RISCV with Sanctum Enclaves

Victor Costan, Ilia Lebedev, Srini Devadas
If computing remotely, what is the **TCB**?
Today, privilege implies trust (2/3)

If computing remotely, what is the TCB?

Sanctum decouples HW protection from trust!

Process boundary

VM boundary

Process

OS

12,000 KLOC

150 KLOC

CPU HW

Hypervisor

??? LOC

trusted computing base

Process

OS

Process

Process
Side channels leak privacy

Sanctum uses hardware-assisted isolation

Strong privacy & integrity with low overhead
Remote Software Attestation (1/2)

Trusted HW creates proof for remote user

Measures (hash) and Signs

Remote user

Diffie Hellman

Software Ecosystem

App
Remote Software Attestation (2 /2)

Remote user decides whether or not to trust certificate
Prior work: TPM, TXT

Trusted Platform Module
Trusted Execution Technology

Remote user
Diffie Hellman
Private data

Trusted HW must keep its keys private!

Measures (hash) and Signs

BIOS, OS, Device drivers and all
App

12,000+ KLOC

Software ecosystem must not be vulnerable

Prior work included too much SW in their attestation
Recent “Success”: Intel SGX

- Intel SGX
- Intel Factory
- Intel SGX CPU
- Process
- Process
- OS
- Enclave

Privilege

Ring 0 (supervisor mode)

Ring 3 (user mode)

12,000 KLOC

Enclave = immutable commitment of resources to one process.
Threat Model (Intel SGX)

Protect privacy* and integrity** of an enclave against a privileged SW adversary (OS/Hypervisor)

SGX prevents:

Directly reading/ tampering with:
- Config. registers
- Enclave memory
- Enclave process structures
- DMA-capable devices

Some specific physical attacks: Physical access!
- DRAM contents
- Device secret

*Indirect observation?
**Can SGX keep its keys private?
Threat Model (Sanctum)

Protect privacy and integrity of an enclave against a privileged SW adversary (OS/Hypervisor)

Sanctum prevents:

Directly read/tamper with:
- Config. registers
- Enclave memory
- Enclave process structures
- DMA-capable devices

Indirectly* observe private state via shared:
- Caches
- Microarchitectural state
- Data structures managed by the OS
- Interrupts / Faults

No protection against physical access or fault injection
Sanctum’s Chain of Trust

Manufacturer

Sanctum HW

Security Monitor (SM)

OS

Process

Certificate Authority

Strongly Isolated Enclave

Machine mode

Privileged (supervisor mode)

Unprivileged (user mode)
Sanctum’s Contributions

- Formally verifiable open source SM
- Truly small TCB for attestation (small SW and HW)
- Hardware-assisted isolation with strong guarantees

Certificate Authority

Open source SW

Stronger security with low overhead
+ 2% area
- 1-13% performance

5 KLOC

12,000 KLOC

Security Monitor (SM)

Manufacturer

Sanctum HW

Unprivileged (user mode)

Privileged (supervisor mode)

Machine mode

Hard-wired

Strongly Isolated Enclave
Sanctum modifies a RISCV Rocket Chip:

Build **hardware support** for small, trusted software to enforce **isolation guarantees** for unprivileged software.

Explicitly multiplex between private and OS-controlled state.
Enclaves execute on private cores

- Private L1 caches
- Private registers,
- Private branch target buffer
- Private TLB

Security monitor cleans up private state when allocating cores to enclaves / OS
Isolated Physical Memory in Sanctum

“DRAM region” is a unit of isolated memory

DRAM regions are non-overlapping

Only security monitor has access

OS Virtual Address Space
- Kernel Memory
- OS Page Tables
- Enclave 1 Private Page Table
- Enclave private data

An enclave’s Virtual Address Space
- Enclave 1 Private
- Enclave private data
- Enclave 1
- Enclave 2

Physical Address Space
- Security Monitor
- OS / non-enclave processes
- Enclave 1
- Enclave 2

OS / non-enclave processes
Isolating in the LLC (1/8)

Physical Address

512 sets, 4 banks

Find way with matching tag

Set associative (banked) cache

Select sets with set index

Select word from line

LLC

8 ways

15

11

6

Tag

Set Index

Line Offset

64 bytes
Isolating in the LLC (2/8)

Physical Address

LLC

OS starves enclave at LLC!

Availability of this set leaks privacy

64 bytes
Isolating in the LLC (2/8)

Physical Address

LLC sharing leaks privacy!

