Reverse Engineering Hardware for Fun and Profit

Kaveh Razavi



About VUSec

~20 members, 3 faculty

- Software protections
- Binary analysis
- Fuzzing
- Network security
- Hardware and OS security



Assuming secure software, what is still possible? and what can we do about it?

General-purpose Hardware Attacks (2015-)



Drammer

Core " i7

Spectre/MDS



Follow

A government entity in a certain country: "can we please have the Drammer exploit?" Priv escalation: Leak of /etc/shadow's content using SPECTRE on Fedora 25 amd64. CANVAS Early Updates users will see the update soon and regular CANVAS users will see it on the next CANVAS release. #Spectre #Meltdown

Understanding These Issues

Hardware is (almost) always closed.

Reverse Engineering!

Hardware Reverse Engineering at VUSec



The Rowhammer Problem

We have reduced transistor without caring for reliability/security



Rowhammer: affects 87% of deployed DDR3 memory, DDR4 as well.

Kim et al., "Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors," ISCA'147



Browser exploitation: hard on x86, not possible on ARM



Drammer: Flip Feng Shui Goes Mobile - VUSec

Drammer is the first instance of mobile Rowhammer and comprehends a deterministic Android root exploit that does not rely on any software vulnerability.





Victor van der Veen @vvdveen · 25 ott 2016 I wouldn't be surprised if we could pull this one from a browser actually...

Traduci dalla lingua originale: inglese

♀ 1 1] 4 ♡ 5 🖂



the grugq @thegrugq



 \checkmark

In risposta a @vvdveen e @vu5ec

love to see it happen. :)

Native Rowhammering

x86: clflush ARM: DMA memory

From JavaScript: eviction sets

Eviction Sets and Rowhammer



Building a Practical JS Rowhammer (on Mobile)

Eviction sets on x86 are slow \rightarrow few flips Eviction sets on ARM are **very** slow \rightarrow no flips

Hardware Reverse Engineering at VUSec



Inside a Phone's SoC

More co-processors



The GLitch Attack



Understanding GPUs: The Rendering Pipeline





Understanding GPUs: The Rendering Pipeline



The Adreno 330 GPU Architecture



The Adreno 330 GPU Architecture



GPU Caches



- 1) Cacheline size
- 2) Size
- 3) Associativity
- 4) Replacement policy

Reverse engineering tool:

GPU performance counters:

L1_hit, L1_miss, L2_hit, L2_miss

Reverse Engineering Shader

```
1 #define MAX max // max offset
2 #define STRIDE stride // access stride
3
   uniform sampler2D tex;
4
5
6 void main() {
7 vec4 val;
  vec2 texCoord;
8
9
    // external loop not required for (a)
    for (int i=0; i<2; i++) {</pre>
11
    for (int x=0; x < MAX; x += STRIDE) {
12
     texCoord = offToPixel(x);
13
      val += texture2D(tex, texCoord);
14
15
    gl_Position = val;
16
17
```

Cacheline Sizes

STRIDE = 1 $MAX = 1 \dots N$ L1 miss != 1 L2 miss != 1 L1 cacheline = 16 bytes L2 cacheline = 64 bytes

```
1 #define MAX max // max offset
2 #define STRIDE stride // access stride
3
   uniform sampler2D tex;
4
5
6 void main() {
    vec4 val;
7
8 vec2 texCoord;
    // external loop not required for (a)
9
10 for (int i=0; i<2; i++) {
   for (int x=0; x < MAX; x += STRIDE) {
11
12 texCoord = offToPixel(x);
       val += texture2D(tex, texCoord);
13
14
15
16
    ql Position = val;
17
```

