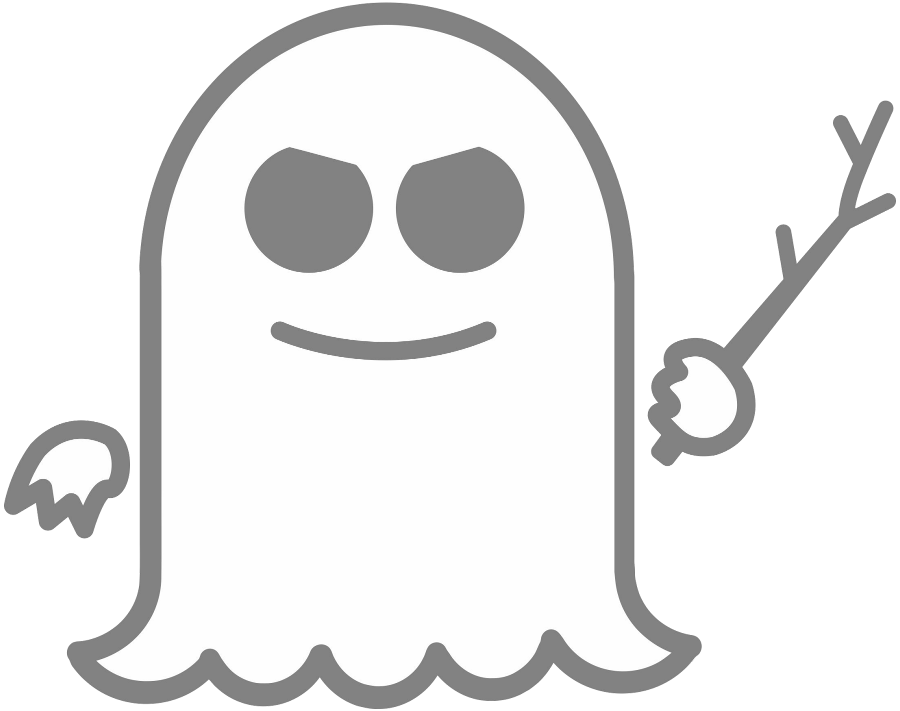
SpecFuzz

Bringing Spectre-type vulnerabilities to the surface

Oleksii Oleksenko, Bohdan Trach, Christof Fetzer
TECHNISCHE UNIVERSITÄT DRESDEN

Mark Silberstein
TECHNION Israel Institute of Technology



```
x = 100
...
if x < 10
    y = array[x]
```

```
x = 100
...
if x < 10
    y = array[x]
```

