SaTC: TTP: Medium: Collaborative: Deployment-quality and Accessible Solutions for Cryptography Code Development

Danfeng (Daphne) Yao[1], Na Meng[1], Barton P. Miller[2]
[1]Computer Science, Virginia Tech, Blacksburg, VA
[2]Computer Science, University of Wisconsin-Madison, Madison, WI

1. Motivation: Deficiencies in Crypto Code

```
public class SymCrypto {

String ALGO = "DES";

  public SymCrypto() throws Exception {
     Cipher c = Cipher.getInstance(ALGO);
     …
  }
}
```

Input: Source Code

Code Screening tools

```
public class SymCrypto {

String ALGO = "DES";

  public SymCrypto() throws Exception {
     Cipher c = Cipher.getInstance(ALGO);
     …
  }
}
```

Insecure cipher used!

Output: Analysis Report

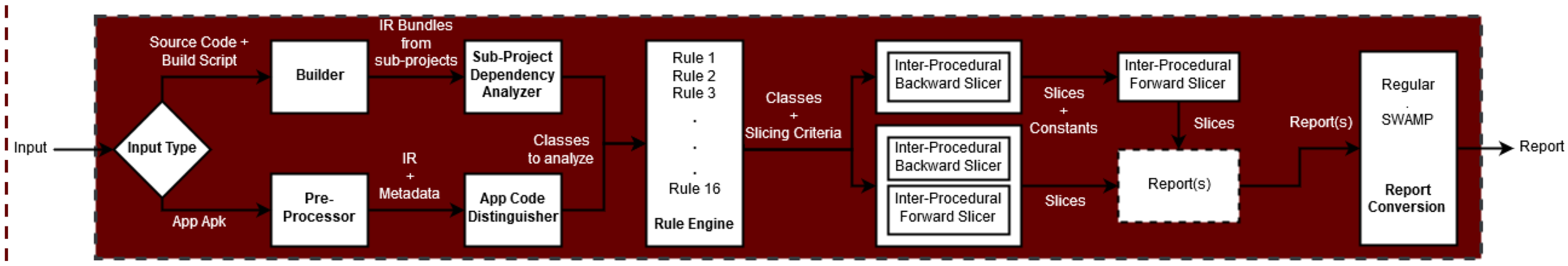
Vision: Accurate and scalable detection of cryptographic coding errors

2. Deployment Challenges

Who would not want to write secure code? But…

- *Many many many false positives*
- *Not scalable to millions LoC*
- *Lack of benchmarks*
- *Few deployment-grade solutions*
- *Lack of security awareness*

3. System Design of CryptoGuard

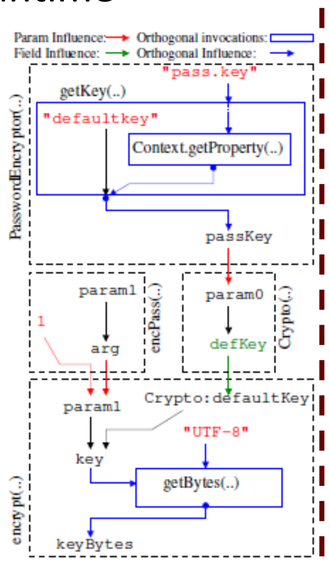


4. Technical Enablers

- *Refinement Strategies* to systematically remove false positives
- *On demand flow-, context-, and field- sensitive analysis* for accuracy/coverage
- *Clipping Orthogonal Explorations* to reduce runtime

```
1 class PasswordEncryptor {
2
3 Crypto crypto;
4
5 public PasswordEncryptor(){
6  String passKey = PasswordEncryptor
                      .getKey("pass.key");
7   crypto = new Crypto(passKey); (p)
8 }
9
10 byte[] encPass(String [] arg){
11  return crypto.encrypt(arg[0], arg[1]); (p)
12 }
13
14 static String getKey(String src){
15  String key = Context.getProperty(src);
16  if (key == null) {
17    key = "defaultkey";
18  }
19  return key;
20  }
21 }
```