Cache Sizes

STRIDE = cacheline size

 $MAX = 1 \dots N$

```
1 #define MAX max // max offset
2 #define STRIDE stride // access stride
3
   uniform sampler2D tex;
4
5
6 void main() {
    vec4 val;
7
    vec2 texCoord;
8
     // external loop not required for (a)
9
    for (int i=0; i<2; i++) {</pre>
10
   for (int x=0; x < MAX; x += STRIDE) {
11
12 texCoord = offToPixel(x);
       val += texture2D(tex, texCoord);
13
14
15
16
     gl_Position = val;
17
```

Cache Sizes



Replacement Policy

Typically LRU or some variant

addr1 + addr2 + addr3 + addr4 + addr1 + target

LLC set: addr3 + addr4 + addr1 + target

On GPU: FIFO

addr1 + addr2 + addr3 + addr4 + addr1 + target

LLC set: addr2 + addr3 + addr4 + target

Complicates Rowhammer - See paper.



LLC Set



Associativity

Goal: find addresses that map to the same cache set **Methodology:** Oren et al. eviction set building algorithm

- Pick a pool virtual addresses
- Pick an observer address
- Reduce the pool to a minimal set that evicts observer

Associativity (and address mapping)

L1 = 16 way set associative

L2 = 8 way set associative

Non-inclusive L2



How to efficiently flush L1 with L2 lines?

GPU Caches





Putting All Together





GLitch

Exploitation: NaN-boxing





int double

string

1	<pre>var arr = new Array(100);</pre>
2	arr[0] = 1 // int
3	arr[1] = 1.878e+65 // double
4	<pre>arr[3] = "Hello World" // string</pre>

. . .

NaN-boxing

Exploitation: NaN-boxing





Exploitation: Type Flipping





Exploitation: Type Flipping





End to End Exploitation with GLitch

Attack	Compromise	Breaking ASLR
GLitch	116 s	27 s
Dedup Est Machina [7]	823 s	743 s
Rowhammer.js [20]	*	-
AnC [18]	-	114 s

2018 Code Blue young researcher award! 2019 best NL security master thesis award!

Meanwhile After Every Rowhammer Talk...

Question from audience:

Doesn't ECC memory fix all of this?
Error-correction Codes (SECDED)

- Original paper demonstrated SECDED not to be enough
- ... but exploitation turned out to be difficult
 - ECC implementation is closed (guarantees unknown)
 - 1 bit flips not visible,2 bit flips crash the system



ECC DRAM as a practical secure defense.

Hardware Reverse Engineering at VUSec



Recovering ECC Functions

- Observing signals are not easy at 1Ghz+
 - Need custom interposer
 - Expensive logic analyzer
- Fault injection with syringe needles!
- Short-circuit data lines with Vss
 - High-to-low voltage flips



• ECC error reports allows for ECC function recovery

Demo

Needle Flip Injection Is Too Painful...



Demo

Results

ID	Pattern	Config.	# flips	Flips location
AMD-1	$[\mathcal{P}_1]$	Ideal	3-BF-16	3 symbols, 1 in control bits
AMD-1	$[\mathcal{P}_2]$	Ideal	4-BF-16	Min. 2 symbols
Intel-1	$[\mathcal{P}_3]$	Ideal	4-BF-8	Min. 2 symbols
Intel-1	$[\mathcal{P}_4]$	Default	2-BF-8	Min. 2 symbols

TABLE V: Error patterns that can circumvent ECC.

TABLE VI: Percentages of rows with corruptions in an ECC DIMM.

$[\mathcal{P}_1]$	$[\mathcal{P}_2]$	$[\mathcal{P}_3]$	$[\mathcal{P}_4]$
0.12%	0.12%	0.06%	0.60%

Avoiding Crashes



Detect single flips and merge them for silent corruptions.

