Smartphone-Angriffsvektoren

www.sit.fraunhofer.de

Fraunhofer SIT

LOGISCHE ANGRIFFE

BROWSER

Neben den üblichen Browser-Schwachstellen (Verarbeitung von Webstandards) bieten Smartphones durch die Interaktionsmöglichkeiten zwischen Browser und Telefon zusätzliche Angriffsziele. Dies ermöglicht es zum Beispiel die mit der SIM-Karte verknüpfte Nutzeridentität zu missbrauchen.

BASEBAND PROZESSOR

Basisstationen sind heute relativ preisgünstig. Angreifer können diese Geräte anpassen, um Angriffe gegen die Mobilfunkschnittstellen auszuführen. Ziel ist dabei oft, Zugriff auf Nutzerdaten zu erlangen. Aber auch Angriffe in der umgekehrten Richtung, vom Smartphone gegen die Infrastruktur von Mobilfunkanbietern, sind möglich.

MULTIMEDIA-PLAYER

Die Komplexität der Verarbeitung komprimierter Datenströme (MP3, WMA, TIFF, PDF, etc.) hat in der Vergangenheit bereits viele Verwundbarkeiten hervorgerufen. Dies ist ein leicht zu übersehender Aspekt bei der Absicherung von Unternehmessmartphones, da nicht nur Anwendungen potentielle Bedrohungen darstellen können.

BETRIEBSSYSTEM

Neben allgemeinen Schwächen in Betriebssystemkomponenten sind durch reduzierte Oberflächen gerade bei Smartphones auch Angriffe auf Schutzmechanismen in der graphischen Benutzeroberfläche, wie etwa die Passwortsperre, möglich. Zudem können Apps Beschränkungen der Laufzeitumgebung (Sandbox) umgehen bzw. potentielle Schwachstellen ausnutzen.

3RD PARTY APPS

Neben der Gefährdung durch die Installation von Schadsoftware auf dem Gerät geht von Apps auch eine Gefährdung durch enthaltene Schwachstellen aus. Die Erfahrung zeigt, dass die Qualität der Absicherungsmaßnahmen vieler Apps noch unzureichend ist, wodurch nicht nur ihre eigenen Anwendungsdaten gefährdet werden können.

