Pacer: Comprehensive Network Side-Channel Mitigation in the Cloud

Aastha Mehta, *University of British Columbia* (*UBC*); Mohamed Alzayat, Roberta De Viti, Björn B. Brandenburg, Peter Druschel, and Deepak Garg, *Max Planck Institute for Software Systems* (*MPI-SWS*)

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

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.

D Artifact Appendix

D.1 Abstract

The artifact consists of the full source code of Pacer's prototype and instructions for building from source. In addition, we provide applications, datasets, scripts, and instructions for reproducing two sets of results from the paper: Pacer's bandwidth overheads and its empirical security evaluation.

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

- **Algorithm:** video-clustering, doc-clustering, CNN classifier
- **Model:** custom CNN classifiers (included in the repository)
- **Data set:**
  (1) clustering dataset: csv containing sizes of files in the corpus,
  (2) attack dataset: network traffic traces to run classifier on
- **Run-time environment:** Linux, python
- **Execution:** manual
- **Metrics:**
  (1) bandwidth overheads vs privacy (cluster size)
  (2) attack performance (classifier accuracy, precision, recall)
- **Output:** table, graphs
- **Experiments:**
  (1) clustering (cluster size vs. bandwidth)
  (2) classifier prediction
  (3) Video latency
  (4) Medical service throughput and client latencies
- **How much disk space required (approximately)?:**
  All source code: 30GB
  Total including compiled models and dataset: 50GB
- **How much time is needed to complete experiments (approximately)?:** 24 hours in total
- **Publicly available (explicitly provide evolving version reference)?:** https://gitlab.mpi-sws.org/pacer/pacer
- **Code licenses (if publicly available)?:**
  Pacer: MIT
  Linux: GPLv2
  Xen: GPLv2 Apache HTTP Server: Apache License 2.0
  wrk2: Apache License 2.0
  Mediawiki: GPLv2
  Memcached: BSD license
- **Data licenses (if publicly available)?:**
  Wiki datasets: CC-BY-SA
- **Archived (explicitly provide DOI or stable reference)?:**
  https://gitlab.mpi-sws.org/pacer/pacer/-/tags/security22-ae

D.3 Description

D.3.1 How to access

The artifact is publicly available at: https://gitlab.mpi-sws.org/aasthakm/pacer

D.3.2 Hardware dependencies

To reproduce the runtime performance results, Pacer must be set up on servers with a Broadcom Corporation NetXtreme II BCM57800 1/10 Gigabit Ethernet NIC and with bnx2x driver.

D.3.3 Software dependencies

Pacer's prototype relies on:

- Xen: 4.10.0
- Linux: 4.9.5
- OS: Ubuntu 16.04 LTS
- gcc: 5.4.0

Experimental evaluation has been done with the following software:

- Apache HTTP Server: 2.4.33
- Mediawiki: 1.27.1
- Memcached: 1.6.9
- OpenSSL: 1.1.0g

D.3.4 Data sets

Relevant datasets are provided as part of this artifact.

D.3.5 Models

Models are provided as part of this artifact.

D.4 Installation

Instructions are provided at: https://gitlab.mpi-sws.org/pacer/pacer/-/blob/main/install.md

D.5 Experiment workflow

Experiments can be run using the scripts provided in the repository. All the instructions are provided at: https://gitlab.mpi-sws.org/pacer/pacer/-/blob/main/experiments.md

D.6 Evaluation and expected results

We provide prepared artifacts to reproduce results of Pacer's bandwidth overheads and empirical security evaluation:

- Bandwidth overhead (section 6.2): https://gitlab.mpi-sws.org/pacer/pacer/-/tree/main/eval/bandwidth
- Attack classifier performance evaluation (section 6.4, appendix A): https://gitlab.mpi-sws.org/pacer/pacer/-/tree/main/eval/attack

D.7 Version

Based on the LaTeX template for Artifact Evaluation V20220119.