Interface Sanitization and Real-Time Scheduling for Enclaved Execution

Fritz Alder

October 19, 2023

Public PhD defense

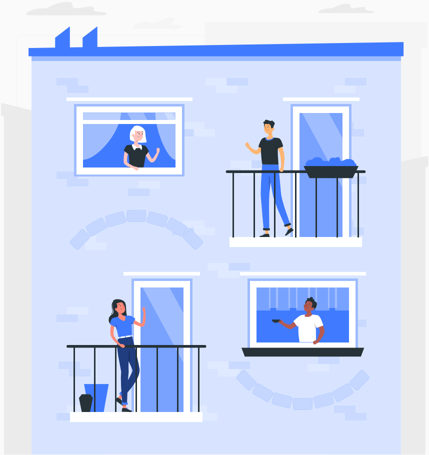
Interface Sanitization

Real-Time Scheduling

}

Enclaved Execution

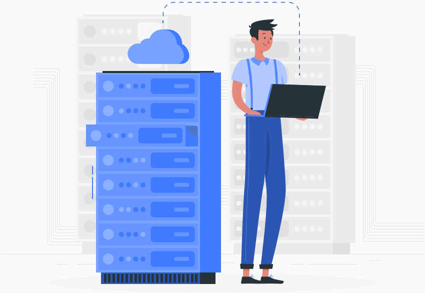
What is the problem?



Wear your
MASK

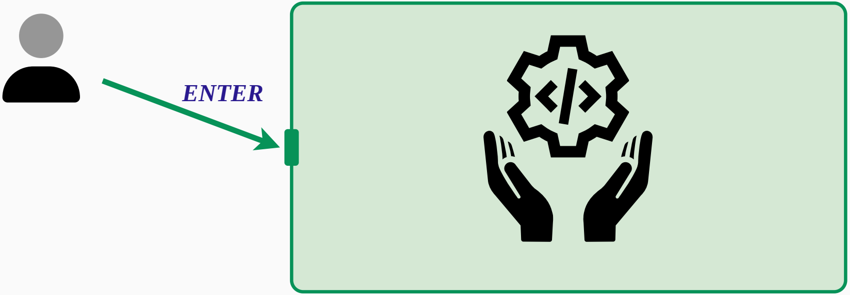
Interim summary

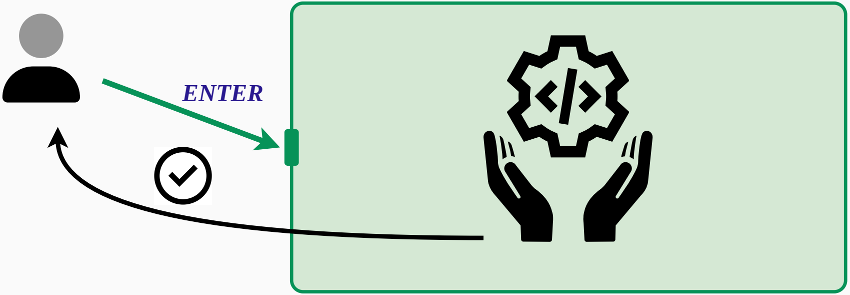
- Sharing resources is increasingly common.
- Sharing can be **dangerous!**

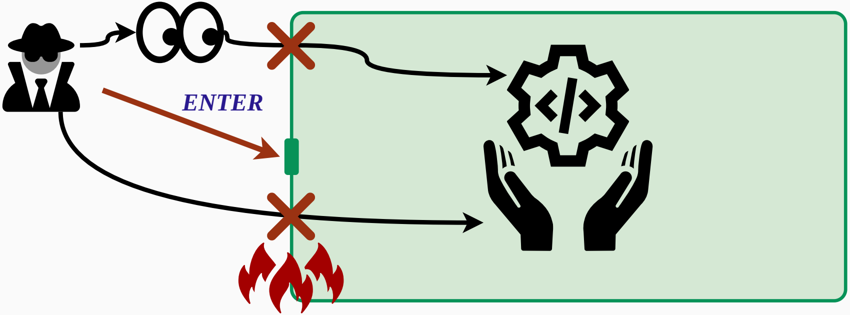


What is enclaved execution?

Source credit: Wikipedia user Ryanhuntmuzik, CC BY 4.0


ENTER


ENTER

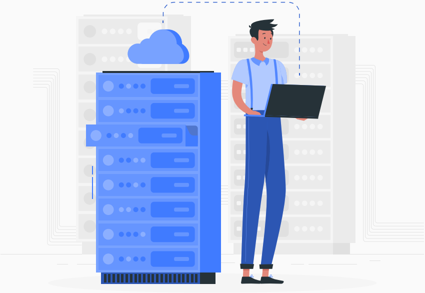

ENTER

Confidential computing properties

- Data confidentiality & integrity
- Code integrity
- Attestation

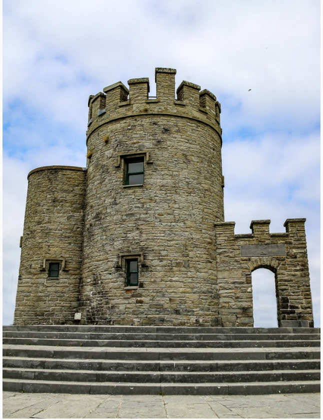
Interim summary

- Sharing resources is increasingly common.
- Sharing can be **dangerous!**
- Enclaved execution is one solution to **protect confidentiality and integrity**.



