KU LEUVEN

UNIVERSITY OF BIRMINGHAM

Faulty Point Unit: ABI Poisoning Attacks on Intel SGX

Fritz Alder[1], Jo Van Bulck[1], David Oswald[2], Frank Piessens[1]

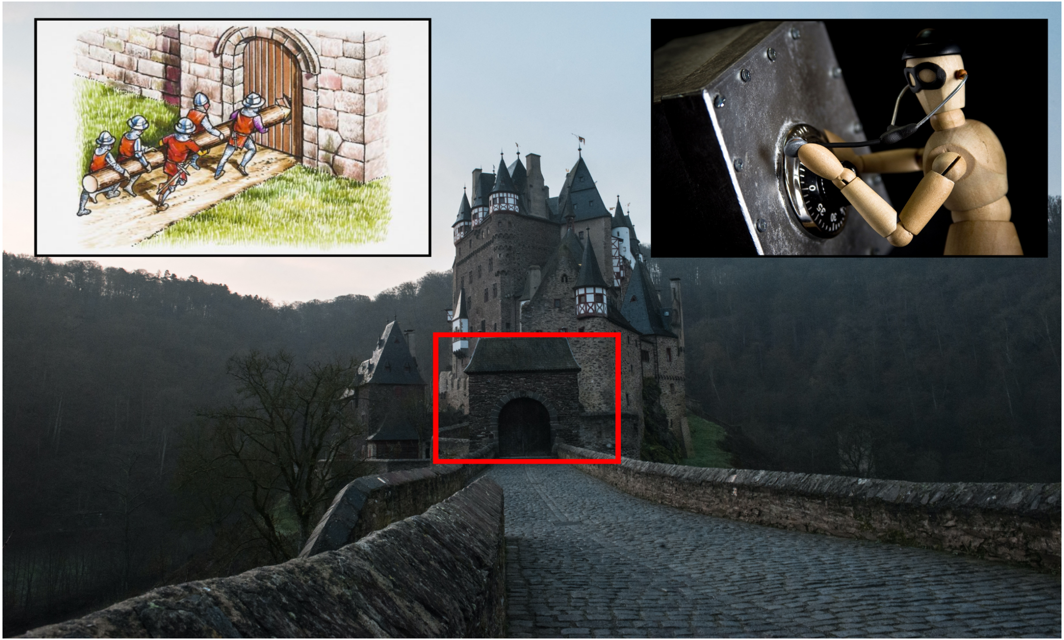
[1]imec-DistriNet, KU Leuven, Belgium [2]The University of Birmingham, UK

December 10, 2020

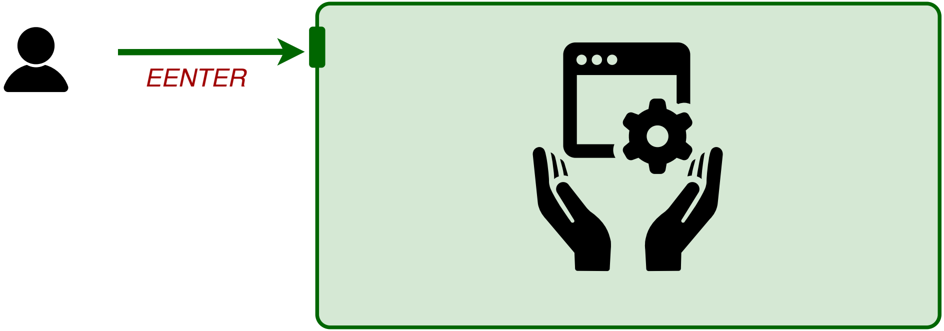
The promise of Trusted Execution Environments

The promise of Trusted Execution Environments

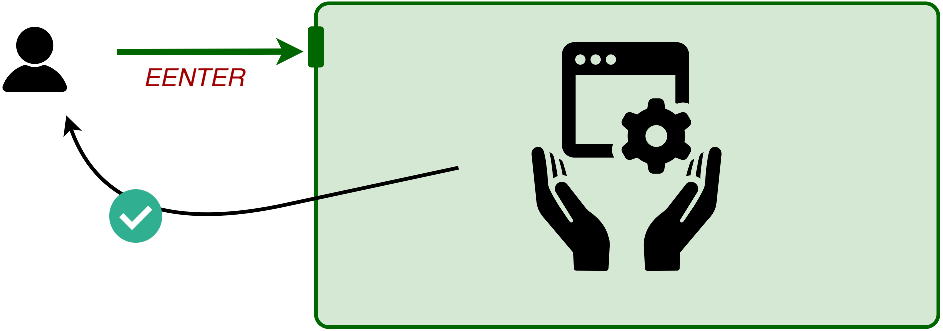
The promise of Trusted Execution Environments