ANWENDER

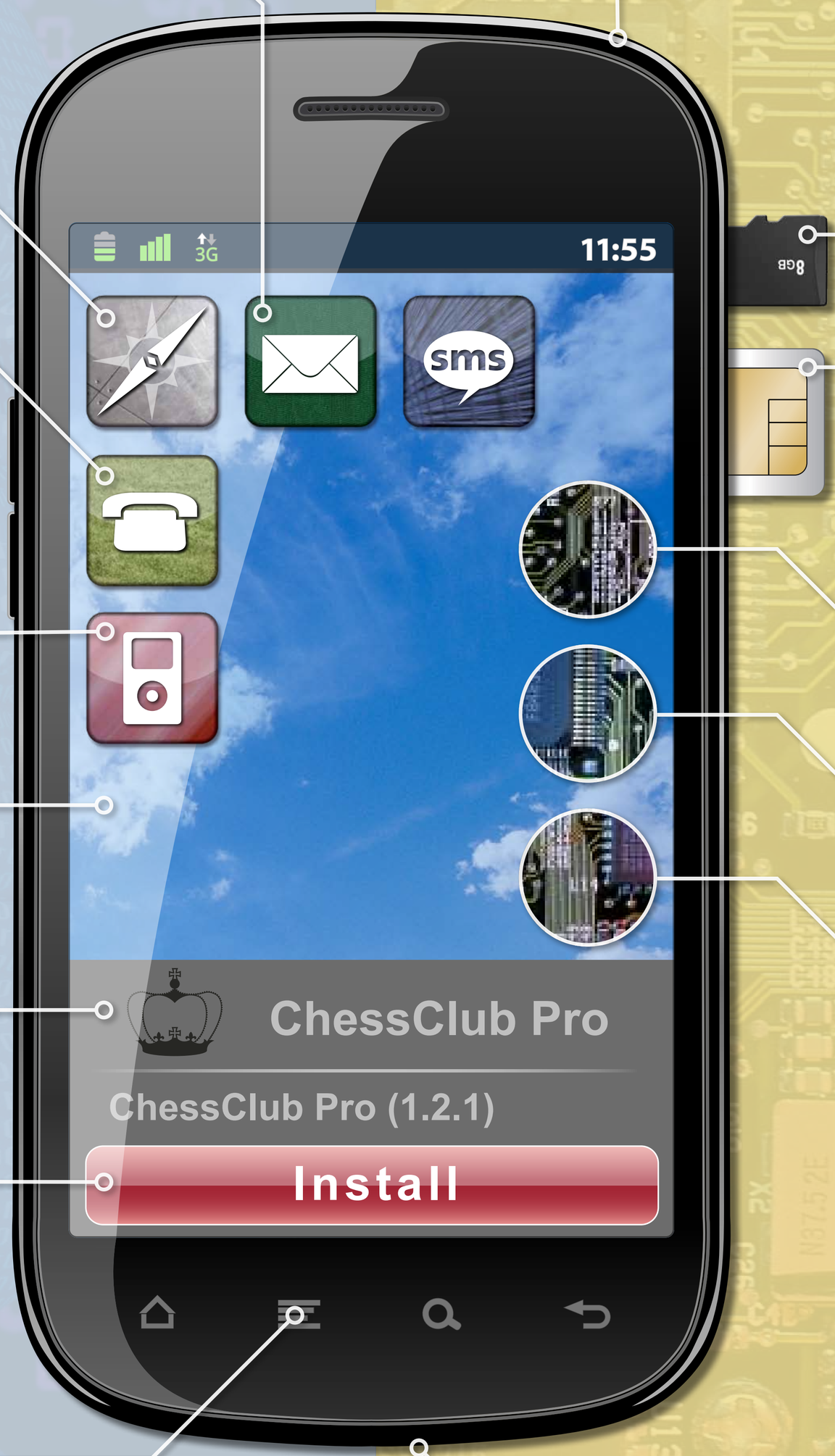
Häufig werden Anwender zum Ausführungsgehilfen eines Angriffs, indem sie getäuscht oder durch Unwissenheit zu sicherheitkritischen Aktionen verleitet werden.

FERNWARTUNG

Fehlende automatisierte Updates oder eine unsichere Konfiguration können genauso für Angriffe dienen wie schlecht gesicherte Schnittstellen zum entfernten Gerätemanagement.

KOMMUNIKATIONSDIENSTE

Dienste wie E-Mail und ActiveSync sind auch bei Smartphones ein mögliches Einfallstor für Angriffe mittels manipulierter Inhalte. Im Gegensatz zu stationären PCs werden zudem aber Dienste wie SMS, MMS oder Over the Air Updates nicht am Unternehmensperimeter geprüft und können so ungefiltert auf verwundbare Schnittstellen im Gerät treffen.



PHYSISCHE ANGRIFFE

DRAHTLOS SCHNITTSTELLEN

Befindet sich der Angreifer in unmittelbarer Nähe des Geräts, kann er manipulierte Daten verschicken und so Schwachstellen in der Verarbeitung von Funkkommunikation (Bluetooth, NFC, WiFi, etc.) ausnutzen, um Zugriff auf Nutzerdaten und Passwörter zu erlangen.

SPEICHERKARTE

Daten auf externen Speichermedien sind häufig ungeschützt. Gelangt ein Smartphone in den Besitz eines Angreifers, können diese direkt ausgelesen werden. Kann ein Angreifer manipulierte Daten auf der Speicherkarte platzieren, lassen sich Verwundbarkeiten des Smartphones ausnutzen. Wird ein manipuliertes Smartphone mit dem Unternehmens-PC verbunden, können Angreifer es als Wirt für Infektionen verwenden und beim Synchronisieren den Rechner und darüber auch das Unternehmensnetzwerk attackieren.