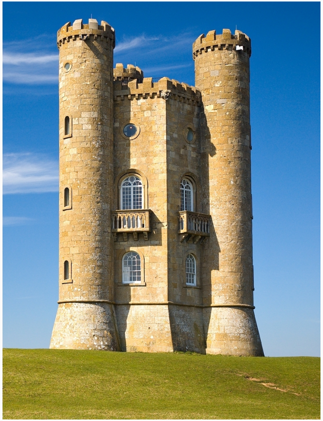
Interface sanitization for enclaved execution

Source credit: Chris Lathom-Sharp, CC BY-SA 4.0



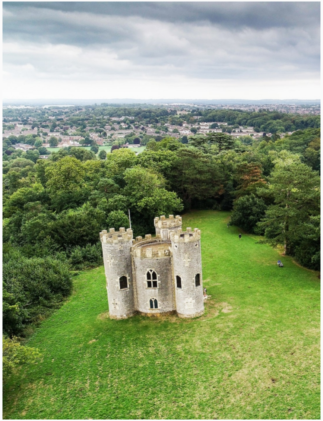
O'Brien's Tower

County Clare, Ireland



Broadway Tower

Worcestershire, England



Blaise Castle

Bristol, England

O'Brien's Tower

County Clare, Ireland

Built: 1835

Broadway Tower

Worcestershire, England

Built: 1799

Blaise Castle

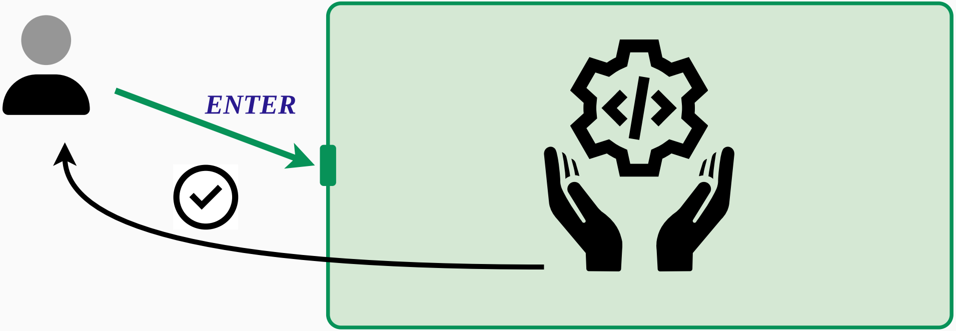
Bristol, England

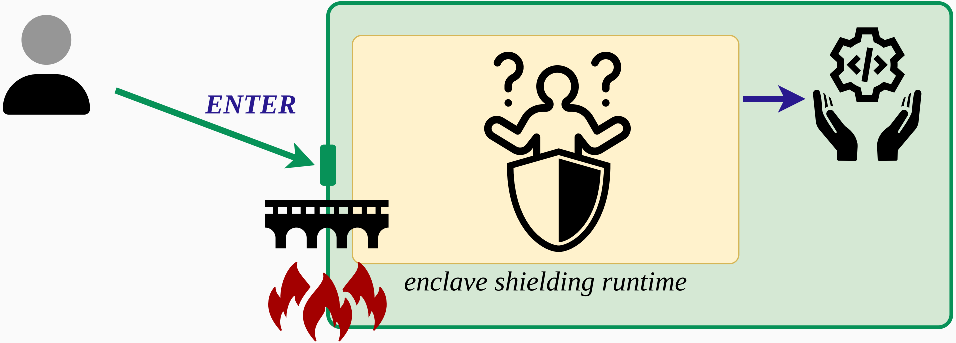
Built: 1766

That’s a folly!

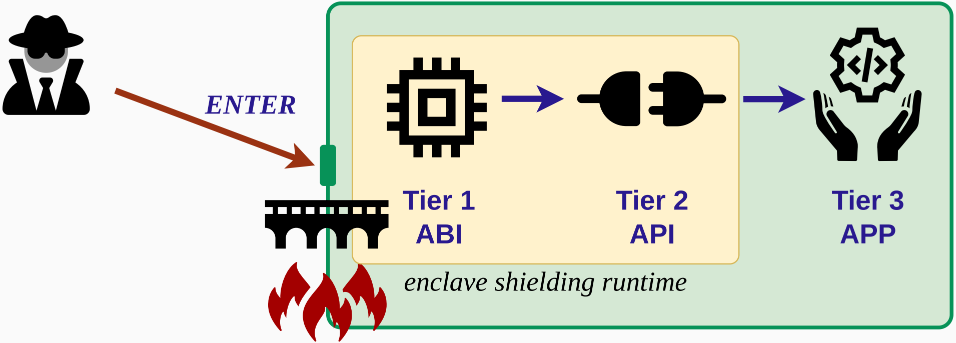
Source credit: Wikipedia user Newton2, CC BY 2.4

