Pandora: Principled Symbolic Validation of Intel SGX Enclave Runtimes

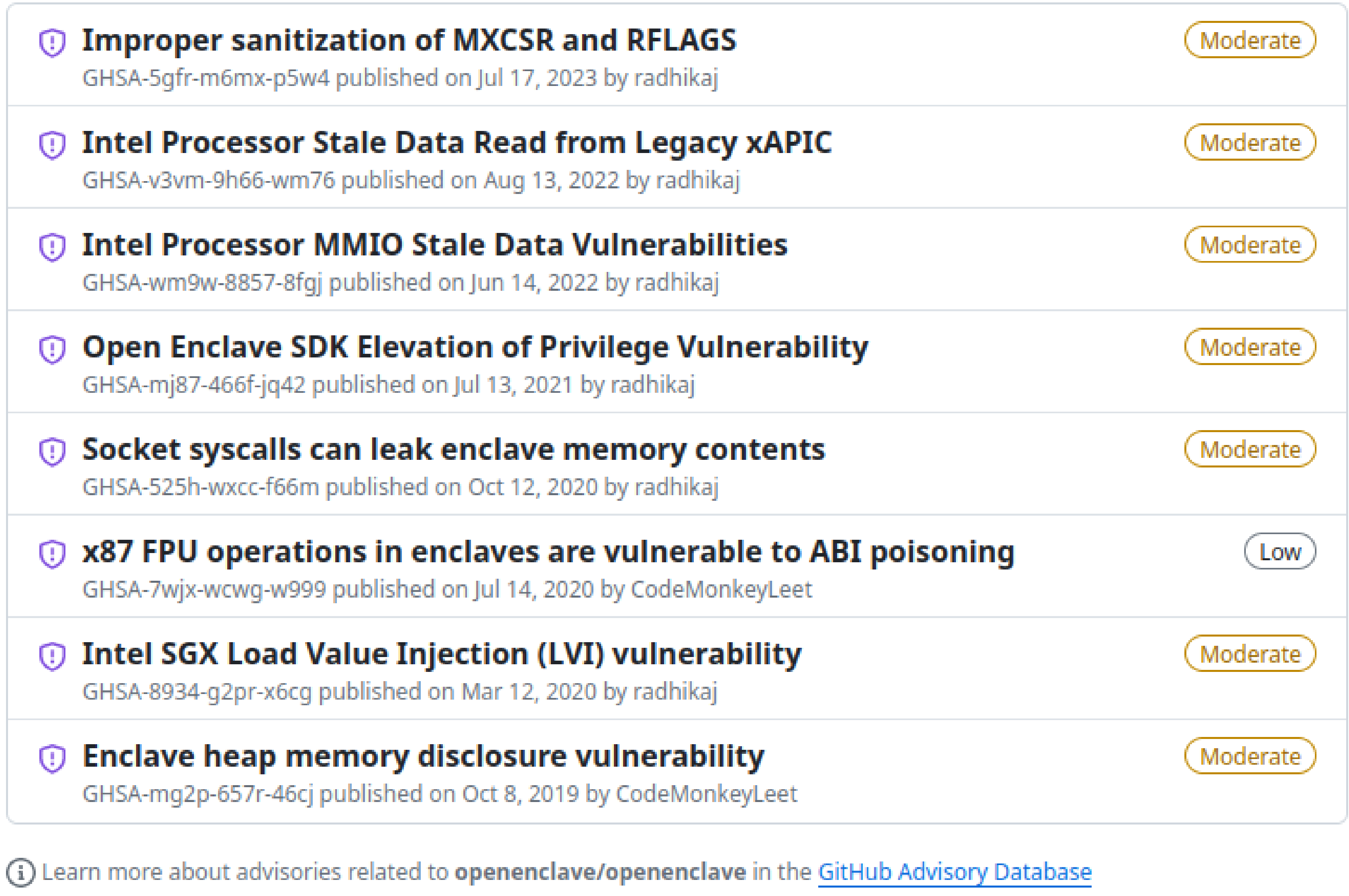
Fritz Alder[1], Lesly-Ann Daniel[1], David Oswald[2], Frank Piessens[1], Jo Van Bulck[1]