⬅ False; Predict **True**

```
x = 100
...
if x < 10
    y = array[x]
```

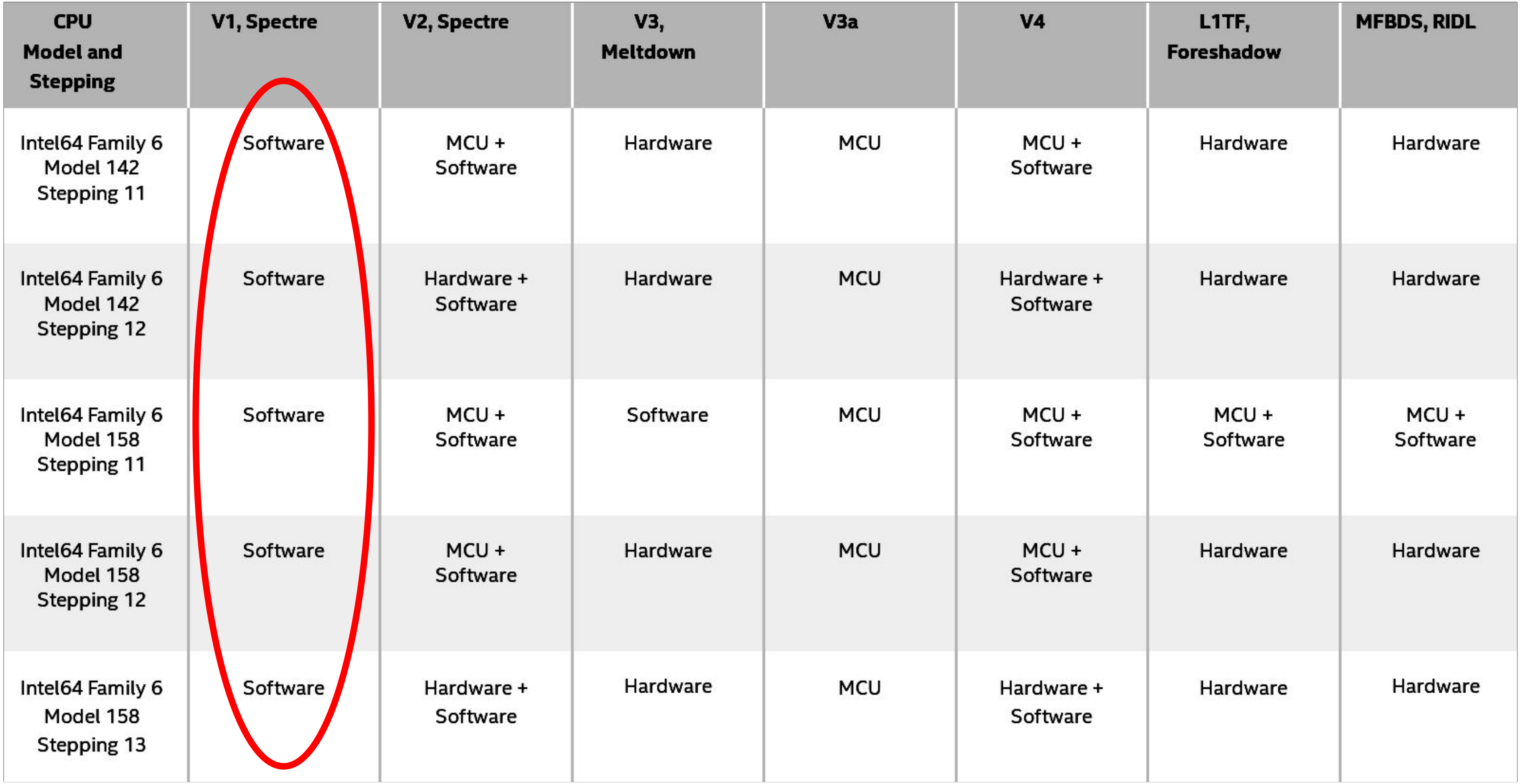
False; Predict True

⬅ **Execute speculatively**

```
x = 100
...
if x < 10                   False; Predict True
    y = array[x]            Execute speculatively
```

- **SW-invisible**
- **leaves HW traces**

Patches?



CPU Model and Stepping	V1, Spectre	V2, Spectre	V3, Meltdown	V3a	V4	L1TF, Foreshadow	MFBDS, RIDL
Intel64 Family 6 Model 142 Stepping 11	Software	MCU + Software	Hardware	MCU	MCU + Software	Hardware	Hardware
Intel64 Family 6 Model 142 Stepping 12	Software	Hardware + Software	Hardware	MCU	Hardware + Software	Hardware	Hardware
Intel64 Family 6 Model 158 Stepping 11	Software	MCU + Software	Software	MCU	MCU + Software	MCU + Software	MCU + Software
Intel64 Family 6 Model 158 Stepping 12	Software	MCU + Software	Hardware	MCU	MCU + Software	Hardware	Hardware
Intel64 Family 6 Model 158 Stepping 13	Software	Hardware + Software	Hardware	MCU	Hardware + Software	Hardware	Hardware

Source:
https://software.intel.com/security-software-guidance/processors-affected-transient-execution-attack-mitigation-product-cpu-model

Software	Defence Mechanism
Chrome	Site Isolation, Reduced Timer Precision, Sandboxing
Linux Kernel	Index masking (171 usages in v5.7.6)
OpenSSL	Outside the threat model [1]
Graphene SGX	None

[1] https://www.openssl.org/policies/secpolicy.html

Software	Defence Mechanism
Chrome	Site Isolation, Reduced Timer Precision, Sandboxing
Linux Kernel	Index masking (171 usages in v5.7.6)
OpenSSL	Outside the threat model [1]
Graphene SGX	None

[1] https://www.openssl.org/policies/secpolicy.html

Software	Defence Mechanism
Chrome	Site Isolation, Reduced Timer Precision, Sandboxing
Linux Kernel	Index masking (171 usages in v5.7.6)
OpenSSL	Outside the threat model [1]
Graphene SGX	None

[1] https://www.openssl.org/policies/secpolicy.html

Software	Defence Mechanism
Chrome	Site Isolation, Reduced Timer Precision, Sandboxing
Linux Kernel	Index masking (171 usages in v5.7.6)
OpenSSL	Outside the threat model [1]
Graphene SGX	None

[1] https://www.openssl.org/policies/secpolicy.html

Software	Defence Mechanism
Chrome	Site Isolation, Reduced Timer Precision, Sandboxing
Linux Kernel	Index masking (171 usages in v5.7.6)
OpenSSL	Outside the threat model [1]
Graphene SGX	None

[1] https://www.openssl.org/policies/secpolicy.html

Why so little?

Why so little?

High overhead

Why so little?

High overhead

Low risk

Our Goal?

Make Defences Affordable!

Our Goal?

Make Defences Affordable!

Our Solution?

Apply Fuzzing!