SIM

Obwohl die SIM-Karte an sich eine hohe Sicherheit bietet, können Angreifer die Kommunikation zwischen ihr und Smartphone-Komponenten (SIM-Toolkit) manipulieren, um Beschränkungen zu umgehen und ggf. IT-sicherheitskritische Informationen mitzulesen bzw. zu verändern.

HARDWARE-SCHNITTSTELLEN

Durch Öffnen des Gerätes kann ein Angreifer Zugriff auf Daten über Speicherbusse und Hardware-Schnittstellen (JTAG) erlangen bzw. darüber Schutzmechanismen der Nutzerschnittstelle umgehen.

SPEICHER

Manipulationen von Flash-Speicher-Inhalten oder von RAM-Disks bieten häufig die Möglichkeit Schutzmechanismen zu entfernen bzw. Nutzerdaten direkt auszulesen.

FIRMWARE

Die Integrität der Firmware stellt die Basis für viele Sicherheitsfunktionen dar. Bleibt die Manipulation der Firmware und das Zurücklegen vom Nutzer unbemerkt (Evil Maid Attack), so kann der Angreifer aus der Ferne die vollständige Kontrolle über das Smartphone und die Daten erlangen.

USB

Durch Low-Level-Zugriff über USB können viele der geschilderten physischen Angriffe durchgeführt werden, ohne das Smartphone zu öffnen. Darüber hinaus stellen viele Smartphones weitere logische Schnittstellen für Modem-Funktionen und Datenzugriff bereit, die ein zusätzliches Einfallstor für Angriffe darstellen können – beispielsweise beim unbedachten Aufladen.

KONTAKT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

Standort Darmstadt
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-399
Fax 06151 869-224
info@sit.fraunhofer.de

Standort St. Augustin
Schloss Birlinghoven
53754 Sankt Augustin
Telefon 02241 14-3272
Fax 02241 14-3007
info-bi@sit.fraunhofer.de

BIZZTRUST FOR ANDROID – ZWEI SMARTPHONES IN EINEM

BizzTrust stellt mehrere getrennte Anwendungsbereiche auf dem Smartphone bereit, die jeweils über ihre eigenen Datensätze und Zugriffsberechtigungen verfügen. Dadurch können private Anwendungen (Apps) ohne Einschränkungen parallel und unabhängig von geschäftlichen Anwendungen ausgeführt werden. Weiterhin erlauben die erweiterten Fernwartungsprotokolle im geschäftlich genutzten Bereich, den Gerätezustand aus der Ferne festzustellen, automatisch Software-Updates einzuspielen und das Gerät vollständig in die zentrale Event-Management-Infrastruktur des Unternehmens zu integrieren. BizzTrust bietet:

- Schutz für Geschäftsdaten
- Uneingeschränkte private Nutzung
- Sichere Kommunikation mit dem Unternehmen (Verschlüsselung)
- Remote-Management und -Update
- Unterstützt Bring-your-own-Device-Strategie
- Automatic Policy Enforcement

GEHT IHR SMARTPHONE FREMD?

Smartphones sind praktische Werkzeuge und aus dem Unternehmensalltag nicht mehr wegzudenken. Wer sich nicht um Smartphone-Sicherheit kümmert, geht jedoch ein hohes Risiko ein: Finanzieller Schaden droht zum Beispiel durch Missbrauch von Premium-Diensten, wie z. B. die Übertragung von Schadsoftware ins Unternehmensnetzwerk oder den unerlaubten Zugriff auf das Unternehmensnetzwerk. Fraunhofer SIT unterstützt Unternehmen und Behörden beim sicheren Einsatz von Smartphones. Geräte-Herstellern und Software-Anbietern bieten wir unabhängige Sicherheitsanalysen und Wissenstransfer zur Umsetzung innovativer Lösungen. Konkret bieten wir:

- Sicherheitsanalysen (mit/ohne Testat)
- Praktische Angriffstests
- Erstellung und Bewertung von Sicherheitskonzepten
- Absicherung von mobilen Geräten und Prozessen
- Anpassung und Ermittlung sicherer Konfigurationen
- Innovative Lösungen