CamBench - Cryptographic API Misuse Detection Tool Benchmark Suite

https://arxiv.org/abs/2204.06447

Authors

Michael Schlichtig[1], Anna-Katharina Wickert[2], Stefan Krüger[3], Eric Bodden[1,4], and Mira Mezini[2]

Affiliations

[1] Heinz Nixdorf Institute at Paderborn University
[2] Technische Universität Darmstadt
[3] Independent
[4] Fraunhofer IEM

Acknowledgments

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) – SFB 1119 – 236615297 and by the German Federal Ministry of Education and Research and the Hessen State Ministry for Higher Education, Research and the Arts within their joint support of the National Research Center for Applied Cybersecurity ATHENE.

1 Context

Cryptographic APIs are often misused in real-world applications.
API misuse detectors aim to mitigate that problem.
Currently, no established reference benchmark for a fair and comprehensive comparison to evaluate these tools exists.

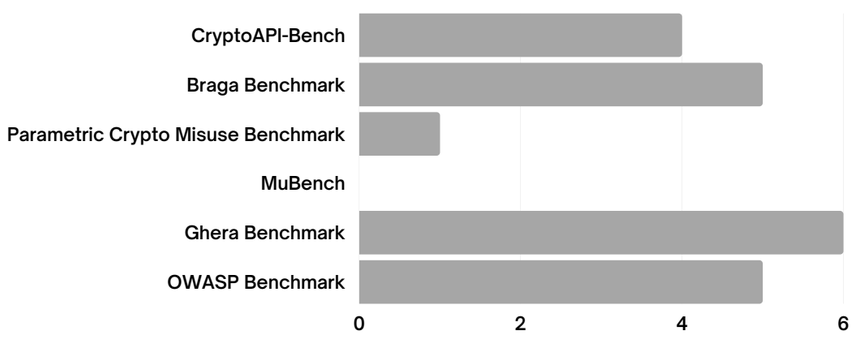
2 Objective

Devise a reference benchmark to fairly compare cryptographic API misuse detection tools and drive future development.

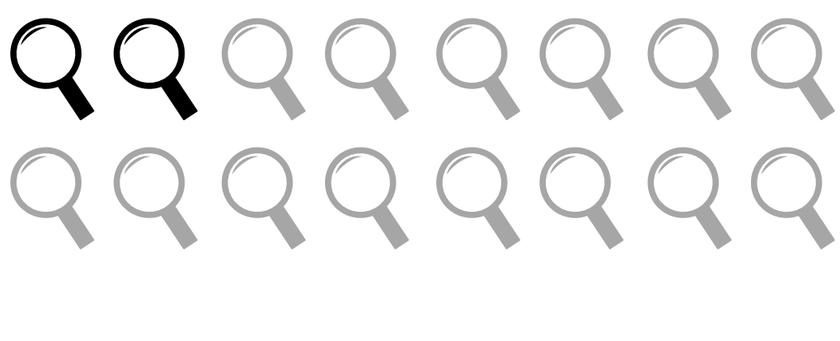
3 Method

Derive benchmark generation from literature [1,2].
Generate the benchmark transparently.
First version of the benchmark targets the JCA and static analysis.

4 Preliminary Study



We identified **6 benchmarks** that can detect crypto misuses and counted the number of misuse detectors that were evaluated with the respective benchmark.



We identified that **only 2 of** the evaluated **18 misuse detection tools** are evaluated on more than one benchmark.

5 Generation of CamBench

Based on a literature review for benchmark generation and an analysis of requirements for a cryptographic benchmark, we derived the design of CamBench.

CamBench_Real

Which misuses can misuse detectors identify in relevant real-world applications? [5]

1. Mining open-source projects
2. Filter for active projects
3. Filter for known build systems
4. Download and build projects
5. Filter for JCA usages
6. Add metadata file with information about secure and insecure JCA usages [3]

Benchmark for real-world applications

CamBench_Cap

Which analysis properties does the misuse detector support? [4]

Several synthetic test cases to cover these properties:

- flow-sensitivity
- context-sensitivity
- field-sensitivity
- object-sensitivity
- path-sensitivity
- intraprocedural
- inter-procedural

Benchmark for analysis capabilities

CamBench_Cov

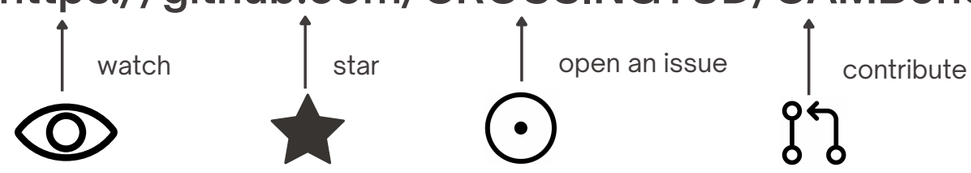
Which API classes are covered by a misuse detector?

Heuristic for crypto API coverage

6 Follow CamBench Development

We will publish our progress on the CamBench creation on GitHub and our evaluation of different cryptographic misuse detection tools.

https://github.com/CROSSINGTUD/CAMBench



[1] Blackburn, Stephen M., et al. "The DaCapo benchmarks: Java benchmarking development and analysis." OOPSLA. 2006.
[2] Do, Lisa Nguyen Quang, Michael Eichberg, and Eric Bodden. "Toward an automated benchmark management system." SOAP. 2016.
[3] Amann, Sven, et al. "MUBench: A benchmark for API-misuse detectors." MSR. 2016.
[4] Afrose, Sharmin, Sazzadur Rahaman, and Danfeng Yao. "Cryptoapi-bench: A comprehensive benchmark on java cryptographic api misuses." SecDev. IEEE, 2019.
[5] Wickert, Anna-Katharina, et al. "A dataset of parametric cryptographic misuses." MSR 2019.
... (all sources can be found in our arXiv paper: https://arxiv.org/abs/2204.06447)

Api Icons created by srip - Flaticon.