ECC: Replicating Existing Attacks



Traditional Cache Attacks



```
if (secret_key[i]) == 1)
{
    something();
}
else
{
    something_else();
}
```

Attacking CPU-internal Components



AnC

ASLR leak

2017

AnC: MMU Leaves a Trace in the CPU Caches



Gras/Razavi et al., "ASLR on the Line: Practical Cache Attacks on the MMU," NDSS'17

AnC from JavaScript



24.457 got level 4 - start slot 148, address 0x94000 24.993 got level 3 - start slot 295, address 0x24e94000 24.993 estimated remaining entropy 6 slot solutions: -1,-1,295,148 68.737 got level 4 - start slot 0, address 0x0 69.502 got level 3 - start slot 359, address 0x2ce00000 70.259 got level 2 - start slot 411, address 0x66ece00000 88.041 got level 1 - start slot 238, address 0x7766ece00000 88 041 estimated remaining entropy 0 slot solutions: 238 411 359 0 data: 0x7766ece00000, code slots: -1,-1,295,148, code: 0x7966e4e94000

Affected Architectures

CPU	Yea
Intel Core i7-7500U (Kaby Lake) @ 2.70GHz	2016
Intel Core m3-6Y30 (Skylake) @ 0.90GHz	2015
Intel Xeon E3-1240 v5 (Skylake) @ 3.50GHz	2015
Intel Core i7-6700K (Skylake) @ 4.00GHz	2015
Intel Celeron N2840 (Silvermont) @ 2.16GHz	2014
Intel Core i7-4500U (Haswell) @ 1.80GHz	2013
Intel Core i7-3632QM (Ivy Bridge) @ 2.20GHz	2012
Intel Core i7-2620QM (Sandy Bridge) @ 2.00GHz	2011
Intel Core i5 M480 (Westmere) @ 2.67GHz	2010
Intel Core i7 920 (Nehalem) @ 2.67GHz	2008
AMD Ryzen 7 1700 8-Core (Zen) @ 3.3GHz	2017
AMD Ryzen 5 1600X 6-Core (Zen) @ 3.6GHz	2017
AMD FX-8350 8-Core (Piledriver) @ 4.0GHz	2012
AMD FX-8320 8-Core (Piledriver) @ 3.5GHz	2012
AMD FX-8120 8-Core (Bulldozer) @ 3.4GHz	2011
AMD Athlon II 640 X4 (K10) @ 3.0GHz	2010
AMD E-350 (Bobcat) @ 1.6GHz	2010
AMD Phenom 9550 4-Core (K10) @ 2.2GHz	2008
Rockchip RK3399 (ARM Cortex A72) @ 2.0GHz	2017
Rockchip RK3399 (ARM Cortex A53) @ 1.4GHz	2017
Allwinner A64 (ARM Cortex A53) @ 1.2GHz	2016
Samsung Exynos 5800 (ARM Cortex A15) @ 2.1GHz	2014
Nvidia Tegra K1 CD580M-A1 (ARM Cortex A15) @ 2.3GHz	2014
Nvidia Tegra K1 CD570M-A1 (ARM Cortex A15; LPAE) @ 2.1GHz	2014
Samsung Exynos 5800 (ARM Cortex A7) @ 1.3GHz	2014
Samsung Exynos 5250 (ARM Cortex A15) @ 1.7GHz	2012

.

Attacking CPU-internal Components





Are these spot mitigations enough?

Attacking CPU-internal Components



Van Schaik et al., "RIDL: Rogue Inflight Data Load," S&P'19



What CPU Buffers?

