PROJECT GROUP CCPP

COGNICRYPT++ - BRINGING SECURE CRYPTOGRAPHY TO C/C++ APPLICATIONS WITH PHASAR

Stefan Krüger, Martin Mory, Philipp Schubert

January 28th, 2019




The Situation with Cryptography Libraries

88% of 11700 analyzed apps violate at least one cryptography rule[1]

SSL Libraries often misused, even by popular apps like amazon[2]

83% of reported vulnerabilites caused by library misuse[3]

[1] Egele et al., An emprirical study of cryptographic misuse in Android application, CCS 2013

[2] Fahl et al., Why eve and Mallory love Android: an analysis of Android SSL (in)security, CCS 2012

[3] Lazar et al., Why does cryptographic software fail?, APSys 2014

What should the developer use and how?

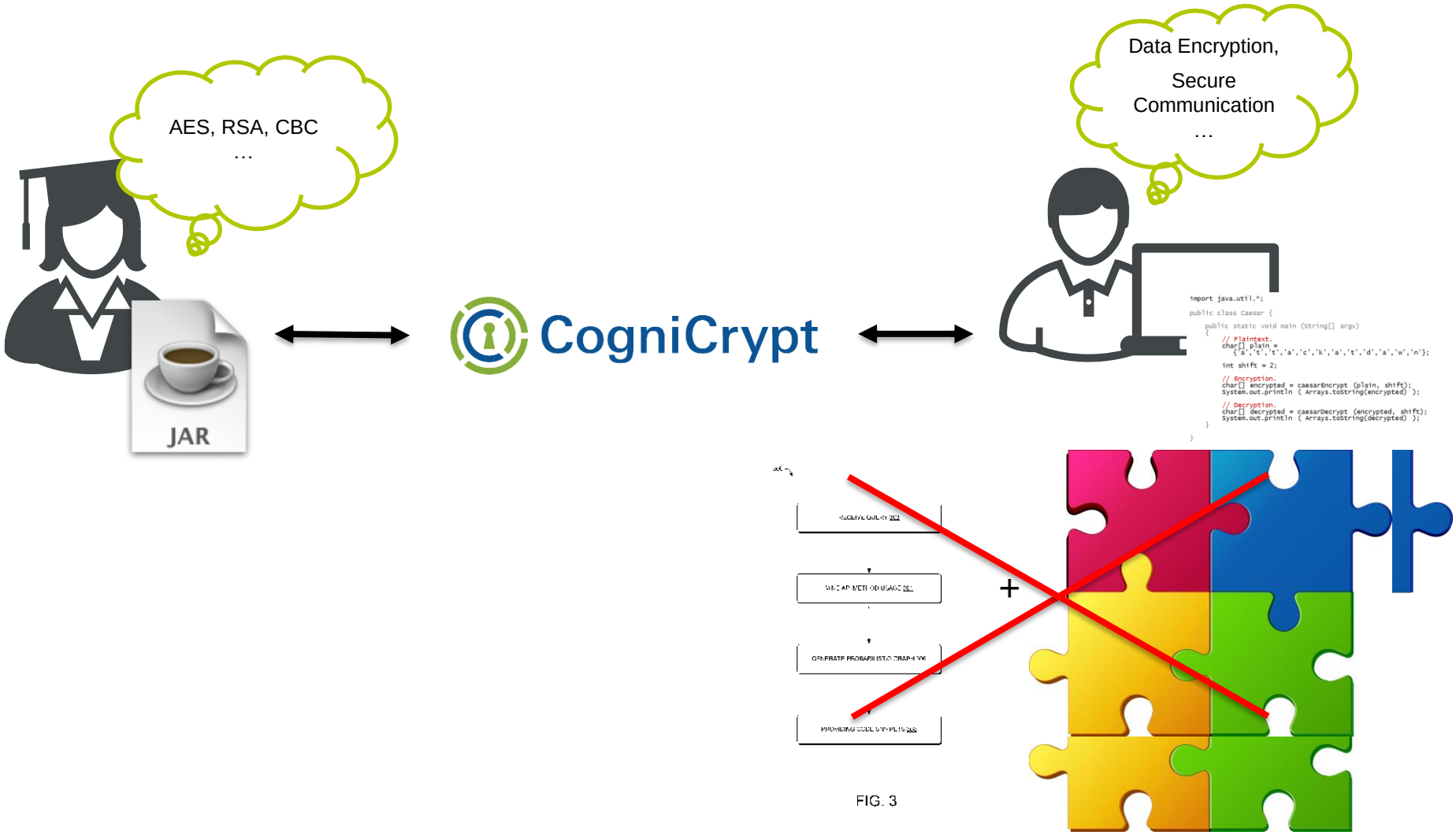
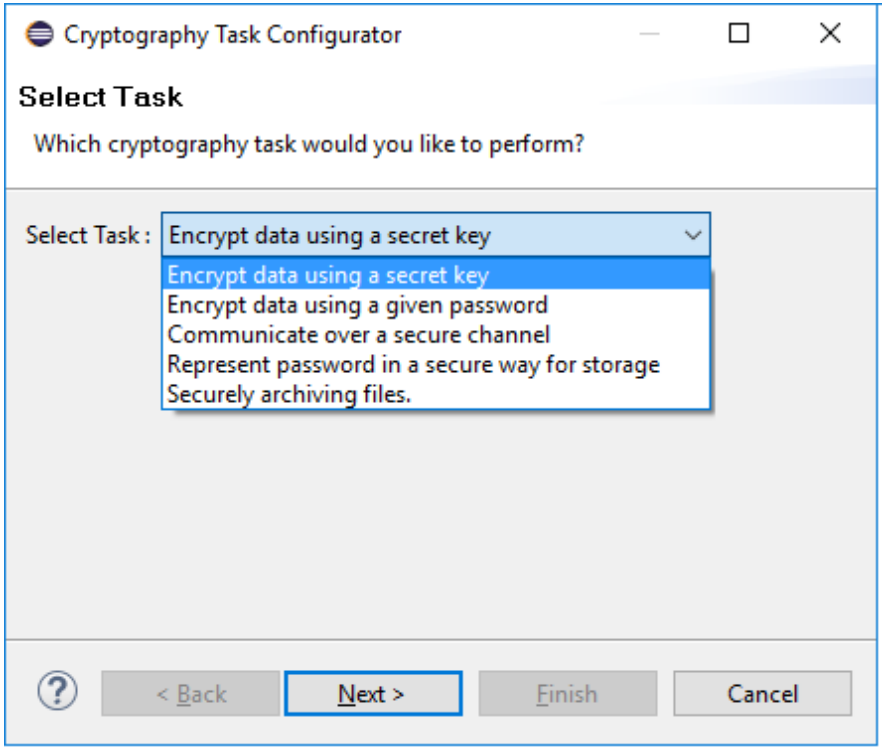


