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]

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

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

Where do the misuses come from?

- Data Encryption,
- Secure Communication

- AES, RSA, CBC

What should be done about it?

© Universität Paderborn
Slide 3
CogniCrypt – Support with Cryptographic APIs

**Code Generation**

![Cryptography Task Configurator]

Select Task

Which cryptography task would you like to perform?

- Encrypt data using a secret key
- Encrypt data using a given password
- Communicate over a secure channel
- Represent password in a secure way for storage
- Securely archiving files.

**Static Analysis**

```java
Cipher c = Cipher.getInstance("AES");
```
CogniCrypt as of now
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

- Creation of Micro-benchmarks
- Task Wizard as IDE plugin
- CrySL Compiler
- 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