Problem

Speculation is invisible

Speculation Exposure

Speculation Exposure

Expose speculative execution…

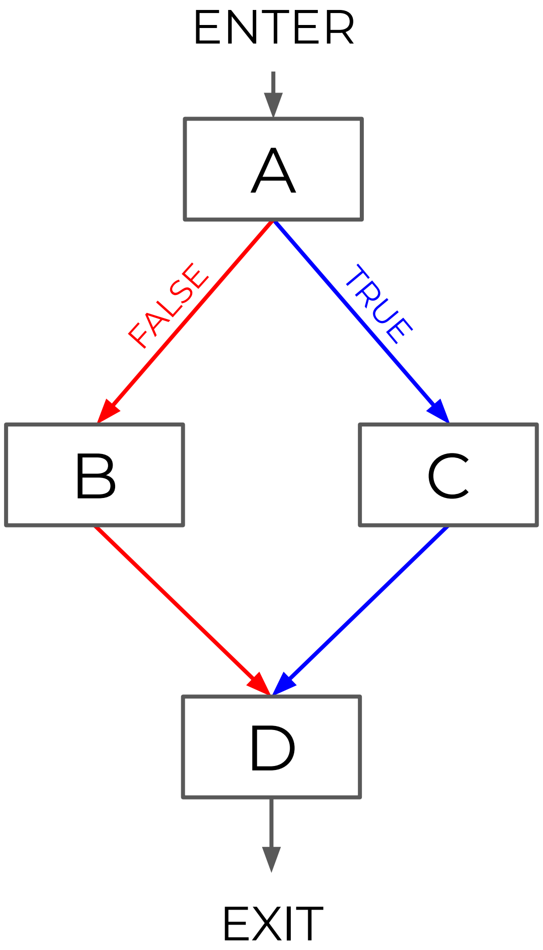
Speculation Exposure

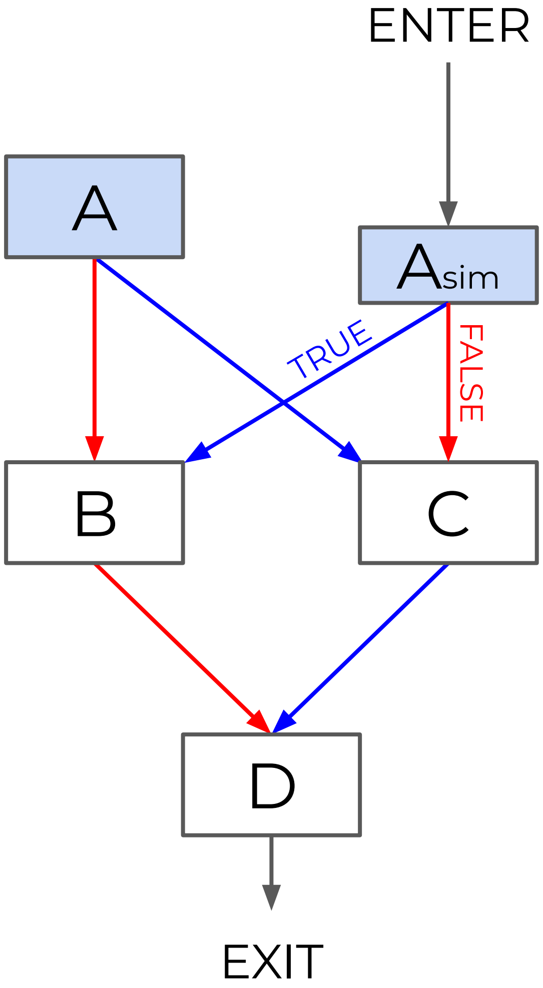
Expose speculative execution…