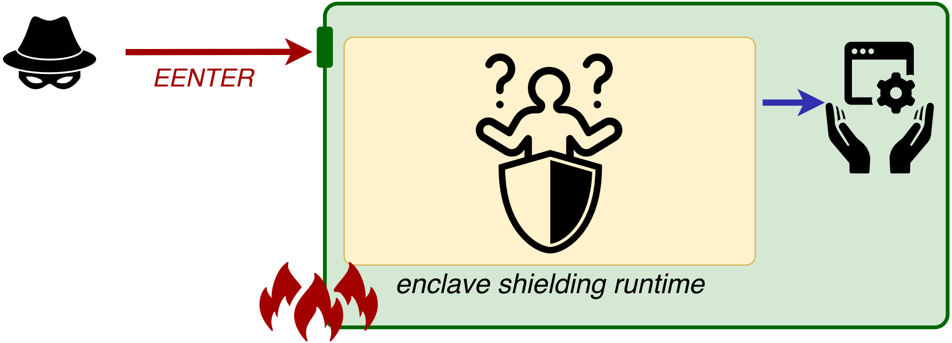
Trusted Execution Environments: Enclave calls



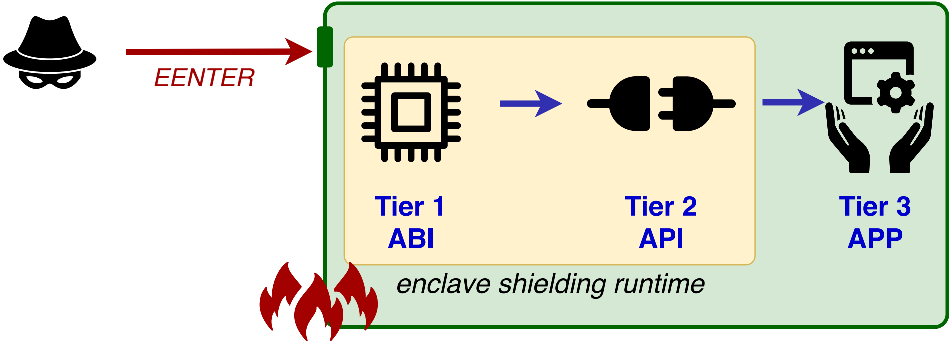
Trusted Execution Environments: Enclave calls



Trusted Execution Environments: Enclave calls



Trusted Execution Environments: Enclave calls



Key insight: split sanitization responsibilities across the ABI and API tiers: *machine state* vs. higher-level *programming language interface*

x87 Floating Point Unit (FPU) and Streaming SIMD Extensions (SSE)

- Older **x87** high-precision floating-point unit: FPU control word
- Newer **SSE** vector floating-point operations: MXCSR register

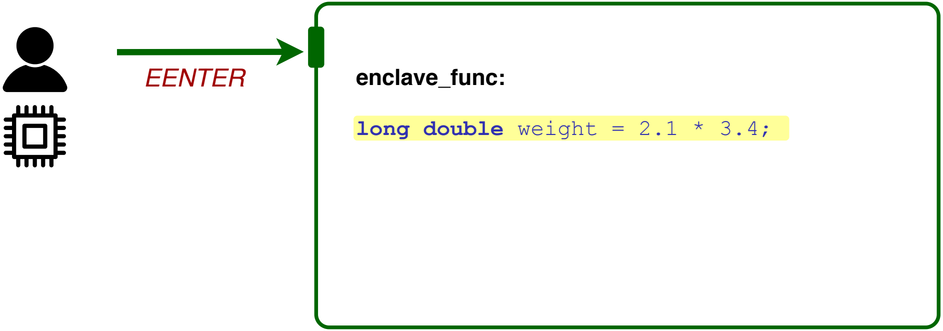
x87 Floating Point Unit (FPU) and Streaming SIMD Extensions (SSE)

- Older **x87** high-precision floating-point unit: FPU control word
- Newer **SSE** vector floating-point operations: MXCSR register

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.

