15 oktober 2024

Side-channels that break security in practise

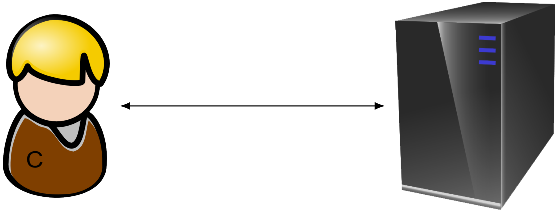
Rasmus Dahlberg

Learning outcomes

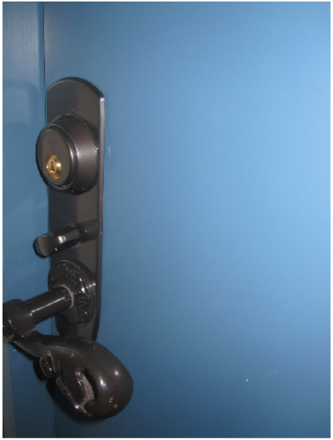
- Understand the threat of side-channels
- Get an intuition of timing attacks

No in-depth programming and cryptographic details

Setting and security



Security on paper

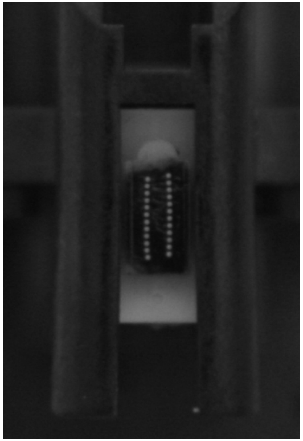


Reality — not a black box

Side channels — Pandora's box

- Power consumption
- EM radiation
- Heat
- Sound
- Cache
- Faults
- Timing
- Size
- ...

Printer sounds — document content leaked

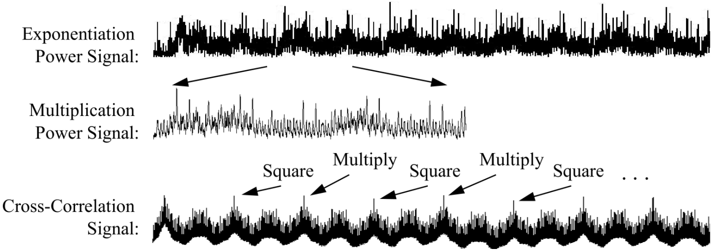


Backes *et al.*: Acoustic Side-Channel Attacks on Printers, In: USENIX Security (2010)

Laptop sounds — secret key leaked

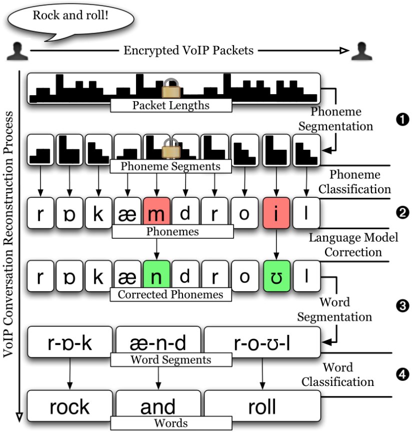
Genkin *et al.*: RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis, In: Crypto (2014)

Energy consumption — secret key leaked



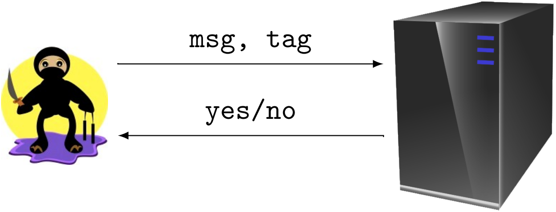
Messerges *et al.*: Power Analysis Attacks of Modular Exponentiation in Smartcards, In: CHES (1999)

Packet size — encrypted content leaked



White *et al.*: Phonotactic Reconstruction of Encrypted VoIP Conversations: Hookt on Fon-iks, In: IEEE SP (2011)