[1] DistriNet, KU Leuven, Belgium, [2] University of Birmingham, UK

SCAN ME

https://github.com/pandora-tee

Writing “Secure” Enclave Software is Hard…



Improper sanitization of MXCSR and RFLAGS — Moderate
GHSA-5gfr-m6mx-p5w4 published on Jul 17, 2023 by radhikaj

Intel Processor Stale Data Read from Legacy xAPIC — Moderate
GHSA-v3vm-9h66-wm76 published on Aug 13, 2022 by radhikaj

Intel Processor MMIO Stale Data Vulnerabilities — Moderate
GHSA-wm9w-8857-8fgj published on Jun 14, 2022 by radhikaj

Open Enclave SDK Elevation of Privilege Vulnerability — Moderate
GHSA-mj87-466f-jq42 published on Jul 13, 2021 by radhikaj

Socket syscalls can leak enclave memory contents — Moderate
GHSA-525h-wxcc-f66m published on Oct 12, 2020 by radhikaj

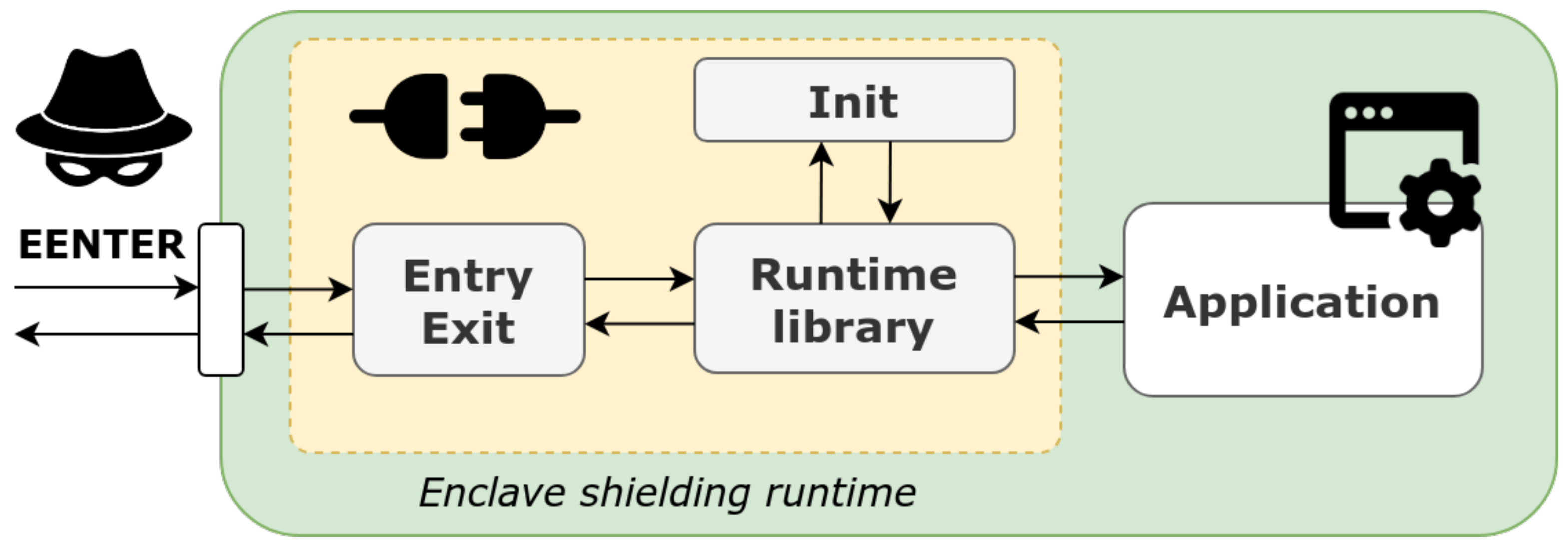
x87 FPU operations in enclaves are vulnerable to ABI poisoning — Low
GHSA-7wjx-wcwg-w999 published on Jul 14, 2020 by CodeMonkeyLeet

