

Mobile Sicherheit

Warum sind Mobiltelefone
lohnenswerte Ziele f. Hacker?

Android

vs.

iOS

Apps automatisch gescannt Play Store nicht verpflichtend	App / Play Store	Apps manuell überprüft
Viele Geräte / Hersteller mit unterschiedlichen Garantien	Sicherheitsupdates	> 5 Jahre offizieller Support
75% Marktanteil	Verbreitung	25% Marktanteil
Open-Source (zum Teil)	Software	Closed-Source
Offen (Management & Overlays)	Sandbox Modell	Streng reglementiert
Verkaufen deine Daten	Produktfokus	Verkaufen teure Geräte
Rooting	Sandbox (Escape)	Jailbreak

ZERODIUM Payouts for Mobiles*

Up to
\$2,500,000

Up to
\$2,000,000

Up to
\$1,500,000

Up to
\$1,000,000

FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

■ iOS
■ Android
■ Any OS

1.001
Android FCP
Zero Click
Android

1.002
iOS FCP
Zero Click
iOS

2.001
WhatsApp
RCE+LPE
Zero Click
iOS/Android

2.002
iMessage
RCE+LPE
Zero Click
iOS

2.003
WhatsApp
RCE+LPE
iOS/Android

2.004
SMS/MMS
RCE+LPE
iOS/Android

Zero - Day - Exploits

Up to
\$500,000

3.001
Persistence
iOS

2.005
WeChat
RCE+LPE
iOS/Android

2.006
iMessage
RCE+LPE
iOS

2.007
FB Messenger
RCE+LPE
iOS/Android

2.008
Signal
RCE+LPE
iOS/Android

2.009
Telegram
RCE+LPE
iOS/Android

2.010
Email App
RCE+LPE
iOS/Android

4.001
Chrome
RCE+LPE
Android

4.002
Safari
RCE+LPE
iOS

Up to
\$200,000

5.001
Baseband
RCE+LPE
iOS/Android

6.001
LPE to
Kernel/Root
iOS/Android

2.011
Media Files
RCE+LPE
iOS/Android

2.012
Documents
RCE+LPE
iOS/Android

4.003
SBX
for Chrome
Android

4.004
Chrome RCE
w/o SBX
Android

4.005
SBX
for Safari
iOS

4.006
Safari RCE
w/o SBX
iOS

Up to
\$100,000

7.001
Code Signing
Bypass
iOS/Android

5.002
WiFi
RCE
iOS/Android

5.003
RCE
via MitM
iOS/Android

6.002
LPE to
System
Android

8.001
Information
Disclosure
iOS/Android

8.002
[k]ASLR
Bypass
iOS/Android

9.001
PIN
Bypass
Android

9.002
Passcode
Bypass
iOS

