Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Dr. Jens Heider
Rheinstraße 75
64295 Darmstadt
Germany

Phone +49 6151 869-233
Fax +49 6151 869-224
appicaptor@sit.fraunhofer.de
www.appicaptor.com

Appicaptor

FRAMEWORK FOR APP SECURITY TESTS

Which apps are safe to install on the company tablet or smartphone? Allowing staff to use apps indiscriminately may endanger the company's own security. Many app developers do not have sufficient IT security knowledge, which frequently leads to inadvertent vulnerabilities. App stores may check for malware, but specific app security features and correct implementation are not the subject to verification. Fraunhofer SIT has developed the »Appicaptor« test framework exactly with this scenario in mind, giving enterprises an opportunity to automatically check if apps are compliant with their IT security policy.

Using mobile devices harbors both chances and risks for enterprises. Apps represent a major threat. They are developed within a very short time, and frequently basic security functions contain security vulnerabilities or implementation errors. For reasons of efficiency, parts of the software code are often being reused such as modules for individual app functions. The errors of one developer are thus sometimes propagated in other apps. Experienced attackers take advantage of this and target such vulnerabilities specifically, for example to steal passwords or corporate secrets.

App Security Tests for iOS and Android Apps

»Appicaptor« provides companies with a test report for each app, which can be customized to meet their own security requirements. The analysis is carried out automatically. If detected security vulnerabilities or insecure use of sensitive data, the system generates warnings and checks whether this violates the security requirements. Since apps are often revised and new insights emerge concerning weaknesses and implementation errors, »Appicaptor« repeats the tests weekly as well, thus constantly evaluating the security features based on the latest technological knowledge.

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.

App security rating of an example app in the »Appicaptor« web interface

»Appicaptor« detects relevant app risks in communication, data usage, input interfaces, privacy sphere and runtime security. By carrying out sophisticated static analyses on the apps' binary files »Appicaptor« is able to recognize security-relevant implementation errors, vulnerabilities or risky behaviour. »Appicaptor« even classifies the applications based on the app descriptions in the app marketplaces. This allows to determine the most important security-relevant app function (for example file viewer, organizer, calculator, password manager, etc.). With this app classification the risk of each application may be determined based on the detected security features and evaluated with regard to the respective company requirements.

Enterprises can create whitelists or blacklists with »Appicaptor«. A whitelist will contain uncritical apps that the staff may use on their smartphones. A blacklist contains all those apps that do not meet the company's IT security policy. In addition, companies may automatically evaluate proprietary apps or apps from company-owned app stores for vulnerabilities on a regular basis. Both lists can be directly synced between »Appicaptor« and enterprise management systems, like AirWatch, MobileIron, or Sophos Mobile.

Flexible Tool Box

»Appicaptor« is a framework composed of different analytical methods and tools, which can be expanded by almost any new tool and test procedures. Fraunhofer SIT has put a lot of development work into the automatic generation of informative and comprehensible test reports. People without comprehensive IT security knowledge can understand these management reports. Although the manufacturer Apple published little about the internal structure of the iOS platform, it was possible to develop and integrate methods into »Appicaptor«, which can identify the risks of iOS app precisely and quickly. The framework is constantly being developed and adopted to new operating system versions. The system may be configured according to the individual requirements. This way, test criteria can be adapted to company-specific app rating.

Enterprises can use standard recommendations or create and deploy customized and fully automated policies to be in-line with their corporate IT security policy. More than 70 distinct parameters can be utilized to define specific custom policies to include App blacklisting or whitelisting based on app security quality, behavior and implementation or deployment characteristics. The complete »Appicaptor« infrastructure is operated in Germany.

Range of Services

- App tests with cyclic update of the respective app security assessment
- App analysis based on individual preferences depending on app classification related to app behavior and IT security requirements
- Recommendation of safer apps depending on customer functionality and security requirements
- Creation of app blacklists and whitelists for customer-specific enterprise management systems
- Integration of results in enterprise management systems (e.g., AirWatch, MobileIron and Sophos Mobile)
- Notification of critical app weaknesses to app developer by »Appicaptor« (feedback to app manufacturer)
- Concepts for the secure use of mobile devices (holistic mobile device management)
- Technical consultation; development and evaluation of IT security guidelines
- Support in secure app development
- Automatic basic tests and compliance checks
- In-depth manual app vulnerability analyses
- Expert tests of app binaries and app source code audits
- Development of concepts, procedures, and tools for IT security testing of mobile services and devices

Get in touch with »Appicaptor«

- Make an appointment for a WebEx Live Demo
- Test the »Appicaptor« service for a month
- Request a customized offer

Investments into your future

HESSEN

The investments for this development were co-financed by the EC's European Regional Development Fund and the State of Hesse.