9

Who should take this course?

This course is aimed at mobile application developers who are interested in security. Security professionals who are interested in the blue team aspect of mobile applications will also benefit.

Information security managers, product and development managers with developer background will gain insight as to how to structure their development and assurance processes.

Student requirements

Experience with development tools, languages and concepts on mobile devices. Basic (mobile) security concepts.

What students should bring

- Laptop with Android Studio/Android Emulator.
- For iOS sections, laptop running macos with Xcode.
- In order to get full value, physical devices rooted and jailbroken are required.
- DO NOT bring any devices that contain company information.

What students will be given

- Training slides
- Sample scripts/test cases for each section
- Tools/scripts discussed and demonstrated
- Lab configuration will be provided so you can setup in advance.
- We will provide all the materials and references needed for the event.

TRAINERS

Chris Archimandritis is an Information Security researcher and professional with over 10 years of experience. Chris is a mobile platform, mobile application and web application security expert, frequently requested to contribute to industry development and provide expert commentary. Chris has delivered Advanced VoIP Security Training at Defcon (The Art of VoIP Hacking - Defcon 23 Workshop) and is a frequent presenter of Sense of Security Training Courses, specifically for Web Application and Web Services security. Along with a Masters of Science in Information Systems, Chris is also an OSCP and general all round mobile security guru, spearheading Sense of Security's R&D program for Mobile Device and Mobile Application Security.

Panos Ainalis has over 10 years of professional experience in Information Security, working in major consulting companies in Europe, Australia and the Middle East, performing security assessments and reviews for key clients in the financial, health and telecommunication sectors as well as the public and government sector. Prior to joining Sense of Security, Panos has worked as an Information Security Assurance Officer and a team leader of penetration testing with major consulting companies performing and managing numerous network, system, web and mobile application penetration tests, wireless assessments and risk assessments for various clients around the globe. Along with an MSc in Electrical and Computer Engineering, Panos is also an OSCP and OSCE.