		United States Par	United States Pate	United States Patent	Glow et al.	Akkary et al. [0] Dute of I	alenst: Oct. 21, 1997
United States Par United State Abramon et al. Abramon et al.	Abramon et al.	Del METROD AND APPARAD	[14] METHOD AND APPARATE PREVENTING INCOMMENT	(14) WHITE COMMINSE REFFER		[24] CACHE MEDICIPE EXPERIENT RAVENCE DOLLA. AND THE AREASY AND MEET PERSONS. BUTTER DATASAND MEET PERSONS. Heady, "The Darks Memory 5.	Harry Rook", 1993, pp. 79-46 hode", 1993, pp. 336-537, 295-856
(19) METRICANN AND APPARE	NAME AND A DATE OF REVERSED LOUD	CUTPET RIPPIRED YTS	AN DWEEL CERDINGS WHEN BE	HYCLA DATACCEDY	Mathicentore	The Mander And	AND', & THE REP IN AND
1////	1		/		/	United Castor Data	(MILVIELE)
United States Paty United States	Pate United States 1	United States Pater	United States Pat Abramon et al.	ou United States Pa	United States Pate Bodas et al.	Voir et al.	Contas Patent and
Give et al. Give et al.	ANTER (14) METHED AND APPEN	D4 METHODS AND APPARATOR	1741 MICTIEGD AND APPARATE EXECUTING AND DESING	(S) THETLOMENING BEARD	[54] MELILAMENT TO IMPROVE OF MELILAMENT LOAVES	(54) METHOD AND APPARATUS FOR PROBETTING WEEN LEAVE INSTRUCTIONS CAN BE EXACUTED FOR OUT OF ORDER	Madat et al.
All TRADE OF MARC IN 1815 COMBEND UNCAN ADD TO CACHER LINE MEDITION CONTROL LINE MEDITION CONTROL LINE MEDITION CONTROL LINE MEDITION CONTROL LINE	INA INT BELACORS	MUNNER LODWY A PLF	CEREATIONS IN A CODER	INCAL DE ANA E SPREES	And Andrew Minut Parker Sector	/	(10) METERARDA AND ADDRESS BOARDA AND ADDRESS BOARDA AND ADDRESS ADDRES ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADDRESS ADD
instructions during	/ /	1	/		/	United States Patent	(11) Applicant Marks Corporation, Source Courses, CAUDIN (12) Browners Market Machine, Son Jone, CAUDIN, 20
at read states Pa	us United State	In United States	United States Pa	United States Patent on	United States Paten Palanca et al.	Aleganico et al.	Chang, Marine Mann, Joans, Cold Million Andrews Mar. Address. Annu. Jones, Cold Million
(13) United States Carriers et al. Palancia et al.	Palance et al.	C4 METROBANDAPPARA	(24) METROD AND APPARAT PROCEEDING MEMORY	DI METHOD AND APPARATUS FOR	14 SENCIERONZATION OF SEA	154 MTARITISTO FOR HAR STREAM OLIGAT	
(26) WHITE COMBINING IN W UNITER COMBINING I	010 METHOD AND APPAL DIPLEMENTING ADD	10 tone of the	DECREMATION WITHIN MECHANICAL	COMPUTER MOTION	MICROSOM	(11) Browney Arthry M. Abramon, Aleka Ken G.	1
CD Amount Daniel M Caras	/	/	1	/	-		us United States Patent
/ / /	an in a States Pat	United States Pa	/				150 STORY MORE AS PREPER TRAVEOR
United States Patent on United Sta	Abramon et al.	Akkary	and the second s		on United States Patent	cm United States Patent Inching et al.	City Applicants Handback Barthand, Child Solida City Applicants Handback Mark Destands, Child Solida City Applicants
Hernitoux et pl.	110 METHOD AND APPARAL PERFORMING METHOD 010	MEMORT MYTEM FOR OUT	ozo United States I Hammond et al.	on United States F		on traditionitation or totals	Theorem V. How, Discuss Linguist 1997 Con- bin Research T. So Subversion, Providentia, COL (US)
Del ALCENDO AND APPARATOR PUB CO ALCENDA DE ALCENDO DE ANTALO E COLLADOR PUBLICADOR PUB	195] Investors Juliary M. Alexet Alberty M. Alexet	MULTINISTAD EXECUTION	DIS UTERADISE AN ADVANCE TABLE FOR MEMORY IN AN OLT OF ORDER PROP	IN BORNES OFFICE	(5) ADTEM AND ME HALLOUT PORTFACTOR FACT TABLE VALUE OF SPECIAL PARTY METTAME REPETCE OF SPECIAL PARTY	OFFICIENTS LINE TAND FINAL PROPERTY AND PROVIDENT STATES	(22) Incommun. Has Suppress Man. Proceedings. OR: 02295 Relaterst 5: 4 Street Transmission Conf. 02255 Cancers 5: Street Transmission, Proceedings, Conf. Cancers 5: Street Transmission, Proceedings, Conf. Concers, 5: Street Transmission, Conf. Conf. Concers, 5: Street Transmission, Conf. C
