arXiv:1801.01207

MELTDOWN

What is meltdown?

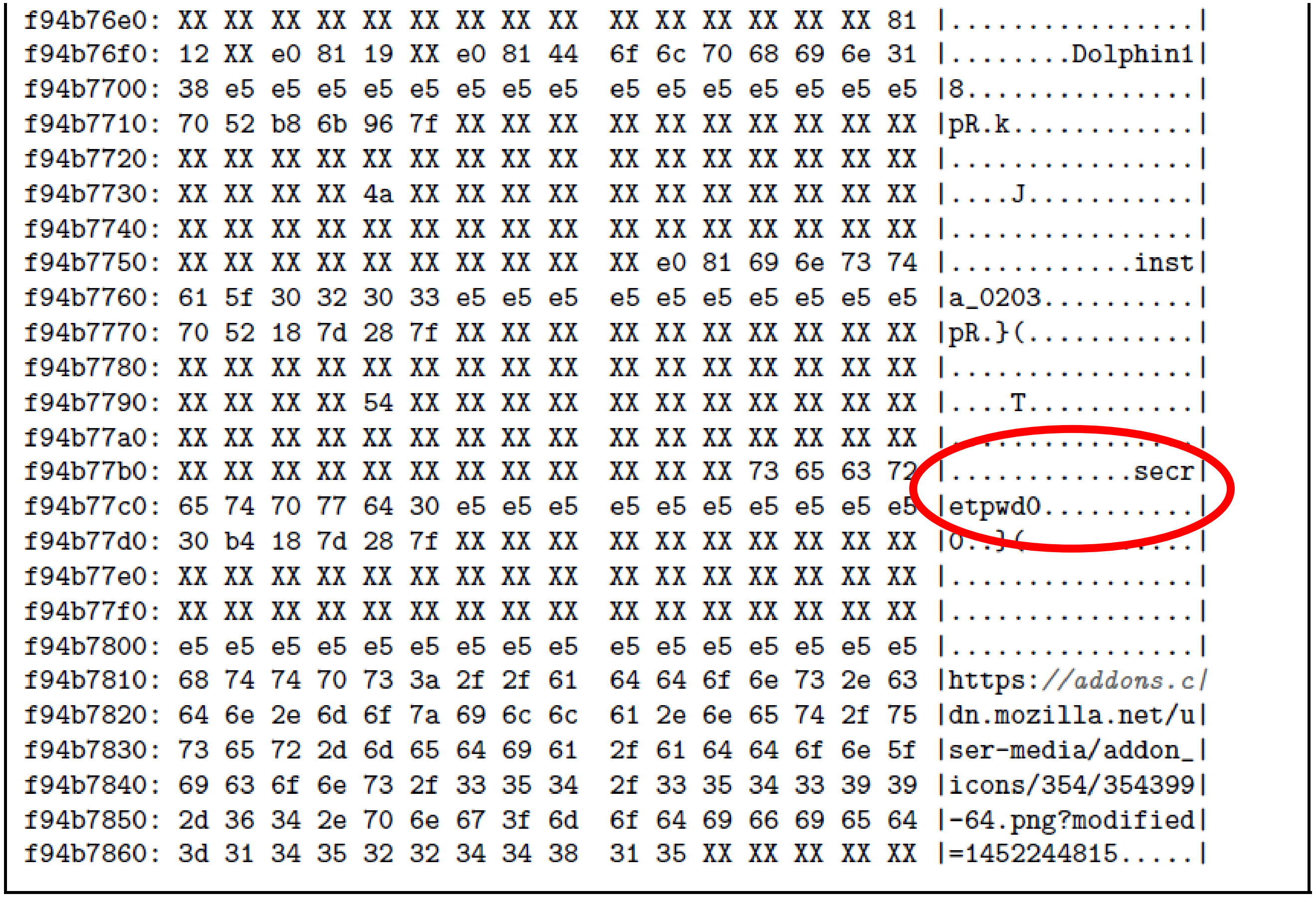
Meltdown is a hardware **exploit** that allows unprivileged *user to access system memory*.

Meltdown takes advantage of “speculative execution”, in particular its ability to “meltdown” security barrier between user and system memory spaces on Intel processors.

Why should I care?

arXiv:1801.01207

I can read your saved password on Firefox or Chrome!

