Outline

Dinh Duy Kha

Introuction

Background and Related Works

PIM

PIM accelerators

PIM architectures

Baseline PIM assumptions

Confidential computing

Secure enclave and the cloud

Secure accelerators

Side-channel attacks and defenses

Overview of PIM-Enclave

Usage Model

is a secure in-memory accelerator

1. trusted by the host enclave
2. have secure communication channel
3. is efficient at processing large data

extends memory of CPU-based enclaves

1. protects confidentiality and integrity of data
2. hide the access pattern of data
    a. accesses from PIM
    b. accesses from host

demonstration with an k-mean example

1. k-mean is a data-intensive application
2. putting data to PIM allows host enclave to process more data
3. communication channel protected by AES
4. access pattern from PIM is hidden with the access control logic
5. access pattern from host is hidden with the secure access interface
6. data integrity is protected by only allows the secure access interface to update memory. Direct update must be requested by the host enclave.

Threat model & Design requirements

threat model

1. scope
    a. we protect
        i. the execution of PIM enclaves
        ii. data packets on the bus
        iii. observable memory changes
    b. out of scope:
        i. EM & power

    ii. Host-side side-channel
2. privileged software
    a. untrusted memory mappings
    b. unauthorized accesses to memory
3. physical attack on the bus
    a. snooping & side-channels
4. other
    a. dma attacks
    b. cold boot

requirements as secure in-memory accelerator

1. R1-a: establish trust with the host
2. R1-b: secure communication channel
3. R1-c: efficiently process large data

requirements as trusted memory

1. R2-a: protect confidentiality of data
    a. R2-a-1: memory encryption
        i. prevent unauthorized accesses & cold boot
    b. R2-a-2: hide the access pattern of PIM
    c. R2-a-3: hide the access pattern of HOST
2. R2-b: protect integrity of data
    a. replay, spoofing, splicng

Enabling in-memory confidential computation

Hardware capabilities

Remote attestation & key exchange

Satisfy R1-a & R1-b

Process large data efficiently with the AES engine

Satisfy R1-c

PIM-enclave as memory extension

keeping memory encrypted with a shared key

Satisfy R2-a-1

thwarting unauthorized accesses with the access control

Satisfy R2-a-2

Satisfy R2-b

enabling memory accesses from host with the secure access interface

Satisfy R2-a-3 by encrypting the access address (trustore, invisimem)

Satisfy R2-b by only allow memory updates through the interface

Implementation

Evaluation

security analysis

in-memory hash table

1. show sensitive application can be offloaded to PIM

secure access interface

1. show the interface can hide the access pattern

Microbenchmark

encrypted data transfer

secure access interface

data-intensive application

k-mean algorithm

1. demonstrate the computation model

Conclusion