Fraunhofer
IEM

FRAUNHOFER-INSTITUT FÜR
ENTWURFSTECHNIK MECHATRONIK IEM

SICHERE SOFTWARE-IMPLEMENTIERUNGEN MIT COGNICRYPT

Ausgangslage

UNSICHERE NUTZUNG VON KRYPTOGRAFIE FÜHRT ZU SOFTWARESCHWACHSTELLEN

Eine Vielzahl aktueller Studien belegt, dass die meisten Softwareanwendungen, die kryptografische Verfahren einsetzen, diese auf unsichere Art und Weise falsch benutzen. Der VeraCode-Report State of the Software Security 2017 listet die unsichere Nutzung von Kryptografie als zweithäufigste Ursache von Softwareschwachstellen, direkt hinter Data Leakage.

Im Rahmen des Sonderforschungsbereichs CROSSING der Technischen Universität Darmstadt und in Zusammenarbeit mit dem Heinz Nixdorf Institut der Universität Paderborn wurde das Werkzeug CogniCrypt entwickelt. Es erlaubt Entwicklern, sicherheitskritische Fehlbenutzungen kryptografischer Bibliotheken schnell und zuverlässig zu identifizieren und zu beheben. Das Fraunhofer IEM hat dieses Werkzeug nun zur Marktreife weiterentwickelt und stellt es als offizielles Eclipse-Projekt zur Verfügung.

CogniCrypt

www.cognicrypt.de

Die Vorteile

ANPASSBARE CODEANALYSE MIT KONFIGURATIONSSPRACHE

Mittels statischer Codeanalyse überprüft **CogniCrypt** vollautomatisch den Binärcode des gegebenen Programms. Hierbei identifiziert es Nutzungen von kryptografischen Schnittstellen und gleicht diese gegen eine vom Fraunhofer IEM definierte Whitelist ab. Die Whitelist orientiert sich hierbei an der Technischen Richtlinie 02102 des BSI und wird vom Fraunhofer IEM laufend gepflegt.

Die Whitelist ist über eine komfortable Konfigurationssprache CrySL (Crypto Specification Language) einfach konfigurierbar. Wo gewünscht, kann sie somit auf einfache Weise auf unternehmensspezifische Vorgaben oder andere Standards angepasst werden. In der Zukunft plant das Fraunhofer IEM auch den Ausbau der Sprache und des Werkzeugs, um andere Arten von Sicherheitsschwachstellen detektieren zu können.

Der Nutzen

VERSTÄNDLICHE, PRÄZISE UND EFFIZIENTE ANALYSEERGEBNISSE

CogniCrypts Codeanalyse baut auf neuesten Erkenntnissen der Forschung am Fraunhofer IEM im Bereich der statischen Datenflussanalyse auf. Sie ist hocheffizient und gleichzeitig hochpräzise, mit einer Falsch-Positiv-Rate von in der Regel unter 10%. Die Analyse integriert sich effizient wie eine Rechtschreibprüfung in die Entwicklungsumgebung Eclipse, kann aber auch einfach in Continuous Integration-Umgebungen eingesetzt werden (Jenkins, Nexus etc.).

Für weitere Ausbaustufen des Werkzeugs plant das Fraunhofer IEM die automatische Generierung von Patches in der Form von Quick Fixes oder Pull Requests sowie die Generierung von beweisbar sicherem Integrationscode für gängige Krypto-Nutzungsszenarien.

In Kooperation mit:

CROSSING

TECHNISCHE UNIVERSITÄT DARMSTADT

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Projektstatus

AKTUELLER STAND

- Vollautomatisches Auffinden sicherheitskritischer Fehlbenutzungen der JCA (javax.crypto), hochpräzise und hocheffizient
- Einfache Anpassung der Whitelist über Konfigurationssprache CrySL
- Integration in die Eclipse IDE
- Integration in Jenkins mit JSON-Export der Ergebnisse
- Alternative Verwendung als Kommandozeilentool

GEPLANTE FEATURES

- Generierung von Patches als Quick Fixes oder Pull Requests
- Codegenerierung für gängige Krypto-Nutzungsszenarien
- Integration in IntelliJ und AndroidStudio
- Whitelists auch für BouncyCastle und andere Java APIs
- Unterstützung für C/C++ und Visual Studio, Whitelist für OpenSSL, etc.

AUF ANFRAGE

- Konnektoren für firmenspezifische Entwicklungs- und Build-Prozesse
- Whitelists für weitere, bisher nicht unterstützte APIs
- Ausbau auf weitere Arten von Schwachstellen

Ihre Ansprechpartner

Prof. Dr. Eric Bodden
Fraunhofer IEM
eric.bodden@iem.fraunhofer.de
Telefon +49 5251 5465-150

Johannes Späth
Fraunhofer IEM
johannes.spaeth@iem.fraunhofer.de
Telefon +49 5251 5465-355

Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM
Zukunftsmeile 1 | 33102 Paderborn
Telefon +49 5251 5465-101 | Fax -102
info@iem.fraunhofer.de
www.iem.fraunhofer.de