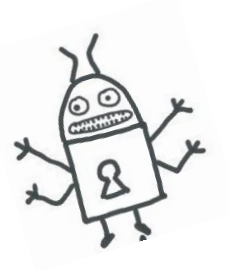
A Dataset of Parametric Cryptographic Misuses

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

Software Technology Group
Technische Universität Darmstadt
Germany

A Parametric Crypto Misuse

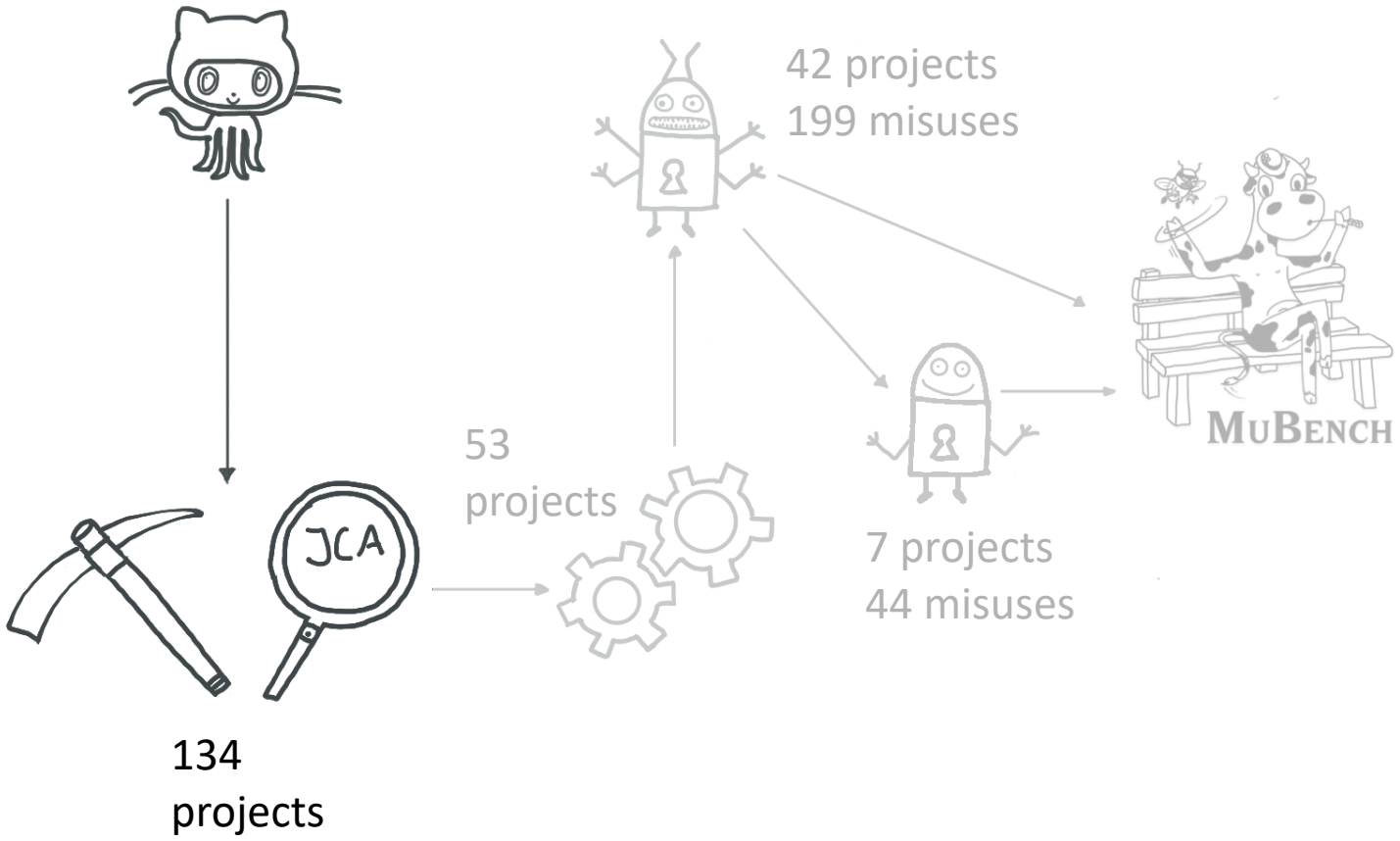
```
public final class AES128Encoder {
   private static final String SECRET = "Sa87LK45Sjsd98HG";

   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);
       }
    }
```