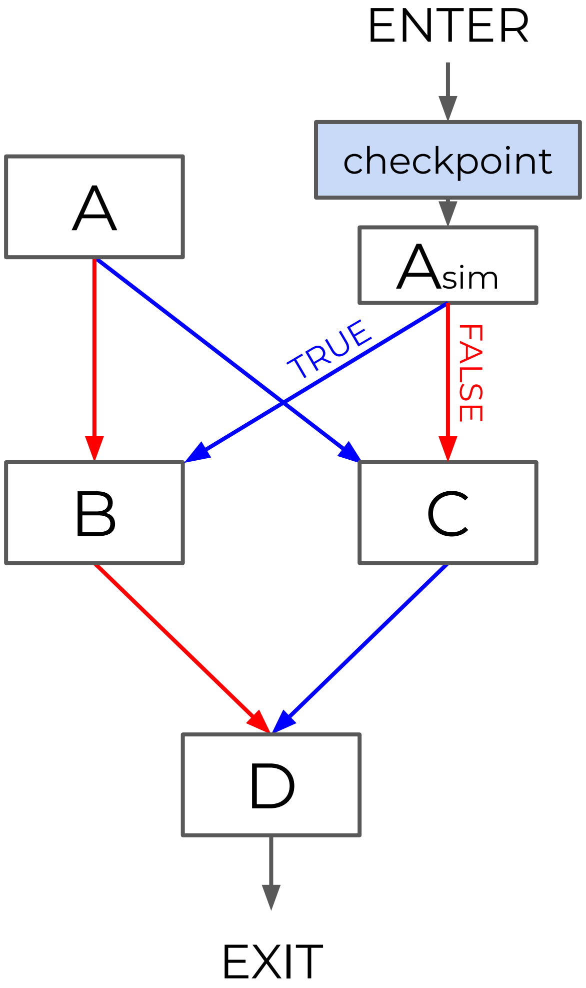
through a worst-case simulation…

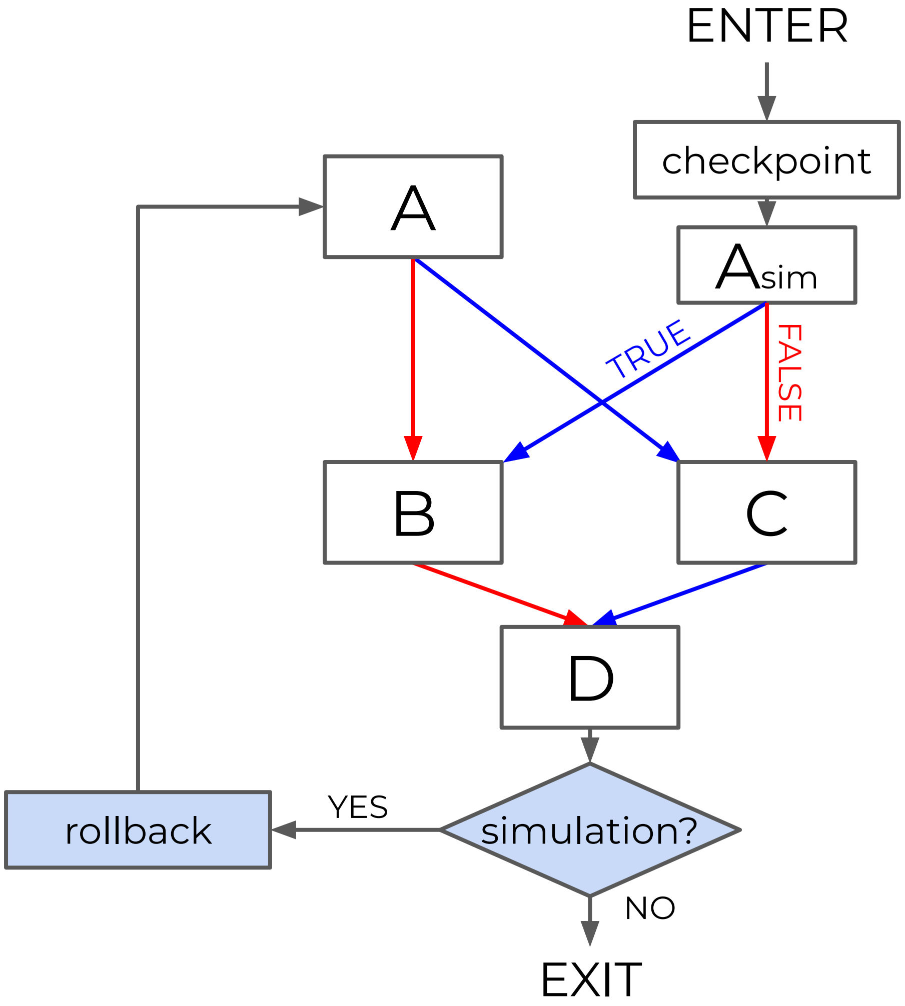
Speculation Exposure

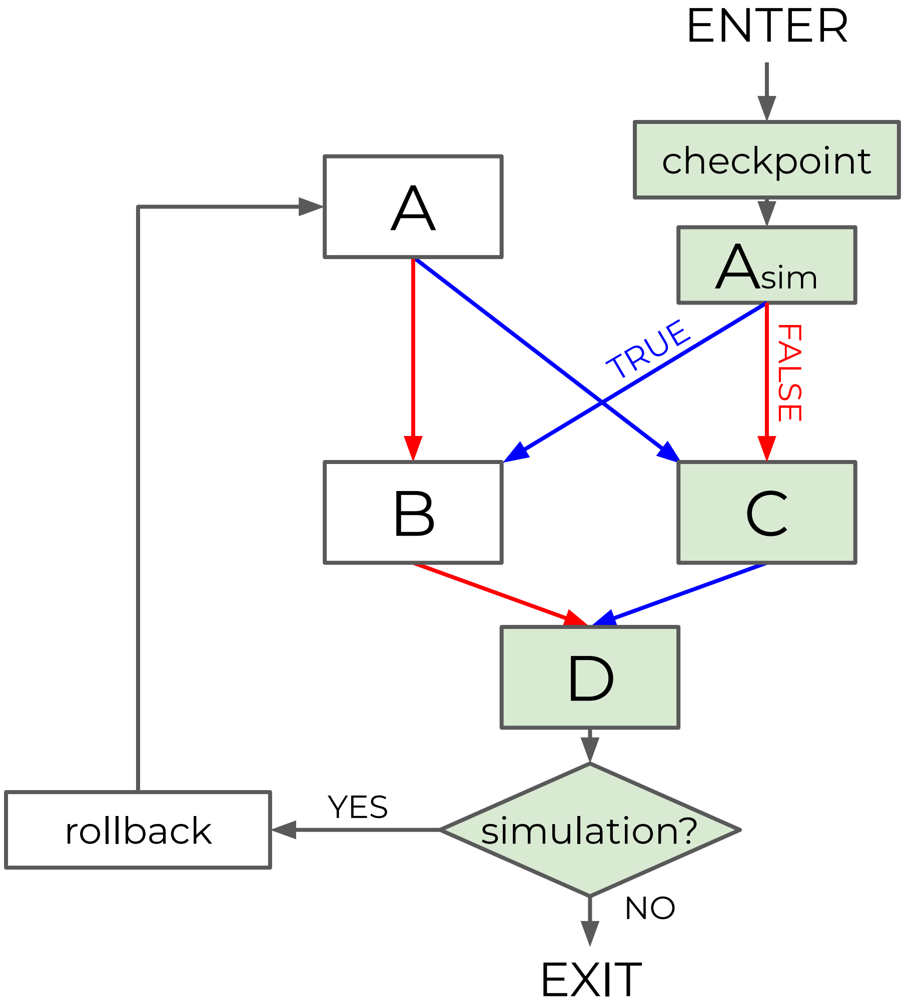
Expose speculative execution…
through a worst-case simulation…
within the process