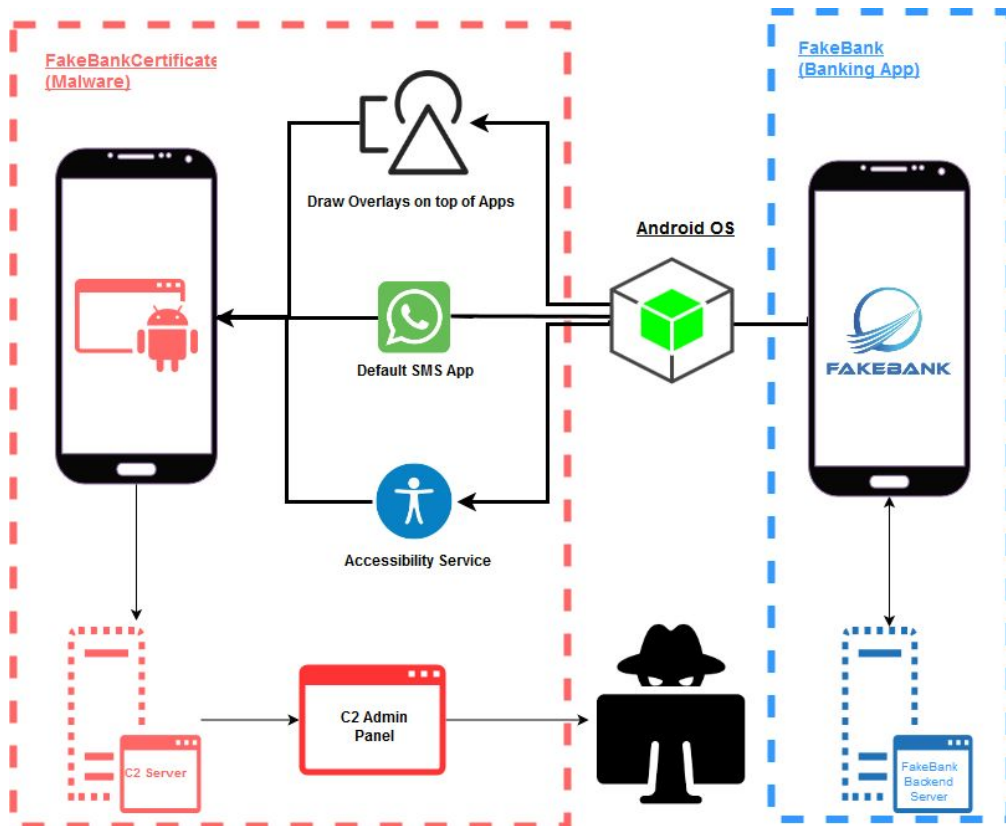
9.003
Touch ID
Bypass
iOS

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/09 © zerodium.com

- **Trojaner:** Diese Art von Malware verbirgt sich in scheinbar harmloser oder nützlicher Software und führt dann schädliche Aktionen aus, oft ohne Wissen des Benutzers.
- **Spyware:** Diese Art von Malware sammelt Informationen über den Benutzer und dessen Gerät ohne dessen Wissen oder Zustimmung.
- **Ransomware:** Diese Art von Malware verschlüsselt die Daten auf dem Gerät und verlangt dann ein Lösegeld vom Benutzer, um den Zugriff auf die Daten wiederherzustellen.
- **Adware:** Obwohl nicht immer schädlich, kann Adware dazu führen, dass störende oder sogar schädliche Werbung auf dem Gerät angezeigt wird.
- **Banking-Malware:** Diese Art von Malware zielt darauf ab, Anmeldedaten für Online-Banking-Systeme oder andere Finanzinformationen zu stehlen.
- **SMS-Malware:** Diese Art von Malware führt Aktionen durch SMS aus, wie z. B. das Versenden von Premium-SMS-Nachrichten, die Gebühren verursachen, oder das Abfangen von eingehenden SMS-Nachrichten.
- **Botnets:** Hierbei handelt es sich um eine Sammlung von Geräten, die durch Malware kompromittiert und dann ferngesteuert werden, oft um Spam zu versenden oder DDoS-Angriffe durchzuführen.

Mobile Malware



Mobile Malware



APPS

JUST A GAME?

Only install apps from official app stores

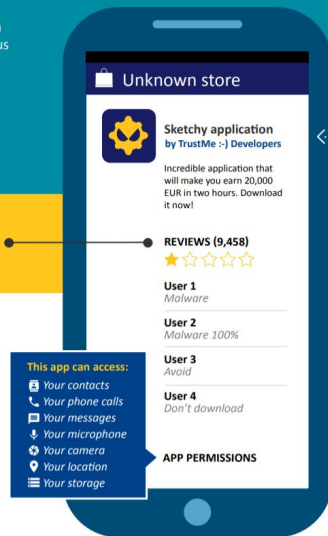


Before downloading an app, research the app and its publishers. Be cautious of links you receive in email and text messages that might trick you into installing apps from third party or unknown sources.

CHECK OTHER USERS' REVIEWS AND RATINGS

READ THE APP'S PERMISSIONS

Check which types of data the app can access, and if it might share your information with external parties. Does it need all these permissions? If not, don't download it.