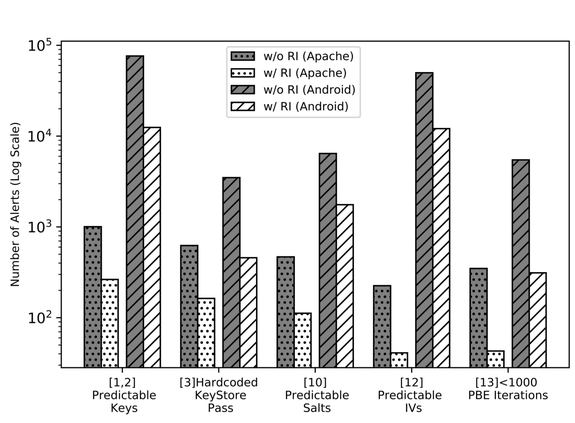
```
22 class Crypto {
23
24  String ALGO = "AES";
25  String ALGO_SPEC = "AES/CBC/NoPadding";
26  String defaultKey;
27  Cipher cipher;
28
29  public Crypto(String defKey){
30   cipher = Cipher.getInstance(ALGO_SPEC);
31   defaultKey = defKey; // assigning field
32  }
33
34  byte[] encrypt(String txt,String key){
35   if (key == null){
36    key = defaultKey; (f)
37   }
38   byte[] keyBytes = key.getBytes("UTF-8");
39   byte[] txtBytes = txt.getBytes();
40   SecretKeySpec keySpc =

   new SecretKeySpec(keyBytes, ALGO);
41   cipher.init(Cipher.ENCRYPT_MODE,keySpc);

42   return cipher.doFinal(txtBytes);}}
```



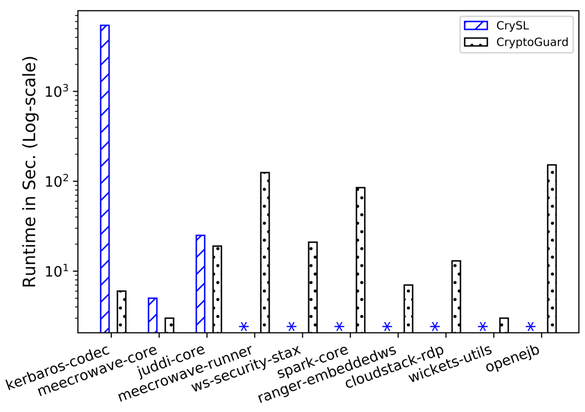
- *Achieved a precision of **98.61%** on real-world Apache projects*
- *CryptoAPI-Bench (basic & advanced cases, covering 16 crypto rules)*
- *Achieved **best precision** and **recall** on CryptoAPI-Bench compared with leading tools CrySL, Coverity and SpotBugs*

5. Ongoing Research Thrusts

- Designing compilers for automatic crypto-to-program-analysis mapping
- Providing repair suggestions to assist with post-detection investigations
- Developing benchmarks for evaluating the precision, recall, and runtime of leading tools
- Integrating tools with the software assurance marketplace (SWAMP)
- Enabling development-time code checking and actively develop training programs on secure coding



Reduction of FPs in 6 rules



Runtime w/ CrySL on 10 Apache projs

6. Broadening the Participation in Computing (BPC)

Inclusive Excellence Efforts: Increasing the numbers of females in various positions of ACM CCS, ACSAC, and IEEE SecDev conferences, including both attendance and organization and technical committees.

Outreach Activities: Presentations at Virginia Tech's Imagination Camp for rising 7-th and 8-th graders, Virginia Tech Women in Computing Day for 6-th grader girls, and various computing diversity venues, e.g., GHC.

Relevant Publications:

[1] S. Rahaman, Y. Xiao, S. Afrose, F. Shaon, K. Tian, M. Frantz, M. Kantarcioglu, D. Yao. CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects. *ACM CCS* 2019. (Acceptance rate: 16%)
[2] S. Afrose, S. Rahaman, D. Yao. CryptoAPI-Bench: A Comprehensive Benchmark on Java Cryptographic API Misuses. IEEE SecDev 2019.

CNS-1929701 (10/01/2019 – 09/30/2023)

For more information, please visit:
http://yaogroup.cs.vt.edu