Secure Design of SGX Enclaves

Taesoo Kim† Zhiqiang Liang§

†Georgia Institute of Technology §The University of Texas at Dallas

Lead PI Photo Optional

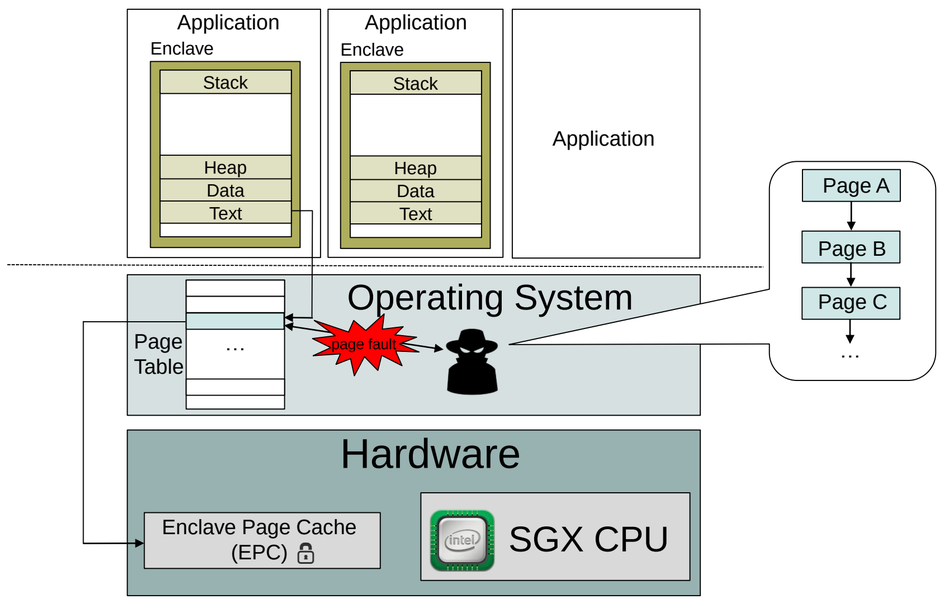
Overview

We proposed two practical design of SGX enclaves against known side-channel attack as well as traditional software attacks.

Current design of SGX enclaves is insufficient to meet the security guarantee provided by the SGX hardware. Recent studies have shown SGX enclaves are vulnerable to an accurate side-channel attack. Moreover, lacking support of Address Space Layout Randomization (ASLR) makes SGX enclaves easily vulnerable to traditional software attacks.

Intel Software Guard Extension (SGX) is a hardware-based Trusted Execution Environment (TEE) that enables secure execution of an application in an isolated environment, called an enclave. The confidentiality and integrity of an enclave are guaranteed, even if its underlying components are compromised.

Controlled-Channel Attack (*Xu et al., Oakland 2015*)



Approach

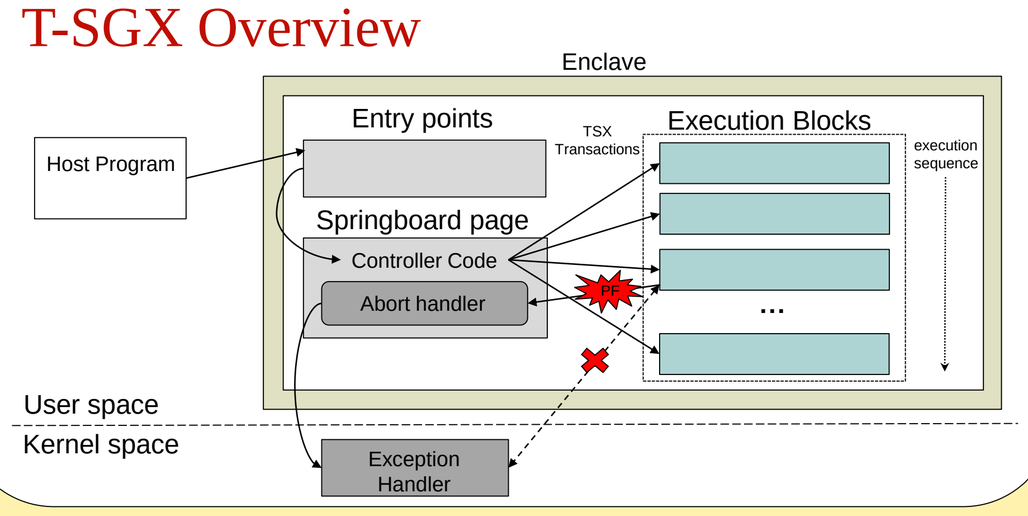
T-SGX

- Protect an enclave against controlled-channel attack
- Utilize Intel Transactional Synchronization Extensions (TSX)
- Detect a page fault in user space