30 min before
goin outside
After sweating
or swimming


ENTER



ENTER
enclave shielding runtime



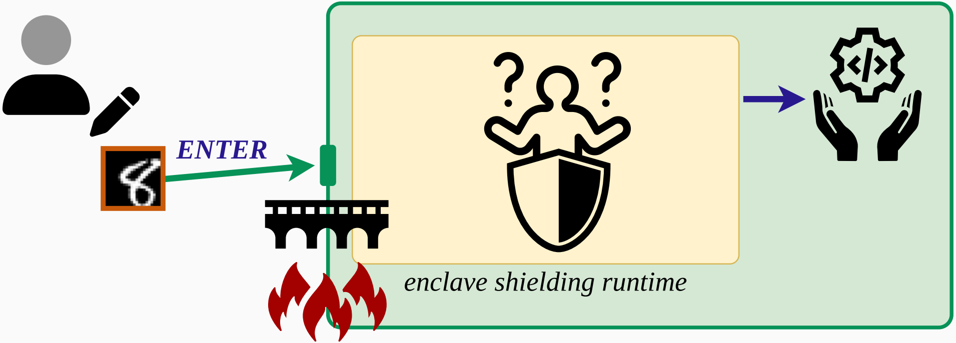
ENTER

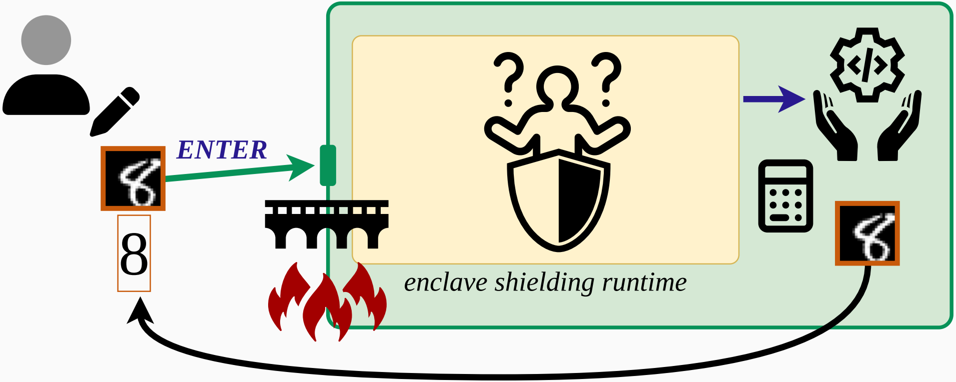
Tier 1
ABI

Tier 2
API

Tier 3
APP

enclave shielding runtime

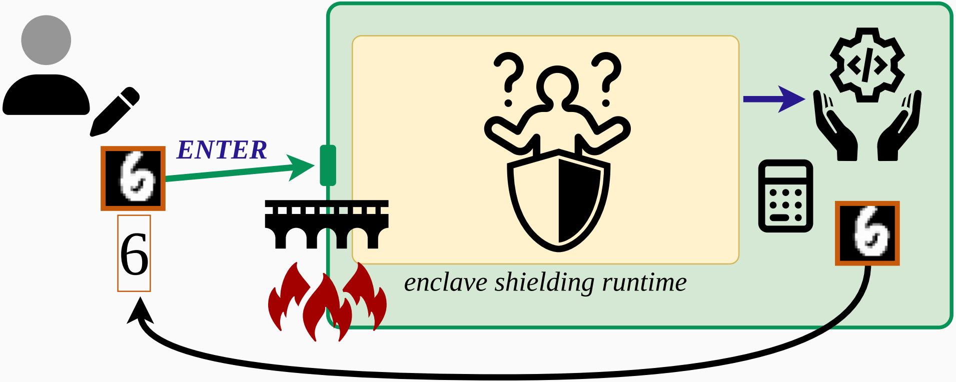

ENTER
enclave shielding runtime

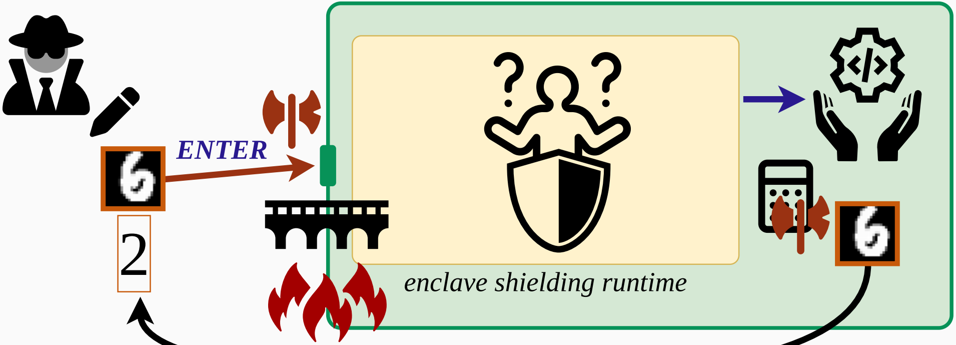


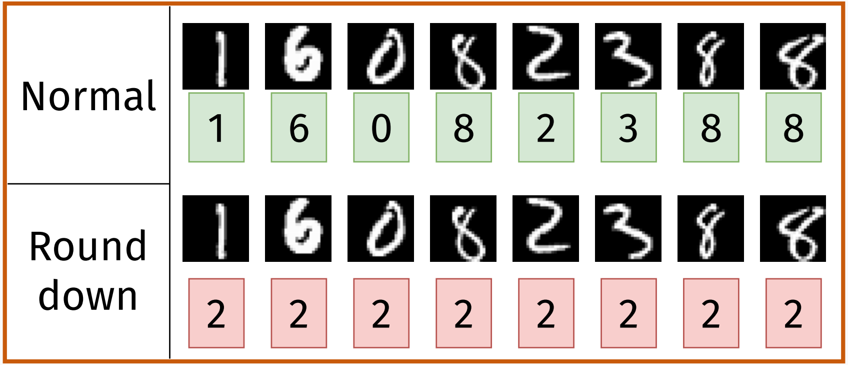
ENTER

8

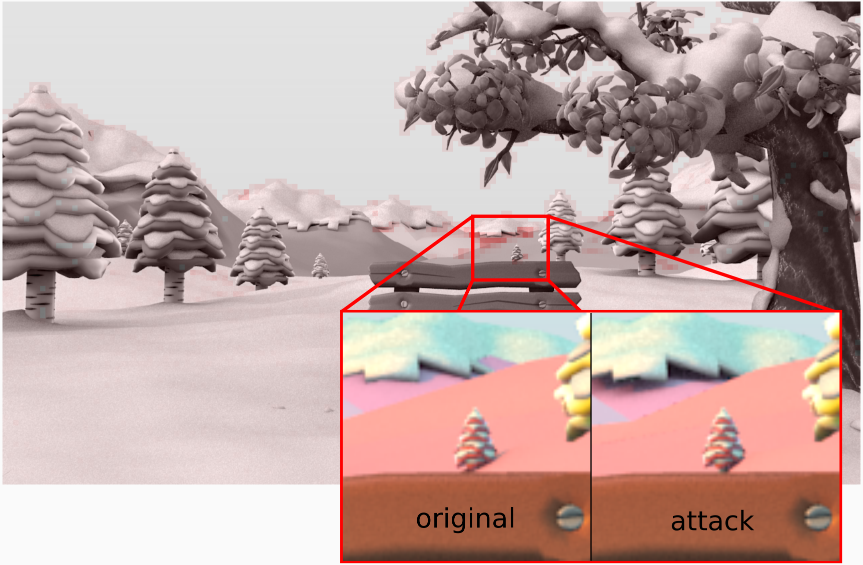
enclave shielding runtime

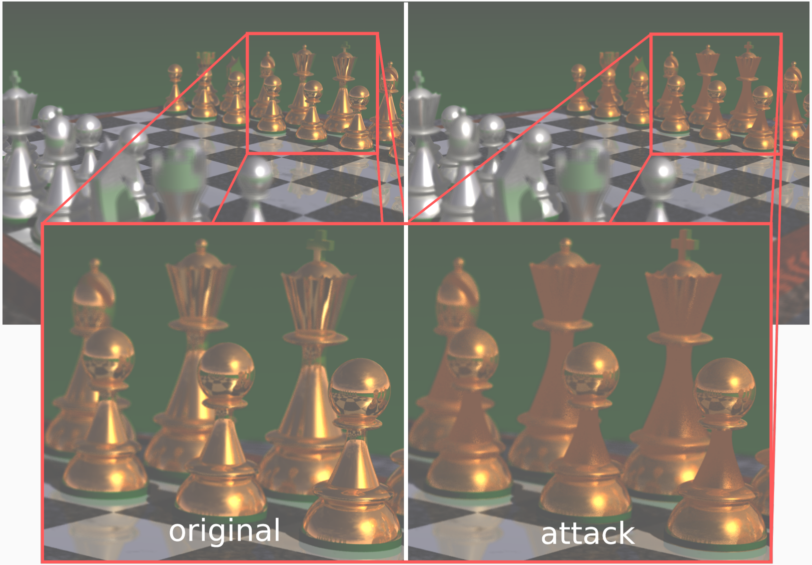

ENTER
6
