Sicherheit in Android und iOS

David Artmann Kristoffer Schneider

Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

10. November 2015

Gliederung

Trusted Execution Environment

Pro App ein Linux-Nutzer

Isolation durch Kernel

Secure Enclave

Secure boot chain

Alle Apps ein Unix-Nutzer

Sandbox pro App aufgesetzt

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Linux-Nutzer

Isolation durch Kernel

Sandbox pro App via Daten

Trusted Execution Environment

Secure Enclave

Trusted Execution Environment

Secure Enclave

Trusted Execution Environment

Secure Enclave

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Linux-Nutzer

Isolation durch Kernel

Sandbox pro App via Profil

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Isolation durch Kernel

Alle Apps ein Linux-Nutzer

Sandbox pro App-Gruppe

Trusted Execution Environment

Secure Enclave

Secure boot chain

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Trusted Execution Environment	Secure Enclave
Secure boot chain	
Pro App ein Linux-Nutzer	Alle Apps ein Unix-Nutzer
Isolation durch Kernel	Sandbox pro App definiert

Trusted Execution Environment

Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Alle Apps ein Unix-Nutzer

Isolation durch Kernel

Sandbox pro App definiert

Gliederung

iOS bis Android M granularer

Abhilfe durch AppOps (<=4.4.2) oder XPrivacy (>=4.0.3 && <=5.1.1)

Mit iOS 9 und Android M gleichauf

iOS bis Android M granularer

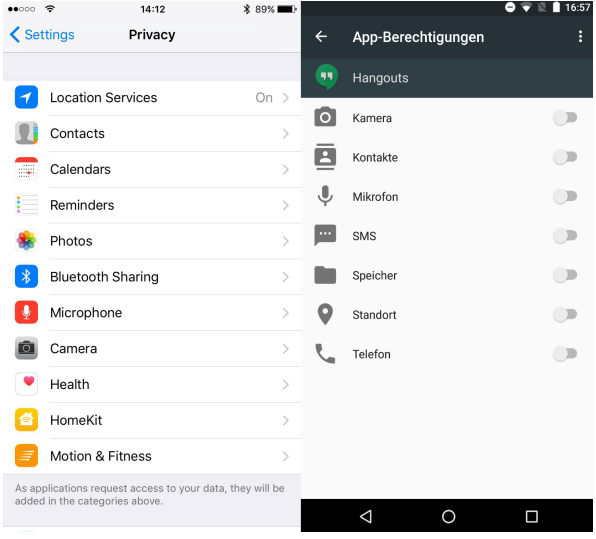
Abhilfe durch AppOps (<=4.4.2) oder XPrivacy (>=4.0.3 && <=5.1.1)

Mit iOS 9 und Android M gleichauf

iOS bis Android M granularer

Abhilfe durch AppOps (<=4.4.2) oder XPrivacy (>=4.0.3 && <=5.1.1)

Mit iOS 9 und Android M gleichauf


14:12
89%
Settings
Privacy
Location Services
On
Contacts
Calendars
Reminders
Photos
Bluetooth Sharing
Microphone
Camera
Health
HomeKit
Motion & Fitness
As applications request access to your data, they will be added in the categories above.
16:57
App-Berechtigungen
Hangouts
Kamera
Kontakte
Mikrofon
SMS
Speicher
Standort
Telefon

Gliederung

iOS nur über Apple's App Store

iOS nur über Apple's App Store 

iOS nur über Apple's App Store 

Android bietet diverse

iOS nur über Apple's App Store 

Android bietet diverse 

iOS nur über Apple's App Store 

Android bietet diverse  

iOS nur über Apple's App Store 

Android bietet diverse   

Gliederung

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3 und mp4 Dateien
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3 und mp4 Dateien
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3 und mp4 Dateien
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3 und mp4 Dateien
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3 und mp4 Dateien
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Gliederung

XcodeGhost (Q3 2015)

- Compiler der Xcode IDE überprüft keine externen Bibliotheken
- Sources aus inoffiziellen Kanälen (FW der Regierung)
- Daten wurden an C&C-Server des Autors versandt
- Ungenügende Signaturprüfung von GateKeeper wurde ausgenutzt
- XcodeGhost S für iOS 9 entwickelt (Q4 2015)

XcodeGhost (Q3 2015)

- Compiler der Xcode IDE überprüft keine externen Bibliotheken
- Sources aus inoffiziellen Kanälen (FW der Regierung)
- Daten wurden an C&C-Server des Autors versandt
- Ungenügende Signaturprüfung von GateKeeper wurde ausgenutzt
- XcodeGhost S für iOS 9 entwickelt (Q4 2015)

XcodeGhost (Q3 2015)

- Compiler der Xcode IDE überprüft keine externen Bibliotheken
- Sources aus inoffiziellen Kanälen (FW der Regierung)
- Daten wurden an C&C-Server des Autors versandt
- Ungenügende Signaturprüfung von GateKeeper wurde ausgenutzt
- XcodeGhost S für iOS 9 entwickelt (Q4 2015)

XcodeGhost (Q3 2015)

- Compiler der Xcode IDE überprüft keine externen Bibliotheken
- Sources aus inoffiziellen Kanälen (FW der Regierung)
- Daten wurden an C&C-Server des Autors versandt
- Ungenügende Signaturprüfung von GateKeeper wurde ausgenutzt
- XcodeGhost S für iOS 9 entwickelt (Q4 2015)

XcodeGhost (Q3 2015)

- Compiler der Xcode IDE überprüft keine externen Bibliotheken
- Sources aus inoffiziellen Kanälen (FW der Regierung)
- Daten wurden an C&C-Server des Autors versandt
- Ungenügende Signaturprüfung von GateKeeper wurde ausgenutzt
- XcodeGhost S für iOS 9 entwickelt (Q4 2015)

Gliederung

Ratschläge für Entwickler

- Passwortrichtlinie
- Sicherung des Hauptschlüssels
- Lokations- und Tempusberücksichtigung
- Bipartite Schlüssel
- Manipulationsschutz

Ratschläge für Entwickler

- Passwortrichtlinie
- Sicherung des Hauptschlüssels
- Lokations- und Tempusberücksichtigung
- Bipartite Schlüssel
- Manipulationsschutz

Ratschläge für Entwickler

- Passwortrichtlinie
- Sicherung des Hauptschlüssels
- Lokations- und Tempusberücksichtigung
- Bipartite Schlüssel
- Manipulationsschutz

Ratschläge für Entwickler

- Passwortrichtlinie
- Sicherung des Hauptschlüssels
- Lokations- und Tempusberücksichtigung
- Bipartite Schlüssel
- Manipulationsschutz

Ratschläge für Entwickler

- Passwortrichtlinie
- Sicherung des Hauptschlüssels
- Lokations- und Tempusberücksichtigung
- Bipartite Schlüssel
- Manipulationsschutz

Gliederung

Tips für Endnutzer

- Lockscreen nutzen und konfigurieren
- Zwei-Faktor-Authentifizierung
- Privacy Einstellungen

Tips für Endnutzer

- Lockscreen nutzen und konfigurieren
- Zwei-Faktor-Authentifizierung
- Privacy Einstellungen

Tips für Endnutzer

- Lockscreen nutzen und konfigurieren
- Zwei-Faktor-Authentifizierung
- Privacy Einstellungen