CASPER

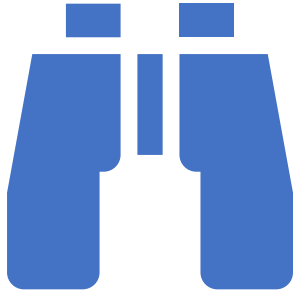
CS773-2022-Autumn: Computer Architecture for Performance and Security

Lecture 1: Course Logistics

https://www.cse.iitb.ac.in/~biswa/

No More (thanks to in-person CS773)

Can you hear me?



Can you see me?

Of course, ☺

Join Piazza now (course website)

https://www.cse.iitb.ac.in/~biswa/courses/CS773/main-autumn22.html

About Me: ~~Prof./Dr./Mr./Sir~~ Biswa

Member of faculty at CSE-IITB
one year old at IITB
CASPER group: https://casper-iitb.github.io/
Office hours: Tuesday 11:35 AM

Primary research interests:
Architecture for *performance and security*
Cross systems-stack interactions: *compiler, OS, networks, applied-ML on systems*

Soft-spoken TAs
Sumon: MS@CSE-IITB, Architecture security, office hour: Mon/Thurs
Veerendra: Ph.D. @CSE-IITB, ML for architecture, office hour: Mon/Tues

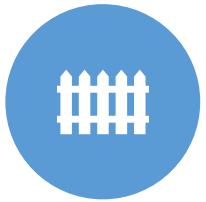
Introduce Yourself (Maybe Next week)

CS773: 100K Feet View

AN ENGINEERING COURSE (REMEMBER CSE)

A SYSTEMS COURSE

HANDS-ON ONLY AND CRITICAL THINKING/QUESTIONING



NO EXAMS (JEE AND GATE HAVE PROVED THAT YOU ARE GOOD AT IT)

NO TEXTBOOKS (TIME TO LEARN BY DOING STUFF AND READING PAPERS)

NO

……

…..

Pre-req (Please drop the course if you feel it is not you)

- Open mind to learn, debate, discuss, and code in C/C++/python
- Interested in asking questions and not only in providing answers ☺
- Ready to spend time in thinking rather than *ing.
- Team player: Trustworthy and professionalism, respecting others' time/suggestions.
- Rest we will take care.

