Fraunhofer
IEM

FRAUNHOFER INSTITUTE FOR
MECHATRONIC SYSTEMS DESIGN

SECURE SOFTWARE IMPLEMENTATIONS WITH COGNICRYPT

Current Situation

INSECURE USE OF CRYPTOGRAPHY LEADS TO SOFTWARE VULNERABILITIES

A large number of recent studies have shown that most software applications that use cryptographic procedures misuse them in an unsafe manner. The VeraCode Report State of the Software Security 2017 lists the unsafe use of cryptography as the second most common cause of software vulnerabilities, right after data leakage.

The **tool CogniCrypt** was developed within the collaborative research center CROSSING of the Technical University of Darmstadt and in cooperation with the Heinz Nixdorf Institute of the University of Paderborn. It allows developers to quickly identify and fix security-critical misuses of crytographic libraries. Fraunhofer IEM has now developed this tool to market maturity and makes it available as an official Eclipse project.

CogniCrypt

www.cognicrypt.com

Advantages

CUSTOMIZABLE CODE ANALYSIS WITH CONFIGURATION LANGUAGE

Using static code analysis, **CogniCrypt** automatically checks the binary code of the given program. It identifies uses of cryptographic interfaces and compares them against a white-list defined by Fraunhofer IEM. The whitelist is based on the Technical Guideline 02102 published by the German Federal Office for Information Security and is continuously maintained by Fraunhofer IEM.

The whitelist is easily configurable via a comfortable configuration language CrySL (Crypto Specification Language). Where desired, it can thus be easily adapted to company-specific specifications or other standards. In the future, Fraunhofer IEM also plans to expand the language and tool to detect other types of security vulnerabilities.

Benefits

UNDERSTANDABLE, PRECISE AND EFFICIENT ANALYSIS RESULTS

CogniCrypt`s code analysis is based on latest research results in static data-flow analysis achieved by researchers at Fraunhofer IEM. It is highly efficient and at the same time highly precise, with a false-positive rate of usually below 10%. The analysis integrates efficiently like a spell checker into the Eclipse development environment, but can also be easily used in continuous integration environments (Jenkins, Nexus etc.).

In the future, Fraunhofer IEM plans the automatic generation of patches in the form of quick fixes or pull requests as well as the generation of verifiably secure integration code for common crypto usage scenarios.

In cooperation with:

CROSSING

TECHNISCHE UNIVERSITÄT DARMSTADT

HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

Project Status

CURRENT STATUS

- Fully automatic detection of security-critical JCA (javax.crypto) misuses, highly precise and highly efficient
- Simple whitelist customization via CrySL configuration language
- Integration into the Eclipse IDE
- Integration in Jenkins with JSON export of results
- Alternative use as command line tool

PLANNED FEATURES

- Generation of patches as quick fixes or pulls requests
- Code generation for common crypto usage scenarios
- Integration with IntelliJ and AndroidStudio
- Whitelists also for BouncyCastle and other Java APIs
- Support for C/C++ and Visual Studio, Whitelist for OpenSSL, etc.

ON REQUEST

- Connectors for company-specific development and build processes
- Whitelists for other APIs not yet supported
- Detection of other types of vulnerabilities

Contact

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

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

Fraunhofer Institute for Mechatronic Systems Design
Zukunftsmeile 1 | 33102 Paderborn
Phone +49 5251 5465-101 | Fax -102
info@iem.fraunhofer.de
www.iem.fraunhofer.de/en