

C++ Club Meeting Notes

Gleb Dolgich

2018-11-29

San Diego trip reports

- ▶ Ben Craig
- ▶ Corentin Jabot
 - ▶ Reddit
- ▶ René Rivera
- ▶ CppCast with Ashley Hedberg

CppCon 2018 Trip Reports

JeanHeyd Meneide

The Jerk Problem is a very simple one: the larger community seems to value technical excellence over all other values. This means that decency – and being polite during such things as discussion or evaluation – is optional. This is how a lot of people conducted themselves: being successful / making money / having influence somehow justifies their ability to be complete blockheads.

Also:

Nobody believes I have dark skin ever when they see my videos or meet me. And for some people, that's a good surprise (but still a problem). Other people think it's a bad idea I'm here to begin with, which is much more of a problem.

Better template support and error detection in C++ Modules with MSVC 2017 version 15.9

[VC Blog](#)

► What's New

- ▶ [Viva64: C++17 Refresher](#)
- ▶ [VCBlog: Standard Library Algorithms: Changes and Additions in C++17](#)

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (1/9)

Video

The screenshot shows a presentation slide titled "Impacts Code In" with a table comparing various Spectre variants across different platforms and their impact on code. To the right, Chandler Carruth is visible on stage, gesturing while speaking.

	App	OS	SMT Only?	SW Fix?	HW Fix?	
Spectre v1	v1	yes ☺	yes ☺	no ☺	slow	no ☺
	v1.1	yes ☺	yes ☺	no ☺	slow	no ☺
	v1.2	yes ☺	yes ☺	no ☺	slow	no ☺
	ret2spec	yes ☺	yes ☺	no ☺	slow	no ☺
Spectre v2	v2	yes ☺	yes ☺	yes ☺	yes ☺	yes ☺
	SpectreRSB	yes ☺	yes ☺	yes ☺	slow	yes ☺
	Spectre v4	yes ☺	yes ☺	no ☺	no ☺	???
Spectre + CPU Bug	v3	no ☺	yes ☺	no ☺	yes ☺	yes ☺
	Lazy FPU	no ☺	yes ☺	no ☺	yes ☺	no
	L1TF	no ☺	yes ☺	yes ☺	no ☺	yes ☺

46

CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (2/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

Retpolines

- Developed by Google
- Requires recompiling source
- Mitigates Spectre v2 (and SpectreRSB in restricted cases)
- May be faster than STIBP for current CPUs.
- Likely slower and less strong than STIBP on future CPUs

<http://bit.ly/2R50i8J-retpoline>, <http://bit.ly/2NOxtPJ-retpoline-intel>

63



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (3/9)

No Service 09:41
X 56:46 -30:48
47:18 Secrets, Side-Channels, Sandboxes, and Security" CppCon - 20181002 - CppCon -25:40

Rethpolines overhead: under 3%
(PGO+ThinLTO)

75

CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security
dts HEADPHONE

9 / 19

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (4/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

```
# %bb.1:                                # %bb.1:  
    movq  (%rdi), %rax  
    leaq  8(%rsp), %rsi  
    leaq  24(%rsp), %rdx  
    callq *48(%rax)  
    movq  24(%rsp), %rdi  
    testq %rdi, %rdi  
    je    .LBB0_3  
  
    movq  (%rdi), %rax  
    movq  48(%rax), %r11  
    leaq  8(%rsp), %rsi  
    leaq  24(%rsp), %rdx  
    callq __llvm_retpoline_r11  
    movq  24(%rsp), %rdi  
    testq %rdi, %rdi  
    je    .LBB0_3
```

65



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (5/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

```
__llvm_retpoline_r11:          # @_llvm_retpoline_r11
# %bb.0:
    callq  .LBB1_2
.LBB1_1:                      # Block address taken
                                # =>This Inner Loop Header: Depth=1
    pause
    lfence
    jmp   .LBB1_1
    .p2align 4, 0x90
.LBB1_2:                      # Block address taken
    movq   %r11, (%rsp)
    retq
```

74



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (6/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

Speculative Load Hardening (SLH)

- Automatic hardening against v1
- Developed by Google
- Changes compiler generated code to make v1 attacks impossible
- Very complex: one of the most complicated low-level transforms in LLVM
- Easy to deploy: clang++ -fspeculative-load-hardening ...