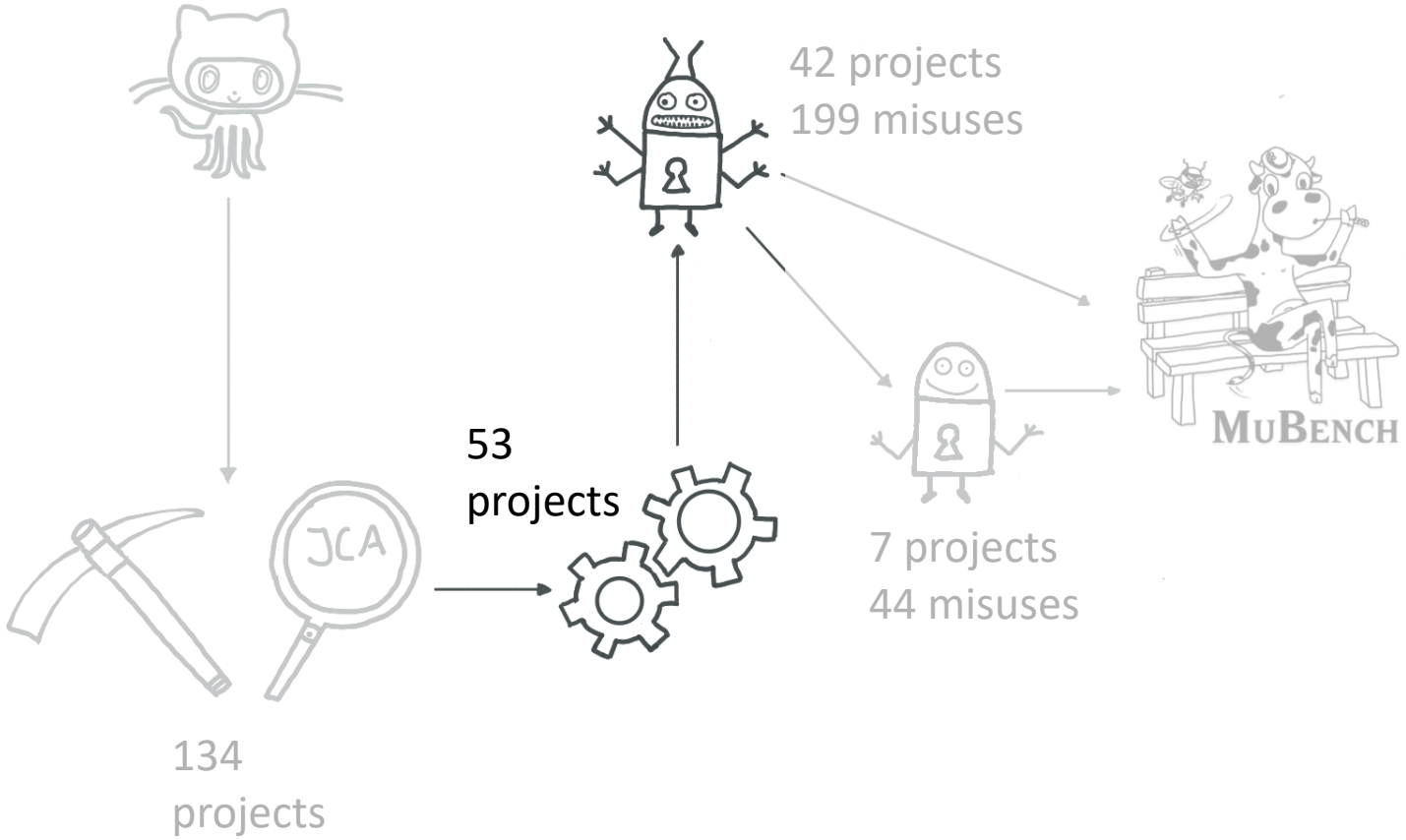
88% (Egele et al. 2013) **/ 95%** (Krüger et al. 2018) Android Apps have at least one misuse

