SECURING MOBILE DEVICES IN THE ENTERPRISE

Course Code: 7336

In this course, you will learn about a methodical and practical approach to enterprise device security.

The ongoing proliferation of mobile devices has caused us to rethink the way we implement enterprise security. Mobile devices don't run corporate operating systems. They can go anywhere, they have heterogeneous and ubiquitous network access, and they may not be owned or managed by the enterprise themselves. In this course, you will learn about a methodical and practical approach to enterprise device security that considers all these factors.

What You’ll Learn

• Mobile Security Threats
• Mobile Security Technologies
• Mobile Security Threat Mitigation
• Configuring Enterprise-level Security

Who Needs to Attend

Enterprise network engineers and managers; network security engineers and managers; anyone tasked with providing secure access to company resources from mobile devices.
SECURING MOBILE DEVICES IN THE ENTERPRISE

Course Code: 7336

ON-DEMAND $395 USD

On-Demand Outline

Securing Mobile Devices in the Enterprise: Mobile Security Threats

- Describe current mobile devices and form factors
- Describe the current state of mobile device security
- Describe mobile security considerations
- Describe the process to determine risk in a mobile environment
- Describe sensitive mobile assets
- Describe sensitive usage scenarios for mobile devices
- Describe how mobile data is stored and transported
- List the OWASP top 1 mobile risks, and describe how weak server-side controls affect mobile device back-end systems
- Describe how insecure data storage affects mobile device front-end and back-end systems
- Describe how insufficient transport layer protection affects mobile device front-end and back-end systems
- Describe how unintended data leakage affects mobile device front-end and back-end systems
- Describe how poor authorization and authentication affects mobile device front-end and back-end systems
- Describe how broken cryptography affects mobile device front-end and back-end systems
- Describe how client-side injection affects mobile device front-end systems
- Describe how security decisions via untrusted inputs affect mobile device back-end systems
- Describe how improper session handling affects mobile device front-end systems
- Describe how lack of binary protections affects mobile device front-end systems
• Describe the potential technical impacts of mobile exploits
• Describe the potential business impacts of mobile exploits
• Describe requirements for secure device data handling
• Describe requirements for secure device authorization and authentication
• Describe requirements for secure device sensors, jailbreaking, and mobile device management systems
• Describe requirements for secure device connectivity and apps
• Describe requirements for users of secure devices
• Assess threats from OWASP top 1 and their impact on mobile systems

Securing Mobile Devices in the Enterprise: Mobile Security Technologies
• Describe usage scenarios for cryptography
• Describe the theory of one-way cryptographic functions and hashes
• Describe hashing and identify the main hashing algorithms
• Perform hashing using Windows PowerShell
• Describe symmetric encryption
• Describe asymmetric encryption and its common uses
• Encrypt and decrypt a message using OpenSSL
• Encrypt and decrypt a message using OpenSSL
• Describe digital signing
• Describe digital signing
• Perform digital signing using OpenSSL
• Perform digital signing using OpenSSL
• Describe key distribution in cryptographic systems
• Describe key distribution in cryptographic systems
• Describe digital certificates and the process of issuing certificates in a CA system
• Describe digital certificates and the process of issuing certificates in a CA system
• Create a certificate in Visual Studio makecert
• Create a certificate in Visual Studio makecert
• Describe requirements for back-end security for mobile applications
• Describe measures to harden services for mobile applications
• Describe requirements for securing app mobile app deployment
• Describe measures to protect mobile apps at the transport layer
• Describe measures to protect mobile apps at the transport layer
• Describe infrastructure security requirements to support secure mobile apps
• Describe the architecture of a demilitarized zone to protect mobile app services
• Describe the use of a reverse proxy in protecting mobile app back-end services
• Describe processes for securing directory services and certificate authorities used in mobile app back-end systems
• Describe the use of S/MIME to secure e-mail in the enterprise
• Describe the use of rights management systems to secure document content
• Describe measures to protect data in transit and at rest
• Describe the use of mobile device management systems to fully manage
Secure mobile devices
- Describe threats to back-end systems, and strategies to mitigate them

Securing Mobile Devices in the Enterprise: Mobile Security Threat Mitigation
- Describe the requirements for establishing a mobile enterprise
- Describe mobile device ownership models and how they relate to a coherent mobile threat mitigation strategy
- Describe mitigation strategies for unmanaged devices in a small organization
- Describe mitigation strategies for unmanaged company-owned devices
- Describe appropriate user policies for risk mitigation with unmanaged devices
- Configure security settings on unmanaged Android devices
- Configure security settings on unmanaged Windows Phone devices
- Describe requirements for secure cloud storage
- Use Boxcryptor to encrypt and secure cloud data
- Describe Microsoft Exchange ActiveSync functionality for managing mobile devices
- Configure Office 365 Exchange ActiveSync to manage mobile devices
- Describe challenges with transport layer security, and how they can be solved with short-lived session keys and perfect forward secrecy
- Configure perfect forward secrecy in Internet Information Services
- Describe virtual private networks for securing network connections
- Connect a mobile device to a VPN server
- Describe BYOD containers for segregating data on BYOD devices
- Describe usage scenarios for BYOD containers
- Configure BYOD containers using Good Work
- Describe security functionality offered by app wrapper technologies for mobile devices
- Describe methods to mitigate malicious functionality in mobile apps
- Describe methods to mitigate code vulnerabilities in mobile apps
- Describe Microsoft Azure Rights Management cloud-based rights management system
- Configure Microsoft Azure Rights Management System to protect confidential documents
- Describe mitigation strategies for BYOD and COD devices in the enterprise
Securing Mobile Devices in the Enterprise: Configuring Enterprise-level Security

- Describe network architecture challenges for securing enterprise mobile devices
- Describe a solution for enterprise mobile device security challenges based on Microsoft’s product portfolio
- Create an account for Microsoft Intune
- Navigate the Microsoft Intune interface
- Enroll devices in Microsoft Intune
- Target devices in Microsoft Intune
- Enforce configurations in Microsoft Intune
- Enforce configurations in Microsoft Intune
- Handle certificates in Microsoft Intune
- Deploy enterprise profiles in Microsoft Intune
- Distribute apps in Microsoft Intune
- Protect data in Microsoft Intune
- Describe Microsoft System Center Configuration Manager and Intune interoperability
- Configure the Microsoft Intune Connector Role
- Prepare for Windows Mobile device enrollment in Microsoft System Center Configuration Manager
- Prepare for iOS device enrollment in Microsoft System Center Configuration Manager
- Create an account on Microsoft Intune, enroll devices, and deploy enterprise profiles

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 7/29/2020 3:12:00 AM
Copyright © 2020 Global Knowledge Training LLC. All Rights Reserved.