NATURA II DIN CALLED		/	· · · · · ·			/	(25) (20) Assignment Back/Comparation, Jones Class. CA
		States and States					(*) Statical Reduct to any declarate, for terms of Transition in manufactor or migratule and Transition to the terms of devi-
on United State	Data United States Pat 029	United States Pat Palmer et al.	2 1 2 2 2 2		(ii) United States Patent Atkary et al.	United States Patent	(21) Juppl No. 18930595
to United States Bogge et al.	10 MPINELAND LITENCE MEM	CLATENT NOCIO ANT MILLY	CD United Sta Durdas	on United States P	150 MEMORY DISAMINIZATION FOR LARCE	Karts et al.	(2) Find. Sup. 20, 2013 (2) Vine Polyteration Data (2) Mar. 26, 2015
ACCEPTION IN SALES	ARCHITECTURAL IMPLEMENT METROD AND SYSTEM (70)	INPLEMENTATION MICTION Investor: Julyador Palance, Feb	(S) MITMOFILIG	CONTRA NO NETROD IN	(19) Investory Hakkam Akkory, Dyrland, OR (US), Subarder Hilly, Milleton, OR (US)	124. APPARATUS AND METHOD FOR RES SECAL TERMENATION COMPLEXIBILITY	(5)) Kat. CL 6947-5392 (2006-81)
/		and a second second		DEPENDATC & HELDE		/	(c) D.C. DHA VIENT COLT 1, CO
			/				(30) Field of Chantlewidon Seam's New Seam
Palases et al. Can et al.					(11) INTERNATIONAL APPLICATION PORTSHIP	ini	-,
CO MITIND AND AN	us United States	h LCL L P	United Sec	United States Be	(19) World Instituces Property Organization	on United States Patent	
(D) Investory Salvadar Sa	(%) ACOTERCOTATELON	nited States P. udatyappan et al.	Avadalyappan e	Acadalyappas et al.	(4)) International Pathlenium Date 31 June 2003 (27.06.2002)	150 VETBOD AND SYSTEM FOR ACCIDENTS	1 11-7
CALDON Filing CD Investors Devid W COP, Italia Based Dorrol D. Baggs Add	(70) Applease field Carporat (30) CP	ND ME AND METHODS I IN BEDRICKE DIFFERNT	DU SYSTEMS AND A CACHE WITH S	SAMERICAND METROPOLIC MANYARANG THE COHERT STORE COLLEGENCE CACHE	(1) International Printed Chevelination (GMIP 60		(aller F-
(71) Anger, Forta (73) Anger,	(5) Investors: Along Robox 8 (15) Thomas 7 (15) Thomas 7 (15) Thomas 7	please land Corporation, I (US)	(70) Inconvers Alastidite Zonogradi Abdullak	CATHE () Applease haad Corporation No. (15)	 (11) International Application Number: 15/25/201103 (2): International Filing Tute. 		1
(*) Notice (*) Makes Andrew South Common Stations in Stations of S	Femilyrain, GA (17) Inv 170 Anigan: field Corporate 170	Sanapone CA (DD) Abduffié, D Darid		[1] Investore: Konthibuyan Braduly Insurtivity, C.A. U.S.L. Abdullah, 12 Davids.	(15) Filog Loopoop. Regis	(1)1 Antigane Intel Corporation Some Care, CA (10)	
0.5.C 25 (77) Appl. Soc. 00.175, 640	(2) Notice Solicit to say do press is except	againe - Eachd Contparticlicat, (UR) Sectored to mar from the	USC 15	19 Assigner INDELCORPORAD	(b) Publishes Language Duffe On Provide Poly.		
(22) Filed Jan. 95, (3) And CC ² (0) Princ Pag (5) And CC ² (5) Princ Pag (5) CC (7) (7) (7) (7) (7) (7) (7) (7) (7) (7)	20 Apr No. 14122206	parents to enhanced of U.S.C. 15430 Pp 40	(22) Filml. Pul. 38, 3	*) Notice Subject to say clicitles point is expended sets U.S.C. 154(5) By 4-Am	19 (20) 40 (20) 21 December 2000 (2) 12,2000 4 (70) Applicant: INTEL CORPORATION (2007)), 22	clause. (21) Appl. Soc. (19854)753	
Robust E.S. (20) Related Search	NJ PCTNO, PCTAN2203 (22) The	4 Oct. 23, 2012	US DELEMENTALE AT	2() Appl No. (14921.942 2() 7008 Oct. 23, 2015	(2) Invation: TRATCHER, Lory: 1100 DC Londo No.	(22) Filed. Sep. 3, 2003 (55) Pyles Publication Data	Printy East av - Alter 11
