Sicherheit in Android und iOS

David Artmann[1] Kristoffer Schneider[1]

[1]Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

8. Oktober 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-Gruppe

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-Gruppe

Trusted Execution Environment

Secure Enclave

Secure boot chain

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

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

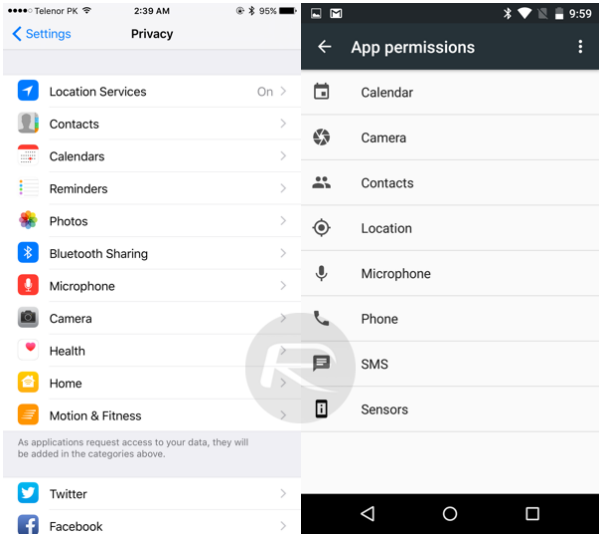
- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)

App-Berechtigungen

- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Distribution

- iOS nur über Apple's App Store
- Android bietet diverse (Google Play, F-Droid, Amazon App-Shop)


Telenor PK
2:39 AM
95%
Settings
Privacy
Location Services
On
Contacts
Calendars
Reminders
Photos
Bluetooth Sharing
Microphone
Camera
Health
Home
Motion & Fitness
As applications request access to your data, they will be added in the categories above.
Twitter
Facebook
9:59
App permissions
Calendar
Camera
Contacts
Location
Microphone
Phone
SMS
Sensors

Stagefright (2015)

- Sicherheitslücken in mehreren Bibliotheken (libstagefright, libutils)
- Betrifft ca. 95% aller Android Geräte
- Manipulierte mp3s und mp4s
- 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 mp3s und mp4s
- 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 mp3s und mp4s
- 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 mp3s und mp4s
- 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 mp3s und mp4s
- Remote Code Execution mit Rechten der Library möglich
- Erste Patches wurden ausgeliefert

Exynos-Exploit (2012)

Sicherheitslücke im Kernel von Android Geräten von Samsung

/dev/exynos-mem ist für **alle** Nutzer nutzbar!

Enthält den kompletten physikalischen RAM

Folgen: RAM Dump, Code Injection, Rooting, etc. möglich

Exynos-Exploit (2012)

Sicherheitslücke im Kernel von Android Geräten von Samsung

/dev/exynos-mem ist für **alle** Nutzer nutzbar!

Enthält den kompletten physikalischen RAM

Folgen: RAM Dump, Code Injection, Rooting, etc. möglich

Exynos-Exploit (2012)

Sicherheitslücke im Kernel von Android Geräten von Samsung

/dev/exynos-mem ist für **alle** Nutzer nutzbar!

Enthält den kompletten physikalischen RAM

Folgen: RAM Dump, Code Injection, Rooting, etc. möglich

Exynos-Exploit (2012)

Sicherheitslücke im Kernel von Android Geräten von Samsung

/dev/exynos-mem ist für **alle** Nutzer nutzbar!

Enthält den kompletten physikalischen RAM

Folgen: RAM Dump, Code Injection, Rooting, etc. möglich

No iOS Zone (2014)

`https://www.youtube.com/watch?v=i2tYdmOQisA`

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Fehler im Parser für SSL-Zertifikate

Behoben mit iOS 8.3

No iOS Zone (2014)

`https://www.youtube.com/watch?v=i2tYdmOQisA`

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Fehler im Parser für SSL-Zertifikate

Behoben mit iOS 8.3

No iOS Zone (2014)

`https://www.youtube.com/watch?v=i2tYdmOQisA`

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Fehler im Parser für SSL-Zertifikate

Behoben mit iOS 8.3

No iOS Zone (2014)

`https://www.youtube.com/watch?v=i2tYdmOQisA`

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Fehler im Parser für SSL-Zertifikate

Behoben mit iOS 8.3

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

GateKeeper würde durch Codesignaturprüfung ausführen von Xcode verhindern

Sandbox weiterhin aktiv (legitimes Verhalten!)

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
- GateKeeper würde durch Codesignaturprüfung ausführen von Xcode verhindern
- Sandbox weiterhin aktiv (legitimes Verhalten!)

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
- GateKeeper würde durch Codesignaturprüfung ausführen von Xcode verhindern
- Sandbox weiterhin aktiv (legitimes Verhalten!)

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
- GateKeeper würde durch Codesignaturprüfung ausführen von Xcode verhindern
- Sandbox weiterhin aktiv (legitimes Verhalten!)

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
- GateKeeper würde durch Codesignaturprüfung ausführen von Xcode verhindern
- Sandbox weiterhin aktiv (legitimes Verhalten!)

AirDrop Exploit (Q3 2015)

Schadcodeverteilung über AirDrop (iOS 7 - 8.4.1, OS X >= Yosemite)

Über directory traversal Angriff wird Payload auch bei Ablehnung der Daten geschrieben

Apps über Developer Enterprise Program signiert -> kein AppStore!

„Trust-prompt“ lässt sich durch enterprise provisioning profile unterdrücken

AirDrop Exploit (Q3 2015)

Schadcodeverteilung über AirDrop (iOS 7 - 8.4.1, OS X >= Yosemite)

Über directory traversal Angriff wird Payload auch bei Ablehnung der Daten geschrieben

Apps über Developer Enterprise Program signiert -> kein AppStore!

„Trust-prompt“ lässt sich durch enterprise provisioning profile unterdrücken

AirDrop Exploit (Q3 2015)

Schadcodeverteilung über AirDrop (iOS 7 - 8.4.1, OS X >= Yosemite)

Über directory traversal Angriff wird Payload auch bei Ablehnung der Daten geschrieben

Apps über Developer Enterprise Program signiert -> kein AppStore!

„Trust-prompt“ lässt sich durch enterprise provisioning profile unterdrücken

AirDrop Exploit (Q3 2015)

Schadcodeverteilung über AirDrop (iOS 7 - 8.4.1, OS X >= Yosemite)

Über directory traversal Angriff wird Payload auch bei Ablehnung der Daten geschrieben

Apps über Developer Enterprise Program signiert -> kein AppStore!

„Trust-prompt“ lässt sich durch enterprise provisioning profile unterdrücken