

Lecture-1 (Logistics and Introduction)

CS665-Fall 2018

Secure Memory Systems

Biswa@cse-IITK



Instructor

Biswa (~~Biswabandan, Sir, Prof., Dr., Er., *-Biswa~~)

Sir/Prof./..... outlawed with CS665 and Biswa

Website: <http://www.cse.iitk.ac.in/biswap>

Contact: KD 203, biswap@cse.iitk.ac.in

Office Hours: Friday, 12 noon, email: [CS665-yourname]

Teaching and Research Interests:

Computer Architecture, Arch-OS interface, and Architecture Security

Course Staff

Biswa



Saurabh



Logistics

When: Mon/Thurs. 09.00-10.15 Hrs,
Where: KD 103, What: You know it

Course website: www.cse.iitk.ac.in/~biswap/CS665.html

Piazza: For online discussions

Submission of assignments: Canvas

<https://www.cse.iitk.ac.in/pages/AntiCheatingPolicy.html>

Register/Drop ASAP (if interested/not interested)

Assessment Policies –I (Red ones: You will evaluate)

60 = 20 (Programming Assignments) * 3

Bonus: 10 points for early (24 hrs before) submission

30 = 10 (Research paper reviews) * 3

Bonus: 5 points for the best paper review

10 = 10 (Paper presentation) * 1 (Bonus: 5 points for the best presentation)

-1 : coming late to the lectures OR
asking for deadline extensions for any assignments

-1 : referring Biswa as Prof., Sir, Dr., *Biswa*

+1 : Piazza/In-class participation (Biswa/Saurabh will decide)

Assessment Policies – II (Red ones: You will evaluate)

70 = 70 (Semester-long project) * 1
Bonus: 10 points for “aha” moments

20 = 10 (Research paper reviews) * 2
Bonus: 5 points for the best paper review

10 = 10 (Paper presentation) * 1 (Bonus: 5 points for the best presentation)

-1 : coming late to the lectures OR
asking for deadline extensions for any assignments

-1 : referring Biswa as Prof., Sir, Dr., *Biswa*

+1 : Piazza/In-class participation (Biswa/Saurabh will decide)

0 Marks : End-term (in November)
(but compulsory)

But Why ??



10+2+JEE : 100 books for \$n years

Then: No comments

B.Tech.: 10 books for every 4 months

Mug it up, then

So no book for CS665

But Why ??



Please, do not credit this course if you are good at

1. Mugging up
2. Writing exams
3. Taking notes: Day in Day out
4. Sitting silently in the class

What I expect from you?

No open-screens (no nomophobics): No open smart-phones (phones) & laptops/tablets. Keep your phones in silent mode

Open-screens will **affect (distract)** you, your friends, and me

Ask questions & participate in in-class discussions (worth bonus points)

Paper reading and writing reviews/reports

Understand, implement, and analyze ideas (Hard work and honesty)

Slides **will not contain** everything. So **attend** lectures.

What I expect?

Timing

Classes start at 9 AM, not 9.10/15 AM

Cheating

In any form will lead to **zero** points. Grade will be capped down (**one level**). To prevent capping down, you have to propose new attacks/mitigations.

Dropping CS665

Not allowed after **August 15th 2018**. Drop the course before that. Why? It will affect your group. Yes (programming assignments are group based)

What I expect?

Ditch your excuses.

Participate in class/Piazza regularly.
Do not fear about your doubts. Just communicate.
We (you, T.A., and me) will try our best to address
(not answer) it.

Just shout if you do not like something about me or about the course. However, be on the right side and then shout.

Prerequisite

Instruction pipelining

LOAD/STORE, PC

Cache, L1/L2, TLBs, page tables

Tag/Index/Offset

Direct/Associative mapping

SRAM/DRAM

Latency/Throughput

Virtual/Physical address

Process/Thread

Programming in C/C++

Score yourself

10 – Good

5 – Knowledgeable

0 – No Knowledge

Your score

> 50

– Welcome

> 30 & \leq 50

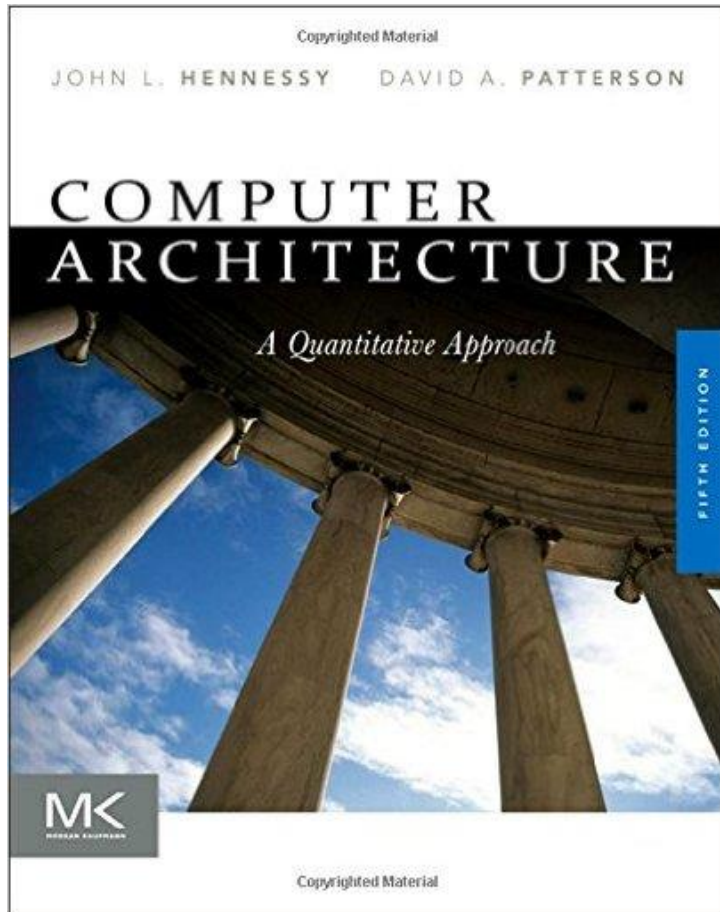
– Let's Talk

< 30

– Next Time

However, if you are motivated to learn:
I will be there to help you

Prerequisite: Standard Books and video lectures



Written by Turing Award Winners

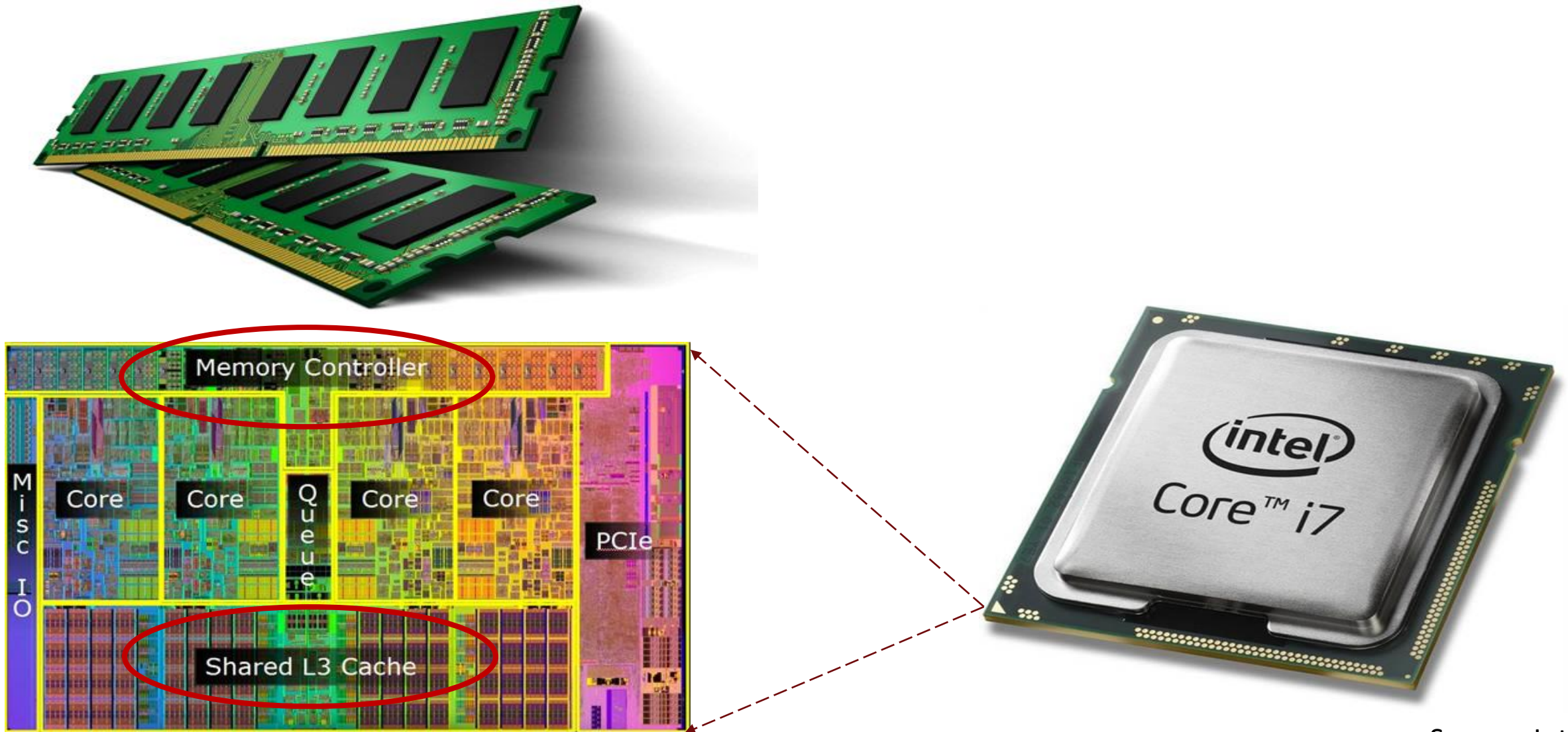
<https://www.cse.iitk.ac.in/users/biswap/CASS18/cass.html>