5 Devices of application 1976, not for \$4,52 1976, not for \$4,52 1976, and \$4,52 1977, and \$4,52 1977, and \$4,52 1977, and \$5,52 1977,	0) Date: New 26, 201 US 1 () POX Pob. Nev 1000014192	NERGERTIO AL APR. 1	0007 1237 0007 12370 0007 124003	(2) Prior Publication F LIX 2006/061106 A1 7th 11	Winhers Way, Austin, TX 2021 (US): PATEL, Repr 1013 SIX Ont Cost, Austin, TX 2024 (US):	US 2004-004433 A1 Mor A 2004 Reduced U.X. Application from	Lashnaw Dummur - Compt Dawn (24) January Agrad or Pres - History, Solution, Taylor 8 Zalassi LLP
Tield of Source	PCT Publicate CPA	7 75997 (2006.00 7 759977 (2006.00 7 759977 (2006.00)	(71) COCC OBOP 120 DED.1 (70) Field of Chevellowing	Mandod U.S. Application 3 (5) Communication of application No. 1 (6) 30, 2012	(74) Appense COROTTLO, Konardh, R. et al., Konyon, Xamyon, Suitu (10), 533 Bitur San Carlon Sorvet. Jan Ju Cit. 95(10) (10).	(13) Continuation of applement No. 97198-316, 2004 361, 172, 2002, One PAI: No. 6451,1131, which is continuation of applements No. 00477,1133, Bool of continuation of applements No. 00477,1133, Bool of continuation of applements No. 00477,1133, Bool of Continuation of the No. 00477,	(37) AINTEACT A system and nation for heaving sensity occurs hierary had only in the set of monory senses and to forced. The
Barkon SATULU A SATUR CARANA (CARANA) DATU DA A SATUR A SATURANA (CARANA) U.S. PAYLIN A SATUR CARANA (CARANA)	US 30140933229 A1 (No. (32) U.S. CPC) 3 Mar. CL S2007 A3mar (2004 CPC) Field	Ch. Gaur 124893 (2023	GPC	Sto line Ch. State Alman (2016-001) Anne Almani (2016-001)		(11) Back Cl. Grant your (2006-02)	synthesis resortions a Denschap and provides Albert regulations sensitively another providence into colder accession with theorem accesses. A bacillar worksing the indexestry sensitivity sensitivity is allocated by the bacillar worksing the indexest instructivity memory them the indexed providence. The indexest instructivity memory them the indexed providence of the indexest instructivity memory the indexest instructivity memory the indexest instructivity of the indexest instructivity memory the indexest instructivity in the indexest instructivity memory the indexest instructivity in the indexest instructivity memory the indexest instructivity memory the indexest instructivity in the indexest instructivity indexest instructivity indexest instructivity indexest instructivity indexest instructivity instructity instructivity instructity instructivity instructivity in
	CPC GBGF (2)004/ (241) 15F CPC GBGF (2)004/ (241) 15F C0411811 C0007 (200	e applement the for complete	(M) Bebree U.S. INTERT	(II) LUC CL CTC		(22) U.S. CL. (3000.00) (32) U.S. CL. (3000.00) (32) U.S. CL. (3000.00) (30) U.S. CL. (3000.00)	instruction are stilled. The older servers instruction over a gardedy served. When all older inservers and over servers, the factory inserverse in deputition true the buffles.
794 196		Radianasian Chad U.S. PATENY DOCUM	ASSISSE A BETTER	(Contenant)		The application file for complete much biology	37 Claims, 9 Depending Scherts
accordin and TSRS						Village A Discovery	
			and the second second		-		
			and the second second second		CALINE STREET AND STREET AND		
100			A CONTRACTOR OF THE OWNER	and the second	10% Adaptation The property investions relation to the test of a		and in the second secon
			Sector States		der skalt effects af der enstelletigt ihr inter at soner store gemeinten in der skalt effects af der enstelletigt ansatzerigt soner i micht ihr sonerskeure wirte an arbeitelissen der present interest omstructum meteory ansatz includes executing meteorie store if	Las diversion	
			Section 2 and the section	and the second second	P instruction disposity control the memory regist addressed in		
the second se			the same the same is a subscription of the	the state of the s	the second s	and the second	and the second