Response timing — message forgery

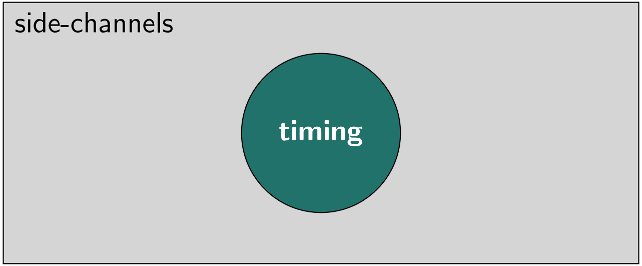


msg, tag

yes/no

Crosby *et al.*: Opportunities and Limits of Remote Timing Attacks, In: TISSEC (2009)
Hale: A lesson in timing attacks, URL: https://codahale.com/a-lesson-in-timing-attacks/ (2009)

Scope



Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

144555105949057024

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	**f**	**T**	**B**	**s**	**v**	**g**	**O**	**e**	**t**
52	52	52	52	52	52	52	52	52	52

144555105949057024

52^{10} combinations and 100M queries/s → 46 years

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	**f**	**T**	**B**	**s**	**v**	**g**	**O**	**e**	**t**
52	52	52	52	52	52	52	52	52	52

144555105949057024

52^{10} combinations and 100M queries/s → 46 years

Experiment — are these strings equal?

Experiment — are these strings equal?

0000000000000000 9389349108837912

Experiment — are these strings equal?

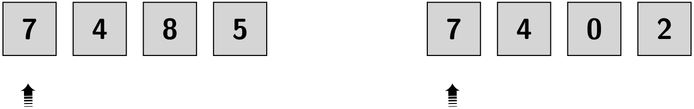
0000000000000000
0000439513027213

9389349108837912
0000431513027213

Experiment — are these strings equal?

0000000000000000	9389349108837912
0000439513027213	0000431513027213
7485820126271479	7485820126371479

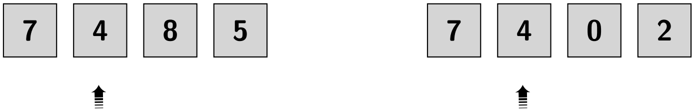
Comparing strings like a programmer



7 4 8 5

7 4 0 2

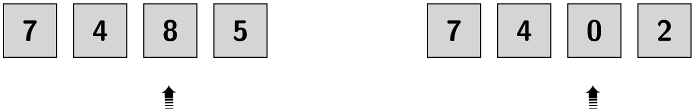
Comparing strings like a programmer



7 4 8 5

7 4 0 2

Comparing strings like a programmer



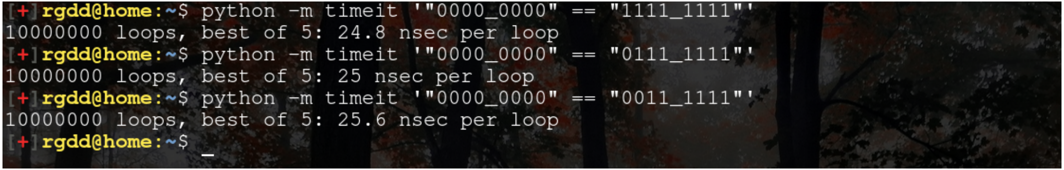
7 4 8 5

7 4 0 2

Comparing strings like a programmer

no need to continue

Timing — an inutitive note



```
[+]rgdd@home:~$ python -m timeit '"0000_0000" == "1111_1111"'
10000000 loops, best of 5: 24.8 nsec per loop
[+]rgdd@home:~$ python -m timeit '"0000_0000" == "0111_1111"'
10000000 loops, best of 5: 25 nsec per loop
[+]rgdd@home:~$ python -m timeit '"0000_0000" == "0011_1111"'
10000000 loops, best of 5: 25.6 nsec per loop
[+]rgdd@home:~$ _
```

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	**f**	**T**	**B**	**s**	**v**	**g**	**O**	**e**	**t**
52	52	52	52	52	52	52	52	52	52
a	**a**	**a**	**a**	**a**	**a**	**a**	**a**	**a**	**a**

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52
z	a	a	a	a	a	a	a	a	a

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

z	f	a	a	a	a	a	a	a	a

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

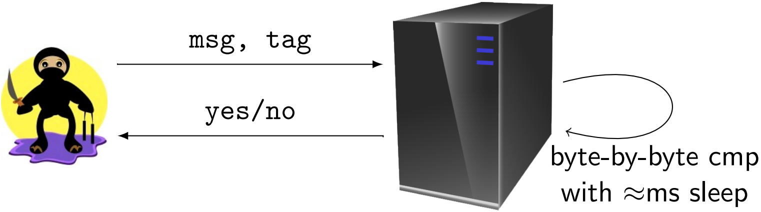
z	f	T	a	a	a	a	a	a	a

Effort to crack this password?

