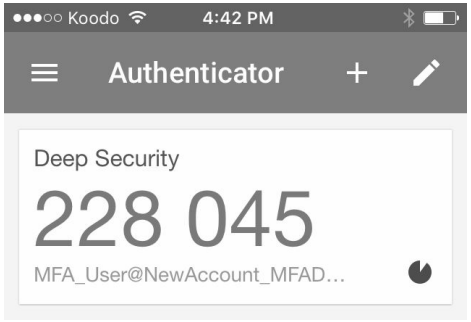
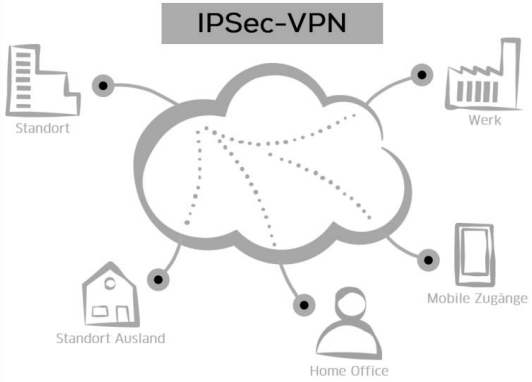
Mobile Sicherheit

Warum sind Mobiltelefone lohnenswerte Ziele f. Hacker?