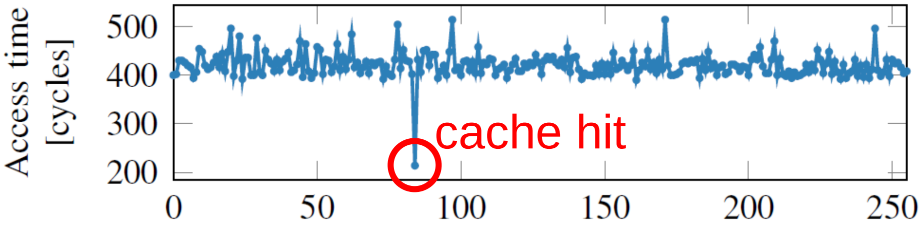


```
f94b76e0: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX 81 |................|
f94b76f0: 12 XX e0 81 19 XX e0 81 44  6f 6c 70 68 69 6e 31 |........Dolphin1|
f94b7700: 38 e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |8...............|
f94b7710: 70 52 b8 6b 96 7f XX XX XX  XX XX XX XX XX XX XX |pR.k............|
f94b7720: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b7730: XX XX XX XX 4a XX XX XX XX  XX XX XX XX XX XX XX |....J...........|
f94b7740: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b7750: XX XX XX XX XX XX XX XX XX  XX e0 81 69 6e 73 74 |............inst|
f94b7760: 61 5f 30 32 30 33 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |a_0203..........|
f94b7770: 70 52 18 7d 28 7f XX XX XX  XX XX XX XX XX XX XX |pR.}(...........|
f94b7780: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b7790: XX XX XX XX 54 XX XX XX XX  XX XX XX XX XX XX XX |....T...........|
f94b77a0: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b77b0: XX XX XX XX XX XX XX XX XX  XX XX XX 73 65 63 72 |............secr|
f94b77c0: 65 74 70 77 64 30 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |etpwd0..........|
f94b77d0: 30 b4 18 7d 28 7f XX XX XX  XX XX XX XX XX XX XX |0..}(...........|
f94b77e0: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b77f0: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b7800: e5 e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |................|
f94b7810: 68 74 74 70 73 3a 2f 2f 61  64 64 6f 6e 73 2e 63 |https://addons.c|
f94b7820: 64 6e 2e 6d 6f 7a 69 6c 6c  61 2e 6e 65 74 2f 75 |dn.mozilla.net/u|
f94b7830: 73 65 72 2d 6d 65 64 69 61  2f 61 64 64 6f 6e 5f |ser-media/addon_|
f94b7840: 69 63 6f 6e 73 2f 33 35 34  2f 33 35 34 33 39 39 |icons/354/354399|
f94b7850: 2d 36 34 2e 70 6e 67 3f 6d  6f 64 69 66 69 65 64 |-64.png?modified|
f94b7860: 3d 31 34 35 32 32 34 34 38  31 35 XX XX XX XX XX |=1452244815.....|
```

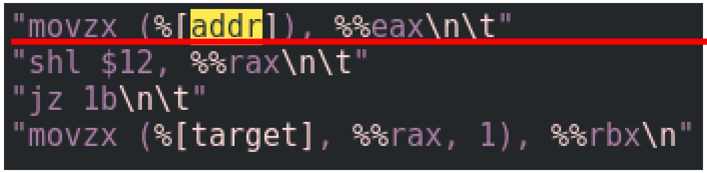
Listing 4: Memory dump of Firefox 56 on Ubuntu 16.10 on a Intel Core i7-6700K disclosing saved passwords (cf.

How does meltdown work?

Step 1: setup “covert channel” to monitor a “probe array”.



Step 2: access system memory, raising a segmentation fault.