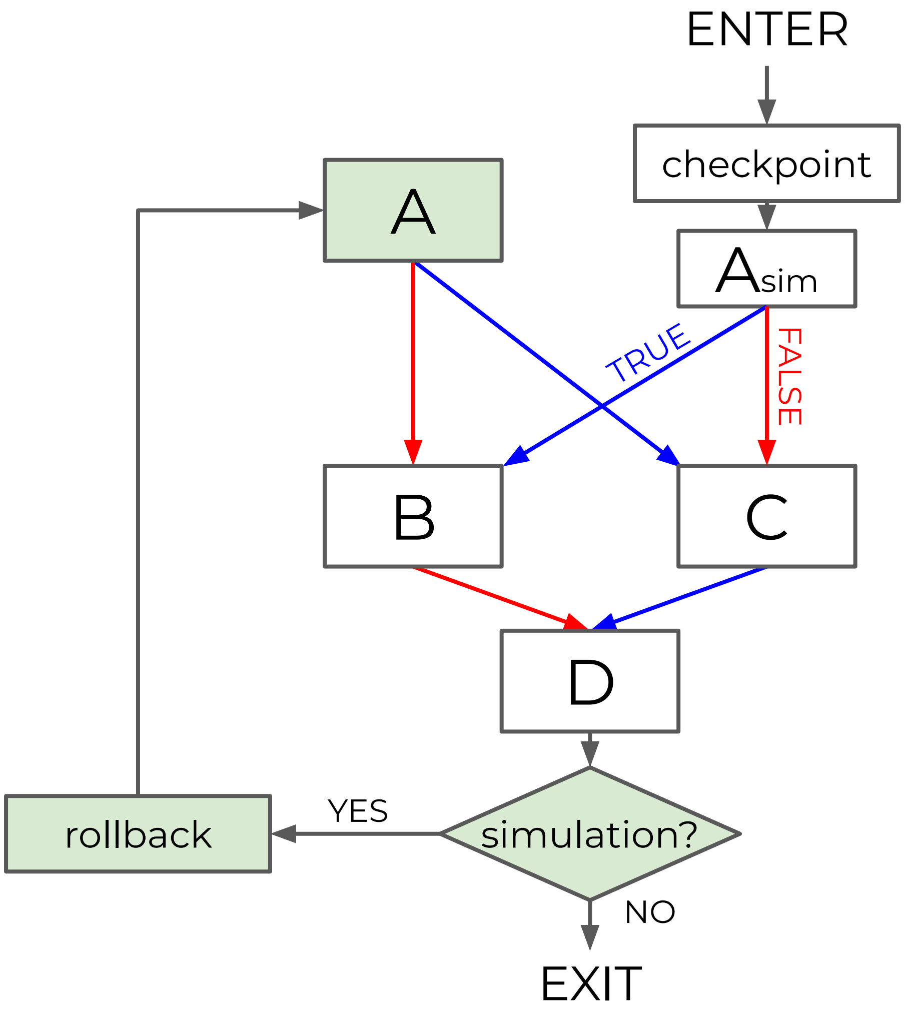

ENTER
A
FALSE
TRUE
B
C
D
EXIT

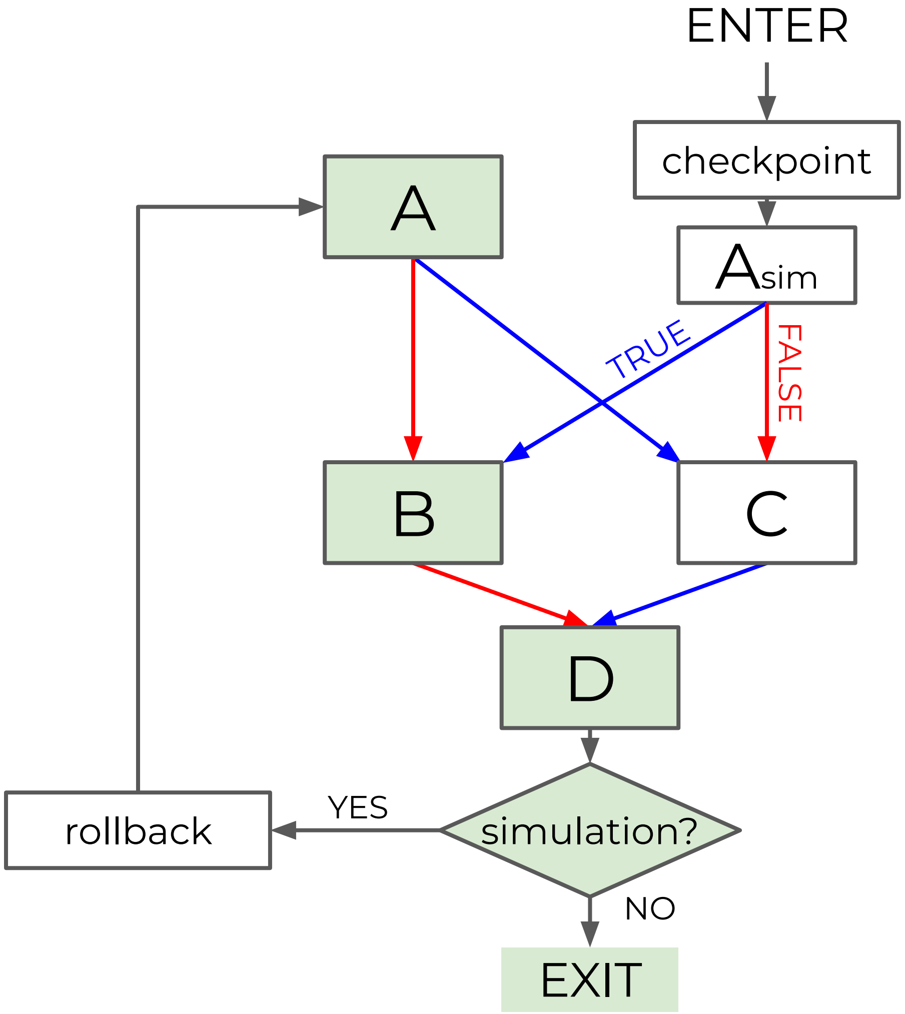

ENTER
A
Asim
TRUE
FALSE
B
C
D
EXIT


ENTER
checkpoint
A
Asim
TRUE
FALSE
B
C
D
EXIT

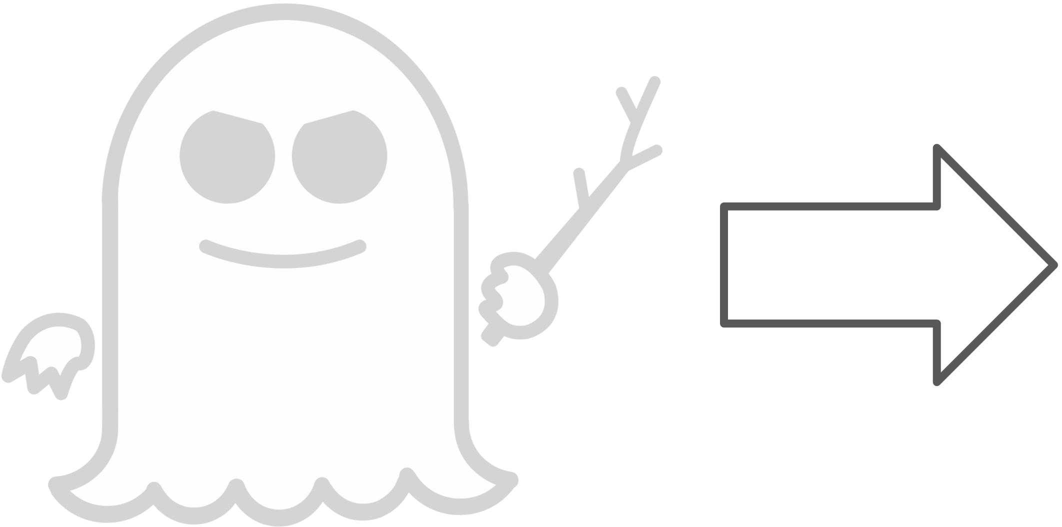

ENTER
checkpoint
A
Asim
TRUE
FALSE
B
C
D
simulation?
YES
rollback
NO
EXIT


ENTER
checkpoint
A
Asim
TRUE
FALSE
B
C
D
simulation?
YES
rollback
NO
EXIT


ENTER
checkpoint
A
Asim
TRUE
FALSE
B
C
D
simulation?
YES
rollback
NO
EXIT


ENTER
checkpoint
A
A_{sim}
TRUE
FALSE
B
C
D
simulation?
YES
rollback
NO
EXIT

Speculation Exposure



Buffer Overflow

SpecFuzz:

Speculation Exposure
(LLVM pass + library)
+ ASan

Technical Challenges

- Nested Speculative Exposure
- External Calls
- Coverage
- Efficient checkpoint-rollback
- Fault Recovery
- Interaction with external libraries
- Speculative control-flow errors

33

Technical Challenges

- Nested Speculative Exposure
- External Calls

See The Paper

- Fault Recovery
- Interaction with external libraries