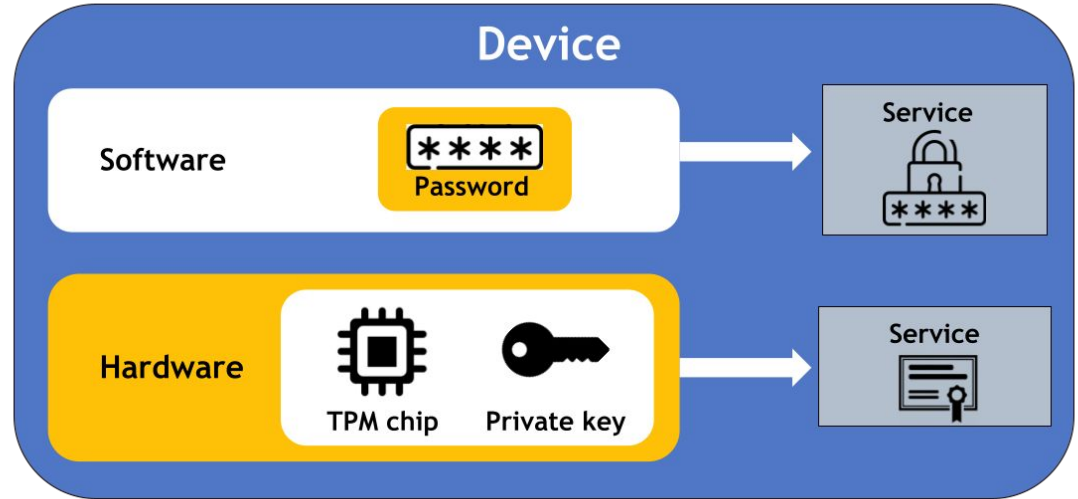


INSTALL A MOBILE SECURITY APP

It will examine all the apps on your device and each new one you install later, alerting you if malicious software is found.



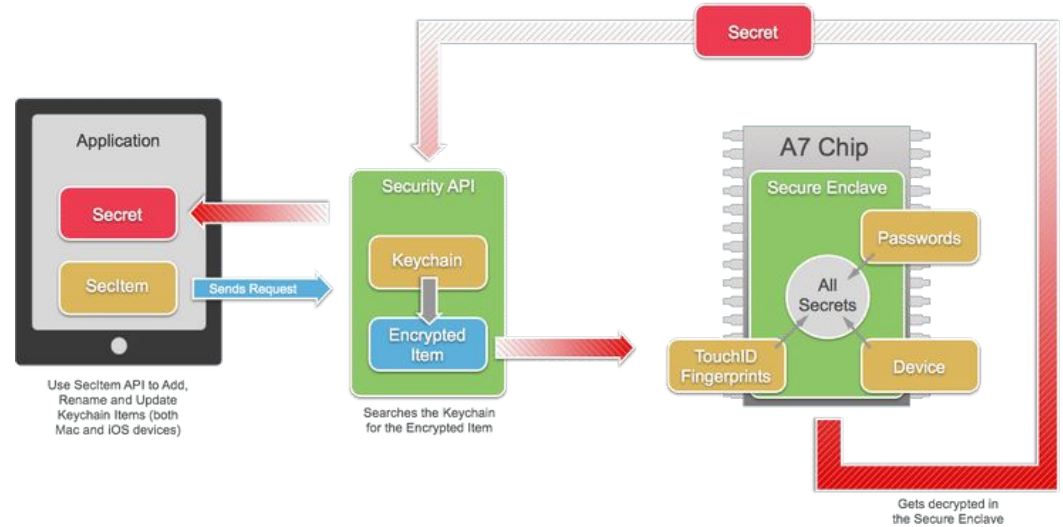
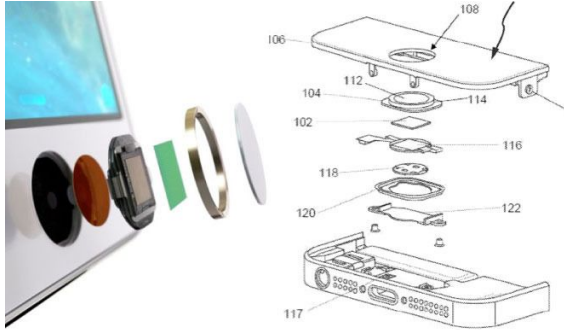
TPM / Secure Enclave



Trusted Platform Module (TPM)

1. Ein spezialisierter Chip auf einem Gerät, der die Sicherheit erhöht, indem er kryptographische Operationen durchführt.
2. Hilft bei der Verifizierung der Integrität der Hardware und ermöglicht sichere Speicherung von Schlüsseln, Passwörtern und digitalen Zertifikaten.
3. Unterstützt das sichere Booten, indem es überprüft, dass jede Komponente, die während des Bootprozesses geladen wird, vertrauenswürdig ist.

TPM / Secure Enclave



Secure Enclave

1. Eine isolierte Komponente im Prozessor bestimmter Apple-Geräte, die sicherheitsrelevante Funktionen unterstützt.
2. Implementiert einen Hardware-verschlüsselten Speicherbereich zum sicheren Speichern von sensiblen Daten wie Schlüsseln, Passwörtern und biometrischen Daten (z. B. Fingerabdrücken).
3. Die Daten innerhalb der Secure Enclave sind selbst dann geschützt, wenn das Betriebssystem kompromittiert ist.

MDM - Mobile Device Management

1. Geräteverwaltung
2. Sicherheitsmaßnahmen
3. Software- und App-Verwaltung
4. Überwachung und Berichterstattung
5. Policy-Management
6. Bring Your Own Device (BYOD)



Mobile Forensik



