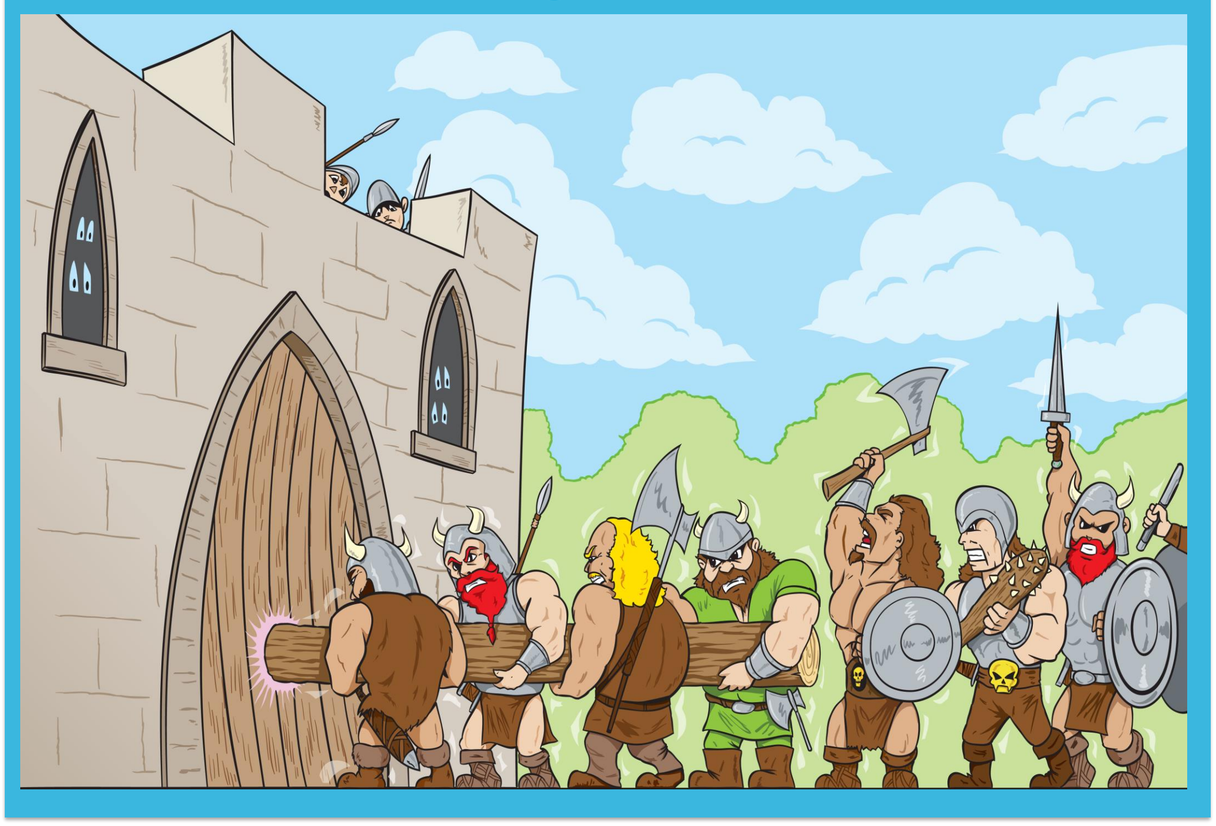
Faulty Point Unit: ABI Poisoning Attacks on Trusted Execution Environments

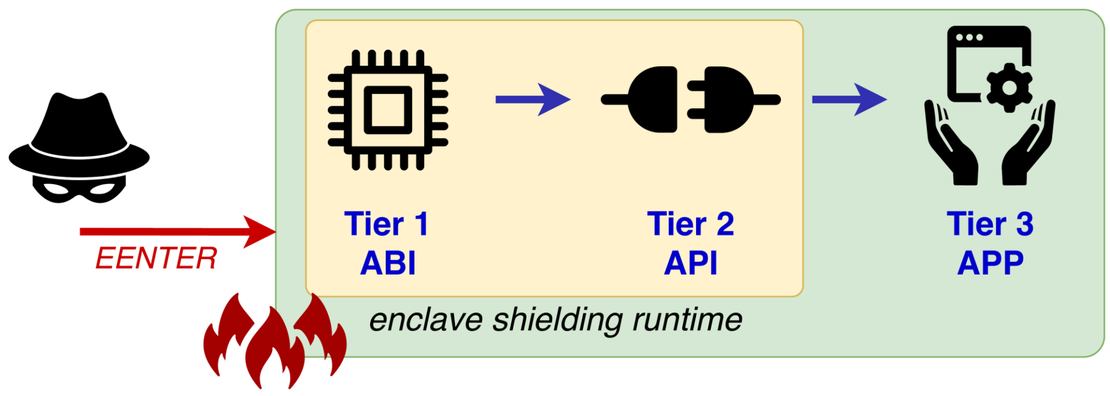
Published at ACSAC'20
Distinguished paper
with artifact award

Fritz Alder[1], Jo Van Bulck[1], Jesse Spielman[2], David Oswald[2], Frank Piessens[1]
[1] imec-DistriNet, KU Leuven, Belgium, [2] University of Birmingham, UK

How to besiege a TEE fortress?

