SEC575: Mobile Device Security and Ethical Hacking

Mobile phones and tablets have become essential to enterprise and government networks, from small organizations to Fortune 500 companies and large-scale agencies. Often, mobile phone deployments grow organically, adopted by multitudes of end-users for convenient email access as well as by managers and executives who need access to sensitive organizational resources from their favored personal mobile devices. In other cases, mobile phones and tablets have become critical systems for a wide variety of production applications from enterprise resource planning to project management. With increased reliance on these devices, organizations are quickly recognizing that mobile phones and tablets need greater security implementations than a simple screen protector and clever password.

Whether the device is an Apple iPhone or iPad, a Windows Phone, or an Android or BlackBerry phone or tablet, the ubiquitous mobile device has become a hugely attractive and vulnerable target for nefarious attackers. The use of mobile devices introduces a vast array of new risks to organizations, including:

- **Distributed sensitive data storage and access mechanisms**
- **Lack of consistent patch management and firmware updates**
- **The high probability of device loss or theft, and more**

Mobile code and apps are also introducing new avenues for malware and data leakage, exposing critical enterprise secrets, intellectual property, and personally identifiable information assets to attackers. To further complicate matters, today there simply are not enough people with the security skills needed to manage mobile phone and tablet deployments.

This course was designed to help organizations struggling with mobile device security by equipping personnel with the skills needed to design, deploy, operate, and assess a well-managed secure mobile environment. From practical policy development to network architecture design and deployment, and from mobile code analysis to penetration testing and ethical hacking, this course will help you build the critical skills necessary to support the secure deployment and use of mobile phones and tablets in your organization.

You will gain hands-on experience in designing a secure mobile phone network for local and remote users and learn how to make critical decisions to support devices effectively and securely. You will also be able to analyze and evaluate mobile software threats, and learn how attackers exploit mobile phone weaknesses so you can test the security of your own deployment. With these skills, you will be a valued mobile device security analyst, fully able to guide your organization through the challenges of securely deploying mobile devices.

giac.org

sans.edu

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

You Will Be Able To

- Develop effective policies to control employee-owned (Bring Your Own Device, BYOD) and enterprise-owned mobile devices, including the enforcement of effective passcode policies and permitted application
- Utilize jailbreak tools for Apple iOS and Android systems such as redsn0w & Absinthe
- Conduct an analysis of iOS and Android filesystem data using SqliteSpy, Plist Editor, and AXMLPrinter to plunder compromised devices and extract sensitive mobile device use information such as the SMS history, browser history, GPS history, and user dictionary keywords
- Analyze Apple iOS and Android applications with reverse-engineering tools including class-dump, JD-GUI, dextranslator, and apktool to identify malware and information leakage threats in mobile applications
- Conduct an automated security assessment of mobile applications using iAuditor, Cycript, MobileSubstrate, TaintDroid, and DroidBox to identify security flaws in mobile applications
- Use wireless network analysis tools to identify and exploit wireless networks, crack WEP and WPA/WPA2 access points, bypass enterprise wireless network authentication requirements, and harvest user credentials
- Intercept and manipulate mobile device network activity using Burp to manipulate the actions taken by a user in an application and to deliver mobile device exploits to vulnerable devices

"With the mad rush towards mobile device adoption at the point of sale and industry regulations and laws struggling to keep up, thank goodness SANS helps companies maintain secure operations."
-Dean Altman, Discount Tire

575.1 HANDS ON: Mobile Device Threats, Policies, and Security Models

The first part of the course looks at the significant threats affecting mobile phone deployment and how organizations are being attacked through these systems. As a critical component of a secure deployment, we guide you through the process of defining mobile phone and tablet policies with sample policy language and recommendations for various vertical industries, taking into consideration the legal obligations of enterprise organizations. We'll also look at the architecture and technology behind mobile device infrastructure systems for Apple, Android, BlackBerry, and Windows devices, as well as the platform-specific security controls available, including device encryption, remote data wipe, application sandboxing, and more.

Topics: Mobile Phone and Tablet Problems and Opportunities; Mobile Devices and Infrastructure; Mobile Phone and Tablet Security Models; Legal Aspects of Mobile; Mobile Device Policy Considerations and Development

575.2 HANDS ON: Mobile Device Architecture Security & Management

With an understanding of the threats, architectural components and desired security methods, we can design and implement device and infrastructure systems to defend against these threats. In this part of the course, we'll examine the design and deployment of network and system infrastructure to support a mobile phone deployment including the selection and deployment of Mobile Device Management (MDM) systems.

Topics: Wireless Network Infrastructure; Remote Access Systems; Certificate Deployment Systems; Mobile Device Management (MDM) System Architecture; Mobile Device Management (MDM) Selection

575.3 HANDS ON: Mobile Code and Application Analysis

With the solid analysis skills taught in this section of the course, we can evaluate apps to determine the type of access and information disclosure threats that they represent. Security professionals can use these skills not only to determine which outside applications the organization should allow, but also to evaluate the security of any apps developed by the organization itself for its employees or customers. In this process, we'll use jailbreaking and other techniques to evaluate the data stored on mobile phones.

Topics: Unlocking, Rooting, and Jailbreaking Mobile Devices; Mobile Phone Data Storage and Filesystem Architecture; Filesystem Application Modeling; Network Activity Monitoring; Mobile Code and Application Analysis; Approving or Disapproving Applications in Your Organization

575.4 HANDS ON: Ethical Hacking Mobile Networks

Through ethical hacking and penetration testing, we examine the mobile devices and infrastructure from the perspective of an attacker, identifying and exploiting flaws that could allow unauthorized access to data or supporting networks. By identifying and understanding the implications of these flaws, we can evaluate the mobile phone deployment risk to the organization with practical, useful risk metrics.

Topics: Fingerprinting Mobile Devices; WiFi Attacks; Bluetooth Attacks; Network Exploits

575.5 HANDS ON: Ethical Hacking Mobile Phones, Tablets, and Applications

Continuing our look at ethical hacking and penetration testing, we turn our focus to exploiting weaknesses on individual mobile devices including, iPhones, iPads, Android phones, Windows Phones and BlackBerry phones and tablets. We'll also examine platform-specific application weaknesses and look at the growing use of web framework attacks.

Topics: Mobile Device Exploits; Web Framework Attacks; Application Attacks; Cloud/Remote Data Accessibility Attacks

575.6 HANDS ON: Secure Mobile Phone Capture the Flag

On the last day of class, we apply the skills, concepts, and technology covered in the course for a comprehensive Capture the Flag event.
In this day-long, in-depth hands-on exercise, you will:

- Have the option to participate in multiple organizational roles related to mobile device security
- Design a secure infrastructure for the deployment of mobile phones
- Monitor network activity to identify attacks against mobile devices
- Extract sensitive data from a compromised iPad
- Attack a variety of mobile phones and related network infrastructure components.

In the exercise, you will use the skills built throughout the course to evaluate real-world systems and defend against attackers, simulating the realistic environment you'll face when you get back to the office. You will leave the course armed with the knowledge and skills you'll need to securely integrate and deploy mobile devices in your organization.

SEC575 COIN

SEC575 Training Formats

(subject to change)

Live Training
sans.org/security-training/by-location/all

OnSite
sans.org/onsite

vLive
sans.org/vlive

Simulcast
sans.org/simulcast

OnDemand
sans.org/ondemand

SelStudy
sans.org/selfstudy

"SEC575 offers invaluable material. [Course Instructor's] energy and enthusiasm are incomparable!"
-Randy Pauli, Chelan County PUD