Please: Be Aware of It



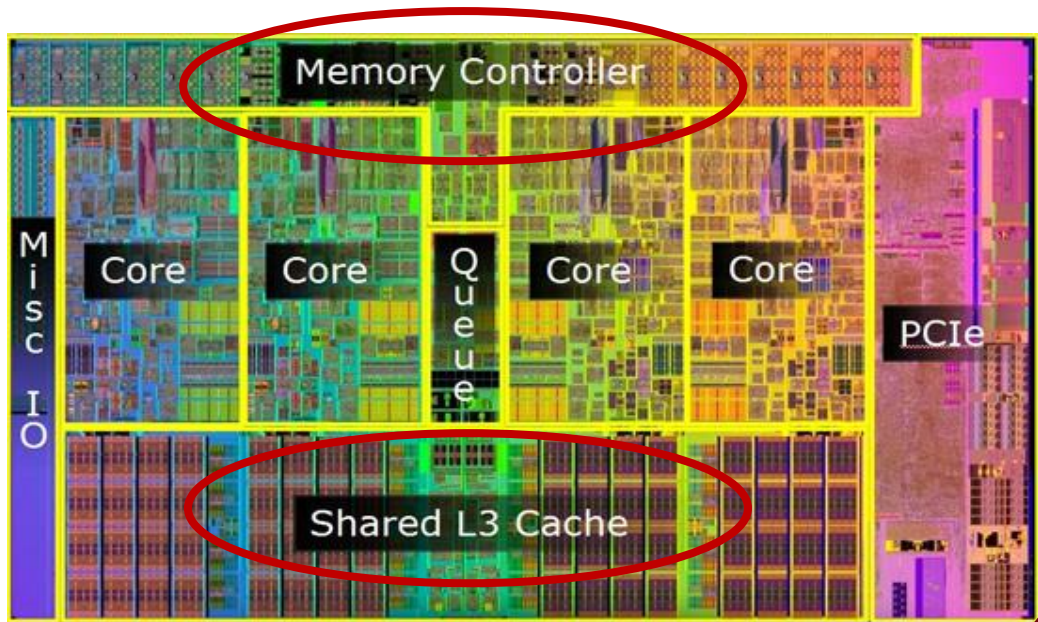
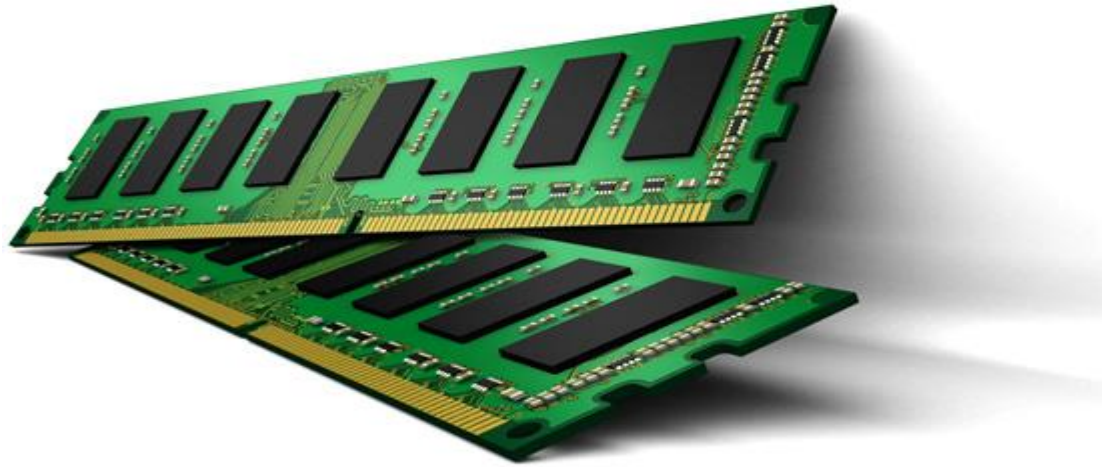
Welcome

Welcome: Secure Memory Systems



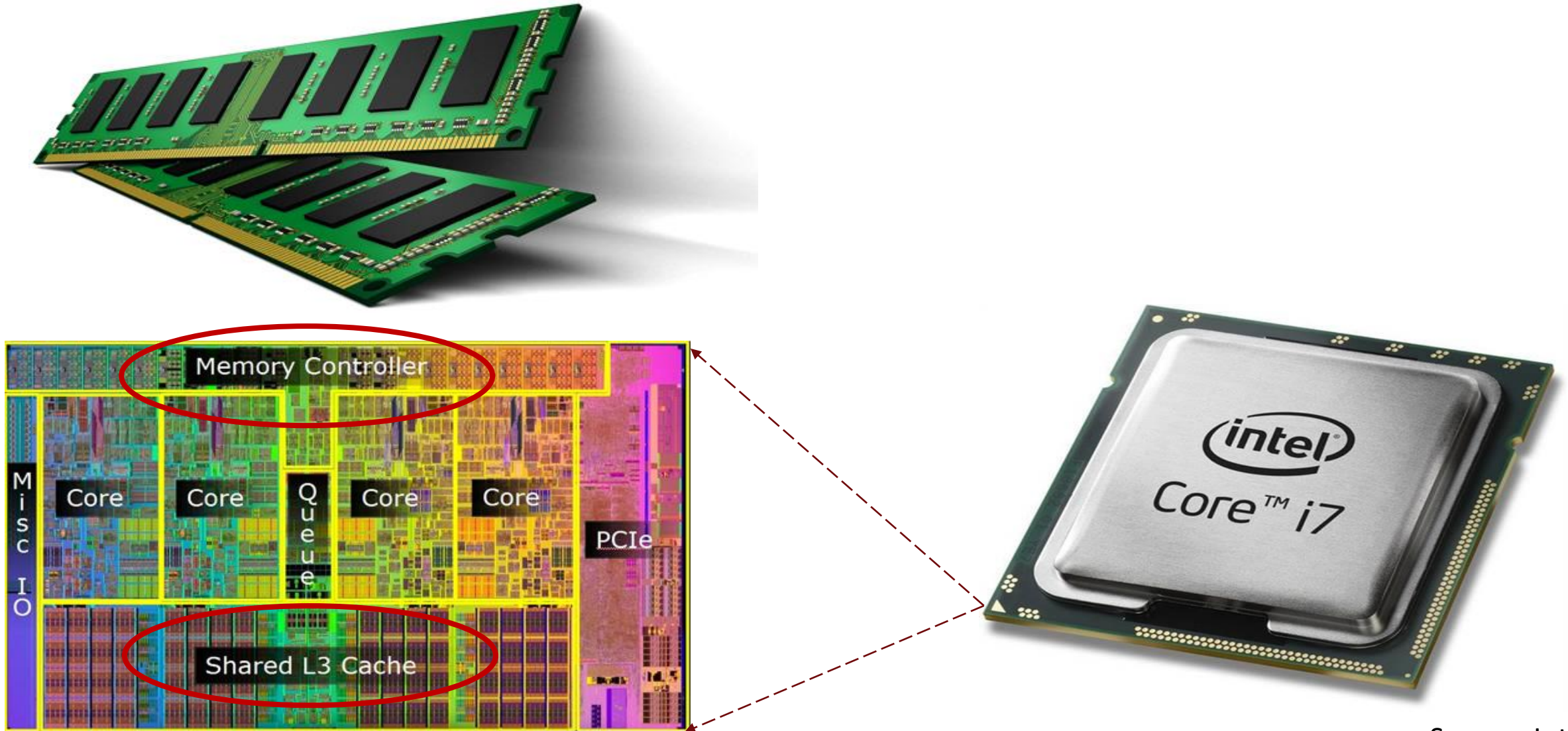
Source: Intel

Memory Systems?



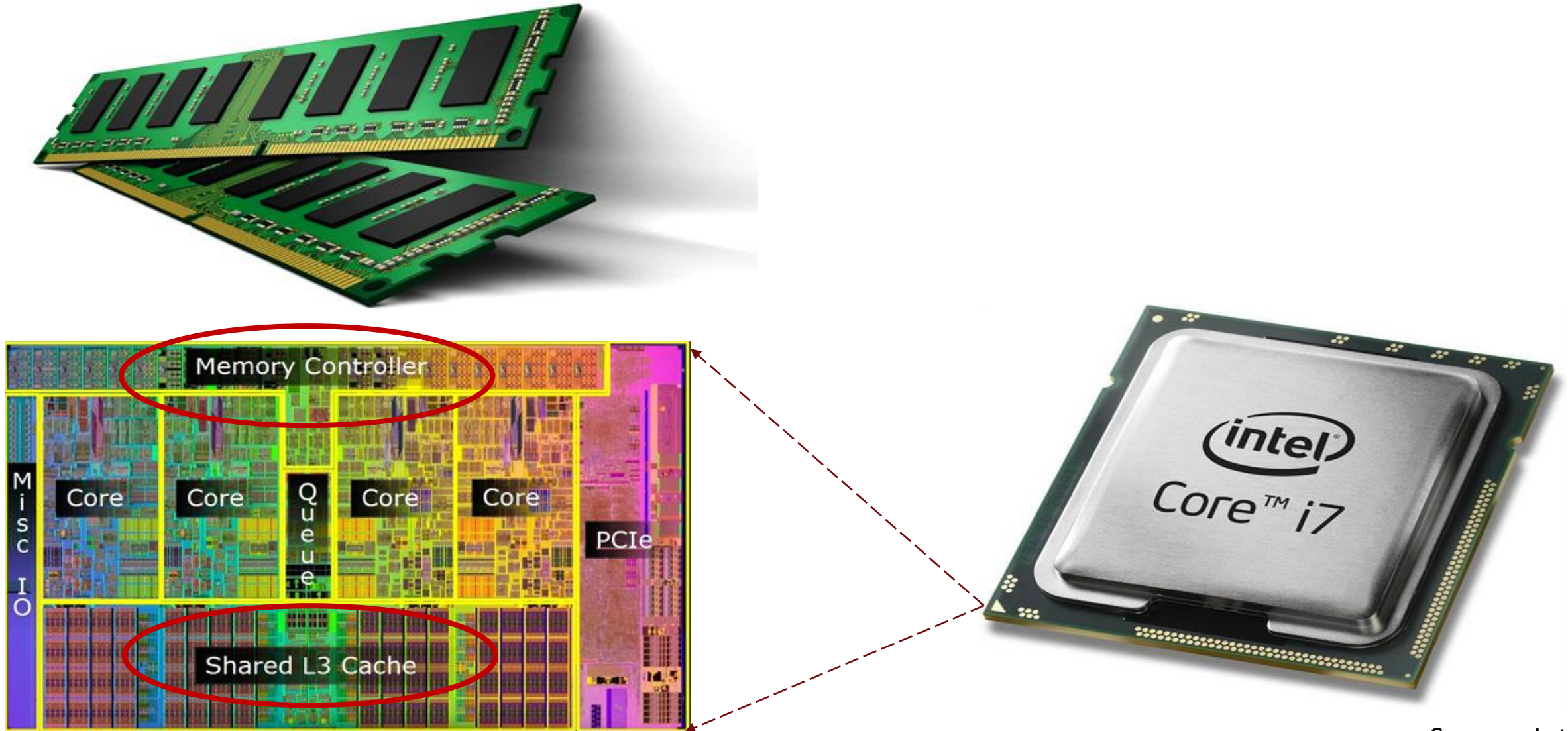
Source: Intel

Systems?