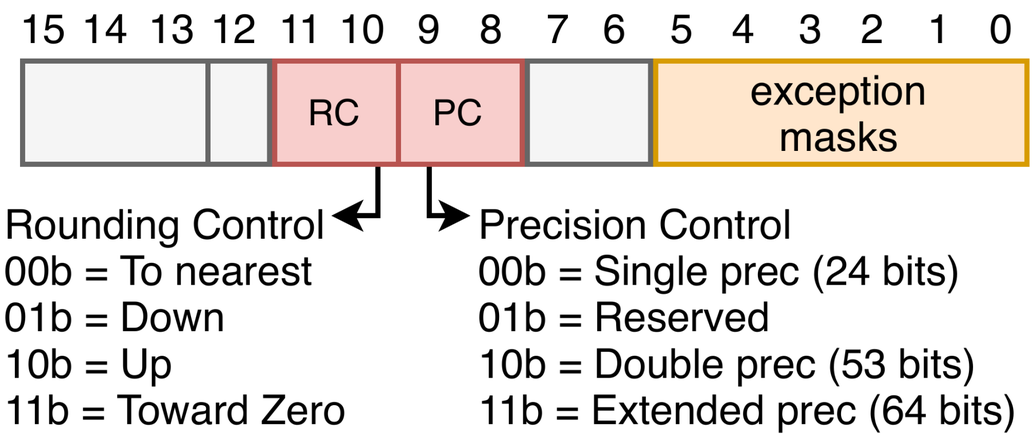


Wash your hands before entering the enclave!



Key insight: Sanitization responsibilities split across ABI and API tiers: machine state vs. higher-level programming language.

x87 floating point unit control word (cf. SSE `mxcsr`, RISC-V `fcsr`, ARM `fpcsr`)



System V ABI expected by compiler

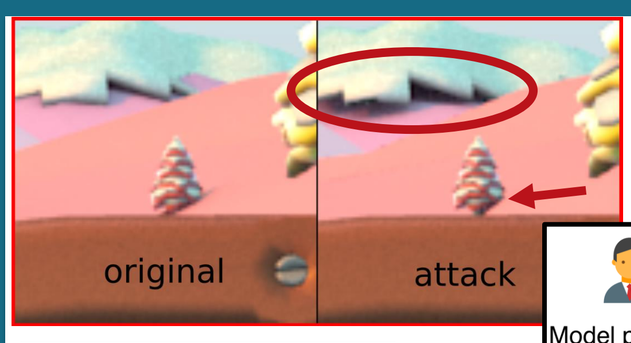
The control bits of the `MXCSR` register are callee-saved (preserved across calls), while the status bits are caller-saved (not preserved). The x87 status word register is caller-saved, whereas the x87 control word is callee-saved.

Is your enclave runtime vulnerable?

FPU	Rounding	`arccos(-1)` $= \pi$	`2.1 * 3.4 = 7.14`
Single precision	To nearest	3.14159265358979323851280896	7.13999986648559570312500000
	Downward	3.14159265358979323829596852	7.13999986648559570312500000
	Upward	3.14159265358979323851280896	7.14000034332275390625000000
	To zero	3.14159265358979323829596852	7.13999986648559570312500000
Double precision	To nearest	3.14159265358979323851280896	7.13999999999999968025576891
	Downward	3.14159265358979323829596852	7.13999999999999968025576891
	Upward	3.14159265358979323851280896	7.14000000000000005684341886
	To zero	3.14159265358979323829596852	7.13999999999999968025576891
Extended precision	To nearest	3.14159265358979323851280896	7.14000000000000001156713613
	Downward	3.14159265358979323829596852	7.14000000000000001152376805
	Upward	3.14159265358979323851280896	7.14000000000000001156713613
	To zero	3.14159265358979323829596852	7.14000000000000001152376805
MMX	Any	`-NaN`	`-NaN`

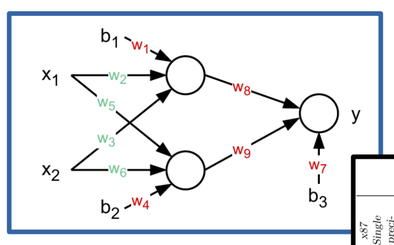
	SGX-SDK*	OpenEnclave	Graphene	SGX-LKL	Rust-EDP	Go-TEE	Enarx	Keystone
Exploit	★	★	○	★	★	★	○	★
Patch 1	`xrstor`	~~`ldmxcsr/cw`~~	`fxrstor`	–	~~`ldmxcsr/cw`~~	`xrstor`	`xrstor`	–**
Patch 2		`xrstor`			`xrstor`			

Case studies: What can go wrong?