Give private LLC sets to enclaves!
Isolating in the LLC (4/8)

Virtual Address

Virtual Page Number

Page Offset

Physical Address

Page tables

Physical Page Number

Page Offset

OS controls

(TLB caches translations)

PTW performs translation

52 or fewer

4KB

20

12
To isolate enclaves in LLC, allocate exclusively, at region granularity!

"DRAM Region Index"
To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!

To isolate enclaves in LLC, allocate exclusively, at region granularity!
Each region is contiguous, 32KB

"DRAM Region Index"

Now top PA bits determine DRAM region

Rotate PPN to make colors contiguous in DRAM

Toy example: 3 DRAM region bits
Hardware-assisted Isolation

Maintain an invariant: *TLB entries are safe!*

HW enforces invariants at page walk
Protect SM memory from everyone

OS could rewrite S.M. code, do evil
fix by...

Never map VAddr to SM memory

S.M. sanitizes mode switch
Isolating Enclaves in Physical Memory

OS could read/write Enclave memory

fix by...

Enforce DRAM Region permissions to at page walk

S.M. updates permissions when scheduling enclaves
Isolating enclave page tables

OS could spy on enclave’s page table entries

fix by...

Implement enclave-private page tables
Sanctum modifies RISCV Rocket Chip (1/3)

Add hardware at interfaces only!

Enclave PTs
PTW invariant checker

~500 Gates, ~700 FFs
Per core
Sanctum modifies RISCV Rocket Chip (2/3)

Add hardware *at interfaces only!*

Enclave PTs

PTW invariant checker

~50 Gates

LLC addr. Rotation

DMA whitelist

(hacks upon hacks)

~6% overall performance overhead!
Sanctum modifies RISCV Rocket Chip (3/3)

Add hardware at interfaces only!

Enclave PTs
PTW invariant checker
LLC addr. Rotation
DMA whitelist

128 FFs  Device secret
Boot ROM

~2% area increase in total!
Measuring Overheads: Experimental setup

- **Platform headers**
- **Spec’06**
  - riscv-linux
  - RISCV Compiler
  - RISCV isa-sim
  - Sanctum LLC model
  - Post-process event log and counters

**Performance counters for Sanctum-related events**

- Estimated static costs for Monitor API calls.
- $ and DRAM access costs modeled after real devices
- >275 billion instructions simulated!
this slide is intentionally left blank
A Detailed Look at Sanctum’s Overheads (2/3)

Enclave overhead with a DRAM region allocation of 1/4 of LLC sets  

**Benefit from a large LLC**

**Perform lots of IO**

**Do not use LLC effectively**

**Overhead due to reduced LLC**

**Page miss overhead**

**Enclave enter/exit overhead**

**Overhead due to private cache flushes**

% completion time increase over insecure baseline
A Detailed Look at Sanctum’s Overheads (3/3)

Enclave overhead for various enclave sizes

% completion time increase over insecure baseline

- enclave with entire LLC
- enclave with 1/2 of LLC sets
- enclave with 1/4 of LLC sets
- enclave with 1/8 of LLC sets

Programs:
- hmmer
- libquantum
- astar
- omnetpp
- sjeng
- gobmk
- h264ref
- perlbench
- gcc
- mcf
- bzip2

% completion time increase:
- 0%
- 0%
- 0%
- 0.1%
- 0.6%
- 2.2%
- 1.6%
- 2%
- 2.8%
- 13.4%
- 11.2%
Trusted Manufacturer as CA

Data Owner’s Computer

Computation Dispatcher

Setup
Verification

Setup Computation
Receive Encrypted Results

Remote Computer

Trusted Hardware

Untrusted Software

Secure Container

Public Loader
Private Code
Private Data

Owns Trusts

Trusts

Data Owner

Authors

Manages

Infrastructure Owner

Builds

Manufacturer

Software Provider

Trusts
Remote Software Attestation

Data Owner’s Computer

Key exchange: $A, g^A$

Shared key: $K = g^{AB}$

Computation Results

$g^A$

Trusted Platform

AK: Attestation Key

Endorsement Certificate

Secure Container

Initial State
Public Code + Data

Key exchange: $B, g^A$

Shared key: $K = g^{AB}$

Secret Code + Data

Computation Results

$g^B, \text{Sign}_{AK}(g^A, g^B, M)$

$M = \text{Hash(Initial State)}$

$\text{Enc}_K(\text{secret code/data})$

$\text{Enc}_K(\text{results})$
Attestation in Sanctum
Physical Memory in Sanctum (1/2)
Physical Memory in Sacntum (1/2)