Source: Intel

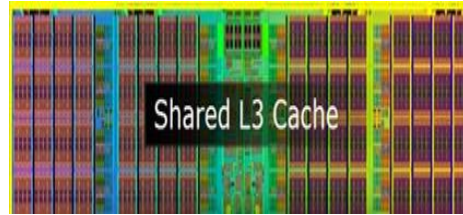
Why Secure?



Source: Intel

Let's See: But who is Spy/Victim?

Spy

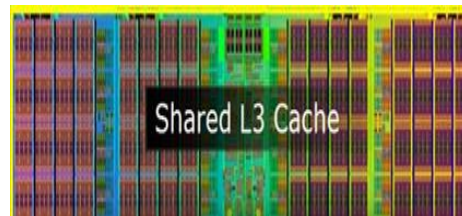


Side-channel attacks

Victim



Let's
play



Covert-channel attacks

Oh Yes!!



Who is The Spy?

Core 0



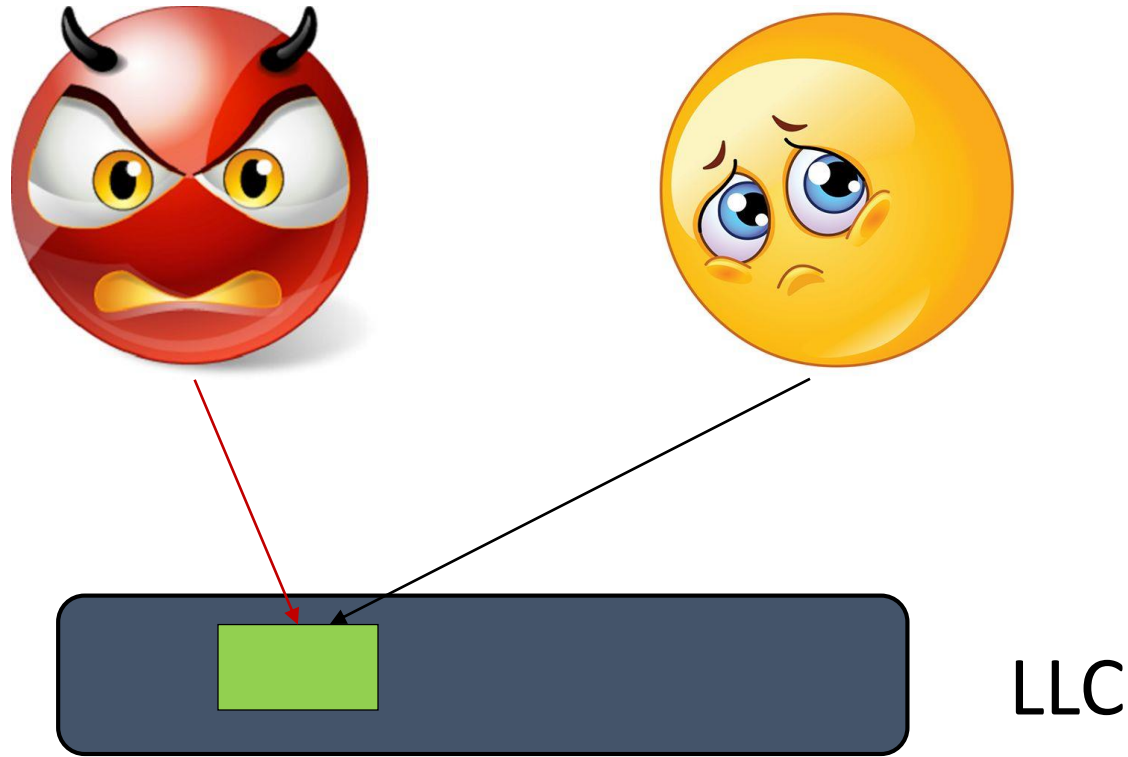
Core 1



L3



Simple Example: Flush + Reload



Step 0: *Spy maps the shared library, shared in the cache*



Flush + Reload



Cflush



LLC

Step 0: *Spy maps* the shared library, shared in the cache

Step 1: *Spy flushes* the cache block



Flush + Reload



LLC

Step 0: *Spy maps* the shared library, shared in the cache

Step 1: *Spy flushes* the cache block

Step 2: *Victim reloads* the cache block



Flush + Reload



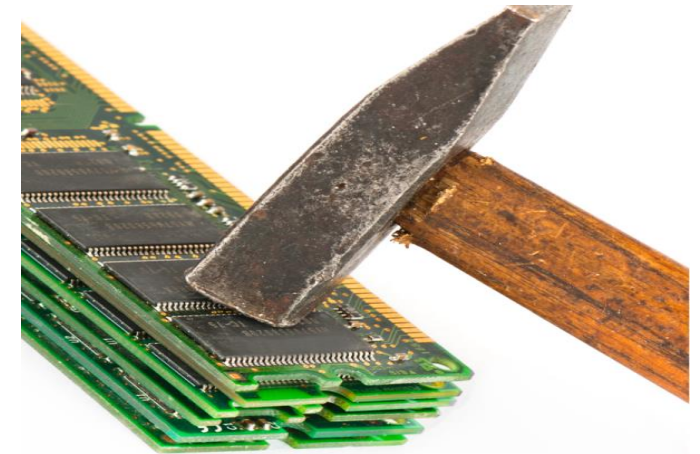
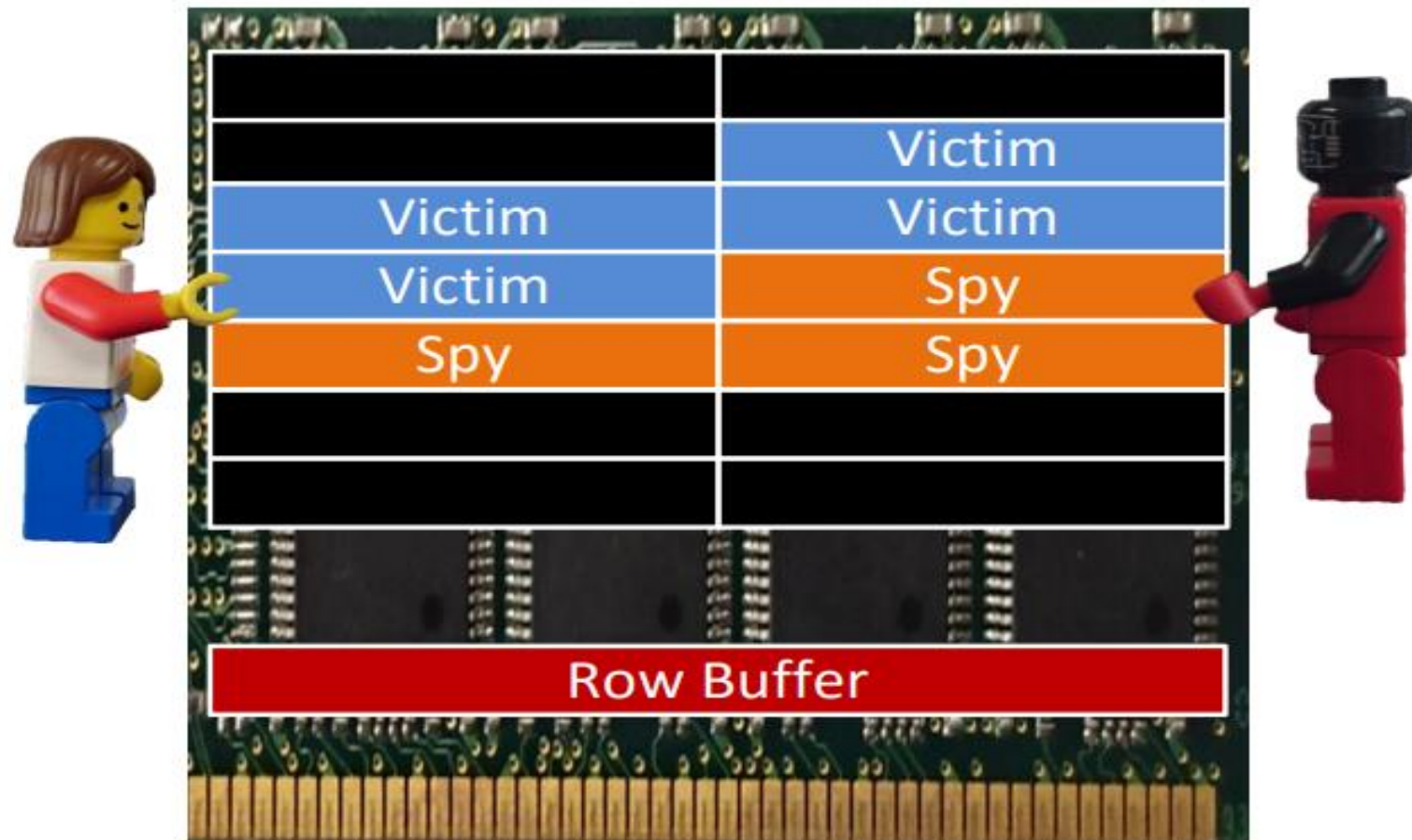
Step 0: *Spy maps* the shared library, shared in the cache

Step 1: Spy *flushes* the cache block

Step 2: Victim *reloads* the cache block

Step 3: *Spy reloads* the cache block (hit/miss)