enclave shielding runtime

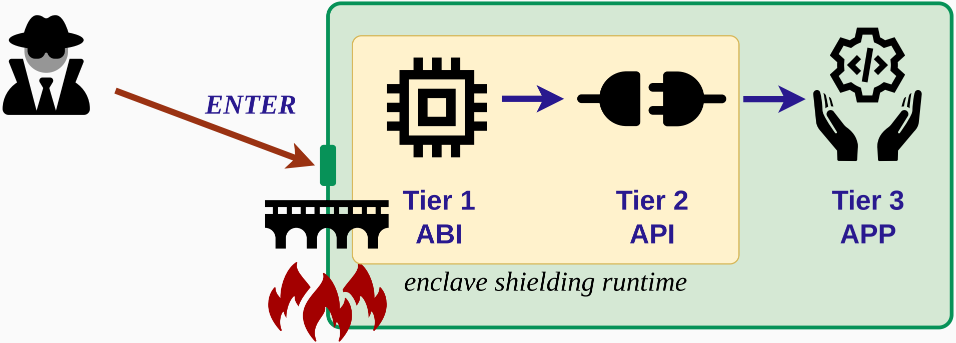

ENTER
2
enclave shielding runtime

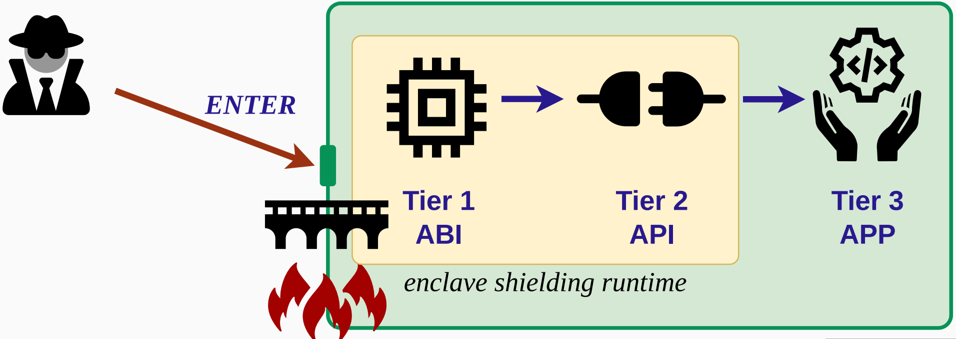


Normal	1	6	0	8	2	3	8	8
Round down	2	2	2	2	2	2	2	2


original
attack


original
attack


ENTER
Tier 1
ABI
Tier 2
API
Tier 3
APP
enclave shielding runtime



ENTER

Tier 1
ABI

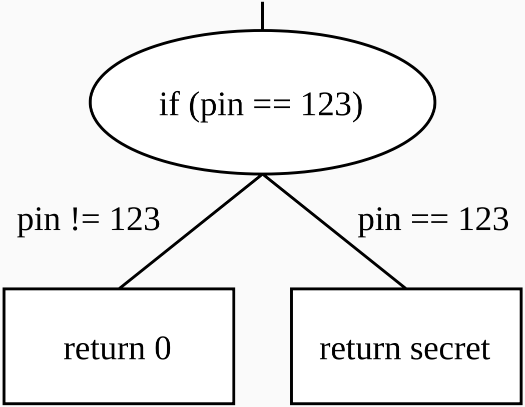
Tier 2
API

Tier 3
APP

enclave shielding runtime

Symbolic execution

```
int ecall(int pin){
    if(pin == 123){
        return secret;
    } else {
        return 0;
    }
}
```



if (pin == 123)

