A Dataset of Parametric Cryptographic Misuses

Anna-Katharina Wickert • Michael Reif • Michael Eichberg • Anam Dodhy • Mira Mezini

Software Technology Group
Technische Universität Darmstadt
Germany
A Parametric Crypto Misuse

```
public final class AES128Encoder {

    private static final String SECRET = "Sa87LK45Sjsd98HG";

    public static String encryptPassword(String decryptedText) {
        try {
            Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");
            cipher.init(ENCRYPT_MODE, generateKey(SECRET), new IvParameterSpec(IV.getBytes("UTF-8")));
            return Base64.getEncoder().encodeToString(cipher.doFinal(decryptedText.getBytes("UTF-8")));
        } catch (Exception e) {
            throw new PlatformRuntimeException(e);
        }
    }
}
```

88% (Egele et al. 2013) / 95% (Krüger et al. 2018) Android Apps have at least one misuse

83% of Cryptographic Issues CVE Entries due to misuses of a crypto library (Lazar et al. 2014)
Methodology to Create the Data Set

134 projects

42 projects
199 misuses

53 projects

7 projects
44 misuses

The MUBench artwork is by Sven Amann - [CC BY-SA 4.0]
Methodology to Create the Data Set
Methodology to Create the Data Set

134 projects

53 projects

42 projects
199 misuses

7 projects
44 misuses

The MUBench artwork is by Sven Amann - [CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/).
Potential Data Set Usage Scenarios

Evaluation of Static Analysis Tools

Find Security Bugs on 10 projects

- Precision: 100%
- Recall: 42.7%

Research on Crypto APIs

Is there a connection between the number of misuses in a project and the code quality of the project?

Training Set for Learning Algorithms

Review site: http://mubenchmsr.akwickert.de/

https://github.com/stg-tud/MUBench/pull/427

Anna-Katharina Wickert | Technische Universität Darmstadt
My talk on one slide. 😊

Anna-Katharina Wickert
wickert@cs.tu-darmstadt.de
@akwickert

The MUBench artwork is by Sven Amann - (CC BY-SA 4.0).

Evaluation of Static Analysis Tools

- Find Security Bugs on 10 projects
- Precision: 100%
- Recall: 42.7%

Review site: http://mubenchmsr.akwickert.de/

88% (Egele et al. 2013) / 95% (Krüger et al. 2018) Android Apps have at least one misuse

83% of Cryptographic Issues CVE Entries due to misuses of a crypto library (Lazar et al. 2014)

Research on Crypto APIs
Is there a connection between the number of misuses in a project and the code quality of the project?

Training Set for Learning Algorithms

https://github.com/stg-tud/MUBench/pull/427
Literature


Anna-Katharina Wickert | Technische Universität Darmstadt