One of you



Source: Hackaday

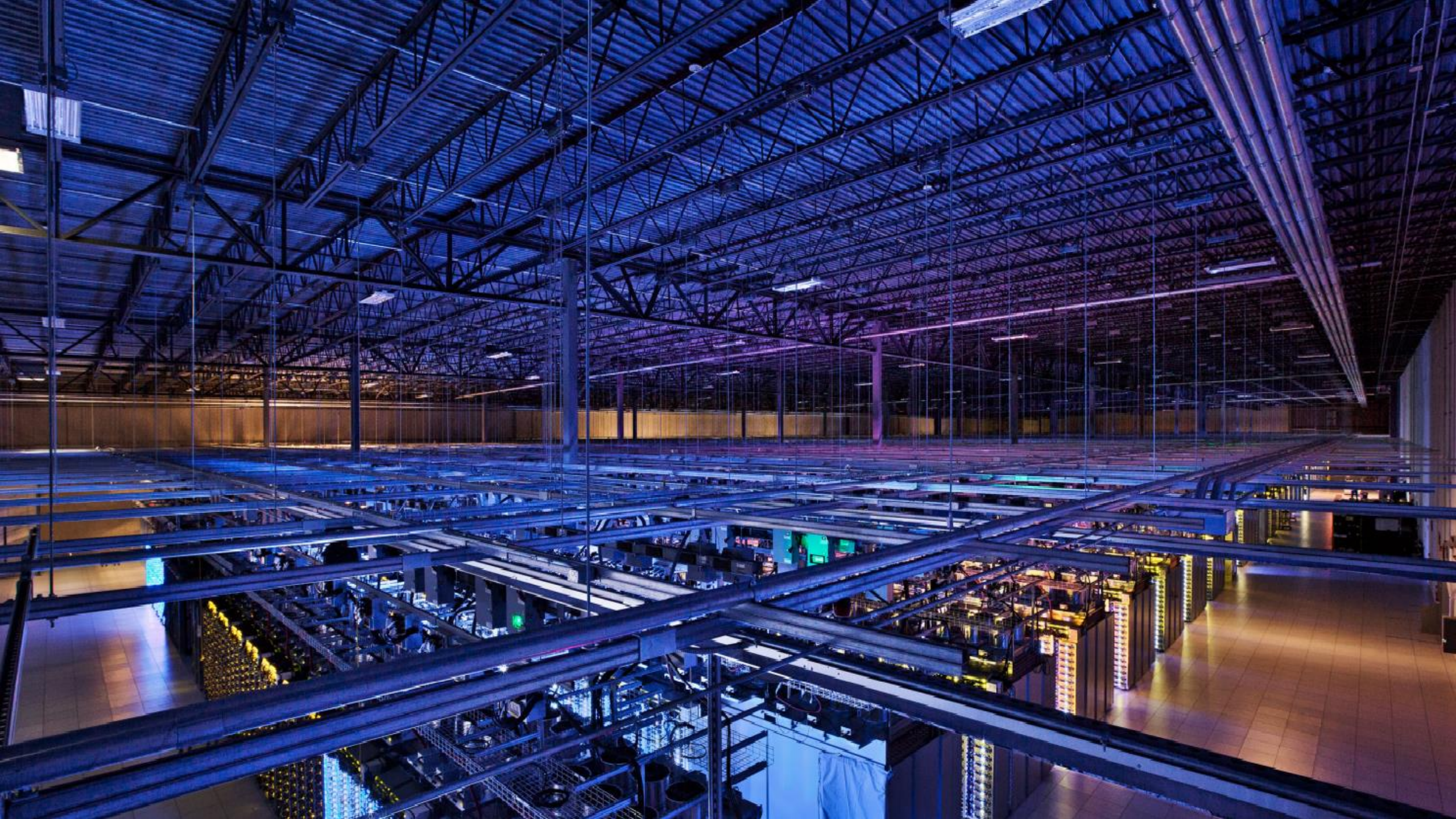
I Use Cloud: He he he



I use cloud

No fear of
information
leakage ??





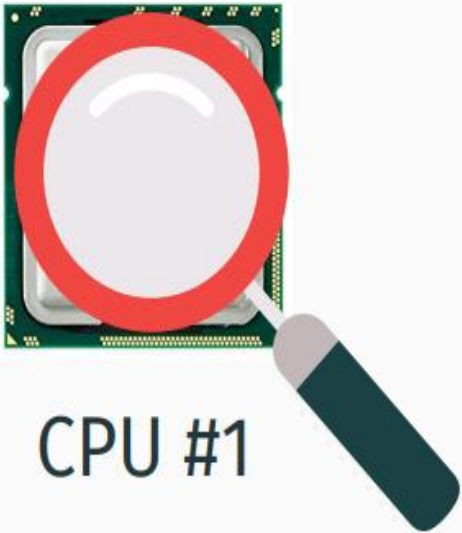


Hmmm



server

Dissect It



CPU #1

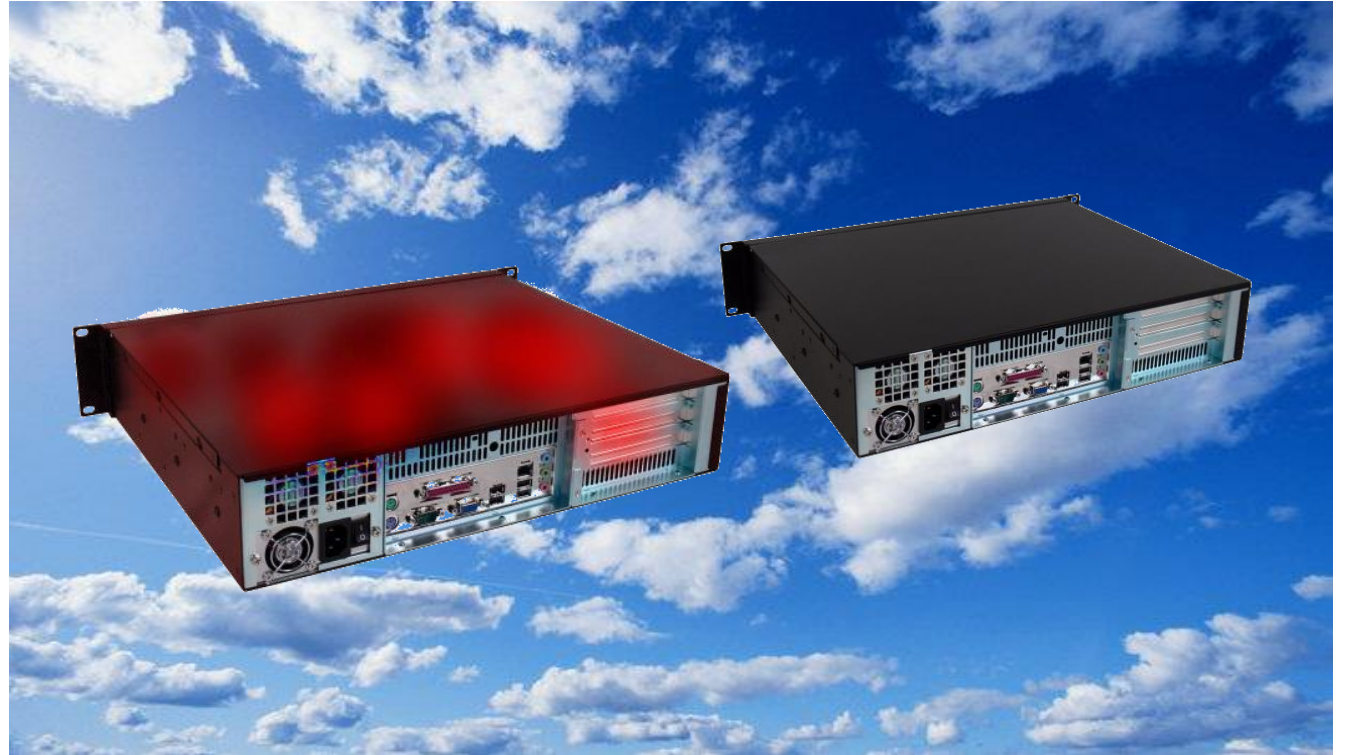


CPU #2



DRAM

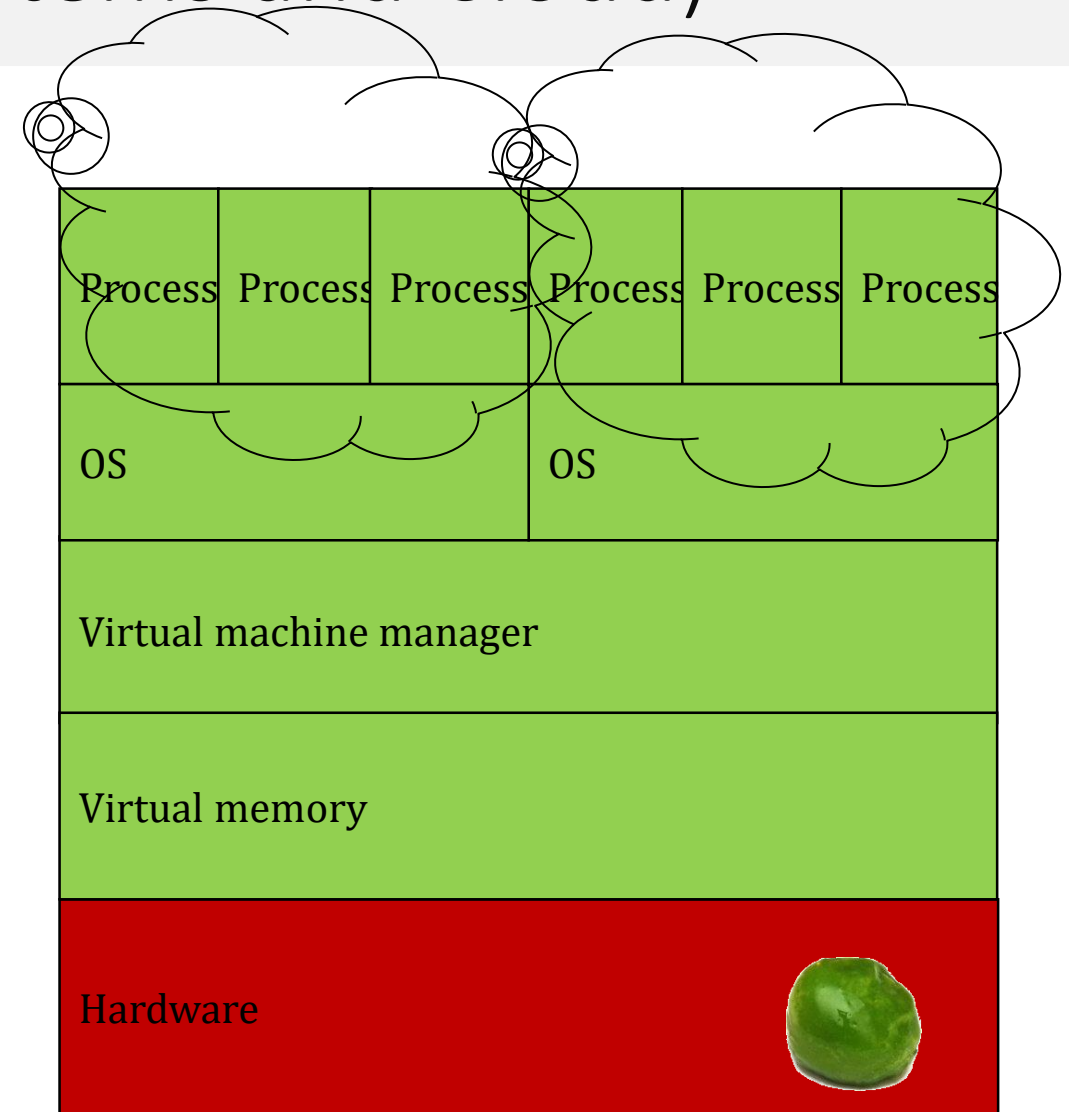
Same Problem Again!



