Faster Yet Safer: Logging System Via Fixed-Key Blockcipher

Viet Tung Hoang, Cong Wu, and Xin Yuan, *Florida State University*

https://www.usenix.org/conference/usenixsecurity22/presentation/hoang

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

Open access to the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium is sponsored by USENIX.

A Artifact Appendix

A.1 Abstract

The artifact contains the source code and installation scripts for the secure logging systems QuickLog and QuickLog2 in the paper. We also provided scripts to evaluate their application-independent signing and verification speeds, so that reviewers can reproduce the experiment results in Section 7.1 of the paper. We also included the code and scripts for installing and evaluating the competitor KennyLoggings.

A.2 Artifact check-list (meta-information)

- **Run-time environment:** CentOS 7 (Linux version 3.10.0-1160.49.1.el7). We also tested our code on Ubuntu 18 (Linux 5.4.0-120-generic) to ensure that our code works with other Linux distributions. The code requires root access.
- **Hardware:** Our code requires that the machine supports AES-NI, which is generally available in modern CPUs.
- **Execution:** Our code runs in Linux. For the evaluation of the signing cost, we provide two separate sets of scripts for Linux version 5 and prior versions.
- **Metrics:** The evaluation scripts report the stand-alone execution time for the signing and verification operations.
- **Output:** For each iteration, the script runs the operation for 200,000 times and computes the median execution time. It runs for 10 such iterations, and outputs the median and standard deviation of those 10 median timings. Users can customize the message size.
- **Experiments:** We provide instructions for how to install our logging schemes in the Linux kernel and evaluate their signing and verification speeds in the `README` file of the github link below. This allows one to reproduce the experiment results in Section 7.1 of the paper.
- **How much disk space required (approximately)?:** 10MB.
- **How much time is needed to prepare workflow (approximately)?:** Two hours (for downloading the Linux kernel source code and patching the kernel).
- **How much time is needed to complete experiments (approximately)?:** 10 minutes.
- **Publicly available (explicitly provide evolving version reference)?:** Our code and scripts are publicly available at `https://github.com/TsongW/QuickLog/tree/1d1cb65ace83308306c1ae80e884a1f4ed68facd`
- **Code licenses (if publicly available)?:** GNU v3.0

A.3 Description

A.3.1 How to access

The code and scripts are publicly available at the github link above.

A.3.2 Hardware dependencies

Our code requires that the machine supports AES-NI, which is generally available in modern CPUs.

A.3.3 Software dependencies

Our code requires the availability of the source code of Linux kernel.

A.3.4 Data sets

N/A

A.3.5 Models

N/A

A.3.6 Security, privacy, and ethical concerns

N/A.

A.4 Installation

- Download the Linux kernel source v3.10.0-1160.49.1.el7.
- Use the patches in the `patches` directory of the github link. Follow the guidelines to patch the Linux kernel at `https://wiki.centos.org/HowTos/Custom_Kernel`.

A.5 Experiment workflow

We provided scripts for compiling and benchmarking the schemes in the `README` file of the github link above.

A.6 Evaluation and expected results

The paper uses three benchmarks to evaluate the secure logging schemes; the artifact however only contains scripts to reproduce the first one. This benchmark measures the application-independent execution time of the signing and verification operations. For signing cost, we expect that (1) QuickLog and KennyLoggings have comparable performance for realistic log sizes (64B–384B), and (2) QuickLog2 is about twice faster than the other two schemes. For verification cost, we expect that (1) QuickLog and QuickLog2 have the same performance, whereas (2) KennyLoggings is 6–10 times slower. In our experiments, the standard deviation is within 5% of the median timing.

A.7 Experiment customization

N/A

A.8 Notes

The submission version of our paper contained only QuickLog. In the final version, we added an improved scheme QuickLog2 that has much faster signing time, better security, and no storage cost.

A.9 Version

Based on the LaTeX template for Artifact Evaluation V20220119.