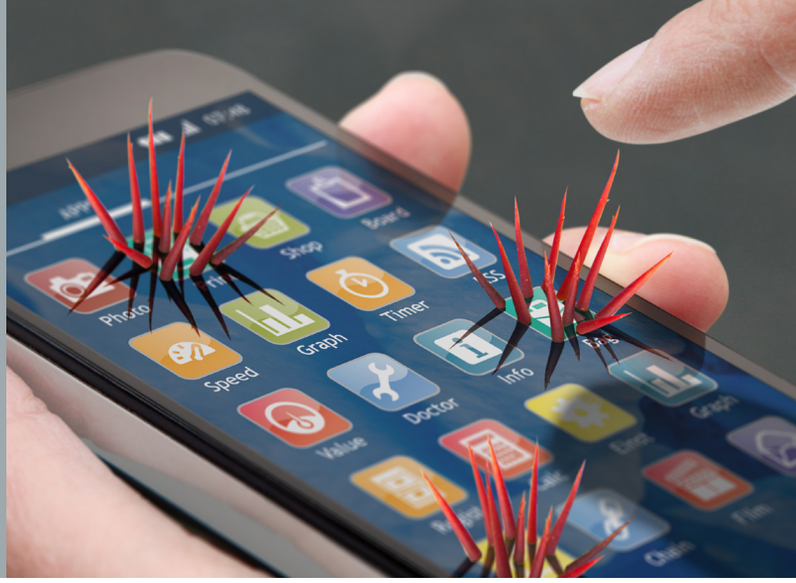
Fraunhofer SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE



Fraunhofer-Institut für Sichere Informationstechnologie SIT

Dr. Jens Heider
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-233
appicaptor@sit.fraunhofer.de
www.appicaptor.de

APPICAPTOR

FRAMEWORK FÜR APP-ANALYSEN

Welche Apps dürfen die eigenen Mitarbeitenden auf Tablets und Smartphones der Firma installieren? Wer die eigenen Angestellten wahllos Apps nutzen lässt, gefährdet die Sicherheit des Unternehmens. Viele App-Entwickler besitzen keine ausreichenden IT-Sicherheitskenntnisse, was oft zu unbeabsichtigten Sicherheitslücken führt. Die diversen App-Stores prüfen zwar auf Malware, die spezifischen App-Sicherheitseigenschaften und deren korrekte Implementierung werden jedoch nicht betrachtet. Hierfür hat Fraunhofer SIT das App-Analyse-Framework »Appicaptor« entwickelt, mit dem automatisiert analysiert wird, ob Apps den kundenspezifischen IT-Sicherheitsvorschriften entsprechen.

Die Nutzung mobiler Geräte birgt für Unternehmen und Behörden Chancen und Risiken. Eine große Gefahr droht durch ungeprüfte Apps. Diese enthalten oft Sicherheitslücken oder Implementierungsfehler in grundlegenden Schutzfunktionen. Aus Gründen der Effizienz werden App-Bestandteile wie einzelne Softwaremodule oft aus Drittquellen verwendet. Dadurch können sich bereits vorhandene Fehler auf zahlreiche Apps übertragen. Cyberkriminelle machen sich dies zunutze und können solche Schwachstellen gezielt ausnutzen, etwa um Passwörter zu stehlen oder Betriebsgeheimnisse auszuspähen. Da Angreifer weitverbreitete, verwundbare Apps leichter ausnutzen können, als Unternehmens- oder Behördennutzern bösartige Apps unterzuschieben, birgt eine schlechte Sicherheitsqualität bekannter Apps erhebliche Risiken für Unternehmen und Behörden. Gleichzeitig steigen die Anforderungen an den Schutz sensibler Daten.