Technically

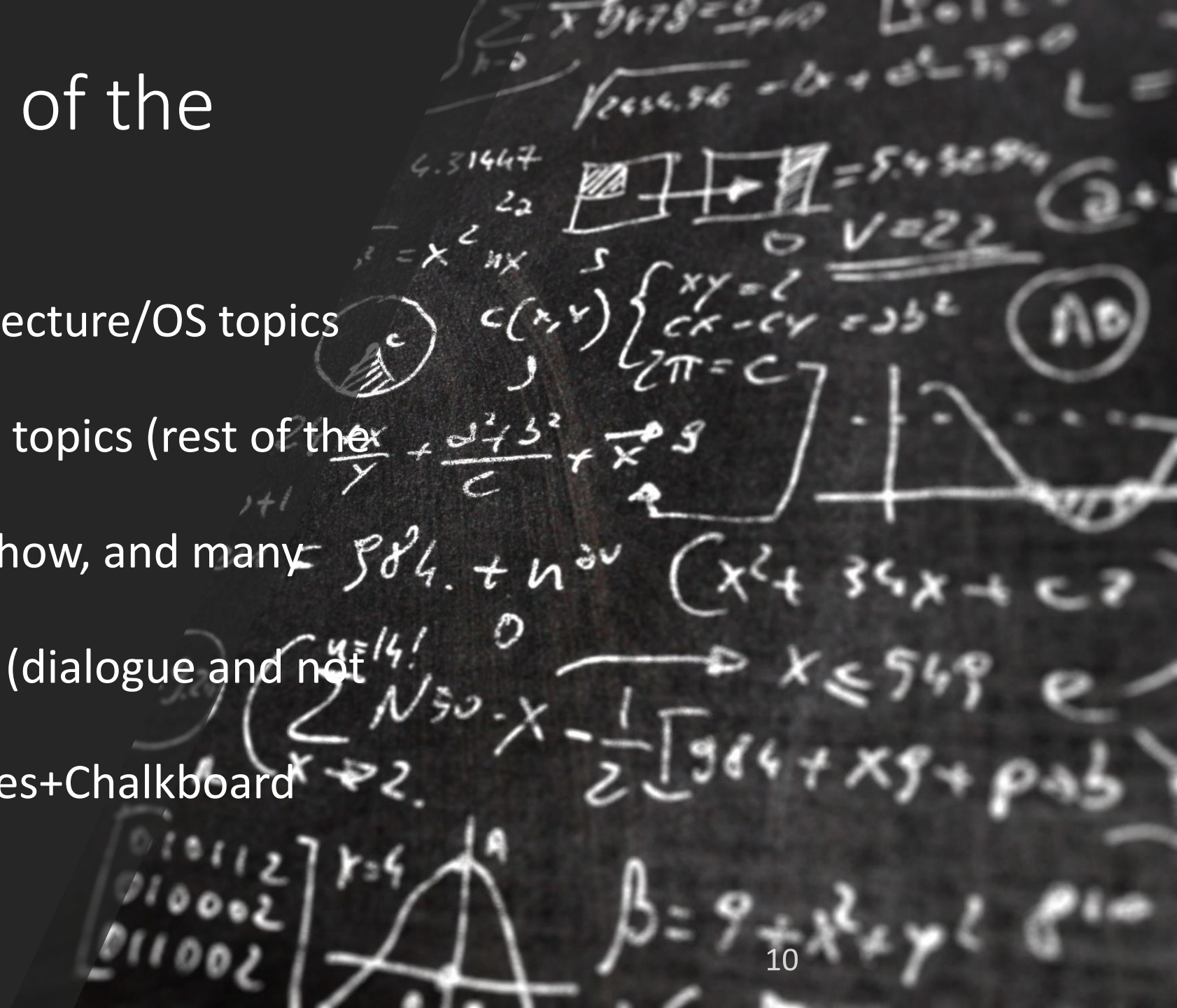
A bit of UG Computer Architecture and a half a bit of OS will be helpful. C/C++/Linux environment

If you know it, it is good

If you do not know it, it is even better.

CS773: Format of the Lectures

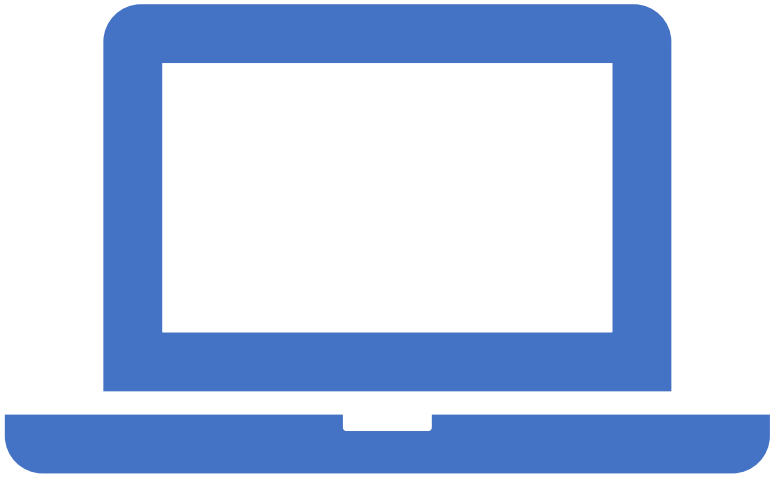
1. Basics of Computer Architecture/OS topics (first few weeks)
2. Advanced state-of-the-art topics (rest of the semester)
3. What can be done? Why, how, and many more
4. Discussion based lectures (dialogue and not monologue)
5. Lectures+discussions: slides+Chalkboard
6. Guest lectures