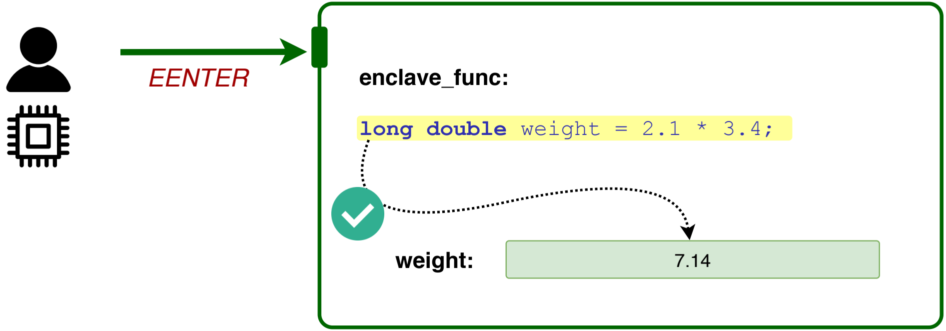
Controlling FPU precision and rounding modes CVE-2020-0561

FPU settings are preserved across calls



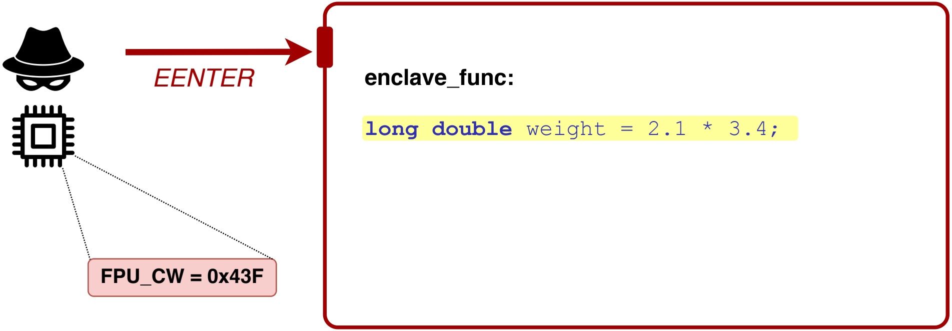
Controlling FPU precision and rounding modes CVE-2020-0561

FPU settings are preserved across calls



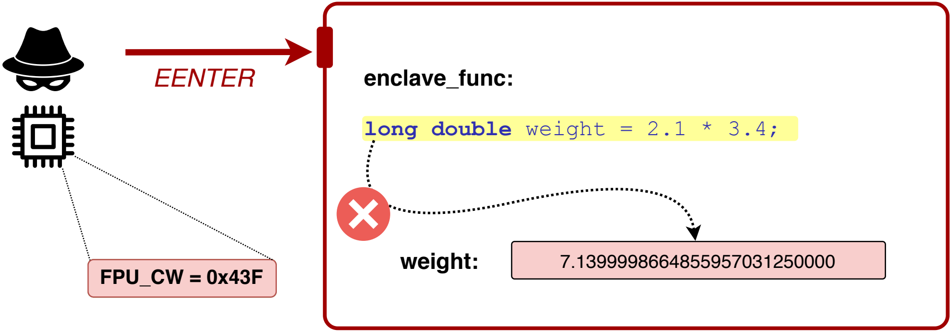
Controlling FPU precision and rounding modes CVE-2020-0561

⚠ Corrupt precision and rounding mode...



Controlling FPU precision and rounding modes CVE-2020-0561

Corrupt precision and rounding mode. . .



Controlling FPU precision and rounding modes CVE-2020-0561

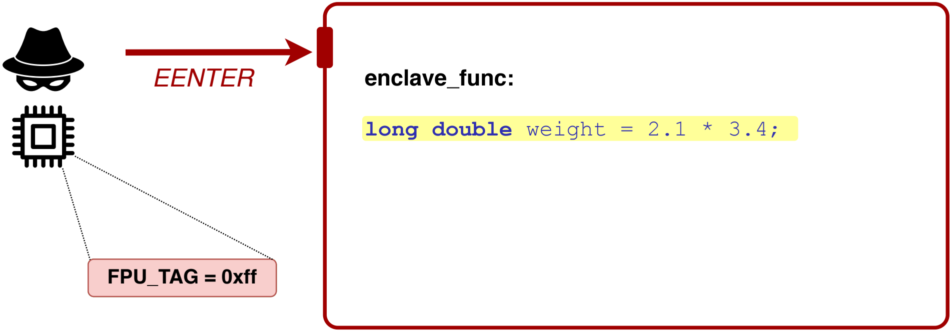
	SGX-SDK*	OpenEnclave	Graphene	SGX-LKL	Rust-EDP	Go-TEE	Enarx
Exploit	★	○	○	★	★	★	○
Patch	`xrstor`	`ldmxcsr/cw`	`fxrstor`	–	`ldmxcsr/cw`	`xrstor`	`xrstor`

