Sicherheit in Android und iOS

David Artmann[1] Kristoffer Schneider[1]

[1]Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

30. Juni 2015

Gliederung

Gliederung

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Gliederung

App-Berechtigungen

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

App-Berechtigungen

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

App-Berechtigungen

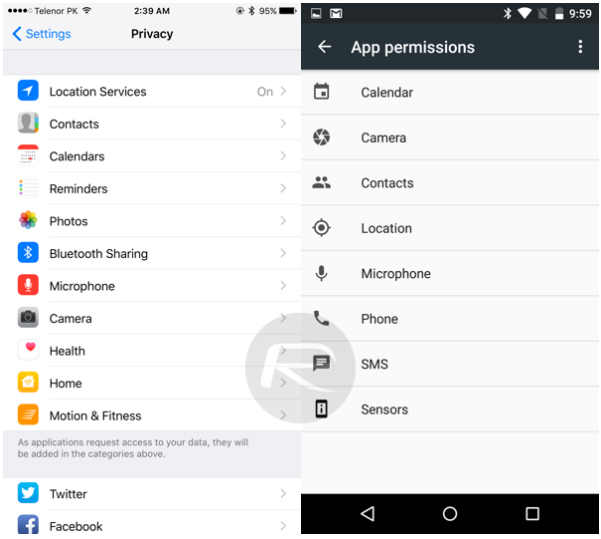
- iOS bis Android M granularer
- Zeitweise Abhilfe durch AppOps
- Mit iOS 9 und Android M gleichauf

App-Berechtigungen

iOS bis Android M granularer

Zeitweise Abhilfe durch AppOps

Mit iOS 9 und Android M gleichauf


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

Gliederung

freie Modifikation

dezentrale Updatepolitik

offener Quelltext

einheitliche Konfiguration

zentrale Updateregelung

geschlossener Quelltext

freie Modifikation

dezentrale Updatepolitik

offener Quelltext

einheitliche Konfiguration

zentrale Updateregelung

geschlossener Quelltext

freie Modifikation

dezentrale Updatepolitik

offener Quelltext

einheitliche Konfiguration

zentrale Updateregelung

geschlossener Quelltext

freie Modifikation

dezentrale Updatepolitik

offener Quelltext

einheitliche Konfiguration

zentrale Updateregelung

geschlossener Quelltext

- freie Modifikation
- dezentrale Updatepolitik
- offener Quelltext

- einheitliche Konfiguration
- zentrale Updateregelung
- geschlossener Quelltext

- freie Modifikation
- dezentrale Updatepolitik
- offener Quelltext

- einheitliche Konfiguration
- zentrale Updateregelung
- geschlossener Quelltext

- freie Modifikation
- dezentrale Updatepolitik
- offener Quelltext

- einheitliche Konfiguration
- zentrale Updateregelung
- geschlossener Quelltext

- freie Modifikation
- dezentrale Updatepolitik
- offener Quelltext

- einheitliche Konfiguration
- zentrale Updateregelung
- geschlossener Quelltext

- freie Modifikation
- dezentrale Updatepolitik
- offener Quelltext

- einheitliche Konfiguration
- zentrale Updateregelung
- geschlossener Quelltext

Gliederung

Verteilte Entwicklung bei Herstellern und privaten Gruppen

Intransparenz durch die Verteilte Entwicklung

Die Update-Problematik

Weitere Modifikationen durch Rooting

- Verteilte Entwicklung bei Herstellern und privaten Gruppen
- Intransparenz durch die Verteilte Entwicklung
- Die Update-Problematik
- Weitere Modifikationen durch Rooting

- Verteilte Entwicklung bei Herstellern und privaten Gruppen
- Intransparenz durch die Verteilte Entwicklung
- Die Update-Problematik
- Weitere Modifikationen durch Rooting

- Verteilte Entwicklung bei Herstellern und privaten Gruppen
- Intransparenz durch die Verteilte Entwicklung
- Die Update-Problematik
- Weitere Modifikationen durch Rooting

Rooting von Androidsystemen

- Möglich durch Exploits oder spezielle Builds
- Gefährdung des Sicherheitssystems
- Schwer zu kontrollieren für Nutzer und Entwickler

Rooting von Androidsystemen

- Möglich durch Exploits oder spezielle Builds
- Gefährdung des Sicherheitssystems
- Schwer zu kontrollieren für Nutzer und Entwickler

Rooting von Androidsystemen

- Möglich durch Exploits oder spezielle Builds
- Gefährdung des Sicherheitssystems
- Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

- Möglich durch Exploits oder spezielle Builds
- Gefährdung des Sicherheitssystems
- Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke
Der Exploit

- Wurde von alephzain, des XDA-Forums entdeckt
- Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)
- Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich
- Fahrlässige Berechtigungsvergabe für /dev/exynos-mem
- Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke
Der Exploit

- Wurde von alephzain, des XDA-Forums entdeckt
- Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)
- Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich
- Fahrlässige Berechtigungsvergabe für /dev/exynos-mem
- Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke
Der Exploit

