

Sicherheit in Android und iOS

David Artmann¹ Kristoffer Schneider¹

¹Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

7. Oktober 2015

Gliederung



Trusted Execution Environment



Secure Enclave

Secure boot chain

Pro Apps ein Linux-Nutzer

Alle Apps ein Linux-Nutzer

Isolation durch Namespaces

Sandbox pro App definiert



Trusted Execution Environment



Secure Enclave

Secure boot chain

Pro Apps ein Linux-Nutzer

Alle Apps ein Linux-Nutzer

Isolation durch Namespaces

Sandbox pro App definiert



Trusted Execution Environment



Secure Enclave

Secure boot chain

All Apps are Linux binaries

All Apps are Universal binaries

Sanction third parties

Sanction pro App developers



Trusted Execution Environment



Secure Enclave

Secure boot chain

All Apps are Linux binaries

Secure boot chain

All Apps are Linux binaries

Secure boot chain



Trusted Execution Environment



Secure Enclave



Trusted Execution Environment



Secure Enclave

Secure boot chain

All Apps are Linux-User

All Apps are Linux-User

Secure boot chain

Secure boot chain



Trusted Execution Environment



Secure Enclave

Secure boot chain

Android app and Linux kernel

Android app and Linux kernel

Android app and Linux kernel

Android app and Linux kernel

Android app and Linux kernel

Android app and Linux kernel



Trusted Execution Environment



Secure Enclave

Secure boot chain



Trusted Execution Environment



Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Isolation durch Kernel

Alle Apps ein Unix-Nutzer

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

Pro App ein Linux-Nutzer

Isolation durch Kernel



Secure Enclave

Secure boot chain

Alle Apps ein Unix-Nutzer

Sandbox pro App definiert



Trusted Execution Environment



Secure Enclave

Secure boot chain

Pro App ein Linux-Nutzer

Isolation durch Kernel

Alle Apps ein Unix-Nutzer

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)

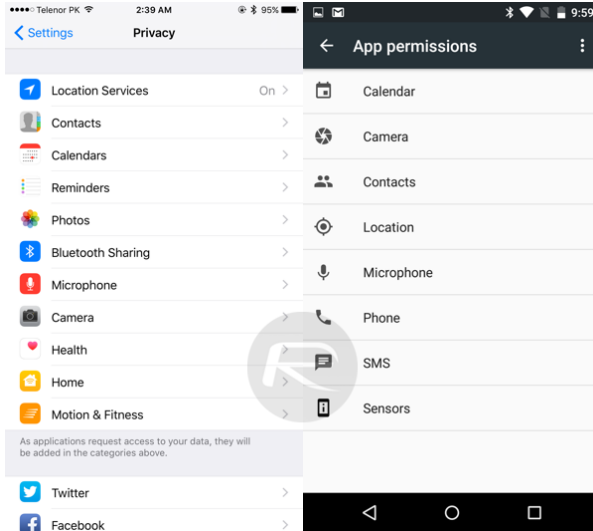


App-Berechtigungen

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)



Stagefright

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