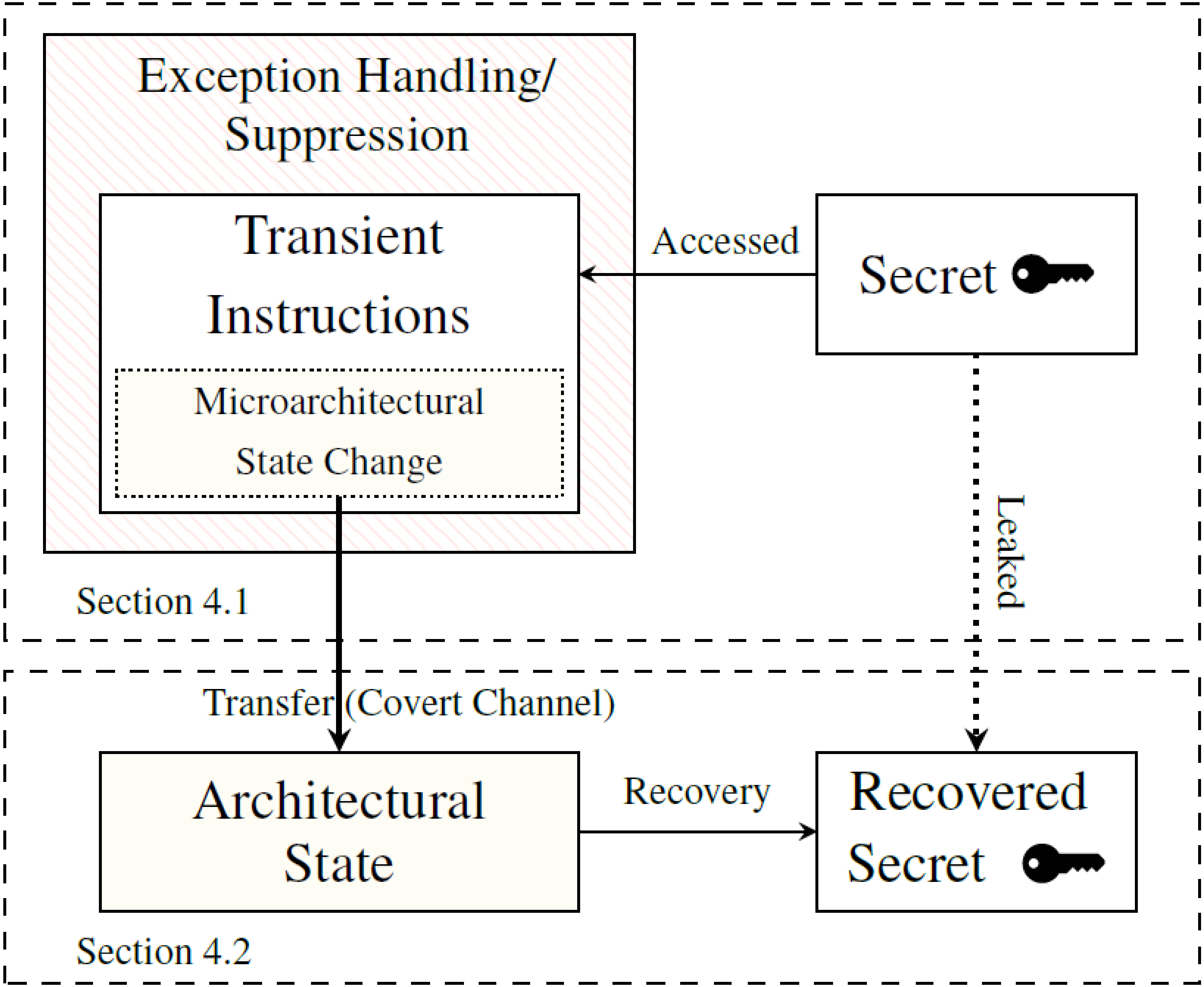
```
"movzx (%[addr]), %%eax\n\t"
"shl $12, %%rax\n\t"
"jz 1b\n\t"
"movzx (%[target], %%rax, 1), %%rbx\n"
```

segmentation fault

speculative execution

Step 3: use speculative execution to cache memory value.

Step 4: use covert channel to read cached value.


Exception Handling/ Suppression
Transient Instructions
Microarchitectural State Change
Accessed
Secret
Leaked
Section 4.1
Transfer (Covert Channel)
Architectural State
Recovery
Recovered Secret
Section 4.2

What to do?

