A Artifact Appendix

A.1 Abstract

This artifact contains the source code of all the experiments that were used to produce the figures and numbers in the research paper. Its hardware requirements are a bare-metal machine with an Intel i7-9700 CPU (however, with some engineering efforts, the code can be ported to other Intel CPU models), and a second machine that can communicate with (i.e., send network requests to) the first machine. Its software requirement is Ubuntu 18.04 or 20.04 with its default system configuration. It will take approximately 10 days to reproduce the entire set of all the experiments in the paper.

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

- **Compilation:** GCC and Golang.
- **Hardware:** Two machines:
  1. A bare-metal machine with Intel i7-9700. However, with additional engineering efforts, the code can be ported to other CPU models (e.g., see Table 1 in the paper).
  2. A second machine that can communicate with (i.e., send network requests to) the first machine.
- **Security, privacy, and ethical concerns:** In the proof-of-concept attacks, you will launch both the attacker and the victim. No production servers are targeted.
- **Experiments:** Please checkout the README in the artifact for details on the experiments included.
- **How much disk space required (approximately)?:** We recommend at least 2 GB of free disk space.
- **How much time is needed to prepare workflow (approximately)?:** Overall, preparing the various workflows should take approximately 30 minutes on the i7-9700 CPU.
- **How much time is needed to complete experiments (approximately)?:** Reproducing all the experiments will take approximately 10 days.
- **Publicly available (explicitly provide evolving version reference)?:** Yes, the artifact is publicly available at `https://github.com/FPSG-UIUC/hertzbleed`
- **Code licenses (if publicly available)?:** University of Illinois / NCSA Open Source License.
- **Archived (explicitly provide DOI or stable reference)?:** `https://github.com/FPSG-UIUC/hertzbleed/releases/tag/usenix2022ae`

A.3 Description

This artifact includes (i) several experiments that reverse engineer the dependency between data, power and frequency on Intel CPUs and (ii) proof-of-concept attacks that leak full cryptographic keys from two SIKE libraries, break KASLR, and establish a covert channel using the frequency side channel.

A.3.1 How to access

`https://github.com/FPSG-UIUC/hertzbleed`.

A.3.2 Hardware dependencies

1. A bare-metal machine with Intel i7-9700. However, with additional engineering efforts, the code can be ported to other CPU models (e.g., see Table 1 in the paper).
2. A second machine that can communicate with (i.e., send network requests to) the first machine.

A.3.3 Software dependencies

A default installation of Ubuntu 18.04 or 20.04, and (if not pre-installed) the programs `gcc`, `golang`, `stress-ng`, and `python3`.

A.3.4 Data sets

N/A

A.3.5 Models

N/A

A.3.6 Security, privacy, and ethical concerns

No production servers are targeted. No sensitive data is collected, and no damage is caused to the machines.

A.4 Installation

Please checkout the README in the artifact for instructions on how to install the software dependencies.

A.5 Experiment workflow

Please checkout the README in the artifact for instructions on how to set up the experiment workflow.

A.6 Evaluation and expected results

The expected results are figures like the ones in the research paper and numbers like the ones reported in the research paper. Some variability is possible due to environmental/machine differences, but the general figure trends should apply.

A.7 Experiment customization

Please checkout the README in the artifact for instructions on how to customize the experiments.

A.8 Notes

N/A

A.9 Version

Based on the LaTeX template for Artifact Evaluation V20220119.