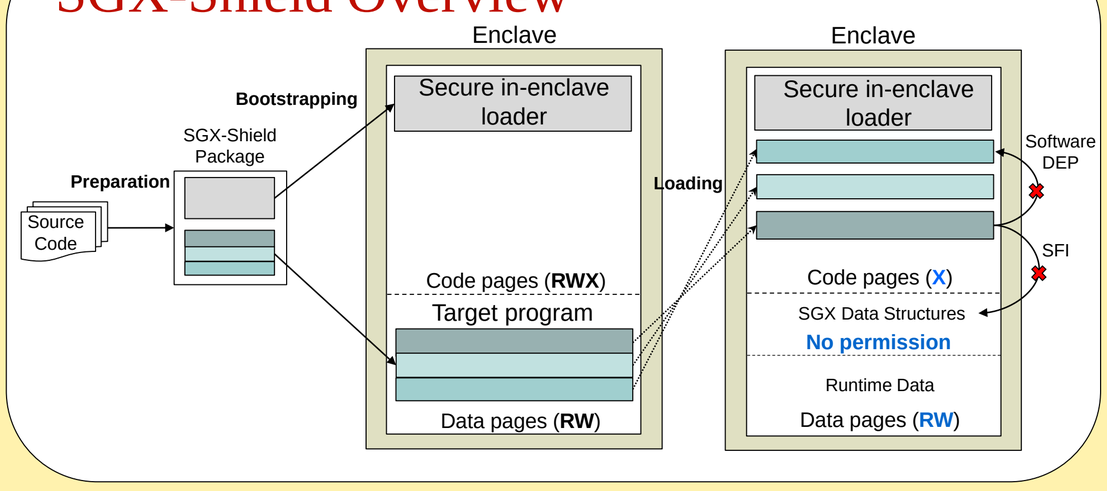
SGX-Shield

- Enable fine-grained ASLR for enclaves
- Implement a secure in-enclave loader that bootstraps a target program
- Incorporate with software DEP and software fault isolation (SFI)

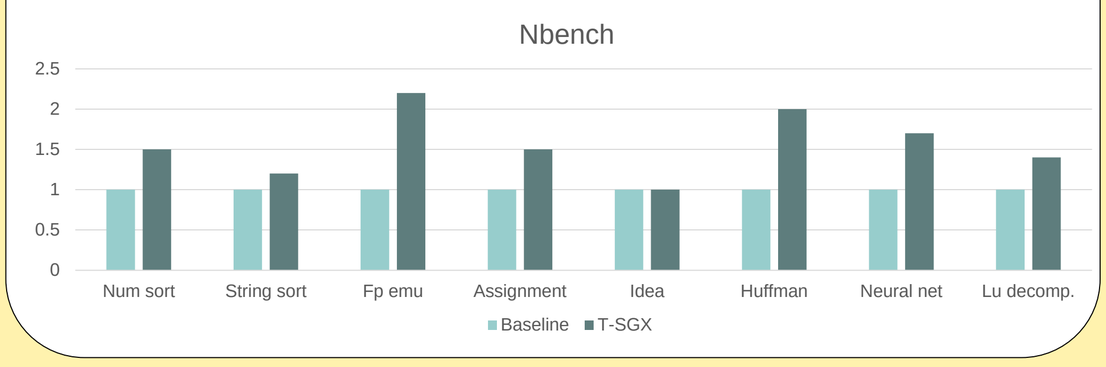
T-SGX Overview



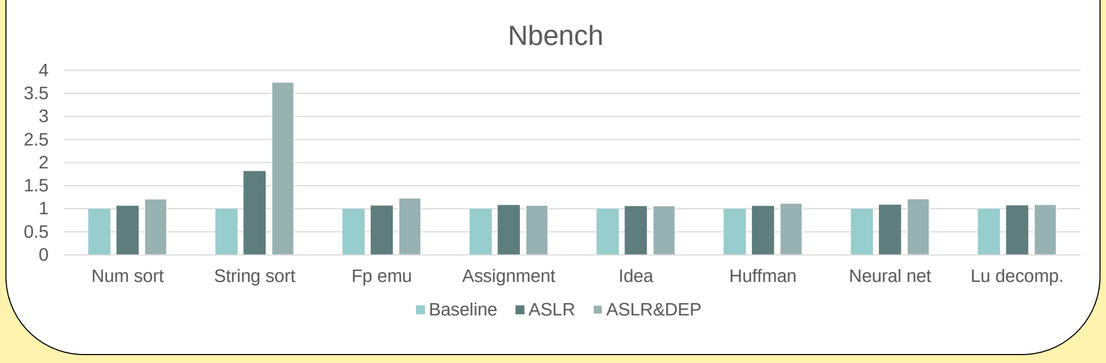
SGX-Shield Overview



T-SGX Performance Evaluation



SGX-Shield Performance Evaluation



Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

University #1 Logo

University #2 Logo