* Includes derived runtimes such as Baidu's Rust-SGX and Google's Asylo.

Fill data registers to fault calculations

CVE-2020-15107

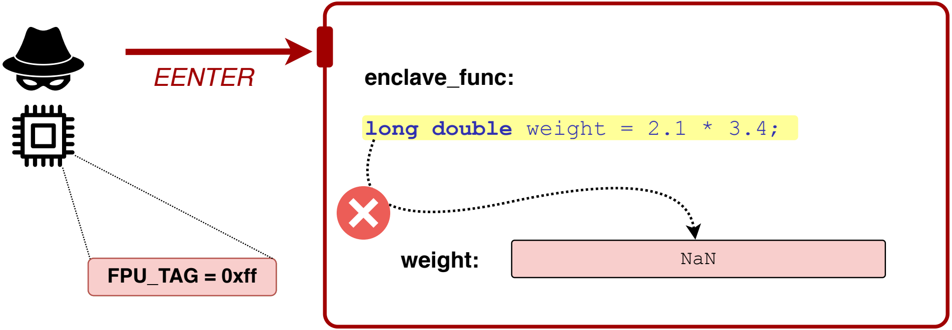
⚠ Mark data registers as in-use before entering the enclave



Fill data registers to fault calculations

CVE-2020-15107

⚠ Mark data registers as in-use before entering the enclave



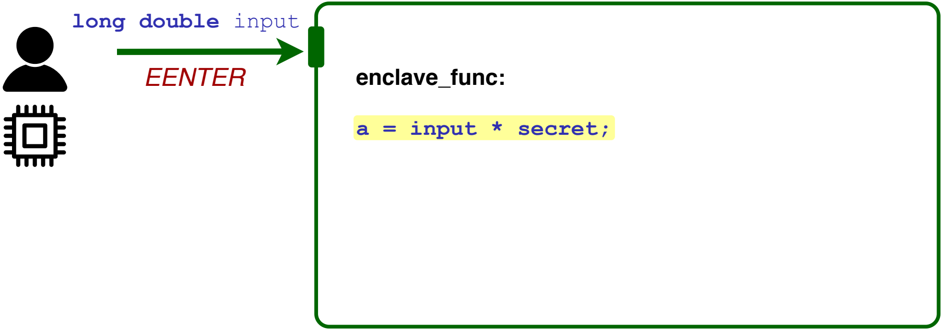
Summary: ABI-level FPU attack surface today

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

* Includes derived runtimes such as Baidu's Rust-SGX and Google's Asylo.

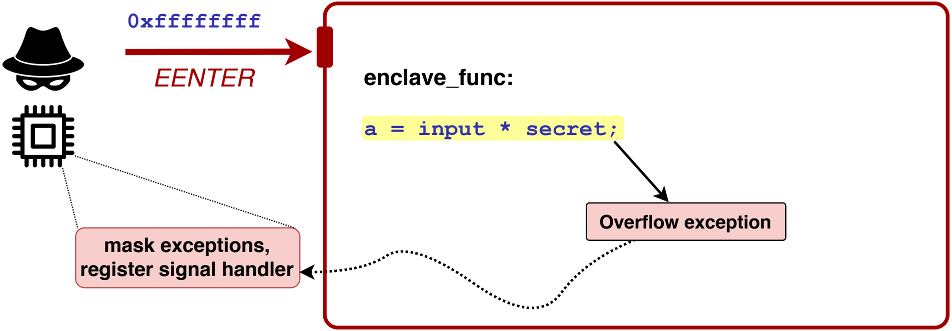
Case study 1: Floating-point exceptions as a side channel

Can we use overflows as a side channel to deduce secrets?