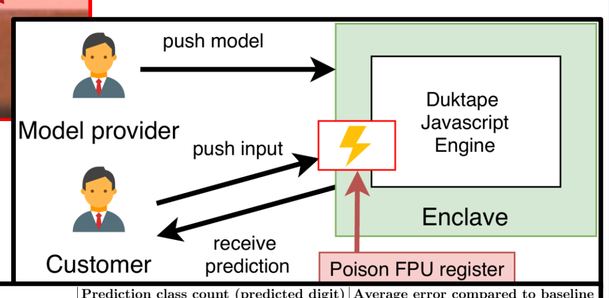


← Blender (SPEC CPU 2017)

↓ MNIST fault injection



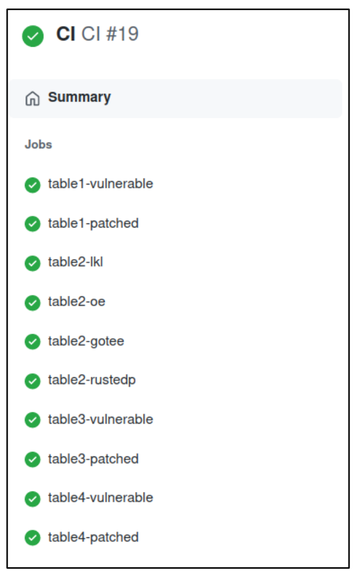
Neural network weight extraction



	Rounding mode	Accuracy	Prediction class count (predicted digit) 0 1 2 3 4 5 6 7 8 9	Average error compared to baseline (SSE, rounding to nearest)
x87 Single precision	Round to nearest	4%	0 12 14 2 10 32 0 30 0 0	0.17604646652708841325640776176 4
	Rounding down	8%	0 0 100 0 0 0 0 0 0 0	0.16796397173637958588621188482 6
	Rounding up	4%	0 12 14 2 10 32 0 30 0 0	0.17604634092910736302073360093
	Round to zero	8%	0 0 100 0 0 0 0 0 0 0	0.16796387552144440014068038635 7
x87 Extended precision	Round to nearest	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000000055406357383
	Rounding down	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000003307334022714 93
	Rounding up	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000003145222475595 79
	Round to zero	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000005241578070654 45
SSE	Round to nearest	100%	9 14 8 10 14 8 9 14 3	11 0.0
	Rounding down	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000003307334022714 93
	Rounding up	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000003145222475595 79
	Round to zero	100%	9 14 8 10 14 8 9 14 3	11 0.00000000000000005241578070654 45

Reusable artifact on GitHub

https://github.com/fritzalder/faulty-point-unit




```
[LD] main.o -o inc
-fPIC -fno-stack-protector -fno-builtin -fno-jump-tables -fno-common -Wno-attributes -g -D_G
################################################################################
# Compiled in SIMULATION mode. You can compile either with SGX_MODE=HW or SGX_MODE=SIM #
################################################################################

--------------------------------------------------------------------------------
SINGLE PRECISION
Rounding  | arccos(-1) = pi                  | 2.1 * 3.4 = 7.14
--------------------------------------------------------------------------------
Nearest:    3.14159265358979323851280896   7.13999986648559570312500000
Down:       3.14159265358979323829596852   7.13999986648559570312500000
Up:         3.14159265358979323851280896   7.14000034332275390625000000
To Zero:    3.14159265358979323829596852   7.13999986648559570312500000
MMX attack: -nan   -nan
--------------------------------------------------------------------------------
DOUBLE PRECISION
Rounding  | arccos(-1) = pi                  | 2.1 * 3.4 = 7.14
--------------------------------------------------------------------------------
Nearest:    3.14159265358979323851280896   7.13999999999999968025576891
Down:       3.14159265358979323829596852   7.13999999999999968025576891
Up:         3.14159265358979323851280896   7.14000000000000056843418861
To Zero:    3.14159265358979323829596852   7.13999999999999968025576891
MMX attack: -nan   -nan
--------------------------------------------------------------------------------
EXTENDED PRECISION
Rounding  | arccos(-1) = pi                  | 2.1 * 3.4 = 7.14
--------------------------------------------------------------------------------
Baseline/
Nearest:    3.14159265358979323851280896   7.14000000000000011567136138
Down:       3.14159265358979323829596852   7.14000000000000011523768051
Up:         3.14159265358979323851280896   7.14000000000000011567136138
To Zero:    3.14159265358979323829596852   7.14000000000000011523768051
MMX attack: -nan   -nan
```

EP/R012598/1, EP/S030867/1, EP/V000454/1.
Work feeds into DsbDtech