Poster: A Comprehensive Benchmark on Java Cryptographic API Misuses

Sharmin Afrose, Sazzadur Rahaman, Danfeng (Daphne) Yao
Computer Science, Virginia Tech, VA, USA
{sharminafrose, sazzad14, danfeng}@vt.edu

1. Motivation

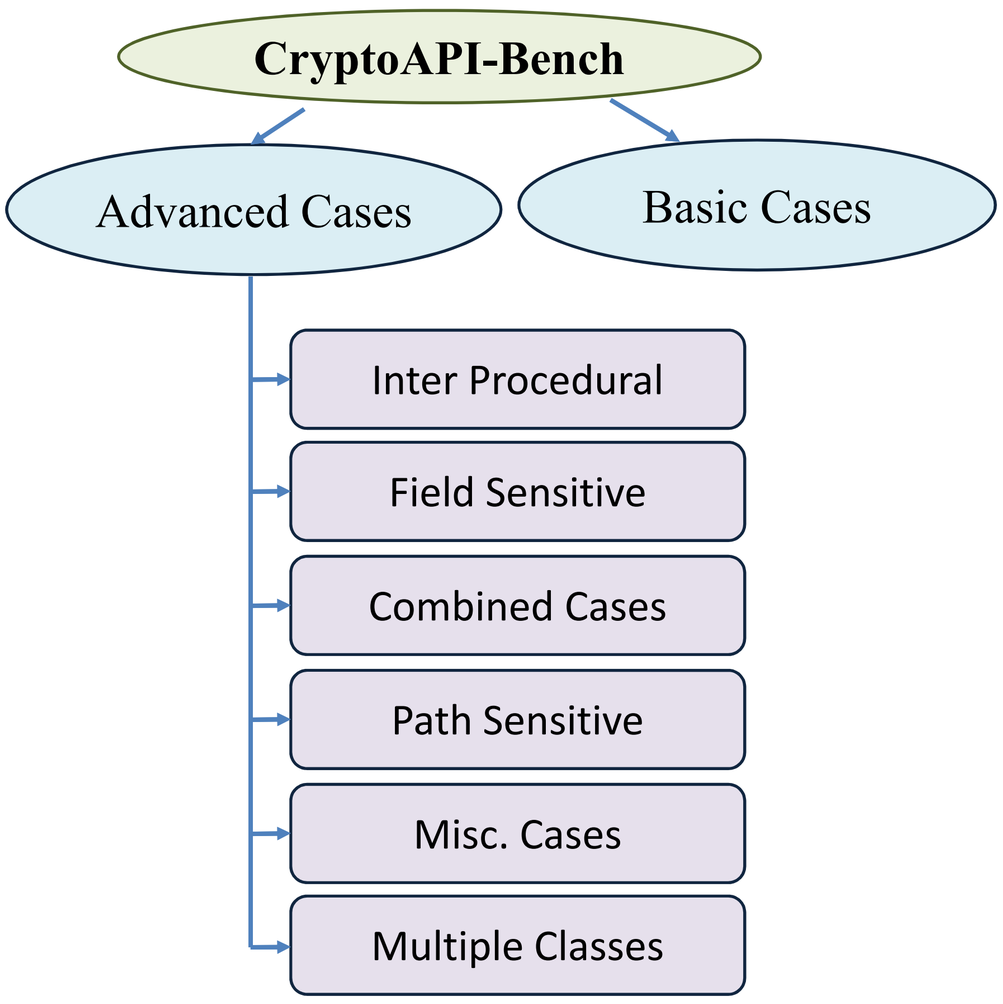
- ❑ Compare tool's accuracy and security guarantee.
- ❑ Decide which tool is suitable for developers to use.
- ❑ Educate cryptographically secure and insecure codes.

2. Threat Models

We consider **sixteen** cryptographic vulnerabilities from **five** attack types

- ❑ Predictable Secret
- ❑ Chosen Ciphertext Attack (CPA)
- ❑ SSL/TLS in MitM
- ❑ Brute-force Attack on Cipher
- ❑ Predictability in PRNG

3. Design of CryptoAPI-Bench



- ❑ Total 171 test cases.
- ❑ Contains 135 vulnerable and 36 non-vulnerable cases.
- ❑ Contains 40 basic and 131 advanced cases.

```
public class LessThan1000IterationPBEABSCase1 {
    CryptoPBEIteration1 crypto;
    public LessThan1000IterationPBEABSCase1() throws ... {
        crypto = new CryptoPBEIteration1(20);
        crypto.method1(0);
    }
}
class CryptoPBEIteration1 {
    int defcount;
    public CryptoPBEIteration1(int count) throws ... {
        defcount = count;
    }
    public void method1(int passedCount) throws ... {
        passedCount = defcount;
        SecureRandom random = new SecureRandom();
        PBEParameterSpec pbeParamSpec = null;
        byte[] salt = new byte[32];
        random.nextBytes(salt);
        pbeParamSpec = new PBEParameterSpec(salt,passedCount);
    }
}
```

Fig 1: Example of a vulnerable test case snippet (combined case)

4. Evaluation

Three Tools Selection Criteria:

- ❑ Open-sourced tool
- ❑ Static analysis tool
- ❑ Free analysis tool

Table 1: Evaluation result on CryptoAPI bench showing tool's performance on six common threat model rules with common 104 basic and advance cases

Tools	Basic Cases		Advanced Cases	
	Precision (%)	Recall (%)	Precision (%)	Recall (%)
SpotBugs	100.00	92.86	0.00	0.00
CryptoGuard	100.00	92.86	83.33	95.59
CrySL	62.50	71.43	55.56	58.82
Coverity	100.00	92.86	52.00	19.12

5. Conclusion

- ❑ CryptoAPI-Bench contributes to improvements in the science of security..
- ❑ CrySL and CryptoGuard improve their tools using CryptoAPI-Bench that incur real world impact.

6. References

[1] https://github.com/CryptoAPI-Bench/CryptoAPI-Bench
[2] Welcome to the SWAMP. https://continuousassurance.org, 2018
[3] S. Rahaman, et. al. CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects, CCS'2019
[4] https://github.com/CROSSINGTUD/CryptoAnalysis
[5] https://www.synopsys.com/software-integrity/security-testing/staticanalysis-sast.html.

This work is supported by Office of Naval Research under grant ONR-N00014-17-1-2498.

VIRGINIA TECH

Yao Group on Cyber Security
http://people.cs.vt.edu/danfeng/

IEEE SecDev 2019