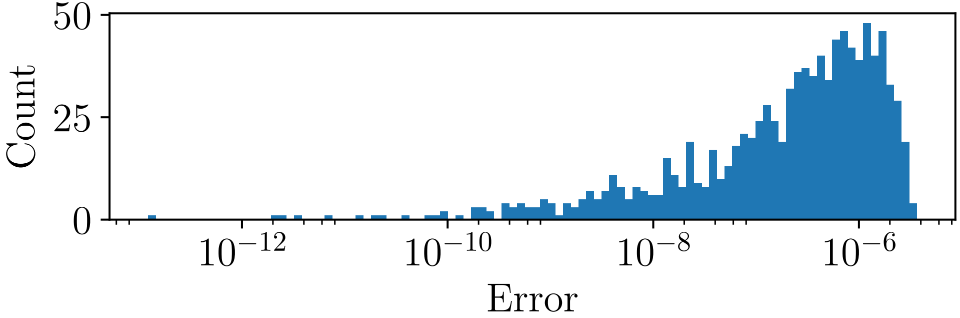
Case study 1: Floating-point exceptions as a side channel

Can we use overflows as a side channel to deduce secrets?

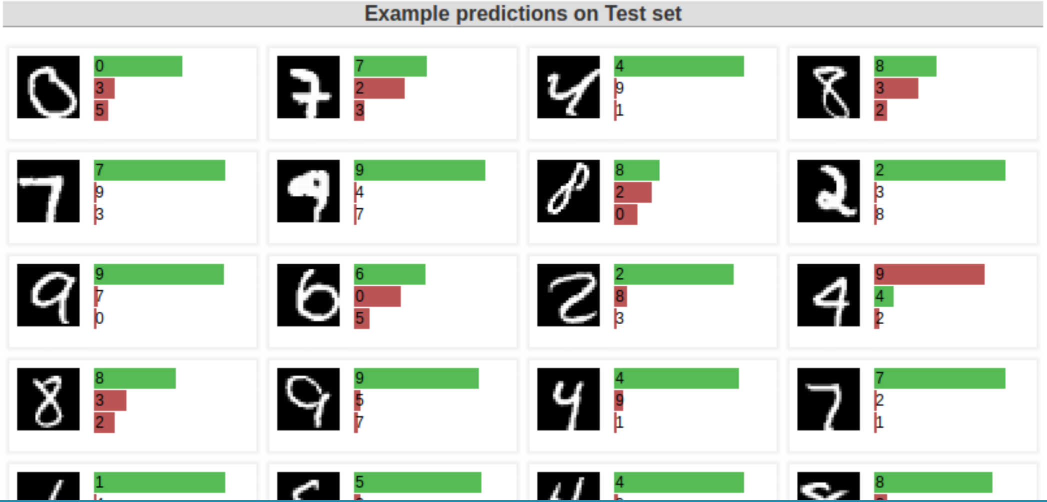


Case study 1: Floating-point exceptions as a side channel

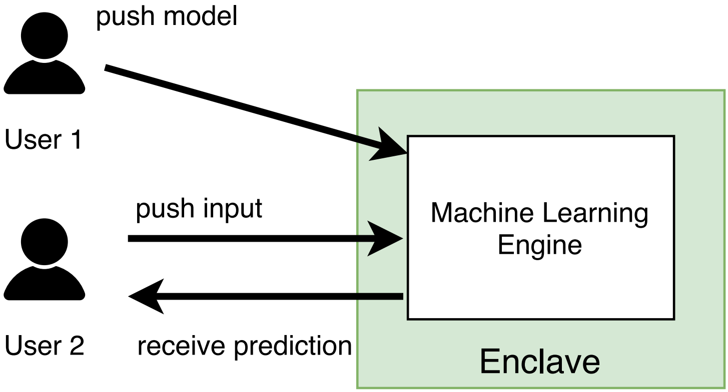
⇄ Binary search with deterministic # of steps retrieves secret