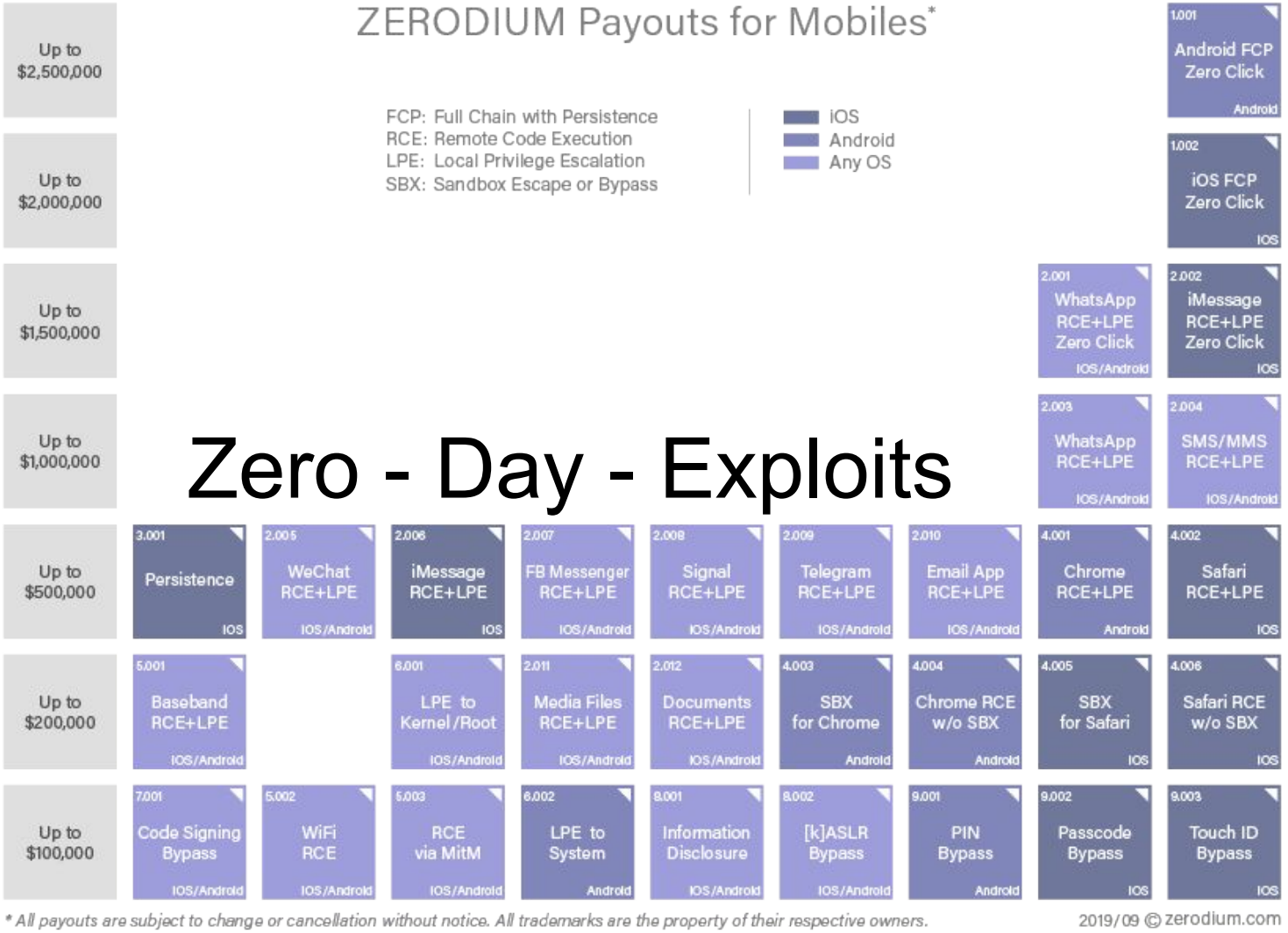


Warum sind Mobiltelefone lohnenswerte Ziele f. Hacker?



Android vs. iOS

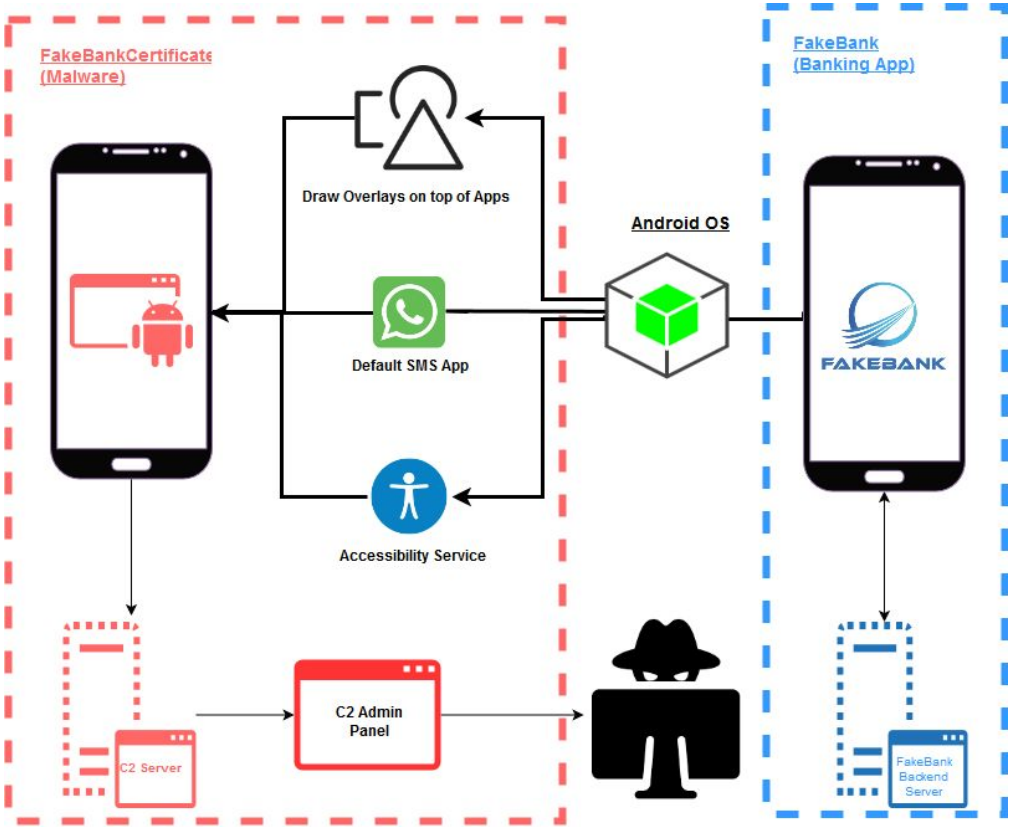
Apps automatisch gescannt Play Store nicht verpflichtend	**App / Play Store**	Apps manuell überprüft
Viele Geräte / Hersteller mit unterschiedlichen Garantien	**Sicherheitsupdates**	> 5 Jahre offizieller Support
75% Marktanteil	**Verbreitung**	25% Marktanteil
Open-Source (zum Teil)	**Software**	Closed-Source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