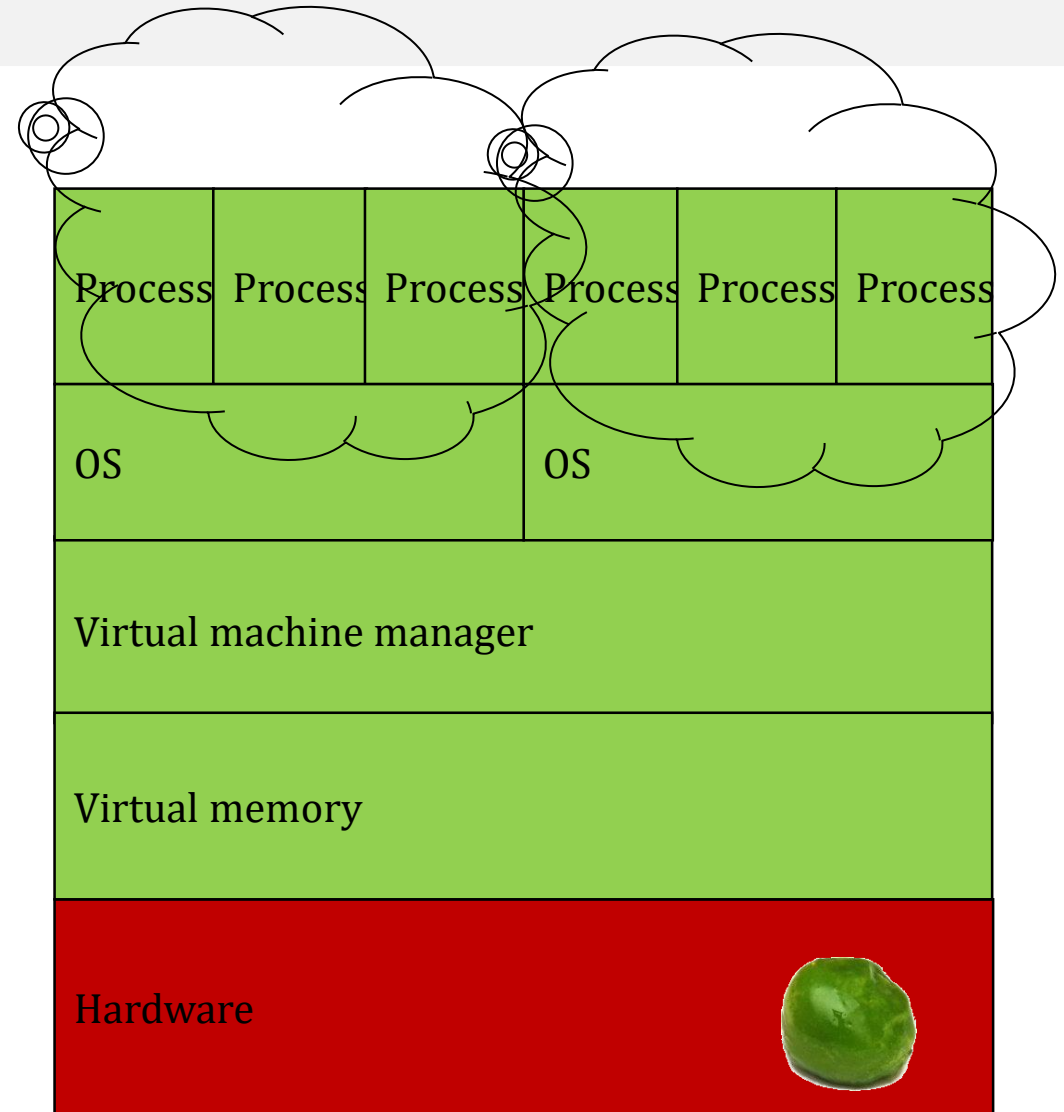
Gotcha!!

[Courtesy: Eran Tromer]

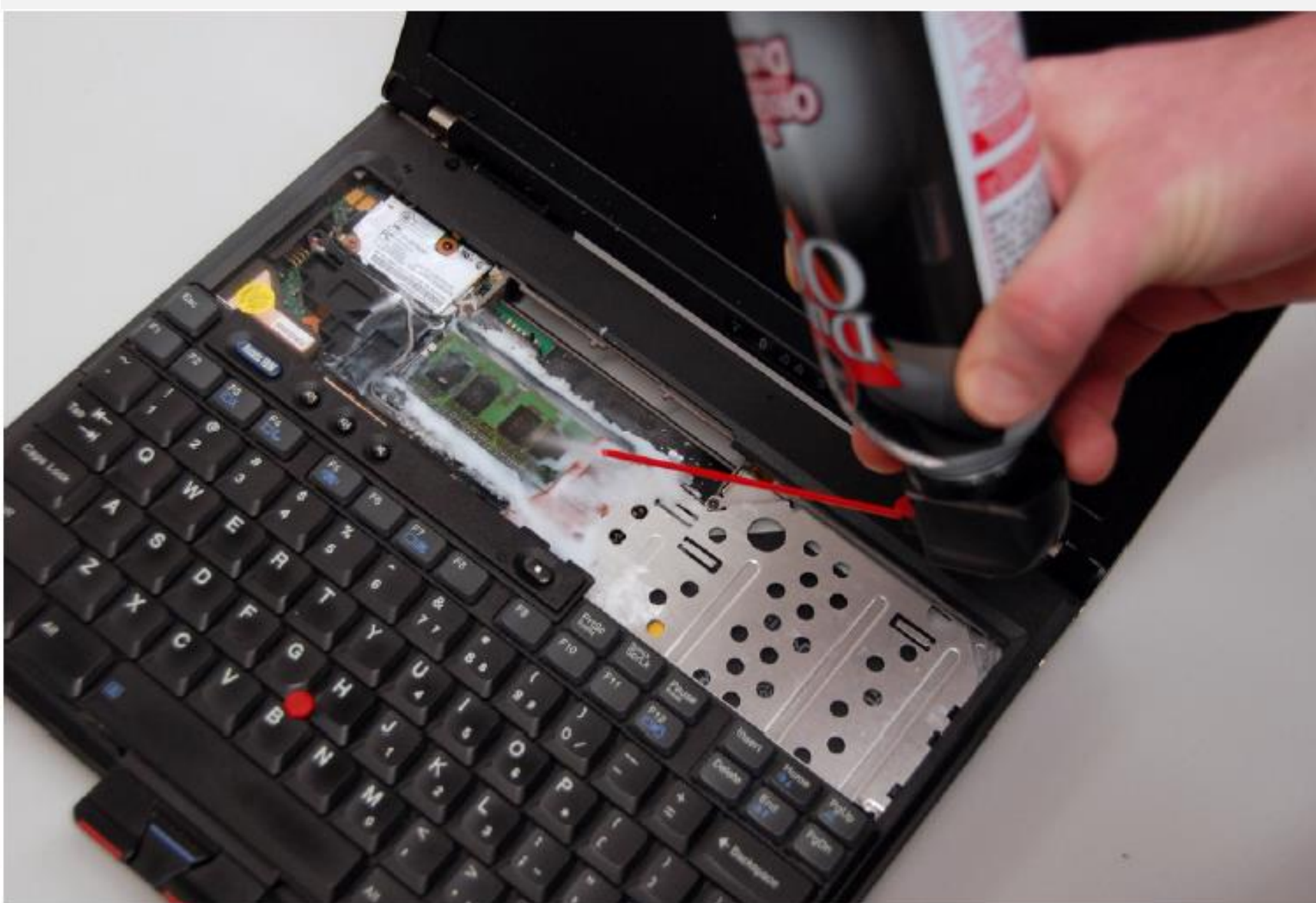
Peas and Princess (Memory Systems and Cloud)



Same Story Again! Oh NO !