Intel SGX Load Value Injection (LVI) vulnerability — Moderate
GHSA-8934-g2pr-x6cg published on Mar 12, 2020 by radhikaj

Enclave heap memory disclosure vulnerability — Moderate
GHSA-mg2p-657r-46cj published on Oct 8, 2019 by CodeMonkeyLeet

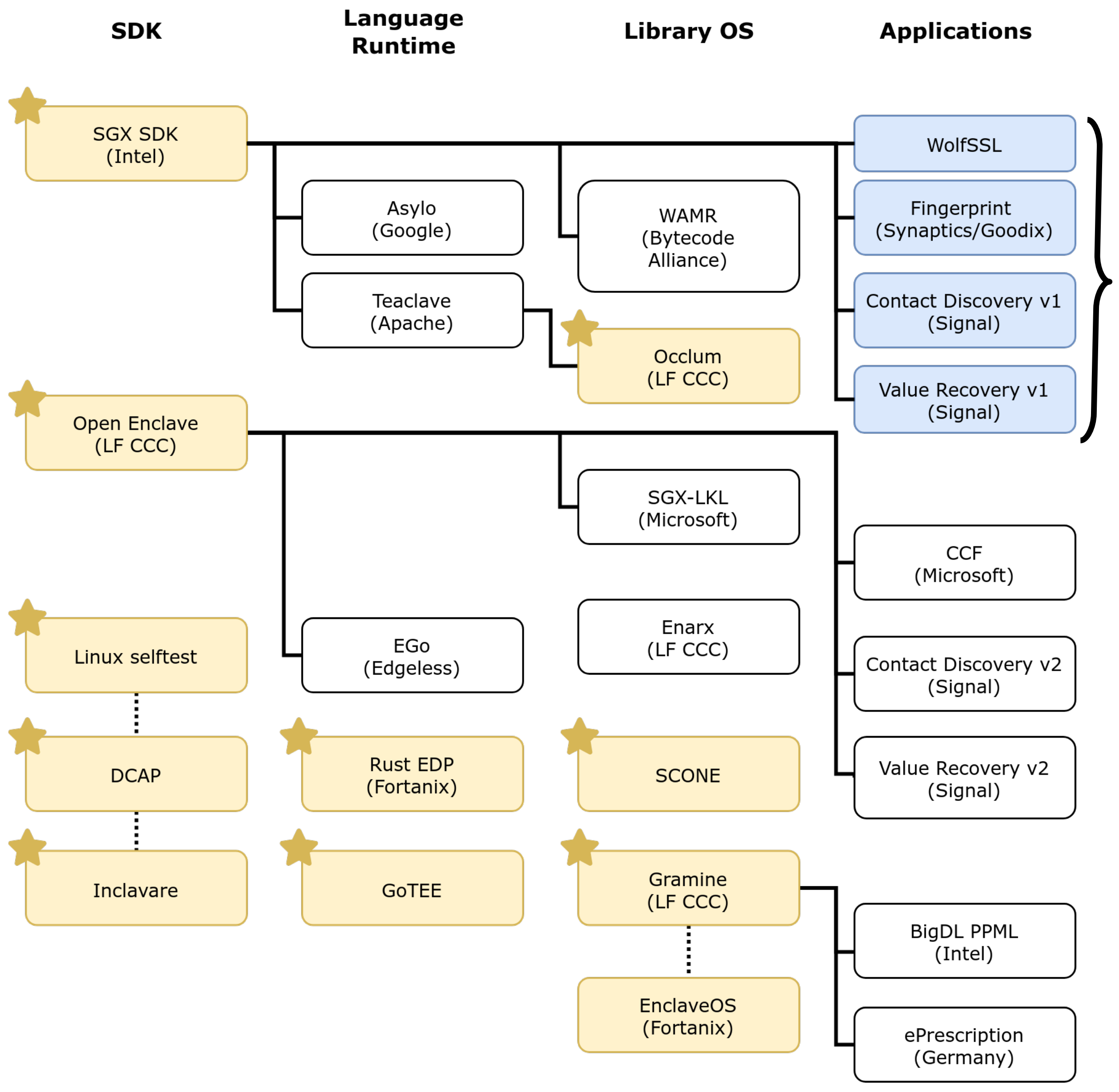
ⓘ Learn more about advisories related to **openenclave/openenclave** in the GitHub Advisory Database