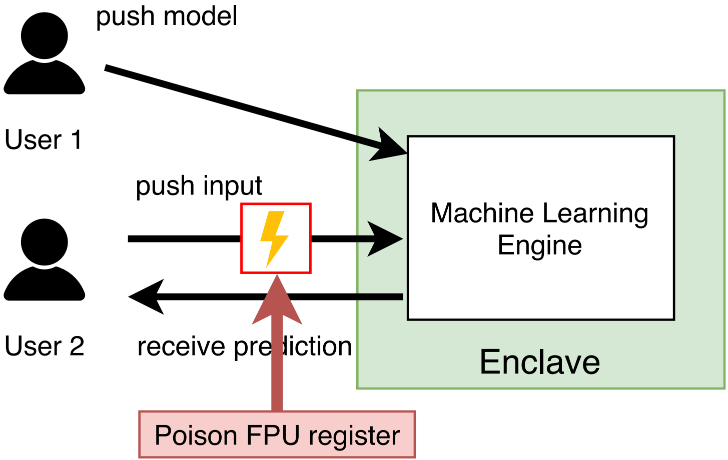
Case study 2: MNIST – ML handwriting recognition



Case study 2: MNIST – ML as an SGX Service



Case study 2: MNIST – ML as an SGX Service



Case study 2: MNIST – Predictions of 100 digits

Extended precision		Predicted digit count									
Rounding mode	Correct	0	1	2	3	4	5	6	7	8	9
Any mode	100%	9	14	8	10	14	8	9	14	3	11

x87 Extended precision: Default predictions

Case study 2: MNIST – Predictions of 100 digits

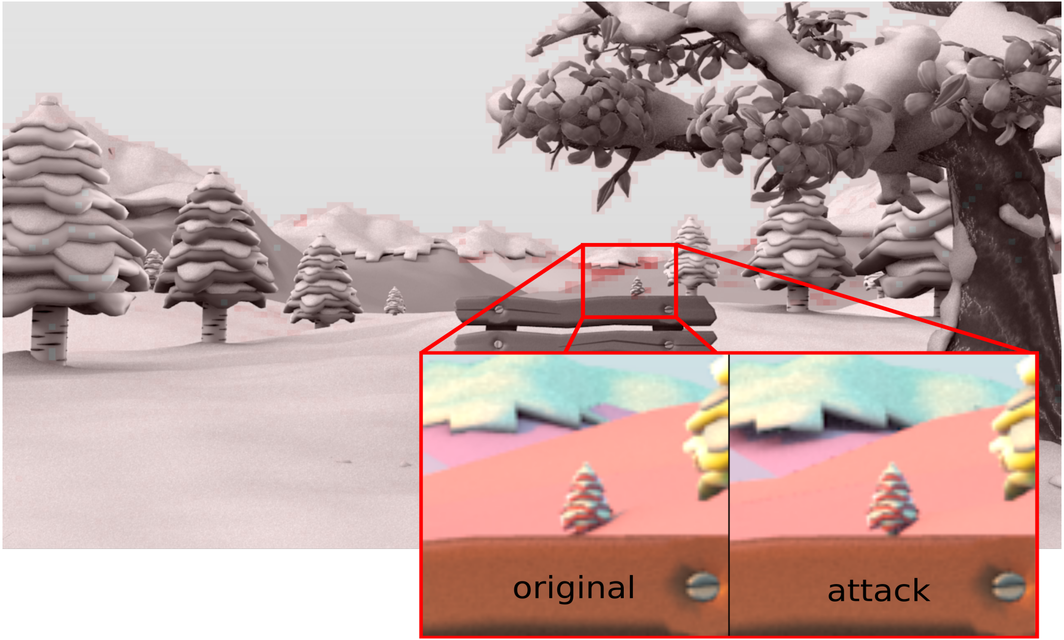
Extended precision		Predicted digit count									
Rounding mode	Correct	0	1	2	3	4	5	6	7	8	9
Any mode	100%	9	14	8	10	14	8	9	14	3	11

x87 Extended precision: Default predictions

Single precision		Predicted digit count									
Rounding mode	Correct	0	1	2	3	4	5	6	7	8	9
Rounding down	8%	0	0	100	0	0	0	0	0	0	0

x87 Single precision: Attacked predictions

Case study 3: SPEC 2017. Image difference in Blender




Washes away Bacteria
Frequent hand washing helps keep your family healthy.
Safeguard®
White with touch of Aloe

Conclusions and outlook

Secure enclave interactions require proper **sanitizations!**

Conclusions and outlook

Secure enclave interactions require proper **sanitizations!**

- Large attack surface, including subtle **side-channel oversights. . .**
- **Defense:** Most investigated shielding runtimes now apply a full XRSTOR sanitization strategy
- Modern x86 architectures are **complex**. Need to investigate alternative processor architectures such as RISC-V

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

Faulty Point Unit: ABI Poisoning Attacks on Intel SGX

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

December 10, 2020