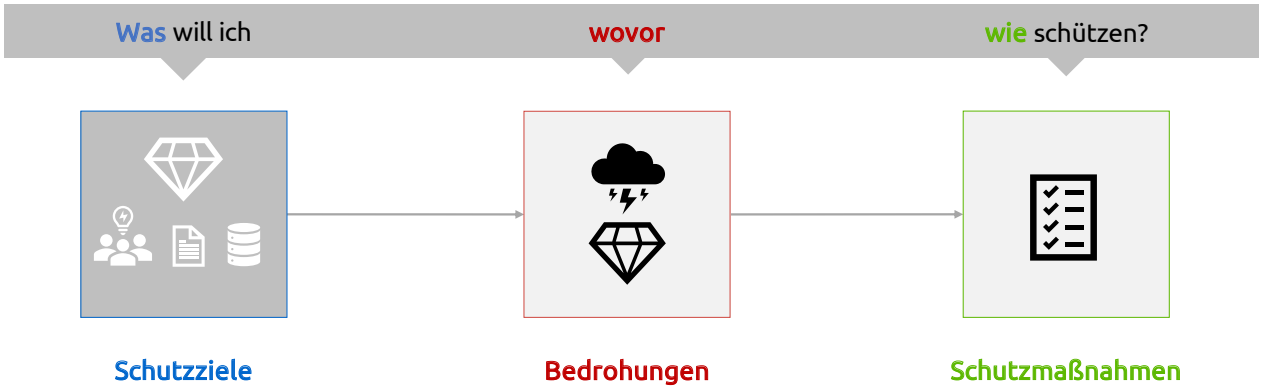
Smartphone Hacking: Threat Modeling



Schutzziele

Smartphones beinhalten viele vertrauliche und sensible Informationen. Zum einen sind das Kommunikationsdaten wie Telefongespräche, E-Mails oder Kurznachrichten, zum anderen weitere persönliche Daten wie Fotos oder Adressbücher. Durch dauerhaft aktive GPS-Sensoren ist die Aufzeichnung detaillierter Bewegungsprofile ebenfalls möglich. Zudem kommen Zugangsdaten wie der Zugang zum Online-Banking oder Social-Media-Plattformen hinzu.

Bedrohungen

Physisch Durch den mobilen Gebrauch ist das Smartphone sehr anfällig gegen physische Attacken. Durch Diebstahl oder versehentlicher Verlust können Datenträger eingesehen werden oder die Authentifikation umgangen werden, um vollen Zugriff auf das Smartphone zu erlangen.

Funkprotokolle WLAN, Bluetooth und Mobilfunk-Protokolle können Schwachstellen aufweisen, die Angreifern das Abhören der Kommunikation ermöglichen.

Internet Die Gefahren des Internet sind vielfältig und reichen vom automatischen Speichern von Daten in der Cloud bis hin zu Zero-Click-Angriffen.

Schutzmaßnahmen

Mobile Device Management (MDM)

Durch den Einsatz einer MDM-Lösung werden Maßnahmen ausgerollt, die das Smartphone schützen sollen. MDM-Lösungen bieten typischerweise folgende Funktionen.

- Manipulationen erkennen
- Vorgaben für die Authentifikation aufstellen
- Synchronisations- und Backupdienste deaktivieren
- Fernlöschung ermöglichen
- App-Installation und -Berechtigungen kontrollieren
- Updates unverzüglich einspielen