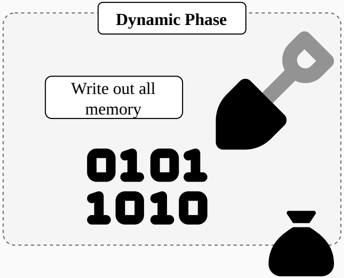
pin != 123

pin == 123

return 0

return secret

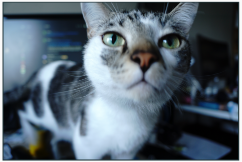
Pandora: Overview



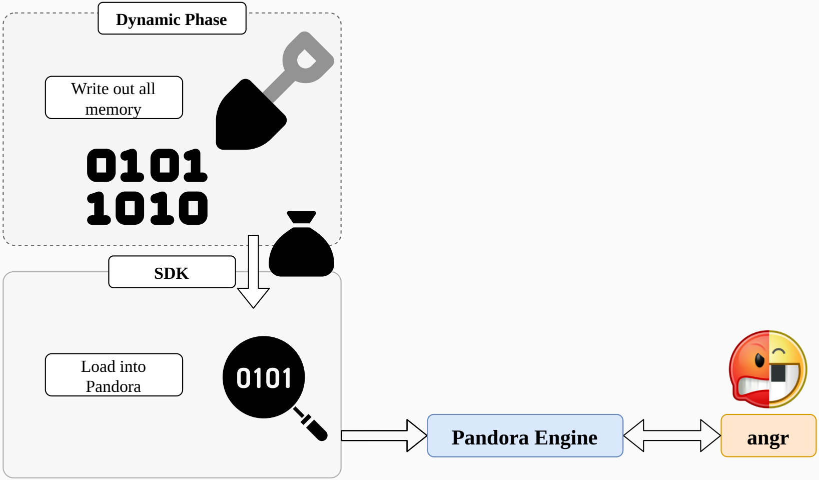
Dynamic Phase

Write out all memory

0101
1010



Pandora: Overview



Dynamic Phase

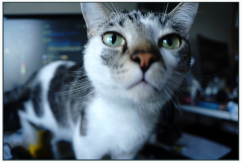
Write out all memory

SDK

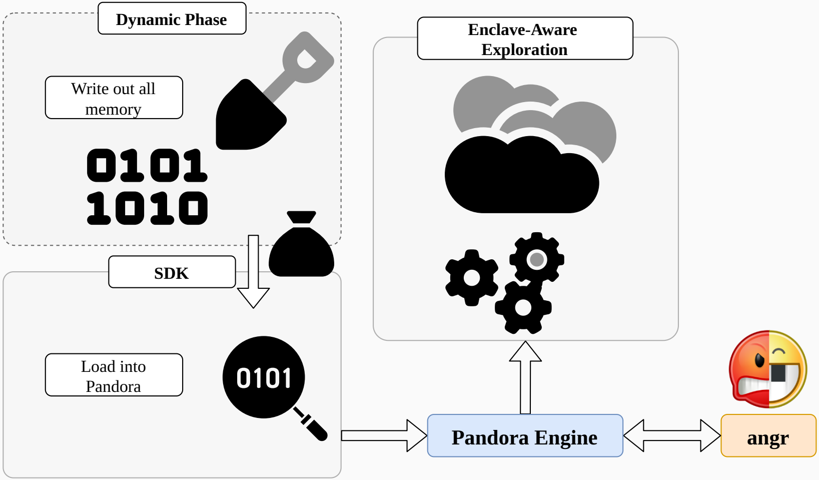
Load into Pandora

Pandora Engine

angr



Pandora: Overview



Dynamic Phase

Write out all memory

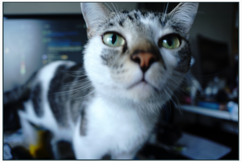
SDK

Load into Pandora

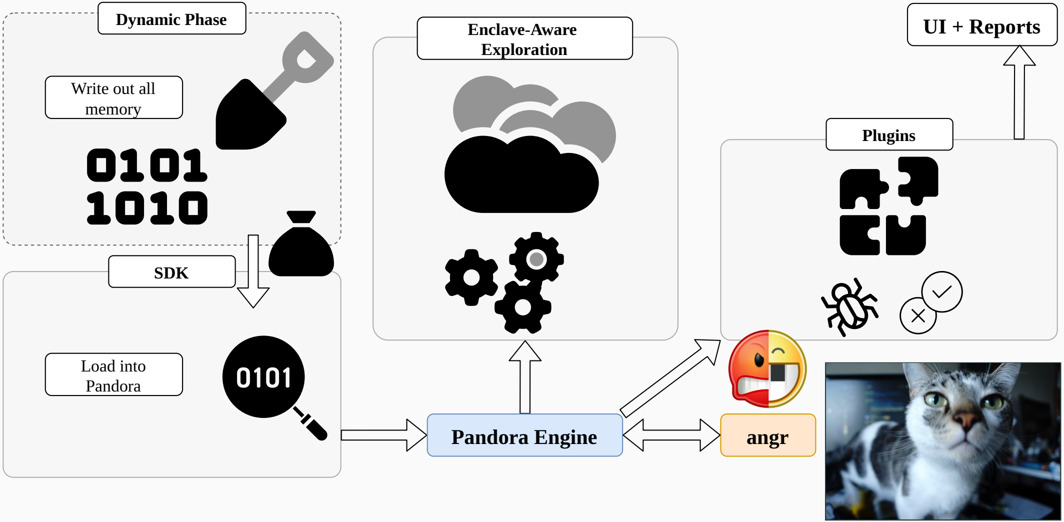
Enclave-Aware Exploration

Pandora Engine

angr



Pandora: Overview



Dynamic Phase

Write out all memory

SDK

Load into Pandora

Enclave-Aware Exploration

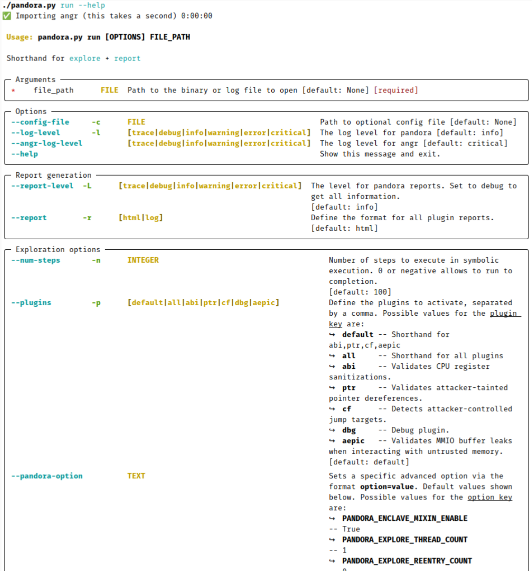
Pandora Engine

angr

Plugins

UI + Reports

Pandora: Usability and extensibility

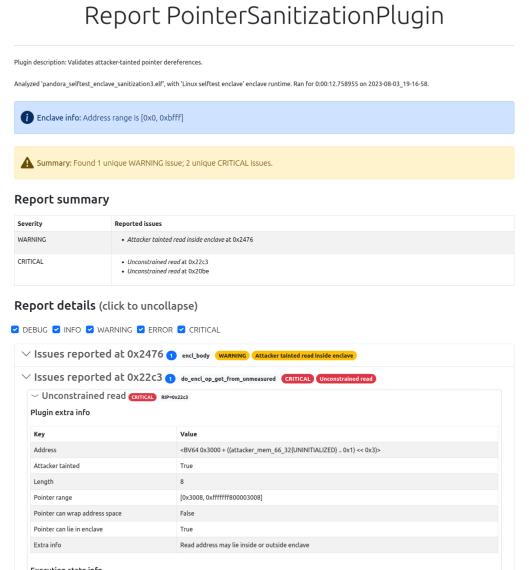


```
./pandora.py run --help
✅ Importing angr (this takes a second) 0:00:00

 Usage: pandora.py run [OPTIONS] FILE_PATH

 Shorthand for explore + report

╭─ Arguments ─────────────────────────────────────────────────────────────────────────────────────────────╮
│ *    file_path      FILE  Path to the binary or log file to open [default: None] [required]             │
╰─────────────────────────────────────────────────────────────────────────────────────────────────────────╯
╭─ Options ───────────────────────────────────────────────────────────────────────────────────────────────╮
│ --config-file     -c      FILE                                          Path to optional config file [default: None] │
│ --log-level       -l      [trace|debug|info|warning|error|critical]    The log level for pandora [default: info]     │
│ --angr-log-level          [trace|debug|info|warning|error|critical]    The log level for angr [default: critical]    │
│ --help                                                                  Show this message and exit.                  │
╰─────────────────────────────────────────────────────────────────────────────────────────────────────────╯
╭─ Report generation ─────────────────────────────────────────────────────────────────────────────────────╮
│ --report-level  -L      [trace|debug|info|warning|error|critical]  The level for pandora reports. Set to debug to │
│                                                                    get all information.                           │
│                                                                    [default: info]                                │
│ --report        -r      [html|log]                                 Define the format for all plugin reports.      │
│                                                                    [default: html]                                │
╰─────────────────────────────────────────────────────────────────────────────────────────────────────────╯
╭─ Exploration options ───────────────────────────────────────────────────────────────────────────────────╮
│ --num-steps       -n      INTEGER                                       Number of steps to execute in symbolic     │
│                                                                         execution. 0 or negative allows to run to  │