Performance
+ counters and
leakage

Hardware Reverse Engineering at VUSec



Theory: Leaking through LFB



RIDLing

1 FLUSH

for (i = 0; i < 256; ++i) {
 _mm_clflush(probe + i * 4096);</pre>

2 RIDL

```
if (_xbegin() == _XBEGIN_STARTED) {
   char byte = *(volatile char *)NULL;
   char *p = probe + byte * 4096;
   *(volatile char *)p;
   _xend();
}
```

3 RELOAD

```
for (i = 0; i < 256; ++i) {
    t0 = __rdtsc();
    *(volatile char *)(probe + i * 4096);
    dt = __rdtsc() - t0;
}</pre>
```

Not Through CPU Caches



LFB Leaks



Sometimes We Get It Wrong..

- RIDL paper: leakage is primarily through LFBs
- Public disclosure: May 14
- Intel on May 10:
 - There are 4 variants, you only leak through LFB
 - 0 !&#&* (heated exchange)
 - You are leaking through LFB, UC, LP



More information on: mdsattacks.com

Which CPUs Are Vulnerable?

Intel Core i9-9900K (Coffee Lake R) - 2018 Intel Xeon Silver 4110 (Skylake SP) - 2017 Intel Core i7-8700K (Coffee Lake) - 2017 Intel Core i7-7800X (Skylake X) - 2017 Intel Core i7-7700K (Kaby Lake) - 2017 Intel Core i7-6700K (Skylake) - 2015 ✓ Intel Core i7-5775C (Broadwel) - 2015 Intel Core i7-4790 (Haswell) - 2014 Intel Core i7-3770K (Ivy Bridge) - 2012 Intel Core i7-2600 (Sandy Bridge) - 2011 Intel Core i3-550 (Westmere) - 2010 Intel Core i7-920 (Nehalem) - 2008 X AMD Ryzen 5 2500U (Raven Ridge) - 2018 X AMD Ryzen 7 2600X (Pinnacle Ridge) - 2018 X AMD Ryzen 7 1600X (Summit Ridge) - 2017

