SEC575: iOS and Android Application Security Analysis and Penetration Testing

GMOB
Mobile Device Security Analyst
giac.org/gmob

6 Day Program | 36 CPEs | Laptop Required

Who Should Attend

- Penetration testers
- Ethical hackers
- Auditors who need to build deeper technical skills
- Security personnel whose job involves assessing, deploying or securing mobile phones and tablets
- Network and system administrators supporting mobile phones and tablets

Author Statement

The first iPhone was released in 2007, and it is considered by many to be the starting point of the smartphone era. Over the past decade, we have seen smartphones grow from rather simplistic into incredibly powerful devices with advanced features such as biometrics, facial recognition, GPS, hardware-backed encryption, and beautiful high-definition screens. While many different smartphone platforms have been developed over the years, it is quite obvious that Android and iOS have come out victorious.

While smartphones provide a solid experience right out of the box, the app ecosystem is probably the most powerful aspect of any mobile operating system. Both the Google Play and Apple App stores have countless applications that increase the usefulness of their platforms and include everything from games to financial apps, navigation, movies, music, and other offerings.

However, many smartphones also contain an incredible amount of data about both the personal and professional lives of people. Keeping those data secure should be a primary concern for both the operating system and the mobile application developer. Yet, many companies today have implemented a bring-your-own-device policy that allows smartphones onto their network. These devices are often not managed and thus bring a new set of security threats to the company.

This course will teach you about all the different aspects of mobile security, both at a high level and down into the nitty-gritty details. You will learn how to analyze mobile applications, attack smartphone devices on the network, man-in-the-middle either yourself or others, and root/jailbreak your device. You will also learn what kind of malware may pose a threat to your company and your employees.

Mobile security is a lot of fun, and I hope you will join us for this course so that we can share our enthusiasm with you!

Imagine an attack surface that is spread across your organization and in the hands of every user. It moves regularly from place to place, stores highly sensitive and critical data, and sports numerous, different wireless technologies all ripe for attack. Unfortunately, such a surface already exists today: mobile devices. These devices constitute the biggest attack surface in most organizations, yet these same organizations often don't have the skills needed to assess them.

SEC575: iOS and Android Application Security Analysis and Penetration Testing is designed to give you the skills to understand the security strengths and weaknesses of Apple iOS and Android devices, including Android 12 and iOS 15. Mobile devices are no longer a convenience technology – they are an essential tool carried or worn by users worldwide, often displacing conventional computers for everyday enterprise data needs. You can see this trend in corporations, hospitals, banks, schools, and retail stores across the world. Users rely on mobile devices today more than ever before – we know it, and the bad guys do too. SEC575 examines the full gamut of these devices.

Learn How to Pen Test the Biggest Attack Surface in Your Entire Organization

With the skills you acquire in SEC575, you will be able to evaluate the security weaknesses of built-in and third-party applications. You'll learn how to bypass platform encryption and manipulate apps to circumvent client-side security techniques. You'll leverage automated and manual mobile application analysis tools to identify deficiencies in mobile app network traffic, file system storage, and inter-app communication channels. You'll safely work with mobile malware samples to understand the data exposure and access threats affecting Android and iOS devices, and you'll learn how to bypass locked screens to exploit lost or stolen devices.

Corellium for Android and iOS Emulation

Throughout the course, students will use the innovative Corellium platform to experience iOS and Android penetration testing in a realistic environment. Corellium allows users to create virtualized iOS and Android devices with full root access even on the latest versions. By using this platform, SEC575 students can immediately test their skills right in their own browser, while still having full SSH/ADB capabilities and access to a range of powerful tools.

Take a Deep Dive into Evaluating Mobile Apps and Operating Systems and Their Associated Infrastructure

Understanding and identifying vulnerabilities and threats to mobile devices is a valuable skill, but it must be paired with the ability to communicate the associated risks. Throughout the course, you'll review ways to effectively communicate threats to key stakeholders. You'll learn how to use industry standards such as the OWASP Mobile Application Security Verification Standard (MASVS) to assess an application and understand all the risks so that you can characterize threats for managers and decision-makers.

Your Mobile Devices Are Going to Come Under Attack: Help Your Organization Prepare for the Onslaught

Mobile device deployments introduce new threats to organizations, including advanced malware, data leakage, and the disclosure to attackers of enterprise secrets, intellectual property, and personally identifiable information assets. Further complicating matters, there simply are not enough professionals with the security skills needed to identify and manage secure mobile phone and tablet deployments. By completing this course, you'll be able to differentiate yourself as someone prepared to evaluate the security of mobile devices, effectively assess and identify flaws in mobile applications, and conduct a mobile device penetration test. These are all critical skills to protect and defend mobile device deployments.

Section Descriptions

SECTION 1: iOS

The first section of SEC575 looks at the iOS platform. In examining the structure of iOS, we will see that it has many security controls built in by default, and that Apple has a very tight grip on both the hardware and software. Next, we'll scuss ways to disable different security controls by jailbreaking a device, which allows us to install various tools that can help us during our penetration tests. Since mobile devices contain a lot of sensitive information, we take a look at the internal file structure of both iOS and any installed applications in order to identify issues such as insecure storage of sensitive information, or examine interesting information to be used during a full penetration test. Of course, applications can also be attacked by other applications, which is why we will examine application interaction on iOS. Finally, we will take a look at iOS malware to see how malicious actors try to attack both the platform and the end user. Hands-on exercises will use Corellium to interact with iOS devices running in a virtualized environment, including low-level access to installed application services and application data.