│                                                                         completion.                                │
│                                                                         [default: 100]                             │
│ --plugins         -p      [default|all|abi|ptr|cf|dbg|aepic]            Define the plugins to activate, separated  │
│                                                                         by a comma. Possible values for the plugin │
│                                                                         key are:                                   │
│                                                                         ↪ default -- Shorthand for                 │
│                                                                         abi,ptr,cf,aepic                           │
│                                                                         ↪ all     -- Shorthand for all plugins     │
│                                                                         ↪ abi     -- Validates CPU register        │
│                                                                         sanitizations.                             │
│                                                                         ↪ ptr     -- Validates attacker-tainted    │
│                                                                         pointer dereferences.                      │
│                                                                         ↪ cf      -- Detects attacker-controlled   │
│                                                                         jump targets.                              │
│                                                                         ↪ dbg     -- Debug plugin.                 │
│                                                                         ↪ aepic   -- Validates MMIO buffer leaks   │
│                                                                         when interacting with untrusted memory.    │
│                                                                         [default: default]                         │
│ --pandora-option          TEXT                                          Sets a specific advanced option via the    │
│                                                                         format option=value. Default values shown  │
│                                                                         below. Possible values for the option key  │
│                                                                         are:                                       │
│                                                                         ↪ PANDORA_ENCLAVE_MIXIN_ENABLE             │
│                                                                         -- True                                    │
│                                                                         ↪ PANDORA_EXPLORE_THREAD_COUNT             │
│                                                                         -- 1                                       │
│                                                                         ↪ PANDORA_EXPLORE_REENTRY_COUNT            │
│                                                                         -- 0                                       │
```