Solution: Enclave Shielding Runtimes



- Transparent **input sanitation** on enclave entry/exit
- **Low-level initialization** and relocation

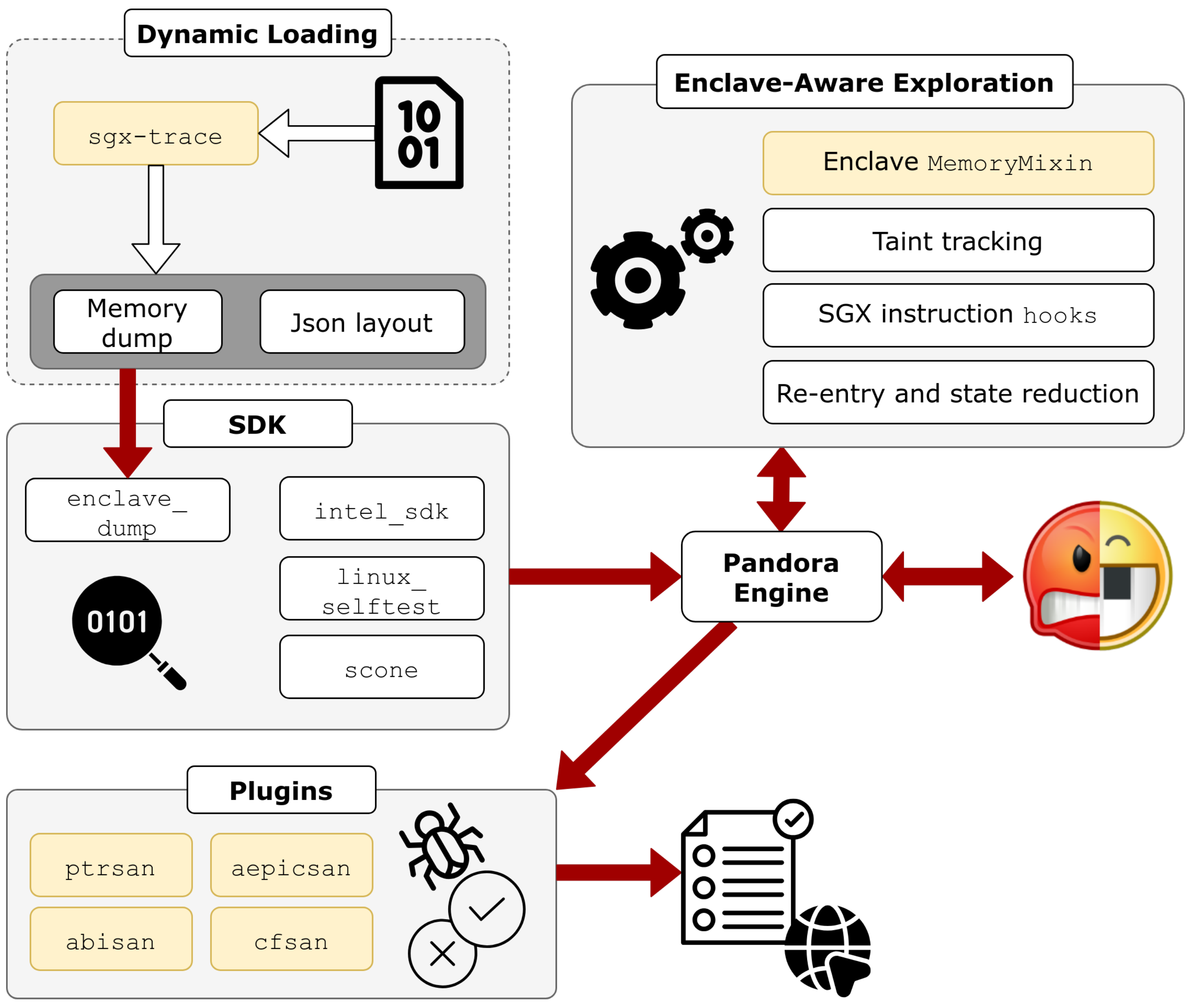
Challenge: Diverse SGX Software Ecosystem