- Wurde von alephzain, des XDA-Forums entdeckt
- Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)
- Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich
- Fahrlässige Berechtigungsvergabe für /dev/exynos-mem
- Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke
Der Exploit

- Wurde von alephzain, des XDA-Forums entdeckt
- Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)
- Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich
- Fahrlässige Berechtigungsvergabe für /dev/exynos-mem
- Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke
Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Hersteller und proprietäre Apps

- Nur schwer zu kontrollieren
- Erweiterte Rechte durch Herstellerzertifikate
- Beispiel: Google Settings

Hersteller und proprietäre Apps

Nur schwer zu kontrollieren

Erweiterte Rechte durch Herstellerzertifikate

Beispiel: Google Settings

Hersteller und proprietäre Apps

- Nur schwer zu kontrollieren
- Erweiterte Rechte durch Herstellerzertifikate
- Beispiel: Google Settings

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten vorinstalliert

Dient zur Synchronisation mit dem Google-Account

Installation durch Google möglich

Weitere versteckte Funktionen?

Gliederung

Produktion HW/SW im eigenen Haus

Ungewissheit durch Proprietät

Umgehen dieser Politik durch Jailbreaking

Produktion HW/SW im eigenen Haus

Ungewissheit durch Proprietät

Umgehen dieser Politik durch Jailbreaking

Produktion HW/SW im eigenen Haus

Ungewissheit durch Proprietät

Umgehen dieser Politik durch Jailbreaking

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013
Nach Zdziarski's Paper

- lockdownd
- com.apple.mobile.pcapd
- com.apple.mobile.file_relay
- com.apple.mobile.house_arrest

lockdownd

- Ermöglicht Zugriff über TCP Port 62078
- Abarbeitung über eigenes Protokoll *usbmux*
- Übergebene Portnummer auf localhost

lockdownd

Ermöglicht Zugriff über TCP Port 62078

Abarbeitung über eigenes Protokoll *usbmux*

Übergebene Portnummer auf localhost

lockdownd

Ermöglicht Zugriff über TCP Port 62078

Abarbeitung über eigenes Protokoll *usbmux*

Übergebene Portnummer auf localhost

com.apple.mobile.**pcapd**

- Sniffingsoftware auf Basis von *pcap*
- Implementierung durch Bibliothek *libcap*
- Kein visueller Hinweis auf Aktivität des Dienstes
- Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

- Sniffingsoftware auf Basis von *pcap*
- Implementierung durch Bibliothek *libcap*
- Kein visueller Hinweis auf Aktivität des Dienstes
- Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

- Sniffingsoftware auf Basis von *pcap*
- Implementierung durch Bibliothek *libcap*
- Kein visueller Hinweis auf Aktivität des Dienstes
- Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

- Sniffingsoftware auf Basis von *pcap*
- Implementierung durch Bibliothek *libcap*
- Kein visueller Hinweis auf Aktivität des Dienstes
- Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**file_relay**

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.**file_relay**

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.**file_relay**

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.**file_relay**

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.**house_arrest**

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

com.apple.mobile.**house_arrest**

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

com.apple.mobile.**house_arrest**

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

Historische Exploits

- libTiff Exploit
- Ikee Virus
- No iOS Zone

Historische Exploits

libTiff Exploit

Ikee Virus

No iOS Zone

Historische Exploits

- libTiff Exploit
- Ikee Virus
- No iOS Zone

Historische Exploits

- libTiff Exploit
- Ikee Virus
- No iOS Zone

Historische Exploits

- libTiff Exploit
- Ikee Virus
- No iOS Zone

libTiff Exploit (2007)

- Pufferüberlauf der libtiff Bibliothek
- Wurde für Jailbreak genutzt
- iOS Prozesse liefen noch mit root (iOS 1)

libTiff Exploit (2007)

- Pufferüberlauf der libtiff Bibliothek
- Wurde für Jailbreak genutzt
- iOS Prozesse liefen noch mit root (iOS 1)

libTiff Exploit (2007)

- Pufferüberlauf der libtiff Bibliothek
- Wurde für Jailbreak genutzt
- iOS Prozesse liefen noch mit root (iOS 1)

Ikee Virus (2009)

- Einer der ersten Würmer unter iOS
- Standardpasswort der Jailbreak SSH Zugänge ausgenutzt
- Bösartige Variante *Ikee.B* stahl Daten

Ikee Virus (2009)

- Einer der ersten Würmer unter iOS
- Standardpasswort der Jailbreak SSH Zugänge ausgenutzt
- Bösartige Variante *Ikee.B* stahl Daten

Ikee Virus (2009)

Einer der ersten Würmer unter iOS

Standardpasswort der Jailbreak SSH Zugänge ausgenutzt

Bösartige Variante *Ikee.B* stahl Daten

No iOS Zone (2014)

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

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

No iOS Zone (2014)

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

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

No iOS Zone (2014)

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

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Gliederung

Gliederung