Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Dr. Jens Heider
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-233
Fax 06151 869-224
appicaptor@sit.fraunhofer.de
www.appicaptor.de

Appicaptor

FRAMEWORK FÜR APP-SECURITY-TESTS

Welche Apps dürfen die eigenen Mitarbeiter 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 Test-Framework »Appicaptor« entwickelt, mit dem Unternehmen automatisiert testen können, ob Apps den eigenen IT-Sicherheitsvorschriften entsprechen.

Die Nutzung mobiler Geräte birgt für Unternehmen Chancen und Risiken. Eine große Gefahr droht durch Apps. Diese werden in kürzester Zeit entwickelt und enthalten oft Sicherheitslücken oder Implementierungsfehler in grundlegenden Sicherheitsfunktionen. Aus Effizienzgründen werden Teile eines Software-Codes, etwa Module für einzelne App-Funktionen, oft wiederverwertet. Dadurch pflanzen sich die Fehler eines Entwicklers mitunter in anderen Apps fort. Versierte Angreifer machen sich dies zunutze und können solche Schwachstellen gezielt ausnutzen, etwa um Passwörter zu stehlen oder Betriebsgeheimnisse auszuspähen.

Sicherheitsüberprüfung für iOS- und Android-Apps

»Appicaptor« erstellt für Unternehmen zu jeder App einen Bericht zur Sicherheitsqualität, der individuell an die eigenen Sicherheitsanforderungen angepasst werden kann. Die Analyse läuft dabei automatisch. Bei erkannten Sicherheitslücken oder unsicherer Verwendung schützenswerter Daten erzeugt das System Warnhinweise und prüft, ob dadurch die Sicherheitsanforderungen verletzt werden.

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://itunes.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

Da Apps regelmäßig überarbeitet werden und sich immer wieder neue Erkenntnisse zu Schwachstellen und Implementierungsfehlern ergeben, wiederholt »Appicaptor« wöchentlich die Tests und bewertet die Sicherheitseigenschaften dadurch stets anhand des aktuellen technischen Wissens.

»Appicaptor« erkennt relevante App-Risiken im Bereich der Kommunikation, der Datennutzung, der Eingabeschnittstellen, der Privatsphäre und der Laufzeitsicherheit. »Appicaptor« führt dazu unter anderem anspruchsvolle statische Analysen der App-Binärdateien durch, um sicherheitsrelevante Implementierungsfehler, Schwachstellen oder riskantes Verhalten zu erkennen. »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 ihrer detektierten Sicherheitseigenschaften bestimmt und hinsichtlich der jeweiligen Unternehmensanforderungen bewertet.

Mithilfe von »Appicaptor« können Unternehmen entweder eine Whitelist oder eine Blacklist erstellen. Eine Whitelist enthält unbedenkliche Apps, die Mitarbeiter auf den Smartphones nutzen können. Eine Blacklist enthält Apps, die nicht die IT-Sicherheitsrichtlinien des Unternehmens erfüllen. Weiterhin können Unternehmen selbst entwickelte Apps oder Apps aus firmeneigenen App-Stores regelmäßig automatisiert auf Schwachstellen überprüfen lassen. Beide Listen können direkt aus »Appicaptor« mit Enterprise-Management-Systemen synchronisiert werden.

Flexibler Werkzeugkasten

Bei »Appicaptor« handelt es sich um ein Framework, das sich aus verschiedenen Analysemethoden und -werkzeugen zusammensetzt und sich nahezu beliebig um neue Tools und Testverfahren erweitern lässt. Viel Entwicklungsarbeit hat Fraunhofer SIT in die automatische Generierung von aussagekräftigen und gleichzeitig verständlichen Testreports gesteckt. Diese Management-Reports sind auch für Menschen ohne tiefe IT-Sicherheitskenntnisse einfach verständlich. Obwohl der Hersteller Apple wenig über den internen Aufbau der iOS-Plattform veröffentlicht, gelang es den Fraunhofer SIT-Experten, Methoden zu entwickeln und in »Appicaptor« zu integrieren, mit denen sich auch Risiken von iOS-Apps schnell und eindeutig identifizieren lassen.
Das Framework wird ständig weiterentwickelt und an neue Betriebssystemversionen angepasst. Das System lässt sich individuell konfigurieren. Testkriterien können so an die spezifischen IT-Sicherheitsrichtlinien des eigenen Unternehmens angepasst werden.

Dabei können Unternehmen Standardempfehlungen nutzen oder eine maßgeschneiderte automatisierte App-Bewertung passend zu ihrer Unternehmens-IT-Sicherheitsrichtlinie verwenden. Mehr als 70 verschiedene Parameter können für eine benutzerdefinierte Richtlinie für ein App-White- oder -Blacklistung im Bereich der App-Sicherheitsqualität, des App-Verhaltens und der Implementierungs- oder Deployment-Eigenschaften verwendet werden. Die komplette »Appicaptor«-Infrastruktur wird in Deutschland betrieben.

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
- Erstellen von App-Negativlisten und -Positivlisten für Enterprise-Management-Systeme
- Integration der Ergebnisse in Enterprise-Management-Systeme
- Meldung kritischer App-Schwächen durch »Appicaptor« an App-Hersteller (Hersteller-Feedback)
- Konzepte für den sicheren Einsatz von mobilen Geräten (ganzheitliches Mobile Device-Management)
- Technische Beratung sowie Erstellung und Prüfung von IT-Sicherheitsrichtlinien
- Unterstützung bei der Entwicklung von sicheren Apps
- Automatisierte Basistests und Compliance-Checks
- Tiefgehende manuelle Schwachstellenanalysen von Apps
- Expertentests von App Binaries und App Source Code-Audits
- Entwicklung von Konzepten, Verfahren und Werkzeugen zur IT-Sicherheitstestung von mobilen Diensten und Geräte

Ihr Weg zu »Appicaptor«

- Vereinbaren Sie einen Termin für eine WebEx Live Demo
- Testen Sie den »Appicaptor«-Dienst einen Monat kostenlos
- Fordern Sie ein individuelles Angebot an

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.