Prior work: Selected apps on Intel SDK

Pandora: Wide-range analysis of SGX shielding runtimes

Runtime-Agnostic & Truthful Symbolic Execution



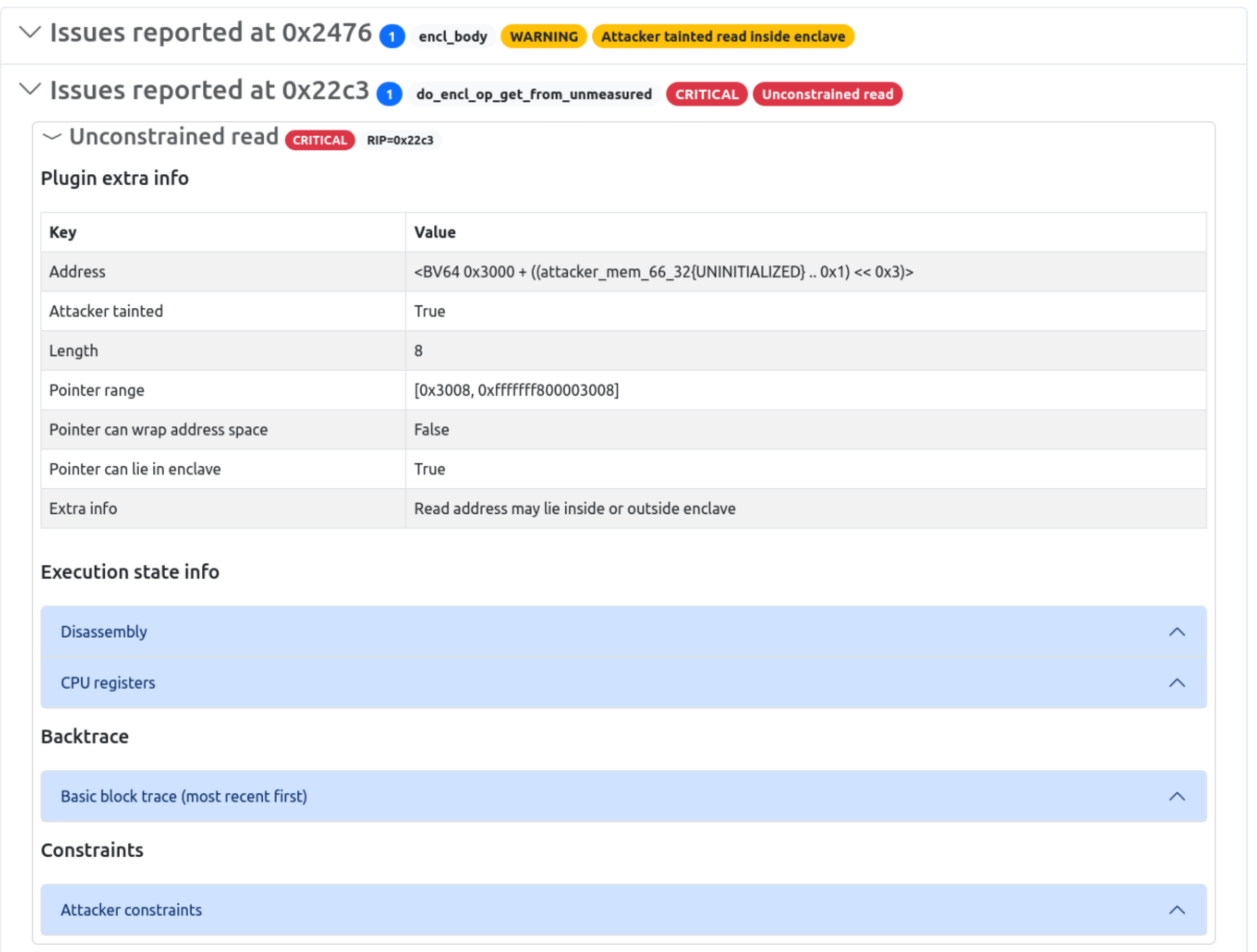
Plugin-Based Vulnerability Detection

- **4 plugins**
- 11 runtimes

- > 200 new and 69 reproduced vulnerability instances
- 7 CVEs

Runtime	Version	Prod	Src	Plugin	Instances	CVE
Newly found vulnerabilities in shielding runtimes (total 200 instances)						
EnclaveOS	3.28	✓	✗†	ABISan	1	
EnclaveOS	3.28	✓	✗†	PTRSan	15	CVE-2023-38022
EnclaveOS	3.28	✓	✗†	ÆPICSan	33	CVE-2023-38021
EnclaveOS	3.28	✓	✗†	CFSan	2	
GoTEE	b35f	✗	✓	PTRSan	31	
GoTEE	b35f	✗	✓	ÆPICSan	18	
GoTEE	b35f	✗	✓	CFSan	1	
Gramine	1.4	✓	✓	ABISan	1	
Intel SDK	2.15.1	✓	✓	PTRSan	2	CVE-2022-26509
Intel SDK	2.19	✓	✓	ÆPICSan	22	
↪ Occlum	0.29.4	✓	✓	ÆPICSan	11	
Linux selftest	5.18	✗	✓	ABISan	1	
