**TRUSTORE**: Side-Channel Resistant Storage for SGX using Intel Hybrid CPU-FPGA

*Hyunyoung Oh*, Adil Ahmad, Seonghyun Park, Byoungyoung Lee, Yunheung Paek
Motivation

- **Intel SGX (Software Guard eXtension)**
  - Processor extension providing shielded execution environment, called an enclave
  - Protected even from the privileged SWs (OS, hypervisor)

- However, SGX is vulnerable to various memory-based side-channels
  - Page-fault-based [S&P15], cache-based [WOOT17], branch-prediction [Security17], ForeShadow [Security18], RIDL [S&P19], Fallout [CCS19], ...
Motivation

• Conventional defense: ORAM (Oblivious RAM)
  ▪ Cryptographically proven protection
  ▪ Dummy objects are appended
  ▪ Shuffled after each access.

  ▪ Protection systems using ORAM for Intel SGX
    - ZeroTrace [Sasy et al., NDSS 2018]
      • data structures
    - Obliviate [Ahmad et al., NDSS 2018]
      • file systems
    - Obfuscuro [Ahmad et al., NDSS 2019]
      • blackbox-based program execution

  ▪ Notorious for high performance overhead (100x~ slower in general)
Motivation

• Our approach: using **FPGA** as an external storage device
  ▪ **Flexible and efficient** programmable hardware
  ▪ **Highly available**
    - Pluggable PCIe cards (Intel PAC, Xilinx Alveo)
    - Amazon, Microsoft clouds and pluggable PCIe cards
  ▪ **Separate from CPU that is vulnerable to various side-channel attacks**

---

If proper security mechanisms are provided...

sgx

FPGA interface
cache

➔ FPGA can be a secure storage device using FPGA as an external storage device

But FPGA is not secure as it is...

CPU

Isolated

Intel Programmable Acceleration Card (PAC) with Intel Arria 10 GX FPGA

Xilinx Alveo U250 Data Center Accelerator Card

---

Data Box Edge facilitates data transfer to Azure

---

Data Box Edge combines IoT Edge, a cloud gateway, and an FPGA for accelerated ML in an edge compute appliance.
Design Overview of **TrustOre**

- Design overview

- Two major components
  - **TrustLib**: In-enclave library establishing and managing the communication channel
    - Various APIs: alloc/dealloc/access, open/close/read/write/fsync
  - **TrustMod**: HW module loaded to the FPGA
TrustOre Designs

• **Secure Loading** of FPGA module

- Baking the keys inside FPGA during manufacturing
  - $k_{AES}$ for bitstream encryption
  - $k_{Priv}$, $k_{Pub}$ for bitstream authentication

- Provisioning FPGA and signing *TrustMod* bitstream by trusted manufacturer
- Introducing $k_{Priv}^{attest}$, $k_{Pub}^{attest}$ to remotely attest *TrustMod*
Secure Channel Establishment

- **Remote attestation**
  - Sending random nonce
  - Verifying the returned nonce signed by $k_{\text{Priv}}^{\text{attest}}$

- **Secret key sharing**
  - Enhancing the security by augmenting authentication on Diffie-Hellman key exchange
  - AES key is shared as session key
• *TrustLib* ↔ *TrusMod* communication on secure channel
  ▪ All requests/responses are transmitted in the form of encrypted transaction packet

• *TrustOre* guarantees
  ▪ *Constant* packet length: dummy padding
  ▪ *Constant* response time: *TrustMod* always takes worst-case cycle
  ▪ *Constant* address access pattern: repeatedly access on fixed MMIO/DMA
    - note) real address of object is concealed within the packet
Evaluation

• Environment
  ▪ *TrustMod* on Xilinx Zynq-7000 ZC706
  ▪ *TrustLib* on SGX-enabled Intel i7-6700 CPU
  ▪ ZC706 card is plugged on the system via PCIe interface

• Compare *TrustOre*-based scheme with ORAM-based scheme:
  ▪ ZeroTrace (for data arrays)
  ▪ Obliviate (for files)
  ▪ Obfusuro (oblivious program execution system based on ORAM)
Evaluation

- **Data array access (vs ZeroTrace)**
  - 49x faster access for various data block sizes (8B~8KB)
  - Constant throughput when # of data blocks increases

- **File access (vs Obliviate)**
  - 10x faster access for 1GB file
  - TrustOre also shows constant throughput for file size

- **Program obfuscation (vs Obfuscuro)**
  - 10.85x faster at micro benchmarks (findmax, sum, matmul)
  - More faster when input data size is increased

- **Nbench, key-value store application**
  - 120x faster at oblivious nbench execution
  - 188x faster at oblivious key-value data access
Conclusion

• We proposed *TrustOre*
  ▪ Side-channel resistant storage for SGX using Intel hybrid CPU-FPGA
  ▪ Implemented on commodity FPGA PCIe card

• *TrustOre* avoids memory-based side-channel attacks
  ▪ Security mechanisms making FPGA be securely isolated from rest of the system
  ▪ Secure loading, secure channel establishment, remote attestation, side-channel mitigations

• *TrustOre* shows higher performance than ORAM-based schemes, scales well as the data size increases
  ▪ 120 – 188 times faster for real-world workloads