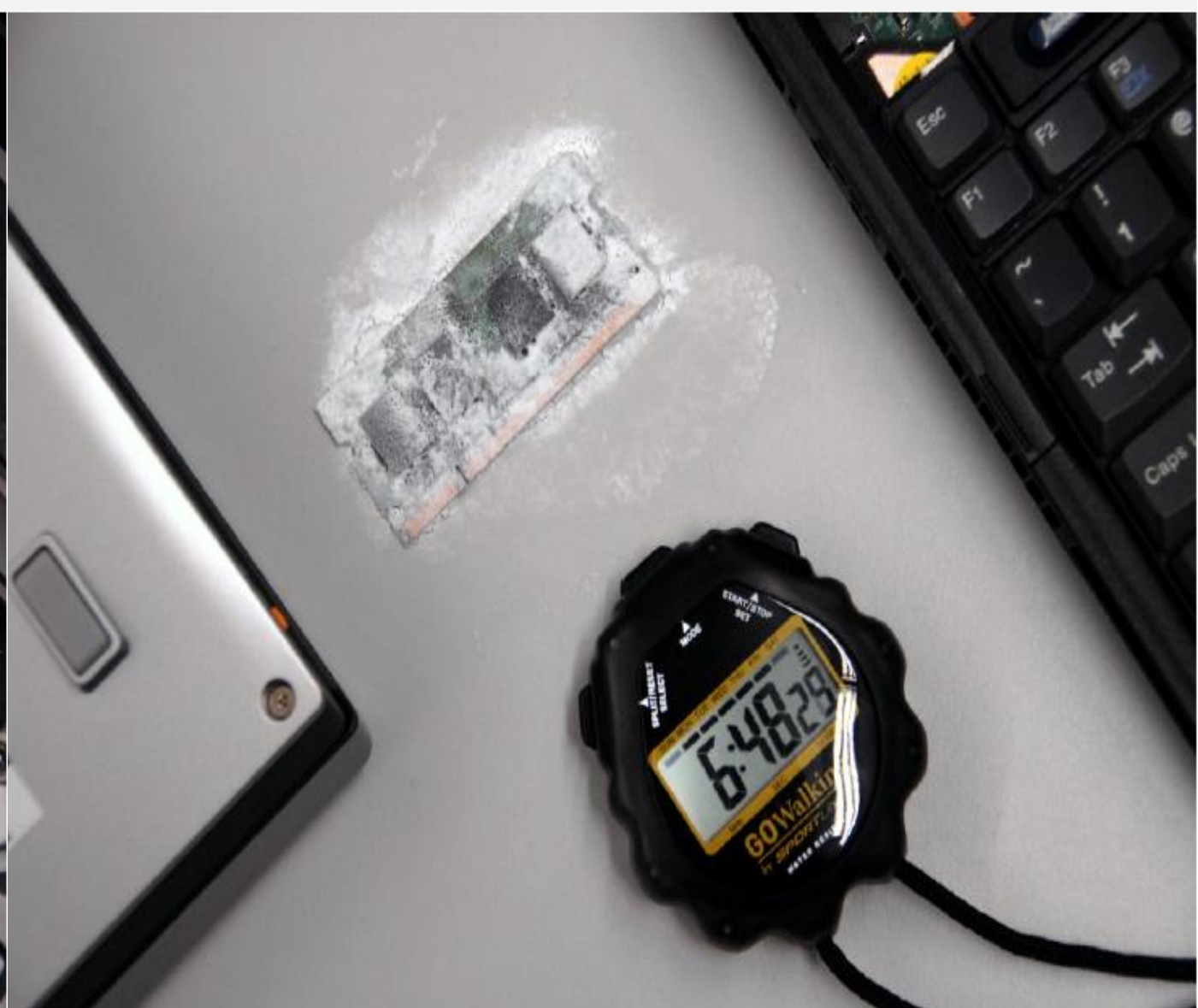
Some Other Forms: Cold Boot Attacks



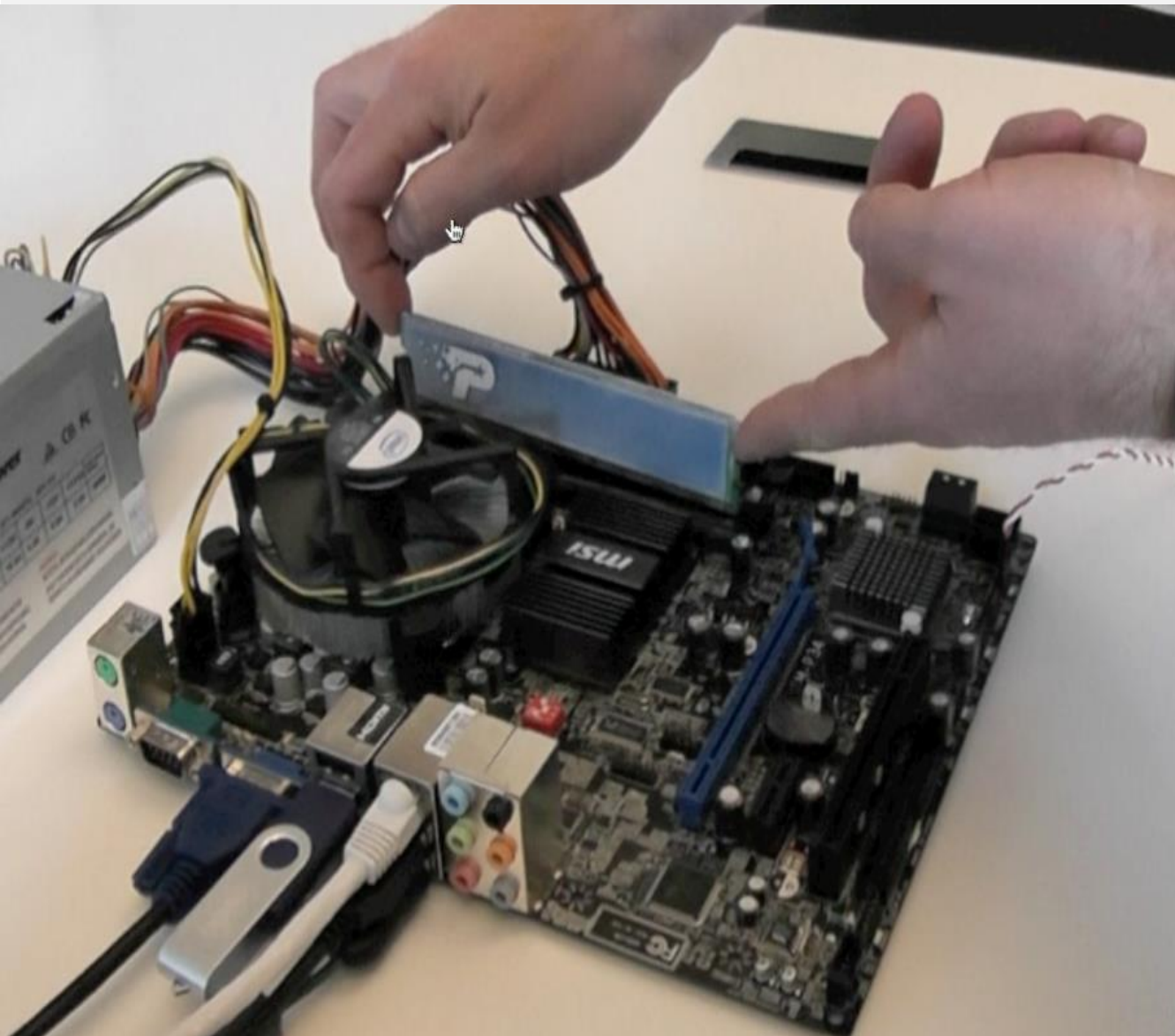
Before powering off

Freeze it to -50°C

Cool It



Put It Back



-196° C

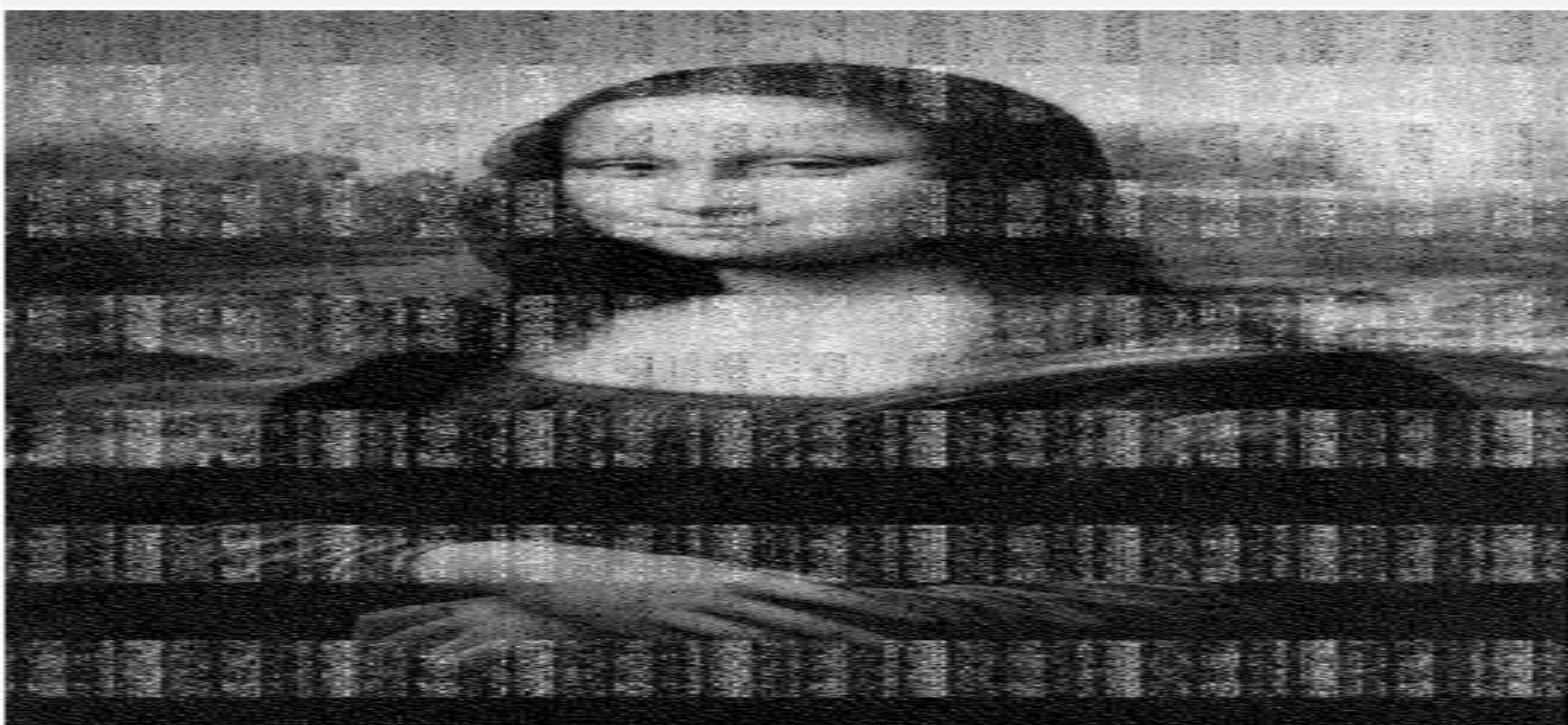
Your Password 😊

Machine	Seconds w/out power	Error % at operating temp	Error % at -50° C
A	60	41	No errors
A	300	50	0.000095
B	360	50	No errors
C	600	50	0.000036
C	120	41	0.00105
C	360	42	0.00144
D	40	50	0.025
D	80	50	0.18