1. Update your browsers! (e.g. Chrome, Firefox)

2. Update operating system – yes, that means Windows updates too

3. Wait for Intel’s microcode/firmware update
   - Intel’s current patch is buggy

Performance Hit

arXiv:1801.04329

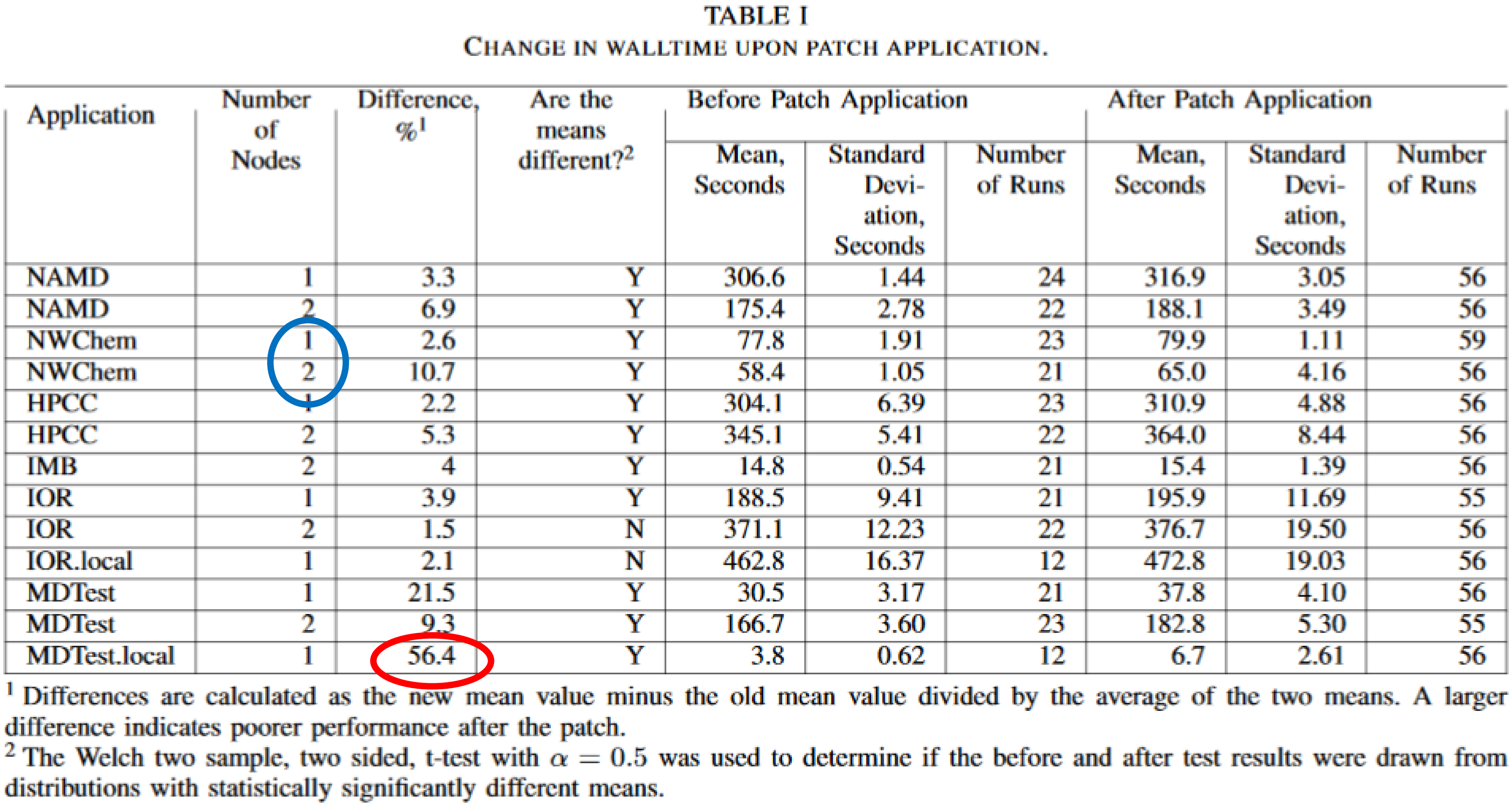


TABLE I
CHANGE IN WALLTIME UPON PATCH APPLICATION.

Application	Number of Nodes	Difference, %[1]	Are the means different?[2]	Before Patch Application			After Patch Application		
				Mean, Seconds	Standard Deviation, Seconds	Number of Runs	Mean, Seconds	Standard Deviation, Seconds	Number of Runs
NAMD	1	3.3	Y	306.6	1.44	24	316.9	3.05	56
NAMD	2	6.9	Y	175.4	2.78	22	188.1	3.49	56
NWChem	1	2.6	Y	77.8	1.91	23	79.9	1.11	59
NWChem	2	10.7	Y	58.4	1.05	21	65.0	4.16	56
HPCC	1	2.2	Y	304.1	6.39	23	310.9	4.88	56
HPCC	2	5.3	Y	345.1	5.41	22	364.0	8.44	56
IMB	2	4	Y	14.8	0.54	21	15.4	1.39	56
IOR	1	3.9	Y	188.5	9.41	21	195.9	11.69	55
IOR	2	1.5	N	371.1	12.23	22	376.7	19.50	56
IOR.local	1	2.1	N	462.8	16.37	12	472.8	19.03	56
MDTest	1	21.5	Y	30.5	3.17	21	37.8	4.10	56
MDTest	2	9.3	Y	166.7	3.60	23	182.8	5.30	55
MDTest.local	1	56.4	Y	3.8	0.62	12	6.7	2.61	56

[1] Differences are calculated as the new mean value minus the old mean value divided by the average of the two means. A larger difference indicates poorer performance after the patch.

[2] The Welch two sample, two sided, t-test with $\alpha = 0.5$ was used to determine if the before and after test results were drawn from distributions with statistically significant different means.

References:

Google Project Zero broke the news

Meltdown and Spectre is the official website

Proof-of-principle code by paboldin