- Speculative control-flow errors

34

Speculative Memory Violations

Type	JSMN	Brotli	HTTP	libHTP	libYAML	OpenSSL
Code	0	2	1	2	3	16
Controlled	16	68	9	91	140	589
Uncontrolled	34	36	6	222	49	1127
Unknown	0	4	0	29	59	423

Speculative Memory Violations

Type	JSMN	Brotli	HTTP	libHTP	libYAML	OpenSSL
Code	0	2	1	2	3	16
Controlled	16	68	9	91	140	589
Uncontrolled	34	36	6	222	49	1127
Unknown	0	4	0	29	59	423

Speculative Memory Violations

Type	JSMN	Brotli	HTTP	libHTP	libYAML	OpenSSL
Code	0	2	1	2	3	16
Controlled	16	68	9	91	140	589
Uncontrolled	34	36	6	222	49	1127
Unknown	0	4	0	29	59	423

Speculative Memory Violations

Type	JSMN	Brotli	HTTP	libHTP	libYAML	OpenSSL
Code	0	2	1	2	3	16
Controlled	16	68	9	91	140	589
Uncontrolled	34	36	6	222	49	1127
Unknown	0	4	0	29	59	423

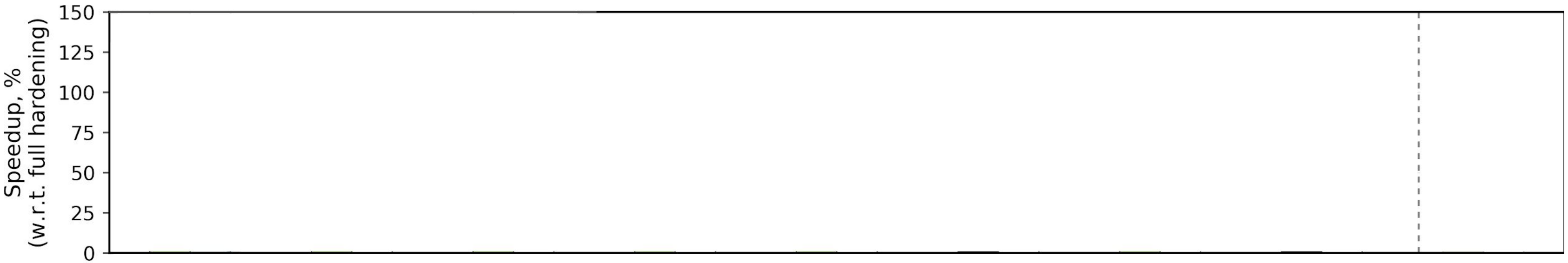
Speculative Memory Violations

Type	JSMN	Brotli	HTTP	libHTP	libYAML	OpenSSL
Code	0	2	1	2	3	16
Controlled	16	68	9	91	140	589
Uncontrolled	34	36	6	222	49	1127
Unknown	0	4	0	29	59	423