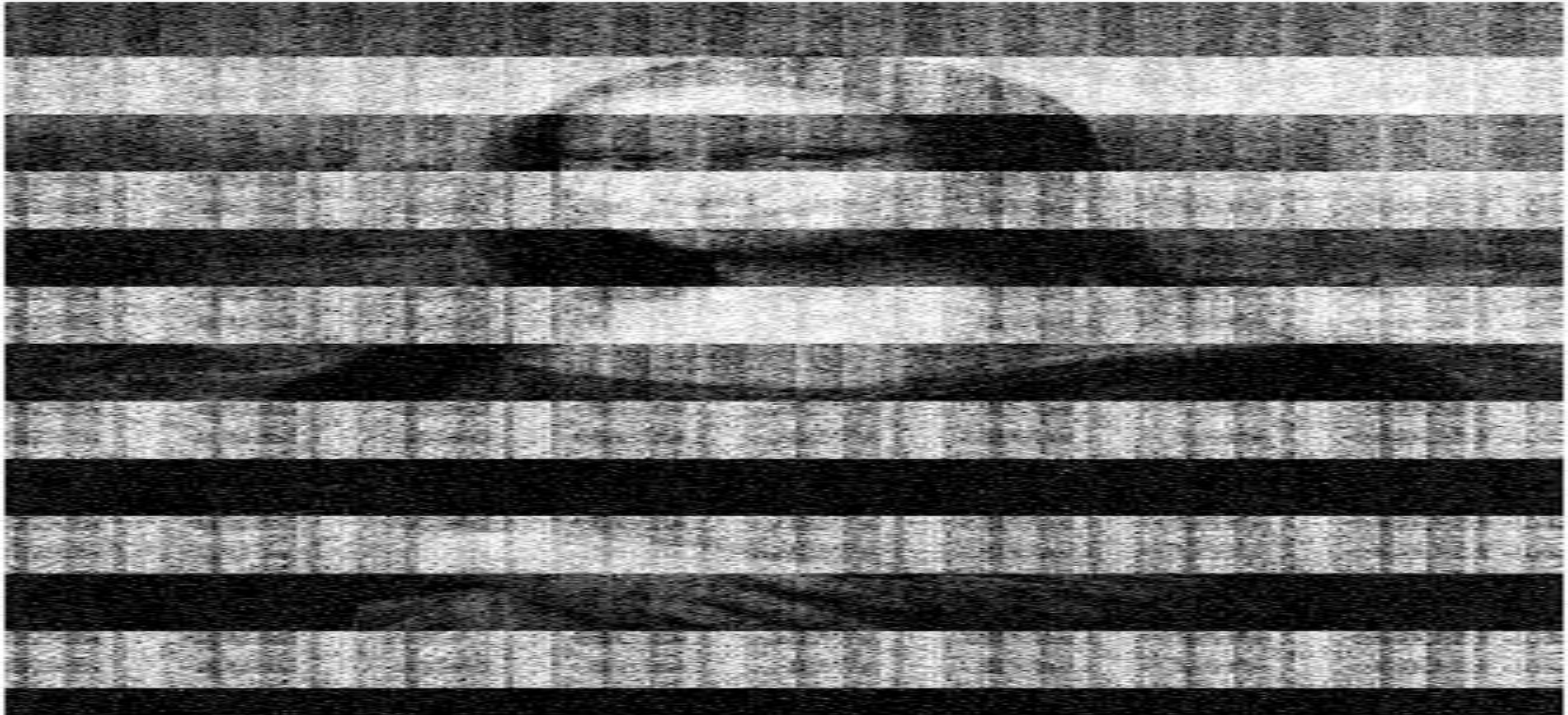
After 5 Seconds [SEC '08]



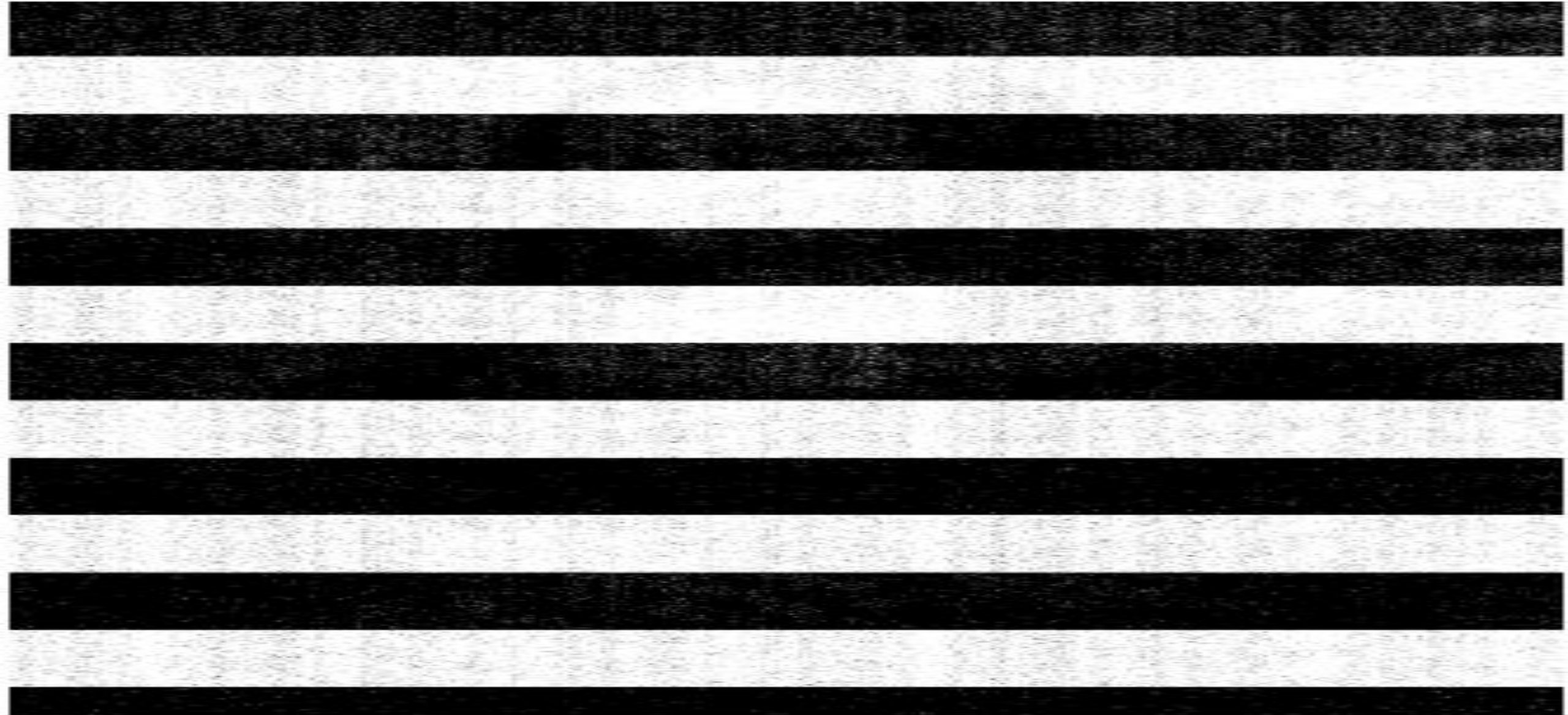
30 Seconds [SEC '08]



60 Seconds [SEC '08]



300 Seconds [SEC '08]



Sounds Good, Is it Real?

New Intel CPU Cache Architecture Boosts Protection Against Side-Channel Attacks

By [Catalin Cimpanu](#)

July 23, 2017 09:10 AM 0

BIZ & IT — Storing secret crypto keys in the Amazon cloud? New attack can steal them

Technique allows full recovery of 2048-bit RSA key stored in Amazon's EC2 service.

DAN GOODIN - 9/29/2015, 12:25 AM

LIBGCrypt 1.7.8 RELEASED (2017-06-29) **IMPORTANT**

We are pleased to announce the availability of [Libgcrypt](#) version 1.7.8. This release fixes a local **side-channel attack** (CVE-2017-7526). See the [announcement mail](#) for details.



Colin Percival

@cperciva

Follow

Replying to [@SteveBellovin](#) [@David_W_Maxwell](#) and 2 others

Attackers sophisticated enough to use side channel attacks usually don't advertise what they're doing.

1:20 PM - 17 Aug 2017



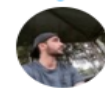
Colin Percival @cperciva · Aug 17

That said, I have reason to believe that cache-based timing attacks have been used to steal cryptographic keys in the wild.

2

11

30



Daniel Moghimi @danielmgmi · Oct 23

Any citable resource on this?

