USENIX'23 Artifact Appendix: CACHEQL: Quantifying and Localizing Cache Side-Channel Vulnerabilities in Production Software

Yuanyuan Yuan, Zhibo Liu, Shuai Wang
The Hong Kong University of Science and Technology
{yyuanaq, zliudc, shuaiw}@cse.ust.hk

A Artifact Appendix

A.1 Abstract

We provide code and data of our paper in this artifact. Our artifact is publicly available at https://github.com/Yuanyuan-Yuan/CacheQL with detailed documents. Using our tool, users can quantify the side channel leaks and localize the leakage sites for different software.

A.2 Description & Requirements

A.2.1 Security, privacy, and ethical concerns

Our artifact does not violate the security and privacy of evaluators. Nevertheless, since evaluators need to perform real-world side channel attacks (which require the root access) in some evaluations, we suggest evaluators using our artifact on test systems without sensitive data.

More importantly, we clarify that our artifact is provided as-is and is only for research purposes; any users should not use our scripts to attack others.

A.2.2 How to access

An archived copy of the initial version is available at: https://zenodo.org/record/8062035.

Our artifact is actively maintained at: https://github.com/Yuanyuan-Yuan/CacheQL.

A.2.3 Hardware dependencies

We do not have any particular requirements for the hardware. Our artifact may need GPUs to speed up training neural networks; we suggest evaluators having at least one GPU.

A.2.4 Software dependencies

Our tool is built based on Pytorch; evaluators need to first install Pytorch. See detailed instructions in our documents.

A.2.5 Benchmarks

None.

A.3 Set-up

A.3.1 Installation

Users only need to install Pytorch first. See details in our documents.

A.3.2 Basic Test

Our artifact requires first preparing some data and then analyzing these data. Please see detailed instructions in our documents.

A.4 Version

Based on the LaTeX template for Artifact Evaluation V20220926. Submission, reviewing and badging methodology followed for the evaluation of this artifact can be found at https://secartifacts.github.io/usenixsec2023/.