Automatic Patching

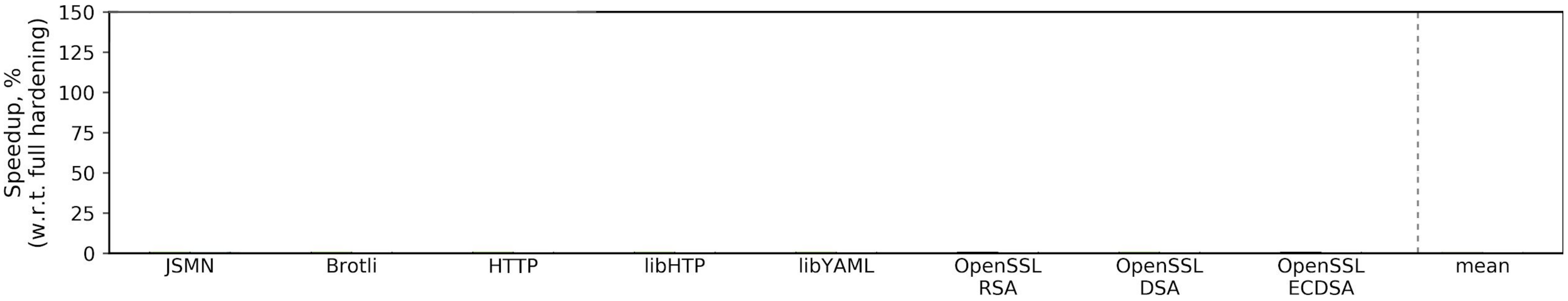
Remove hardening from
"seemingly benign" branches