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

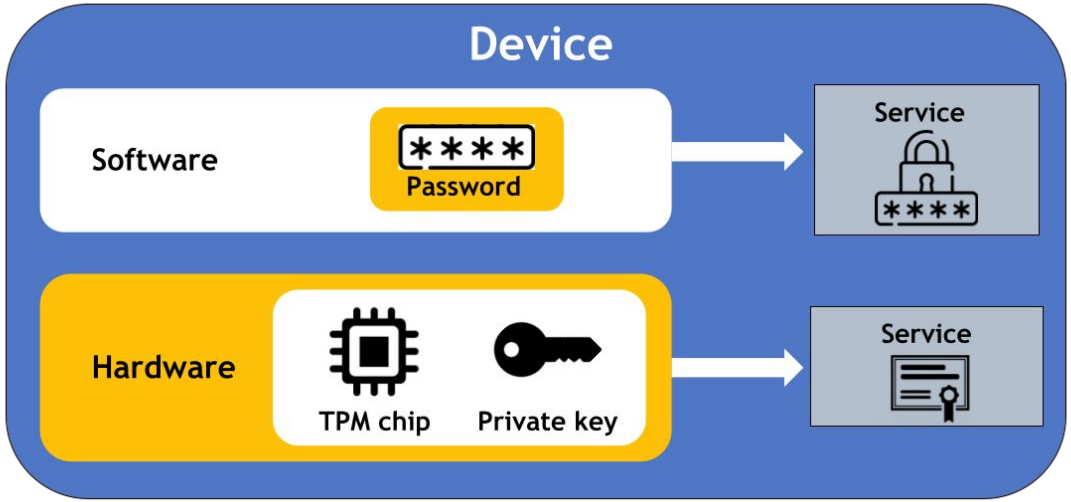
- **Trojaner:** Diese Art von Malware verbirgt sich in scheinbar harmloser oder nützlicher Software und führt dann schädliche Aktionen aus, oft ohne Wissen des Benutzers.
- **Spyware:** Diese Art von Malware sammelt Informationen über den Benutzer und dessen Gerät ohne dessen Wissen oder Zustimmung.
- **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

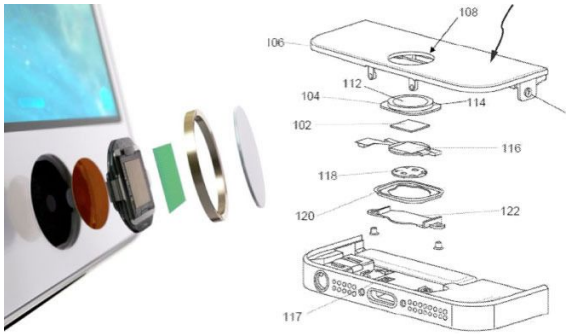
TPM / Secure Enclave

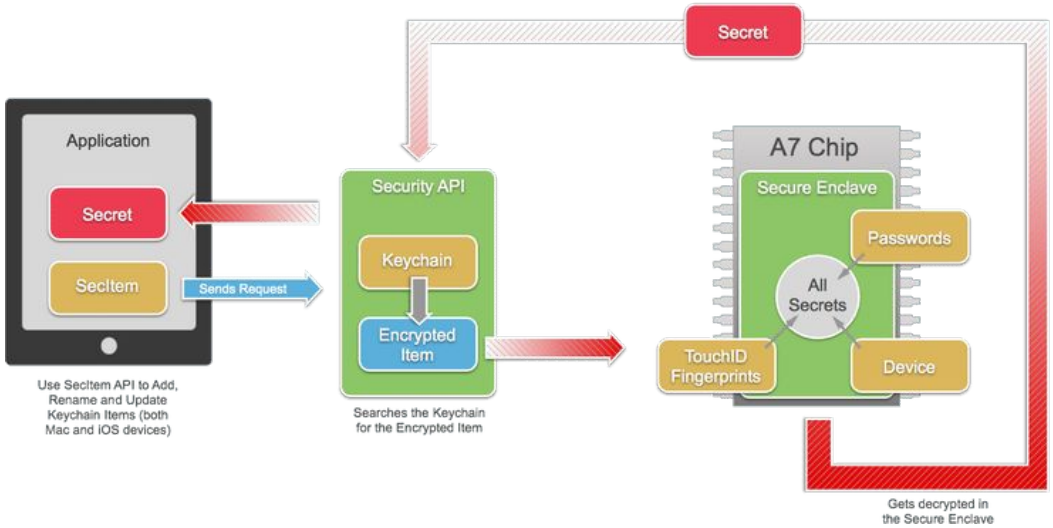


Trusted Platform Module (TPM)

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 Managment

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

Mobile Forensik

Mobile Forensik