1 Year of CVD with Intel

\$100,000 bounty award

Demo

[sebastian@sarek ridl]\$ cat /etc/shadow cat: /etc/shadow: Permission denied [sebastian@sarek ridl]\$ sudo cat /etc/shadow | head -n 1 root:\$6\$sP/i.m6uVkNRJgpV\$vyndShgzWmeWI8Bx8RbGCkj2SVvQ.bjqwRafe6rdnotl8ndQkvH/wf1 u.cF31o9IeOW/Ub/6CVEdbCJioHplW/:17828:0:99999:7::: [sebastian@sarek ridl]\$./hackpasswd root: root:\$6\$sP/i.m6uVkNRJgpV\$vyndShgzWmeWI8Bx8RbGCkj

Traditional Cache Attacks







Proposed Defenses: Cache Partitioning



Issue: Imperfect Partitioning

Can we make meaningful attacks against the TLB?

- Architecture of the TLB is unknown
- Spatial attacks are difficult (4KB page size)



Gras et al., "Translation Leakaside Buffer: Defeating Cache Side-channel Protections with TLB Attacks," SEC'18

Hardware Reverse Engineering at VUSec



Reverse Engineering the TLB Architecture Goal: find virtual addresses that prime a TLB set Methodology: Oren et al. eviction set building algorithm

- Pick a pool virtual addresses
- Pick an observer address
- Reduce the pool to a minimal set that evicts observer

			I	_1 dTI	B				L1 iTL	В				L2 sTL	B	
Name	year	set	W	pn	hsh	shr	set	W	pn	hsh	shr	set	W	pn	hsh	shr
Sandybridge	2011	16	4	7.0	lin	1	16	4	50.0	lin	×	128	4	16.3	lin	1
Ivybridge	2012	16	4	7.1	lin	1	16	4	49.4	lin	×	128	4	18.0	lin	1
Haswell	2013	16	4	8.0	lin	1	8	8	27.4	lin	×	128	8	17.1	lin	1
HaswellXeon	2014	16	4	7.9	lin	1	8	8	28.5	lin	×	128	8	16.8	lin	1
Skylake	2015	16	4	9.0	lin	1	8	8	2.0	lin	×	128	12	212.0	XOR-7	1
BroadwellXeon	2016	16	4	8.0	lin	1	8	8	18.2	lin	×	256	6	272.4	XOR-8	1
Coffeelake	2017	16	4	9.1	lin	1	8	8	26.3	lin	×	128	12	230.3	XOR-7	1

Temporal Attacks with PRIME+PROBE

Timing of misses in a TLB set rather than different sets.

- Help from a SVM classifier

Table 3:	TLBleed	compromising	Intel	CAT.
----------	---------	--------------	-------	------

Microarchitecture	Trials	Success	Median BF
Broadwell (CAT)	500	0.960	$2^{2.6}$
Broadwell	500	0.982	2 ^{3.0}



Elliptic curve point multiplication in libgcrypt.
Example SVM Output



Impact

Security

Meet TLBleed: A crypto-key-leaking CPU attack that Intel reckons we shouldn't worry about

How to extract 256-bit keys with 99.8% success

By Chris Williams, Editor in Chief 22 Jun 2018 at 22:44 60 🖵

60 🖵 SHARE 🔻



Our upcoming **#TLBleed** paper leads to (finally) disabling SMT in security-sensitive environments (**#OpenBSD** in this case).



XLATE Attacks (SEC'18) similarly bypasses imperfect partitioning

Van Schaik et al., "Malicious Management Unit: Why Stopping Cache Attacks in Software is Harder than You Think," SEC'1874

Conclusion

Hardware is the new software except it is harder to fix

Reverse engineering is our main tool in academia

We need to invest in open hardware

Ben Gras, Pietro Frigo, Lucian Cojocar, Stephan van Schaik, Alyssa Milburn, Sebastian Osterlund, Cristiano Giuffrida, Herbert Bos