2

2



Colin Percival

@cperciva

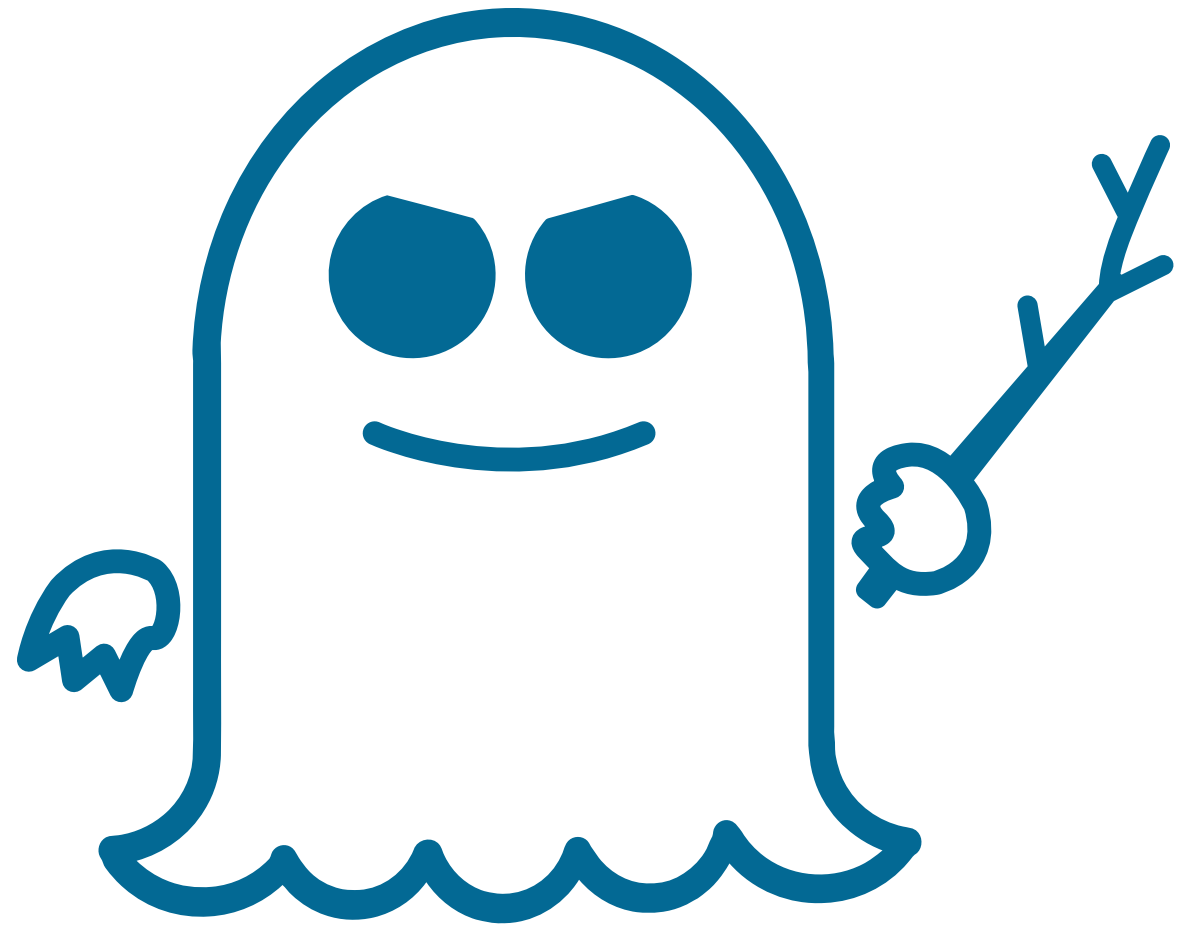
Follow

Replying to [@danielmgmi](#) [@SteveBellovin](#) and 3 others

None that I'm aware of. Actors on both sides have very strong incentives to not publish anything...

2:19 PM - 23 Oct 2017

And 2018 Jan onwards: Spectre and Meltdown



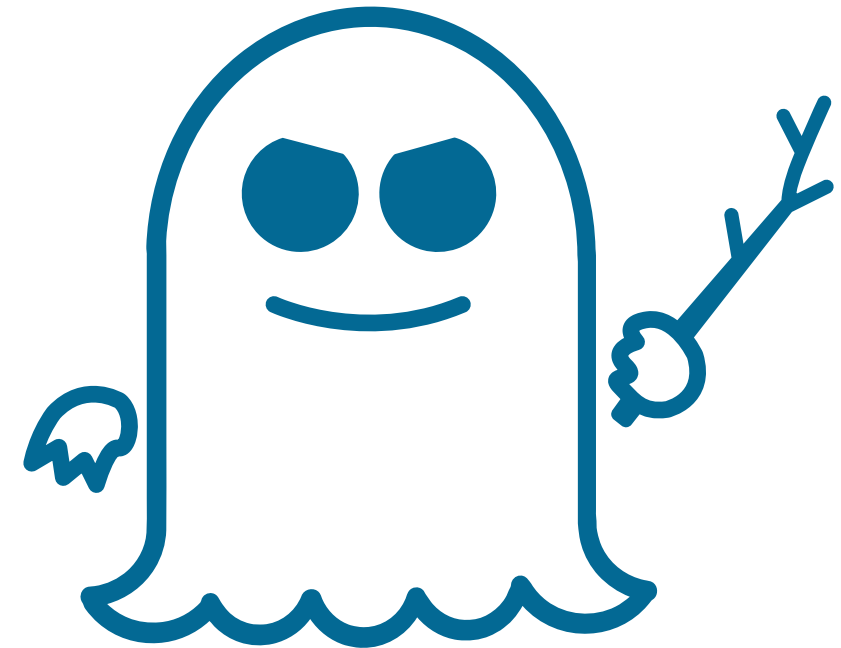
Spectre: Speculative Execution effect: 20K feet view

Step 1

```
int CS665Array = [100, 200, 300];  
int attacker = 1000;  
if (attacker < sizeof(CS665Array))  
    secret = CS665Array[attacker]
```

Step 2

```
char Array = ['a', 'b', ..... 'z']  
LOAD Array[3] 60 ms  
LOAD Array[secret] 60 ms  
LOAD Array[15] 5 ms  
LOAD Array[secret] 5ms
```



10K feet view of CS665

Understand different parts of memory systems

Attack different parts of memory systems

Detect these attacks

Mitigate these attacks

Programming Assignments (Need to bring your laptop)

See for yourself an attack on a real machine

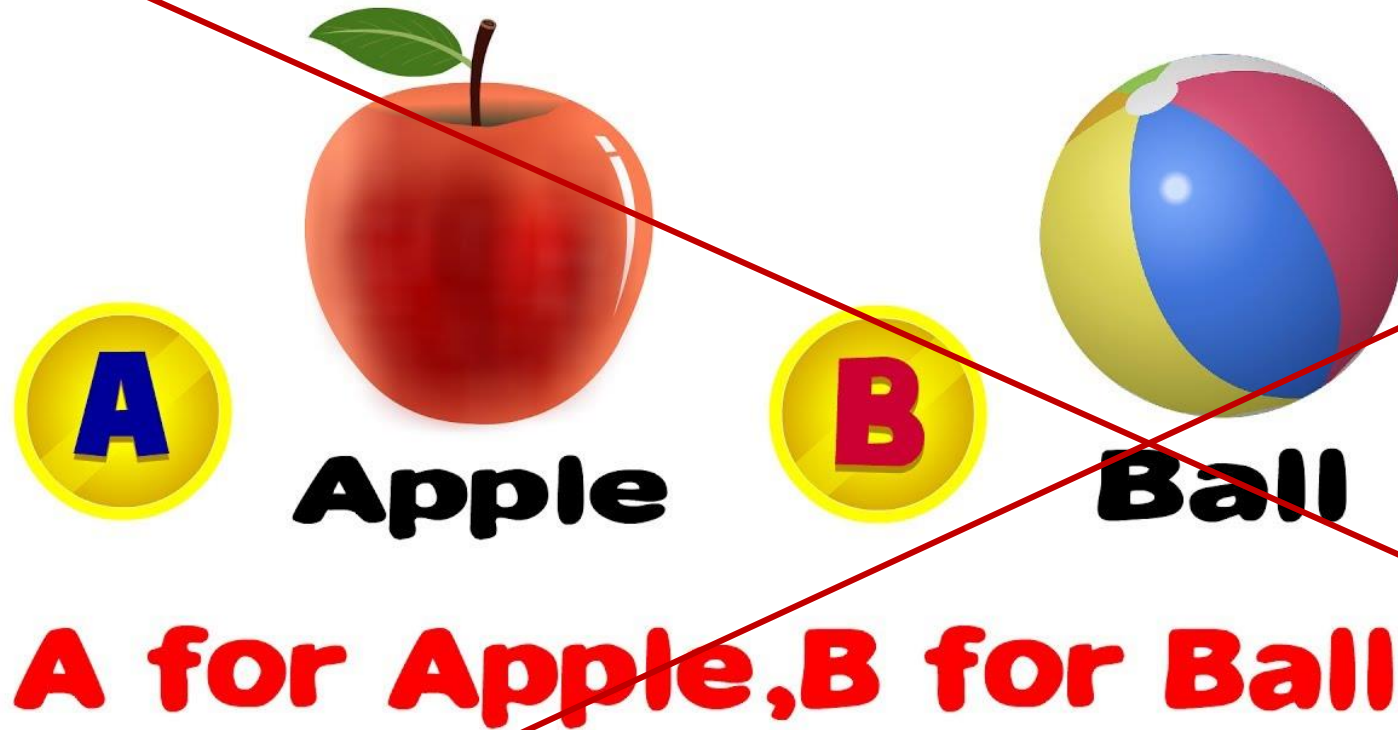
Code and build a variant of an attack

Code to detect these attacks

OR ideas to mitigate these attacks

Paper Reviews and Presentations: We will learn Slowly

Lectures format



C for Cache, D for DRAM

Who Said This?

“You can know the name of a bird in all the languages of the world, but when you’re finished, you’ll know absolutely nothing whatever about the bird... So let’s look at the bird and see what it’s doing—that’s what counts. I learned very early the difference between knowing the name of something and knowing something.”

So let’s learn:

How to learn, how to ask questions, how to find out the answers

Remember: I will respond (not answer)

We will not talk about attacks: We will talk about, why it happened, how it happened, what else can be done?

Lectures = Discussions

Why and How of the attacks through discussions

Everyone (including me) will go through videos/slides/papers before coming to CS665

Lecture Hours: We will discuss/debate on the intricacies

You don't know: how to read papers/..... so many things

We will learn soon

Finally:

CS665: We will learn (not you or me)

CS665: There will not be competition for exam scores
(small class, we will learn as a group **(not as an individual)**)
Bonus points 😊

CS665: Discussions + Hands-ons (no lectures and exams)

CS665: Discussion of basics + SOTA on secure memory systems

Next Lecture: Basics first

BASICS OF PROCESSOR & CACHES

Life Cycle (Biography) of Reads/writes (LOADs/STOREs)

Then Caches

So Brush up your basics

Special Brush-up lectures for M.Tech.(M.S.) and Ph.D.s

Interested in CS665

Not Sure about the background

If you are serious and really committed then

I will arrange brush-up lectures and show my commitment

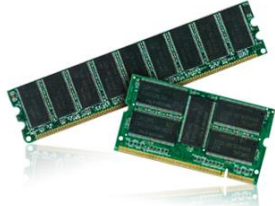
You do not want it, let me know ASAP

Assignment-0

ASSIGNMENT-0

Submit it by tonight (11:59 PM)

Have fun !!

May the secure  *be with you*

“It takes two to speak the truth - one to speak and another to hear” -
Henry David Thoreau

*Thank You &
Have a Good day*