Speedup



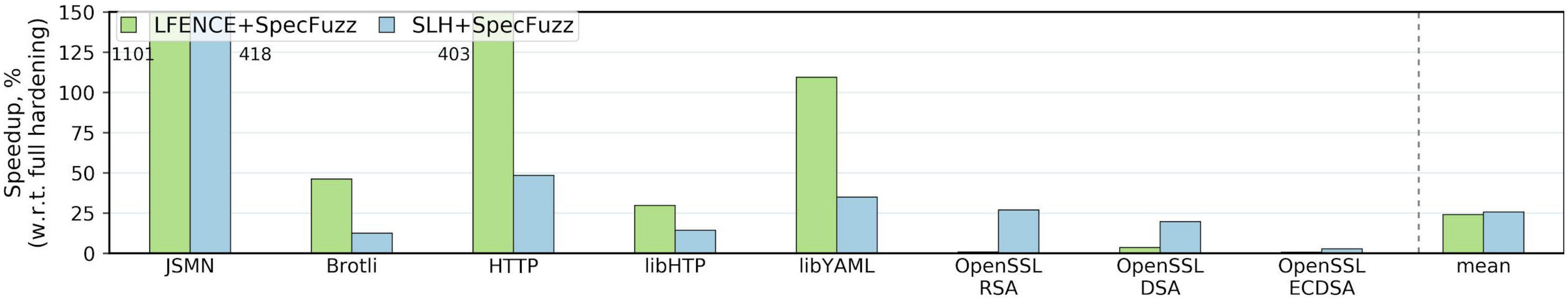
Higher
is better

Speedup



Higher is better

Speedup

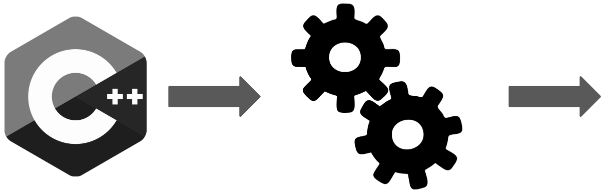


Higher is better

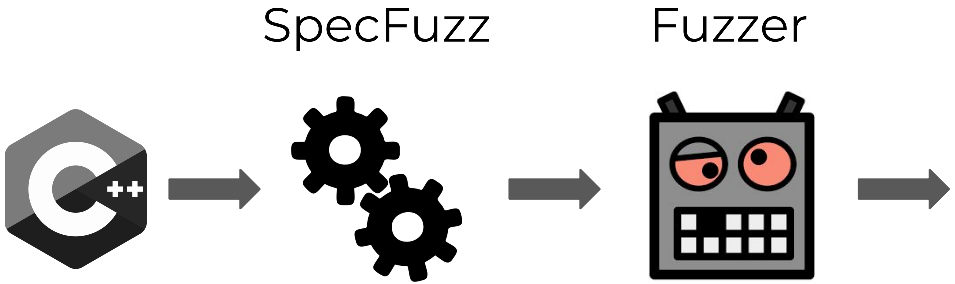
Summary

Summary

SpecFuzz



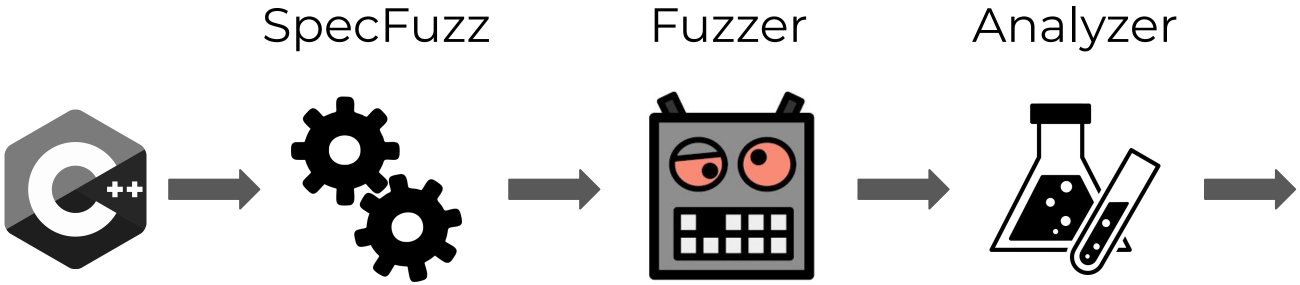
Summary



SpecFuzz

Fuzzer

Summary

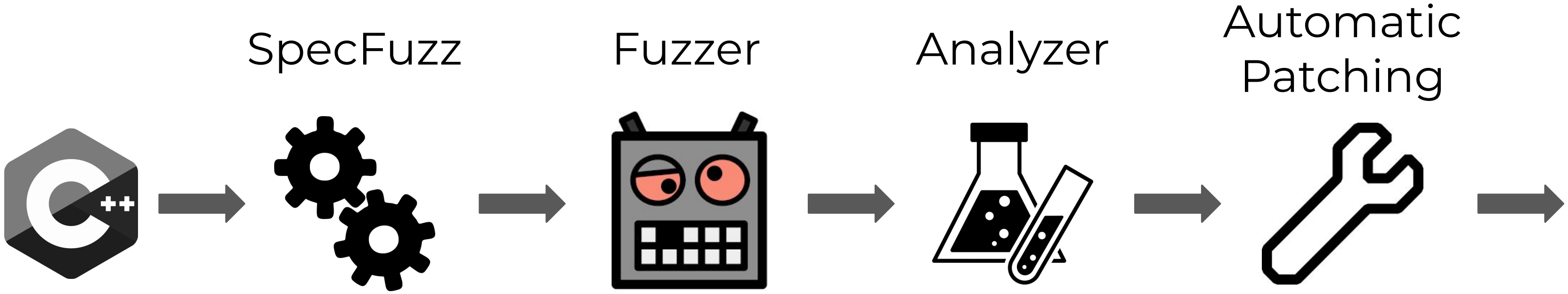


SpecFuzz

Fuzzer

Analyzer

Summary



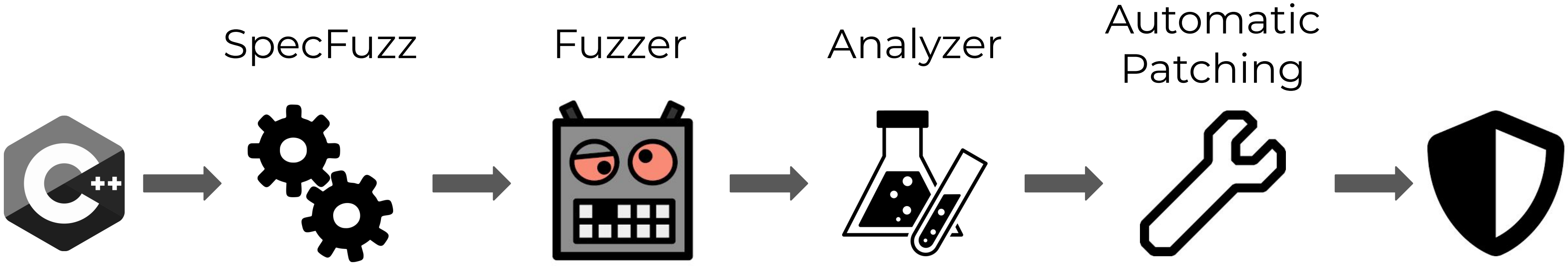
SpecFuzz

Fuzzer

Analyzer

Automatic Patching

Summary



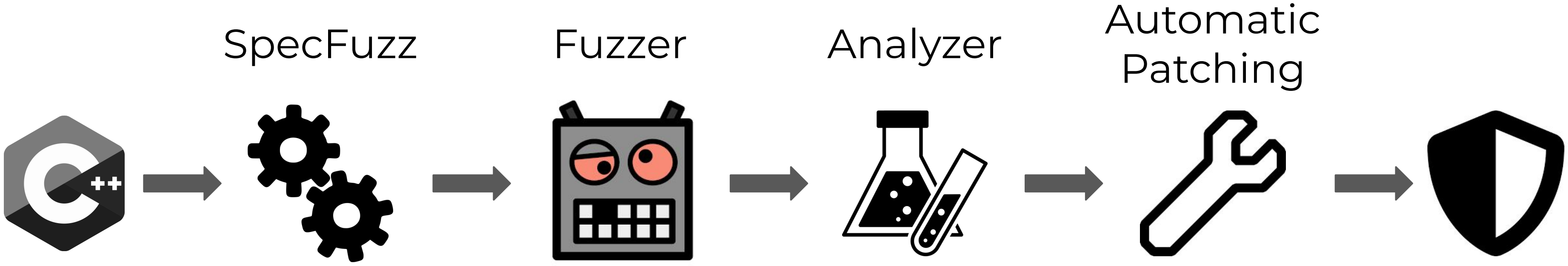
SpecFuzz

Fuzzer

Analyzer

Automatic Patching

Summary



SpecFuzz

Fuzzer

Analyzer

Automatic Patching

https://github.com/tudinfse/SpecFuzz

@oleksii_o

✉ mark@ee.technion.ac.il ✉ oleksii.oleksenko@tu-dresden.de ✉ christof.fetzer@tu-dresden.de