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

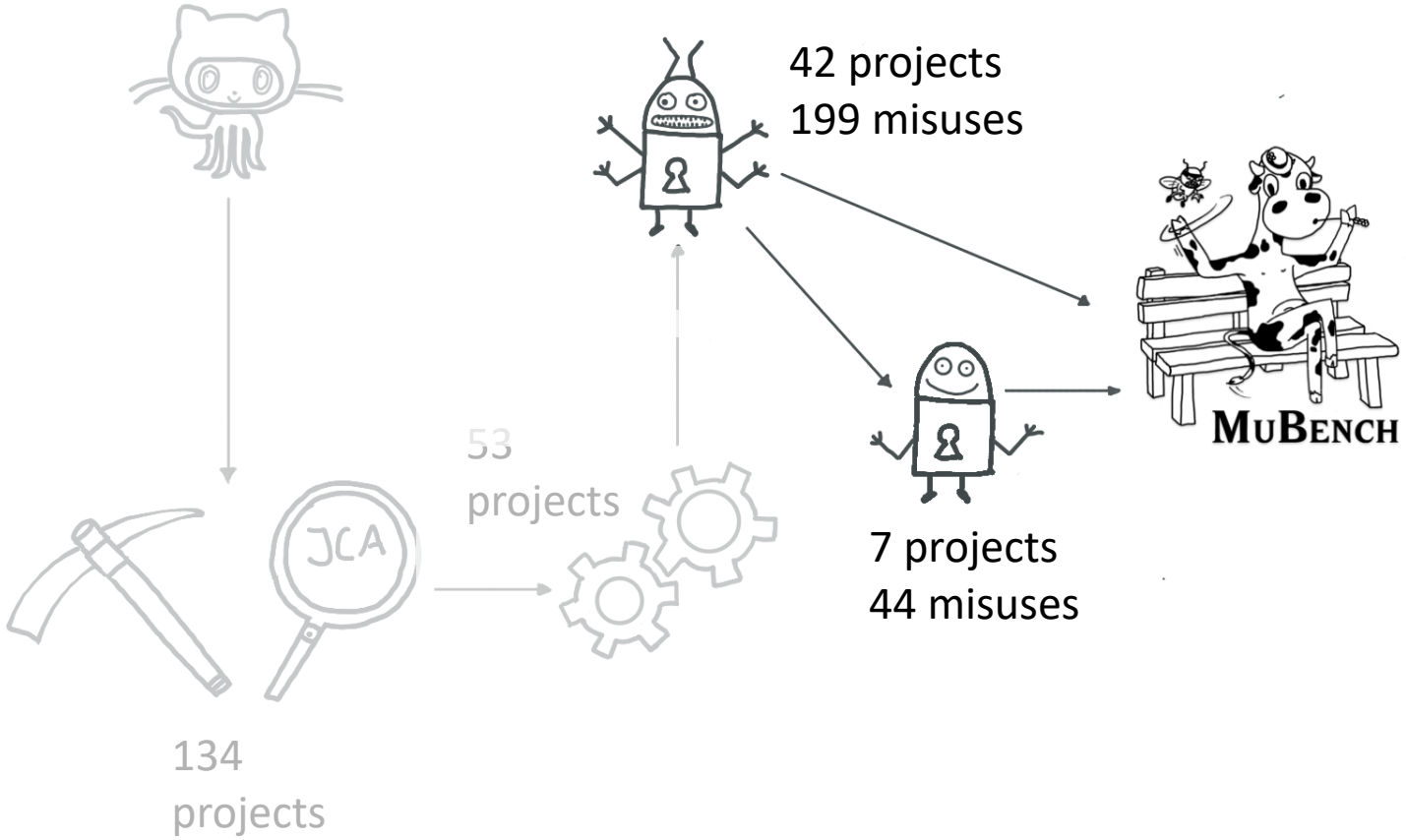
Methodology to Create the Data Set



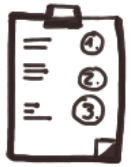
Methodology to Create the Data Set



Methodology to Create the Data Set



Potential Data Set Usage Scenarios



Evaluation of Static Analysis Tools

{  } Find Security Bugs on 10 projects

Precision

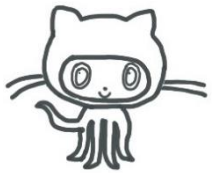
Recall

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

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

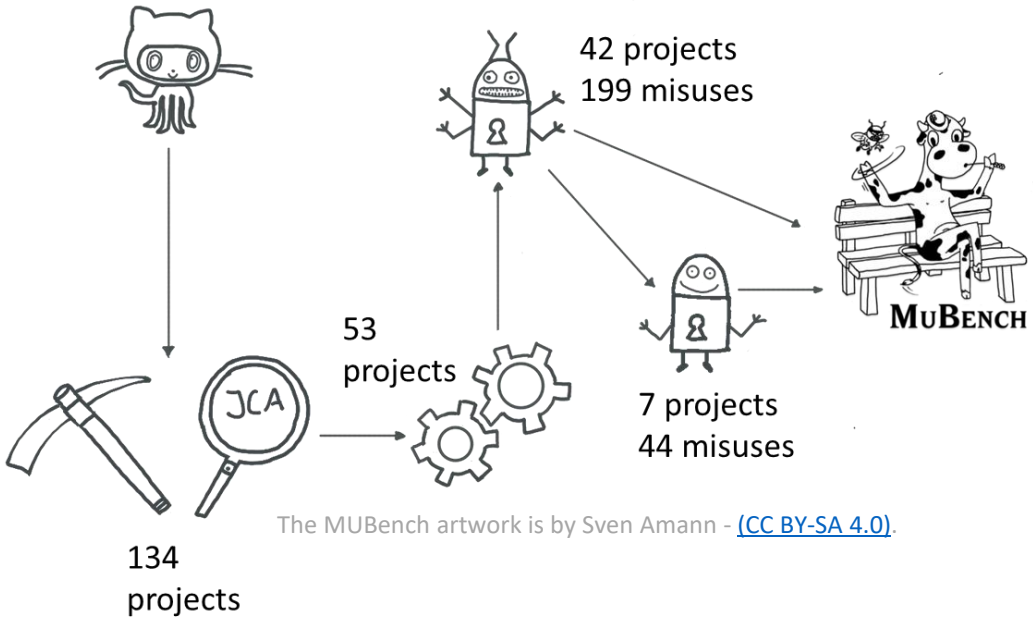
My talk on one slide. ☺

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

```java
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)



Evaluation of Static Analysis Tools

{🐞} Find Security Bugs on 10 projects

Precision

Recall

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

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

- M. Egele, D. Brumley, Y. Fratantonio, and C. Kruegel, “An Empirical Study of Cryptographic Misuse in Android Applications,” in Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, ser. CCS ’13. New York, NY, USA: ACM, 2013, pp. 73–84.
- S. Krüger, J. Späth, K. Ali, E. Bodden, and M. Mezini, “CrySL: An Extensible Approach to Validating the Correct Usage of Cryptographic APIs,” p. 27, 2018.
- D. Lazar, H. Chen, X. Wang, and N. Zeldovich, “Why Does Cryptographic Software Fail?: A Case Study and Open Problems,” in Proceedings of 5th Asia-Pacific Workshop on Systems, ser. APSys ’14. New York, NY, USA: ACM, 2014, pp. 7:1–7:7.