1	2	3	4	5	6	7	8	9	10
z	f	T	B	s	v	g	O	e	t
52	52	52	52	52	52	52	52	52	52

z	f	T	B	s	v	g	O	e	t

Demo — Experimental setup



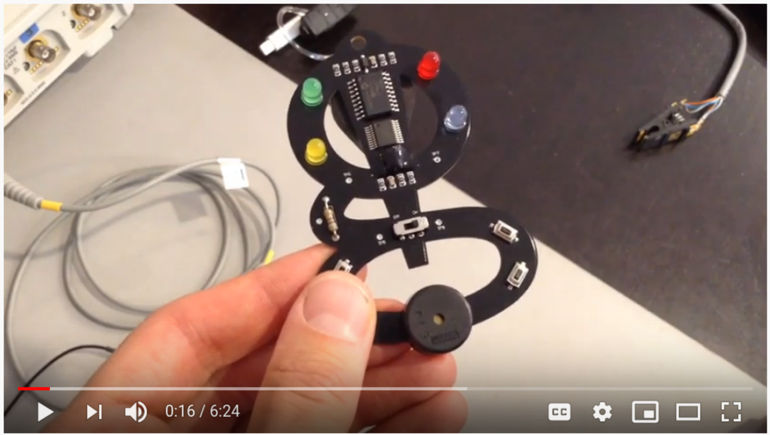
`msg, tag`

`yes/no`

byte-by-byte cmp
with ≈ms sleep

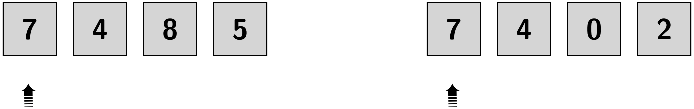
`https://github.com/rgdd/timing-server`

Can you recommend another demo? Asking for a friend



https://www.youtube.com/watch?v=2-zQp26nbY8

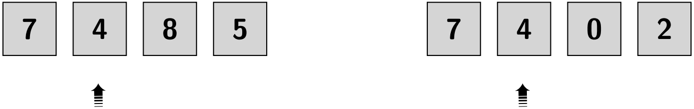
Countermeasure – constant time compare



7 4 8 5

7 4 0 2

Countermeasure – constant time compare



7 4 8 5

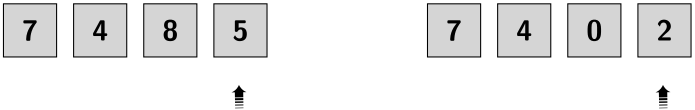
7 4 0 2

Countermeasure – constant time compare

7 4 8 5

7 4 0 2

Countermeasure – constant time compare



7 4 8 5

7 4 0 2

Lessons learned

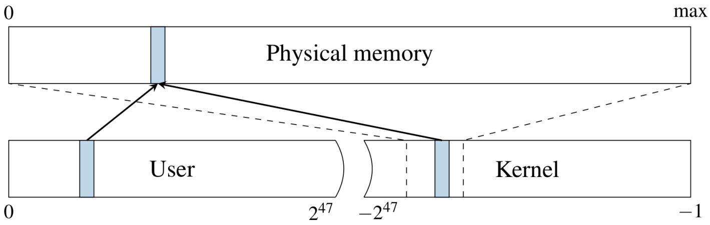
Adversarial input? Think twice before using standard equality operators

Cryptography in code? Stick to cryptographic libraries, hope for the best

Meltdown

Lipp *et al.*: Meltdown, In: CoRR abs/1801.01207 (2018)

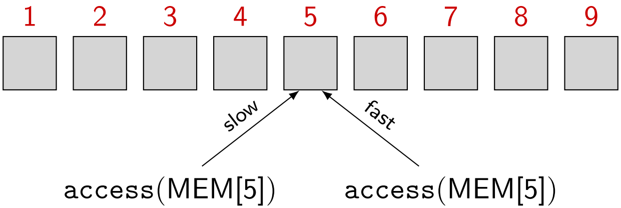
Preliminaries — per-process virtual memory layout