↪ DCAP	1.16	✓	✓	ABISan	1	
↪ Inclavare	0.6.2	✗	✓	ABISan	1	
Linux selftest	5.18	✗	✓	PTRSan	5	
↪ DCAP	1.16	✓	✓	PTRSan	17	
↪ Inclavare	0.6.2	✗	✓	PTRSan	2	
Linux selftest	5.18	✗	✓	CFSan	1	
↪ Inclavare	0.6.2	✗	✓	CFSan	1	
Open Enclave	0.19.0	✓	✓	ABISan	2	CVE-2023-37479
Rust EDP	1.71	✓	✓	ABISan	1	
SCONE	5.7 / 5.8	✓	✗	ABISan	2 / 1	CVE-2022-46487
SCONE	5.7 / 5.8	✓	✗	PTRSan	10 / 3	CVE-2022-46486
SCONE	5.7 / 5.8	✓	✗	ÆPICSan	11 / 3	CVE-2023-38023
SCONE	5.8	✓	✗	CFSan	1	

Human-Readable HTML Reports



∨ 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, 0xffffffff800003008]
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

Disassembly

CPU registers

Backtrace

Basic block trace (most recent first)

Constraints

Attacker constraints

45th IEEE Symposium on Security and Privacy (S&P), 2024

UNIVERSITY OF BIRMINGHAM   KU LEUVEN   DistriNet