System Security Lab

TECHNISCHE UNIVERSITÄT DARMSTADT

Student Assistant for Persistent Memory Security

Emerging Non-Volatile Memories (NVMs) are promising technologies for memory and storage systems, like, e.g., Intel Optane Technology. NVM refers to memory cells that do not lose their contents when the power supply is off.

Nevertheless, adopting such technologies makes systems prone to the serious threat of cold boot attacks. An attacker can detach the memory module and easily manipulate or read out confidential data.

To mitigate such attacks, memory encryption and Merkle-tree for memory integrity enforcement can be applied. However, adopting such mechanisms would increase memory traffic and latency and lead to unintentional corruption of memory content if data and security meta-data are not written back to the memory before a system's power loss.

Our goal is to develop effective security solutions while taking into consideration power and performance metrics. For that, we are looking for excellent student assistants motivated to be part of the ongoing research in this area.

Your tasks include:

- Implement security solutions for the confidentiality and integrity of NVM system memory in the memory controller
- Tune the implementation to balance performance and power overhead

The tasks will be carried out with Gem5, a system simulator. Therefore knowledge of hardware description languages is not required.

Note that the task fits as a Bachelor thesis as well.

Prerequisites

- Knowledge of computer architecture
- Experience with C/C++ and Python
- Recommended: Knowledge or hands-on experience with Gem5
- Motivation and capability to perform independent work as well as readiness to work in a team

Contact

If you are interested in this highly trendy topic, contact Dr. Shaza Zeitouni or Dr. Markus Miettinen via info@trust.tu-darmstadt.de to learn more about it. Please include a brief overview of your study background and a transcript of records.

Technische Universität Darmstadt
FB Informatik – System Security Lab
S2|20 (CYSEC Gebäude)
Pankratiusstraße 2
64289 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

May 2023