Report PointerSanitizationPlugin

Plugin description: Validates attacker-tainted pointer dereferences.

Analyzed 'pandora_selftest_enclave_sanitization3.elf', with 'Linux selftest enclave' enclave runtime. Ran for 0:00:12.758955 on 2023-08-03_19-16-58.

Enclave info: Address range is [0x0, 0xbfff]

Summary: Found 1 unique WARNING issue; 2 unique CRITICAL issues.

Report summary

Severity	Reported issues
WARNING	• *Attacker tainted read inside enclave* at 0x2476
CRITICAL	• *Unconstrained read* at 0x22c3 • *Unconstrained read* at 0x20be

Report details (click to uncollapse)

☑ DEBUG ☑ INFO ☑ WARNING ☑ ERROR ☑ CRITICAL

Issues reported at 0x2476 1 encl_body WARNING Attacker tainted read inside enclave

Issues reported at 0x22c3 1 do_encl_op_get_from_unmeasured CRITICAL Unconstrained read

Unconstrained read CRITICAL RIP=0x22c3

Plugin extra info

Key	Value
Address	<BV64 0x3000 + ((attacker_mem_66_32{UNINITIALIZED} .. 0x1) << 0x3)>
Attacker tainted	True
Length	8
Pointer range	[0x3008, 0xfffffff800003008]
Pointer can wrap address space	False
Pointer can lie in enclave	True
Extra info	Read address may lie inside or outside enclave

Execution state info

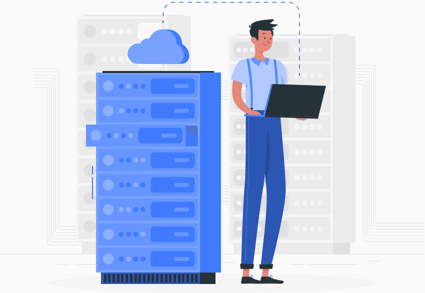
Analyzed **10** enclave runtimes

7 new CVEs

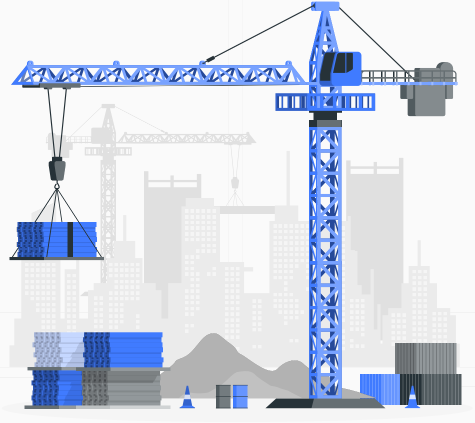
Found over **170** vulnerability instances

Interim summary

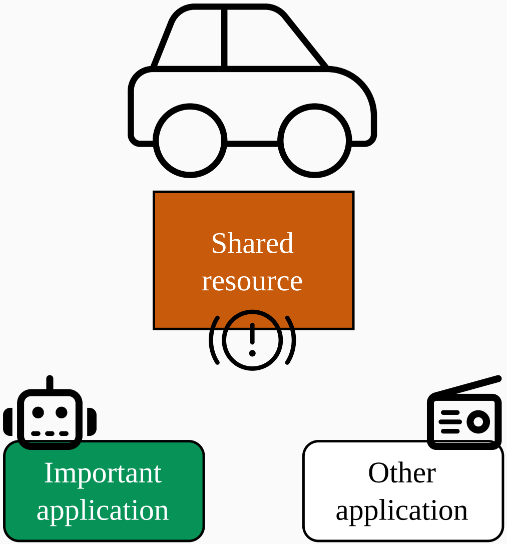
- Sharing resources is increasingly common.
- Sharing can be **dangerous!**
- Enclaved execution is one solution to **protect confidentiality and integrity**.
- Enclave interactions require careful sanitization.



