Implementing and Evaluating Optimized Integrity Trees

Advisor: **Lukas Lamster**

Motivation

Trusted execution environments (TEEs) play a vital role in secure computing. A TEE isolates software from other software running on the same machine. Intel SGX protects their *enclaves* against malicious software and *even against hardware attackers*. This protection is achieved through a combination of **authenticated encryption** and **integrity protection** of DRAM data. Integrity trees such as the one used by SGX are powerful building blocks that detect unwanted manipulation of DRAM data.

Due to their hierarchical structure integrity trees impose non-trivial overheads on each memory access. A single request to main memory will entail a multitude of requests fetching the tree nodes. Researchers have proposed different types of integrity trees aiming to minimize the amount of additional memory operations and, thus, the imposed performance overhead.

This Project

We created a common gem5 framework allowing the simulation and evaluation of different tree implementations under consistent conditions. At the moment, the framework only implements the integrity tree variant used by the original SGX implementation. The goal of this project is to extend the framework with the integrity tree approaches proposed by the scientific community.

Goals and Tasks

- Learn about specific integrity tree implementations and their optimizations
- Extend our gem5 framework with the optimized integrity tree
- Compare the novel implementation with existing tree implementations

Literature

- V. Costan and S. Devadas
  Intel SGX explained
  Cryptology ePrint Archive 2016
- G. Saileshwar et al.
  Morphable counters: Enabling compact integrity trees for low-overhead secure memories
  2018 MICRO

Courses & Deliverables

☑ **Introduction to Scientific Working**
Short report on background
Short presentation

☑ **Bachelor Project**
Project code and documentation

☑ **Bachelor's Thesis**
Project code
Thesis
Final presentation

Recommended if you're studying

☑ CS ☑ ICE ☑ SEM

Prerequisites

- Interest in the topic area
- Programming: C++, Python

Advisor Contact

lukas.lamster@iaik.tugraz.at