Application Security for Android

Duration: 5 days Price: € 3299

Open Schedule

Audience Course Application Security for Android

The course Application Security for Android is intended for IT professionals who want to learn how to protect Android mobile apps against the many security risks.

Prerequisites Course Application Security for Android

To participate in this course, affinity with the development of mobile apps is required. Experience with software development helps in understanding the subject matter but is not required.

Realization Training Application Security for Android

The course Application Security for Android has a hands-on character. The theory is treated on the basis of presentation slides and is interchanged with practical exercises.

Certification Course Application Security for Android

After successfully participating in the training, the attendants receive a certificate of completion in Application Security for Android.

Content Course Application Security for Android

The course Application Security for Android covers how the Android operating system and mobile apps on Android can best be secured. Attention is paid to the Google Security Services, the security architecture of the Android platform and kernel and application security. The training also discusses the implementation of security and the reporting of security issues.

Intro Security

The course Application Security for Android starts with an explanation of important security concepts such as authentication, encryption, data resilience, backup, recovery, confidentiality, integrity and access control.

Google Security Services

Next the Security Services offered by Google are discussed, such as App Services, Safety Net Attestation, Google Play, Penetration Testing and the Android Device Manager.

Platform Security Architecture

Attention is also paid to the Android Platform Architecture that provides protection for Apps, User Data, Networking and Inter Process Communication. App Signing and App and User Permissions are also covered.

Kernel Security

Part of the program of the Application Security for Android course is also a discussion of kernel security that is based on Linux. This includes paying attention to the application sandbox, safe mode, filesystem permissions, storage encryption and the verified boot.

Application Security

Next application security is discussed with a focus on the Android Permission Model for accessing Protected APIs, working with content providers, Sensitive Data Input Devices and Application Signing.

Implementing Security

Attention is also paid to the implementation of security in Android. That security is promoted by code reviews, the use of Android Lint and data logging. Also securing SUID files and configuration files and limiting directory and device driver access is treated.

Security Updates and Reports

Finally the importance of security updates, the reporting of security issues and the triaging of bugs are discussed. Key issues from Android Reports and White Papers from recent years are also reviewed.

Modules Course Application Security for Android

Module 1 : Intro Security	Module 2 : Google Security Services	Module 3 : Platform Security Architecture
Access Controls Authentication Backups and Recovery Data Erasure Data Masking Data Resiliency Encryption Confidentiality Integrity	Google Play Android Updates App Services Verify Apps Safety Net Safety Net Attestation Android Device Manager Penetration Testing Incident Response	App Protection Protecting User Data Protecting System Resources Network Protection Mandatory App Sandbox Secure Inter Process Communication App Signing App Defined Permissions User Granted Permissions
Module 4 : Kernel Security	**Module 5 : Application Security**	**Module 6 : Implementing Security**
Linux Security Application Sandbox System Partition and Safe Mode Filesystem Permissions Verified Boot Cryptography Rooting of Devices Storage Encryption Lockscreen Credential Protection Device Administration	Android Permission Model Accessing Protected API's Binder, Services, Intent Content Providers Cost Sensitive API's SIM Card Access Sensitive Data Input Devices Device Metadata Certificate Authorities Application Signing	Reviewing Source Code Android Lint Signing System Images Signing applications (APKs) Isolating Processes Securing SUID files Logging Data Limiting Directory Access Securing Configuration Files Limiting Device Driver Access
Module 7 : Security Updates	**Module 8 : Security Reports**	
Reporting Security Issues Triaging Bugs Context Types Rating Modifiers Local, Proximal, Remote Network Security Biometric Authentication Android Automotive OS Releasing code to AOSP Receiving Android Updates Updating Google Services	Annual Reviews 2014 Report 2015 Report 2016 Report 2017 Report 2018 Report White Papers 2018 White Paper 2019 White Paper 2020 While Paper 2021 White Paper	

SpiralTrain BV
Standerdmolen 10, 2e verdieping
3995 AA Houten

info@spiraltrain.nl
www.spiraltrain.nl
Tel.: +31 (0) 30 – 737 0661

Locations
Houten, Amsterdam, Rotterdam, Eindhoven, Zwolle, Online