Sicherheitsüberprüfung für iOS- und Android-Apps

»Appicaptor« erstellt für jeden Kunden und zu jeder App einen Bericht zur Sicherheitsqualität, der individuell die kundeneigenen Sicherheitsanforderungen in der App-Bewertung berücksichtigen kann. Die Analyse läuft dabei automatisch. »Appicaptor« führt dazu anspruchsvolle statische Analysen der App-Binärdateien und dynamische Analysen auf physischen Endgeräten durch, um sicherheitsrelevante Implementierungsfehler, Schwachstellen oder riskantes Verhalten zu erkennen. Bei erkannten Sicherheitslücken oder unsicherer Verwendung schützenswerter Daten erzeugt das System Warnhinweise und prüft, ob dadurch die Sicherheitsanforderungen des Kunden verletzt werden. »Appicaptor« erkennt relevante App-Risiken im Bereich der Kommunikation, der Datennutzung, der Eingabeschnittstellen, der Privatsphäre und der Laufzeitsicherheit.

Name	Insecure PDF-Viewer
App Type	File Viewer
Platform	iOS
Internal Name	com.company.insecure.pdf
Version	12.1.3
Vendor	Example Inc.
Appstore URL	https://apps.apple.com/de/app/insecurepdf/id1231231237?mt=8&uo=4
SHA 256	F1A1 45FF 9180 8A86 1B04 D224 3277 7F54 1BFB 29CA 4868 D116E4A6 8619 173F 2297

Blacklisted

4 Risks

✖ Violations of default policy

- Detected risks are not compliant to security policy requirements for apps managing files.
- Enterprise documents maybe at risk in a lost device scenario.
- Enterprise documents maybe at risk during communication processes with external entities.

⚠ App risks for enterprise usage

- Possible flaw: Use of insecure methods to secure communication with SSL/TLS. Common source for flawed communication protection that are vulnerable to man-in-the-middle attacks.
- Possible flaw: Unintended use of insecure HTTP protocol for transmissions of parameters to servers capable of HTTPS.
- Data Protection: App disables iOS default data protection at least in one case and can handle office files, which poses a potential risk as the storage of corporate data is protected lesser than needed for sufficiently targeting the lost device scenario.
- Advertisement/Tracking: App uses more than 5 advertisement and tracking providers.

Zusammenfassende Bewertung einer Beispiel-App in der »Appicaptor«-Webschnittstelle

»Appicaptor« klassifiziert selbst die Anwendungen auf Basis der App-Beschreibungen in den App-Märkten. Hierbei wird die wichtigste sicherheitsrelevante Funktion der App bestimmt (wie Datei-Betrachter, Organizer, Taschenrechner, Passwortmanager, etc.). Auf Grundlage dieser App-Klassifikation wird das Risiko der einzelnen Anwendung anhand der durch „Appicaptor« detektierten Sicherheitseigenschaften bestimmt und hinsichtlich der jeweiligen Anforderungen bewertet.

Dabei können Unternehmen die »Appicaptor«-Standard-App-Bewertungskriterien nutzen oder eine maßgeschneiderte automatisierte App-Bewertung passend zu der Unternehmens- oder Behörden-IT-Sicherheitsrichtlinie für das Blacklisting oder Whitelisting von Apps verwenden. Damit lässt sich die Bewertung der Analyseergebnisse individuell konfigurieren. Mehr als 100 verschiedene Parameter in »Appicaptor« können für eine kundendefinierten Anforderungen für ein App-White- oder -Blacklisting in den Bereichen der App-Sicherheitsqualität, des App-Verhaltens und der Implementierungs- oder Deployment-Eigenschaften verwendet werden. Die App-White- oder Blacklists lassen sich direkt aus »Appicaptor« mit Enterprise-Management-Systemen synchronisieren.

Aktuelle Sicherheitseinschätzungen für mobile Apps

Mit »Appicaptor« betreibt das Fraunhofer SIT ein App-Analyse-Framework für automatisierte App-Analysen. Da Apps regelmäßig überarbeitet werden und sich immer wieder neue Erkenntnisse zu Schwachstellen und Implementierungsfehlern ergeben, aktualisiert »Appicaptor« zyklisch die jeweilige App-Sicherheitseinschätzung und bewertet die Sicherheitseigenschaften dadurch stets anhand des aktuellen technischen Wissens.