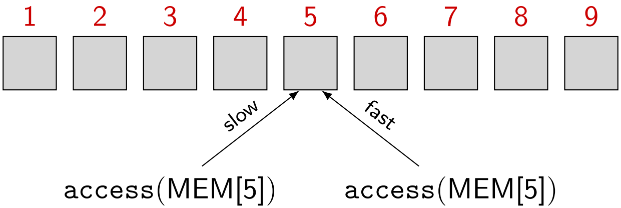
page table

address translation privelege checks

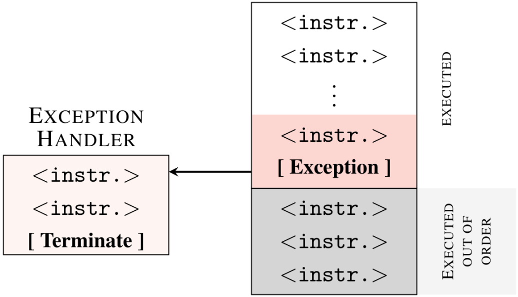
Preliminaries — caching and out-of-order execution



Preliminaries — caching and out-of-order execution



```
read(MEM[5]);
read(MEM[5]);
...
raise_exception();
data = read(MEM[7]);
read(MEM[data])
...
```

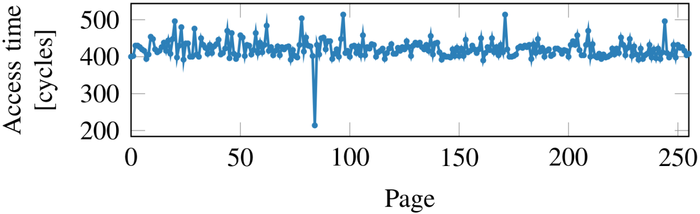


Ooops — leaked privileged memory?

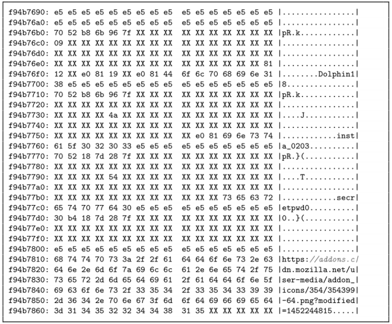
```
data = read(MEM[addr])
raise_exception();
read(probe_array[data * 4096])
```

Ooops — leaked privileged memory?

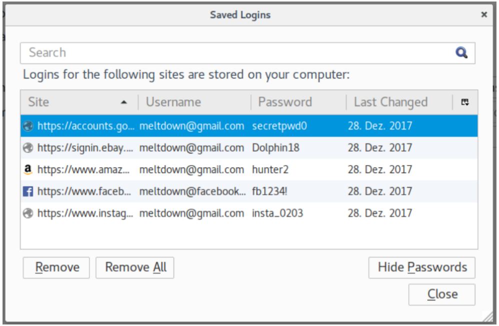
```
data = read(MEM[addr])
raise_exception();
read(probe_array[data * 4096])
```



Proof of concept



```
f94b7690: e5 e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |................|
f94b76a0: e5 e5 e5 e5 e5 e5 e5 e5 e5  e5 e5 e5 e5 e5 e5 e5 |................|
f94b76b0: 70 52 b8 6b 96 7f XX XX XX  XX XX XX XX XX XX XX |pR.k............|
f94b76c0: 09 XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
f94b76d0: XX XX XX XX XX XX XX XX XX  XX XX XX XX XX XX XX |................|
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.....|
```



Saved Logins

Logins for the following sites are stored on your computer:

Site	Username	Password	Last Changed
https://accounts.go...	meltdown@gmail.com	secretpwd0	28. Dez. 2017
https://signin.ebay....	meltdown@gmail.com	Dolphin18	28. Dez. 2017
https://www.amaz...	meltdown@gmail.com	hunter2	28. Dez. 2017
https://www.faceb...	meltdown@facebook...	fb1234!	28. Dez. 2017
https://www.instag...	meltdown@gmail.com	insta_0203	28. Dez. 2017

That’s it — questions?