TOPICS: Mobile Problems and Opportunities; iOS Architecture; Jailbreaking iOS Devices; iOS Data Storage and File System Architecture; iOS Application Interaction; iOS Malware Threats; iOS Labs

SECTION 2: Android

Android is by far the most popular mobile operating system. Devices with Android come in many shapes and sizes, which leads to a lot of fragmentation. In this course section we will take a look at Android internals and all the different security controls that are implemented to keep the user safe. In contrast to iOS, Android is open-source. It also gives developers many different ways to let their applications interact with other applications, including services, intents, broadcast receivers, and content providers. As these interactions define the attack surface of the application, we will take a close look at how they can be properly protected and exploited. Android can give us shell access through Android Debug Bridge tools, but if we really want full access, we still need to root the device by unlocking the bootloader or using a device-specific exploit. Once rooted, we will take a look at the internal file structure of both a typical Android device and installed applications to identify useful information. Finally, we will examine Android malware, which includes many different malware types such as ransomware, mobile banking Trojans, and spyware.

TOPICS: Android Architecture; Rooting Android Devices; Android Data Storage and File System Architecture; Android Application Interaction; Android Malware Threats; Android Labs; Android Platform Analysis

GMOB

Mobile Device Security Analyst
giac.org/gmob

GIAC Mobile Device Security Analyst

The GIAC Mobile Device Security Analyst (GMOB) certification ensures that people charged with protecting systems and networks know how to properly secure mobile devices that are accessing vital information. GMOB certification holders have demonstrated knowledge about assessing and managing mobile device and application security, as well as mitigating against malware and stolen devices.

- Managing Android and iOS devices and applications; jailbreaking, and rooting mobile devices
- Mitigating against mobile malware and stolen mobile devices; penetration testing mobile devices
- Analyzing applications and network activity; intercepting encrypted network traffic
- Assessing application security; manipulating mobile application behavior; static application analysis

SECTION 3: Static Application Analysis

One of the core skills you need as a mobile security analyst is the ability to evaluate the risks and threats a mobile app introduces to your organization. The lectures and hands-on exercises presented in this course section will enable you to use your analysis skills to evaluate critical mobile applications to determine the type of access threats and information disclosure threats they represent. We will use automated and manual application assessment tools to statically evaluate iOS and Android apps. Initially, the applications will be easy to understand, but towards the end of the section we will dig into obfuscated applications that are far more difficult to dissect. Finally, we will examine different kinds of application frameworks and how they can be analyzed with specialized tools.

TOPICS: Static Application Analysis; Reverse-Engineering Obfuscated Applications; Third-Party Application Frameworks

SECTION 4: Dynamic Mobile Application Analysis and Manipulation

After performing static analysis on applications in the previous course section, we now move on to dynamic analysis. A skilled analyst combines static and dynamic analysis to evaluate the security posture of an application. Using dynamic instrumentation frameworks, we see how applications can be modified at runtime, how method calls can be intercepted and modified, and how we can gain direct access to the native memory of the device. We will learn about Cycript, Frida, Objection, and method swizzling to fully instrument and examine both Android and iOS applications. The section ends with a look at a consistent system for evaluating and grading the security of mobile applications using the OWASP Mobile Application Security Verification (MASVS) Standard. By identifying these flaws, we can evaluate the mobile phone deployment risk to the organization with practical and useful risk metrics. Whether your role is to implement the penetration test or to source and evaluate the penetration tests of others, understanding these techniques will help you and your organization identify and resolve vulnerabilities before they become incidents.

TOPICS: Manipulating and Analyzing iOS Applications; Manipulating and Analyzing Android Applications; Mobile Application Security Verification Standard

SECTION 5: Penetration Testing

After analyzing the applications both statically and dynamically, one component is still left untouched: the back-end server. This course section will examine how you can perform Address Resolution Protocol spoofing attacks on a network in order to obtain a man-in-the-middle position, and how Android and iOS try to protect users from having their sensitive information intercepted. We will examine how you can set up a test device to purposely intercept the traffic in order to find vulnerabilities on the back-end server. In some engagements, we will need to access someone elses device, so we will examine whether we can break into a mobile device that's protected with a pin code or biometrics. We will end the section by creating a Remote Access Trojan (RAT) application that can be installed either on a remotely compromised device or on a physically acquired device during a red team engagement in order to target users and gain access to internal networks.

TOPICS: Intercepting TLS Traffic; Man-in-the-Middle Troubleshooting; Accessing Locked Devices; Using Mobile Device Remote Access Trojans

SECTION 6: Hands-On Capture-the-Flag Event

In this final section we will pull together all the concepts and technology covered throughout the course in a comprehensive Capture-the-Flag event. In this hands-on mobile security challenge, you will examine multiple applications and forensic images to identify weaknesses and sources of sensitive information disclosure, and analyze obfuscated malware samples to understand how they work. You'll put the skills you have learned into practice in order to evaluate systems and applications, simulating the realistic environment you will be need to protect when you get back to the office.