Real-time scheduling for enclaved execution



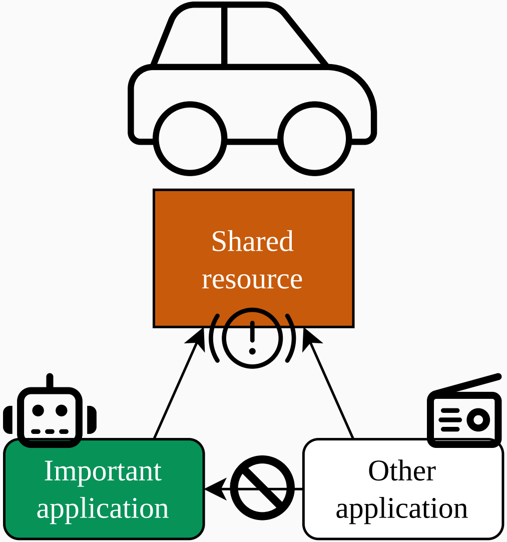
Locating...
1:43

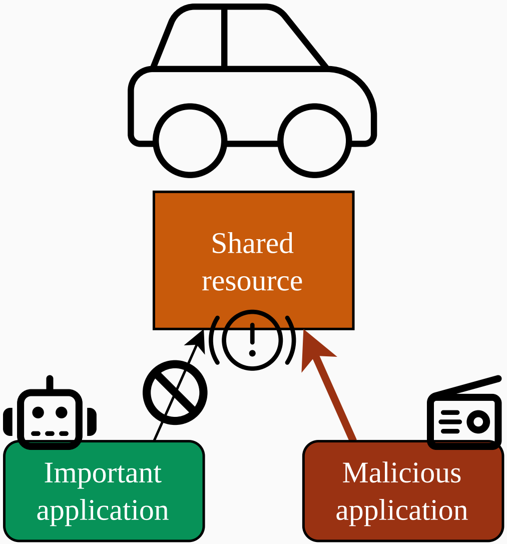


Shared resource

Important application

Other application


Shared resource
Important application
Other application

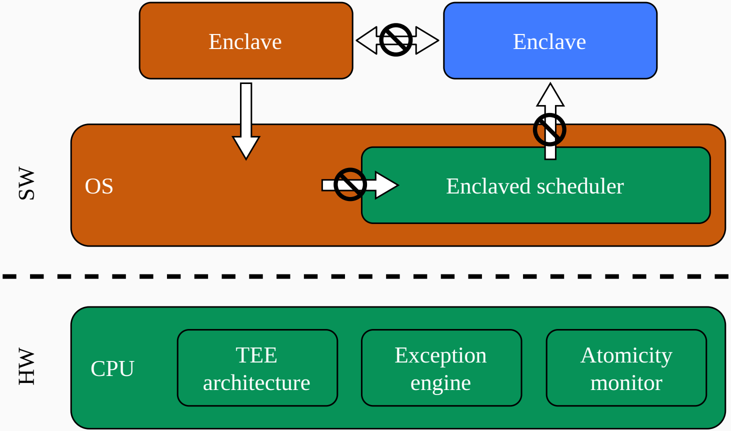


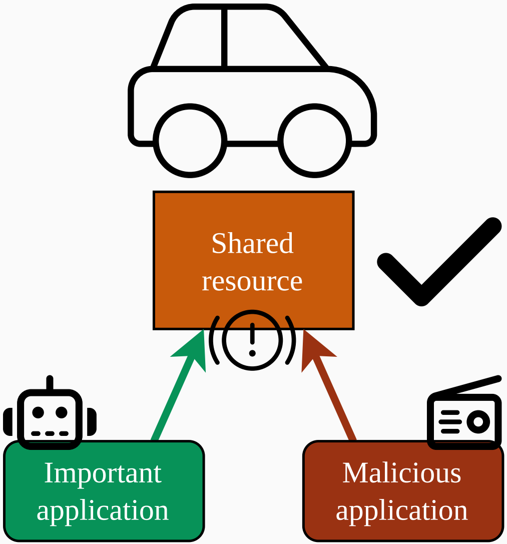
Shared resource

Important application

Malicious application

Aion: Strong Availability Guarantees for Enclaves




Shared resource
Important application
Malicious application

Contributions

Faulty Point Unit: ABI Poisoning Attacks on Intel SGX

- Fault-injection **attack** on Intel SGX.

Pandora: Principled Symbolic Execution of Intel SGX Enclaves

- A **tool** to check SGX runtimes for a range of known vulnerabilities.

Aion: Strong Availability Guarantees for Enclaves

- Architecture with **availability guarantees** for enclaves.

Summary

- Sharing resources is increasingly common.
- Sharing can be **dangerous!**
- Enclaved execution is one solution to **protect confidentiality and integrity**.
- Enclave interactions require careful sanitization.
- Additionally guaranteeing **availability is possible**.

All fancy illustrations by Storyset (storyset.com)

Interface Sanitization and Real-Time Scheduling for Enclaved Execution

Fritz Alder

October 19, 2023

Public PhD defense

Interface Sanitization and Real-Time Scheduling for Enclaved Execution

Fritz Alder

October 19, 2023

🏠 Public PhD defense