»Appicaptor« erstellt zu jeder App einen Bericht zur Sicherheitsqualität, der in einem Webinterface eingesehen oder als PDF-Bericht heruntergeladen werden kann, um objektive Fakten für Entscheidungen im App-Genehmigungsprozess und den Stand des Wissens über eine App zu einem Zeitpunkt zu dokumentieren. Zur Integration in eigene softwaregesteuerte Prozesse steht die Verwendung von XML-formatierten Daten und eine REST-API zur Verfügung.

Seit der Einführung 2014 werden die Analysemethoden in »Appicaptor« kontinuierlich angepasst und weiterentwickelt, um neue Bedrohungen in Apps erkennen zu können, beispielsweise um die Nutzung neu eingeführter oder veränderter sicherheitsrelevanter APIs der mobilen Betriebssystem-Plattformen iOS und Android in Apps zu identifizieren. Diese fortlaufende Weiterentwicklung der Analysen ermöglicht es Unternehmen und Organisationen, den wachsenden und sich wandelnden Anforderungen der mobilen Sicherheit zu begegnen und eine aktuelle und objektive Einschätzung der Sicherheitsqualität der eingesetzten Apps zu gewährleisten.

»Appicaptor« legt großen Wert auf den Schutz der Daten seiner Kunden. Aus diesem Grund wird die gesamte »Appicaptor«-Infrastruktur ausschließlich in Deutschland innerhalb des Fraunhofer SIT betrieben. Die Datenverarbeitung erfolgt somit vollständig innerhalb einer sicheren, rechtlich klar geregelten Umgebung.

Funktion

- Automatisierte IT-Sicherheitsanalysen für iOS und Android
- Suche nach Implementierungsfehlern in IT-sicherheitskritischen App-Funktionen
- Detektion von Zugriffen auf sensible Nutzerdaten/-prozesse
- Spezifische Auswertung der Analyseergebnisse in Abhängigkeit kundenspezifischer IT-Sicherheitsanforderungen

Vorteile

- Einschätzung der generellen App-Sicherheitsqualität
- Unterstützung in der Risikobewertung von Apps und in der Einhaltung von Compliance-Vorschriften
- App-Suche in Abhängigkeit von Funktionalitäts- und IT-Sicherheitsanforderungen
- Erstellen von App-Negativlisten und -Positivlisten für Enterprise-Management-Systeme
- Integration der Ergebnisse in Enterprise-Management-Systeme
- Umfangreiche Statistikdarstellung in Web-Frontend und direkte API-Integration in Unternehmens-/Behördenprozesse
- Meldung kritischer App-Schwächen durch »Appicaptor« an App-Hersteller (Hersteller-Feedback)

Leistungsangebot

- Durchführung von App-Tests mit zyklischer Aktualisierung der jeweiligen App-Sicherheitseinschätzung
- Prüfung individueller Vorgaben in Abhängigkeit der App-Klassifizierung bezüglich des App-Verhaltens und der IT-Sicherheitsanforderungen
- Einsatzempfehlung sicherer Apps nach kundenspezifischen Funktionalitäts- und Sicherheitsanforderungen

Ihr Weg zu »Appicaptor«

- Vereinbaren Sie einen Termin für eine Live Demo und testen Sie »Appicaptor« unverbindlich für Ihr Nutzungsszenario
- Fordern Sie ein individuelles Angebot an

appicaptor@sit.fraunhofer.de

Investition in Ihre Zukunft

HESSEN

Investitionen für diese Entwicklung wurden von der Europäischen Union aus dem Europäischen Fonds für regionale Entwicklung und vom Land Hessen kofinanziert.