<http://bit.ly/2NPcgVY-slh>

77



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (7/9)

The slide features a dark blue background with a large white rectangular frame on the left side. Inside this frame, the text "SLH overhead is HUGE: 30% - 40% CPU" is displayed in a large, bold, white sans-serif font. In the bottom right corner of the frame, the number "90" is visible. On the right side of the slide, there is a photograph of Chandler Carruth, a man with short brown hair, wearing a light blue button-down shirt and grey trousers, standing on a stage and gesturing with his hands. Above him, the "cppcon | 2018" logo is displayed in orange and white, with the subtitle "THE C++ CONFERENCE • BELLEVUE, WASHINGTON" underneath. Below the photo, the name "CHANDLER CARRUTH" is written in a white box. At the bottom right of the slide, there is another white box containing the text "Spectre" in a large font, followed by "Secrets, Side-Channels, Sandboxes, and Security" in a smaller font. At the very bottom right, the website "CppCon.org" is shown in a white box.

SLH overhead is **HUGE**: 30% - 40% CPU

90

CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (8/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

Isolate secret data from risky code

- Sandbox untrusted code (or code handling untrusted input) from data w/ OS/HW barrier (process boundary for example)
- Effective against essentially all known vulnerabilities
- Only realistic mitigation for v4 (SSB)
- Also protects against non-spectre side channel attacks like Heartbleed
- Every browser moving to this model via site- (or origin-) isolation

<http://bit.ly/2zEivmN-chromium-post-spectre>

91



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

CppCon 2018: Chandler Carruth “Spectre: Secrets, Side-Channels, Sandboxes, and Security” (9/9)

cppcon | 2018

THE C++ CONFERENCE • BELLEVUE, WASHINGTON

Conclusion

- Spectre: misspeculation + side channel -> leak secrets
- New, active area for research -> ongoing influx of vulnerabilities
- Have a threat model, because we can't afford to mitigate everything
- Tailor mitigations to each application's risk and performance
- Convince CPU vendors to make these problems go away

97



CHANDLER CARRUTH

Spectre
Secrets, Side-Channels,
Sandboxes, and Security

CppCon.org

Meltdown, Spectre etc.

- ▶ Matt Klein
- ▶ Graham Sutherland via Frank Denneman

Hardware Effects

This repository demonstrates various hardware effects that can degrade application performance in surprising ways and that may be very hard to explain without knowledge of the low-level CPU and OS architecture. For each effect I try to create a proof of concept program that is as small as possible so that it can be understood easily.

► GitHub – Reddit

- ▶ Demonstrates: bandwidth saturation, branch misprediction, branch target misprediction, cache aliasing, cache/memory hierarchy bandwidth, data dependencies, denormal floating point numbers, false sharing, hardware prefetching, memory-bound program, non-temporal stores, software prefetching, write combining.

Twitter



Sam Grittner
@SamGrittner

↑ 1 Reply, 36 Quotes



I can relate to blenders because I also scream while I'm doing my job.

15/08/2018, 22:28 (Wednesday)
Twitter for iPhone

Retweeted by @rosyna
19/08/2018, 10:23

7910 Likes | 1861 Retweets | Thread >

Twitter



chrisk5000
@chrisk5000

Almost made fun of an electrician today like "is it an electrician's guild rule that you have to perform 5 minutes of ritual complaining about What Was The Previous Electrician Thinking before you're allowed to fix anything?" but then I remembered I'm a software engineer

8,883 Likes **2,464** Retweets

15 Nov 2018 at 17:25 via Twitter Web Client