FIG. 3

CogniCrypt – Support with Cryptographic APIs

CogniCrypt

Code Generation



Static Analysis

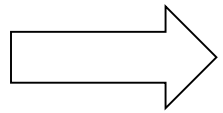
```
23
24  ECB is used Cipher c = Cipher.getInstance("AES");
25
```


HEINZ NIXDORF INSTITUT
UNIVERSITÄT PADERBORN

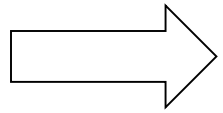
CogniCrypt as of now

CogniCrypt

javalogo



CogniCrypt



CogniCrypt

Project overview

- Goal: Create CogniCrypt++ by applying and extending concepts of CogniCrypt to be usable for C/C++ development
- Tasks:
  - Get familiar with involved concepts (e.g. cryptography, static analysis in PhASAR, CrySL)
  - Design Cognicrypt++ components
  - Develop these components in smaller teams
  - Ensure usability of tooling
  - Evaluate on real-world programs
  - (IDE Integration)

Project setting

- Requirements:
  - Advanced C++ skills
- Beneficial:
  - Knowledge of good software design and efficient programming.
  - Knowledge of cryptography, static analysis, variability modelling.
- Outcome:
  - Direct contribution to research project
  - Deepened understanding of program analysis and programming languages
- Number of Students: 5 or more

CogniCrypt++ – Subprojects

CogniCrypt

Creation of Micro-benchmarks

Task Wizard as IDE plugin

CrySL Compiler

PhASAR

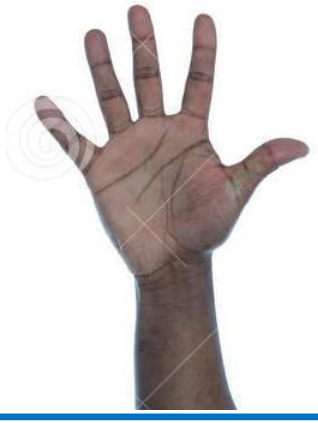
LSP Integration

Evaluation on Existing Software

Interested?

Talk to us after the presentation.

Contact us by email.



Contact information

- Stefan Krüger
  - stefan.krueger@upb.de
  - HNI/Paderborn University

- Martin Mory
  - martin.mory@upb.de
  - HNI/Paderborn University

- Philipp Schubert
  - philipp.schubert@upb.de
  - HNI/Paderborn University