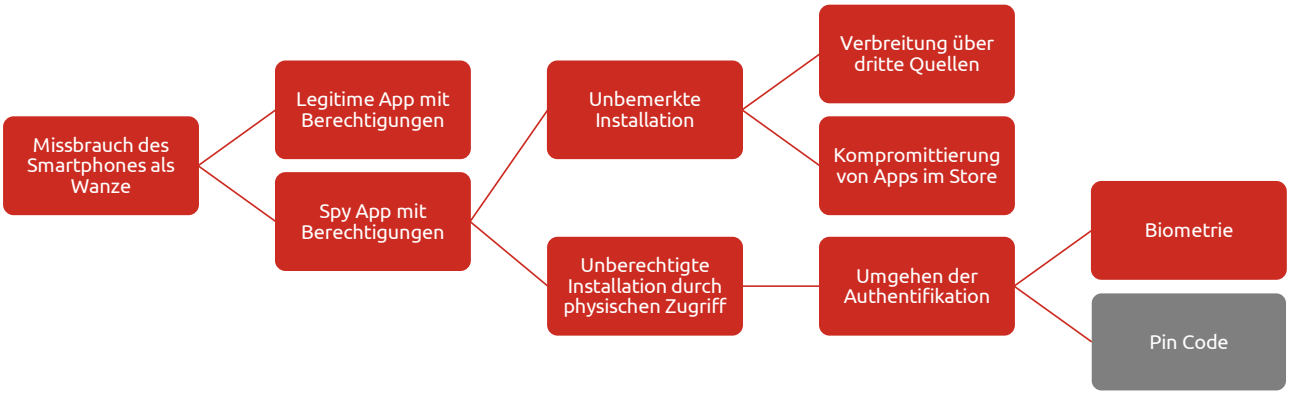
Maßnahmen für App-Entwickler

- Die Bedrohungen für die App mit einem Threat Model verstehen
- Durch Penetrationstests typische Schwachstellen aufdecken

aramido GmbH
Beratung für Informationssicherheit
Durlacher Allee 75 - 77
76131 Karlsruhe

ÖFFENTLICH
+49 721 451 991 0
armin.harbrecht@aramido.de
maximilian.stauss@aramido.de

Mögliche Angriffe



Biometrie – Traue ihr nie

Man hinterlässt sie überall, auf jeder Türklinke, auf jedem Glas und an jeder Oberfläche: Fingerabdrücke. Durch die Einzigartigkeit der Papillarleisten auf dem Finger bietet sich der Fingerabdruck als eine der wenigen Merkmale des Körpers an, um den User zu Identifizieren. Jedoch sollte die Authentifikation niemals nur über solche biometrischen Faktoren stattfinden.

Mit dem IPhone 5S erschien 2013 die erste Version mit TouchID-Unterstützung, die dem IPhone-User erstmals die Authentisierung durch den eigenen Fingerabdruck ermöglicht. Doch schon zwei Tage nach dem Verkaufsstart erschienen die ersten Beiträge, wie sich der Fingerabdrucksensor durch einen gefälschten Fingerabdruck überlisten lässt. Heutzutage sind hochauflösende Bilder eines Fingers ausreichend, um eine Kopie des Fingerabdruckes anzufertigen, der den Fingerabdrucksensor erfolgreich täuschen kann.

Auch aramido hat sich der Fälschung von Fingerabdrücken angenommen und eine kinderleichte Methode entwickelt, wie mit Kerzenwachs und Holzleim die effektive Herstellung von Fingerabdruckattrappen gelingt.

Apps mit ungewollten Features

Trends gehen und kommen, besonders in der Mobile-Game-Branche. So auch das bekannte Spiel Flappy Birds, das heutzutage nur noch auf Drittanbieterplattformen erhältlich ist. Wenn Apps von zweifelhaften Quellen versteckte, trojanische Inhalte besitzen oder es Angreifern gelingt schadhafte Apps in die App Stores zu schmuggeln, stehen Angreifern viele Möglichkeiten offen.

Je mehr Rechte an die schadhafte App vergeben werden, desto mehr Schaden kann die App potentiell anrichten. So können Kommunikationsdaten ausgelesen und Kameras und Mikrophone aktiviert werden. Zusätzlich können Angreifer Schwachstellen in anderen auf dem Smartphone installierten Apps ausnutzen, um so beispielsweise Zugangsdaten zu stehlen oder bösartige Inhalte zu verbreiten.