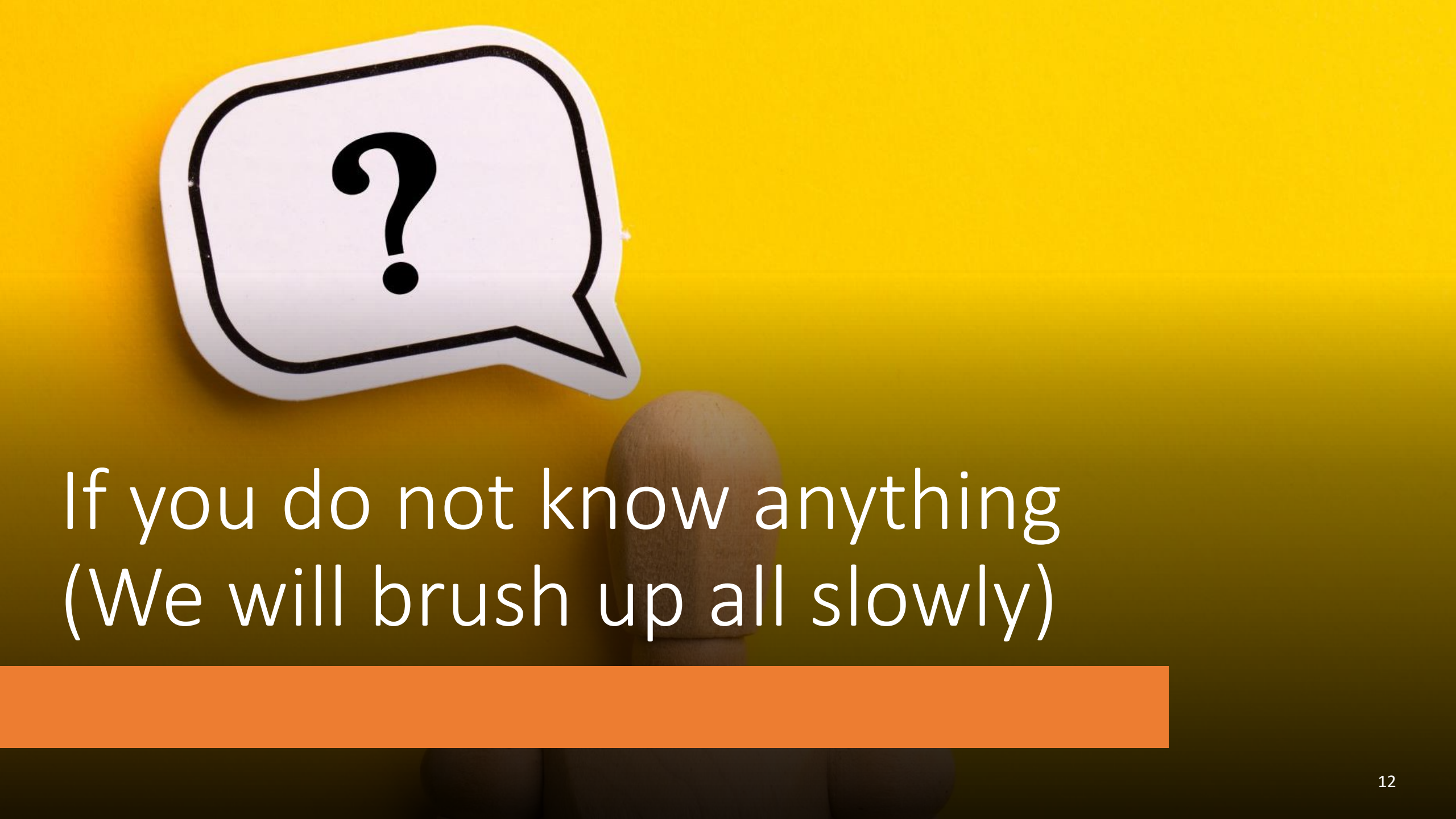


Bring your laptop

- For some lectures, we will have hands-on during lecture hours. So, bring your laptop with Linux installed.

- We will inform before time.





If you do not know anything (We will brush up all slowly)

What I expect from you (learn and develop skills)

- Forget about your JEE/GATE/…. rank. Congrats. But move on.
- No open-screens during lectures/discussions
- COVID-19 induced nomophobia, it will distract me and your friends. Switch-off/make it silent
- Understand, implement, and analyze ideas
- Ditch your excuses. Respect integrity and academic honesty. Take pride in honest hard work.

Email me for anything/everything [CS773]

ESPECIALLY FIRST YR. MASTERS AND PHDS

IITB – YOU MAY FIND IT OVERWHELMING

WE WILL TRY OUR BEST TO HELP YOU. BUT DO REACH OUT WELL AHEAD IN TIME.

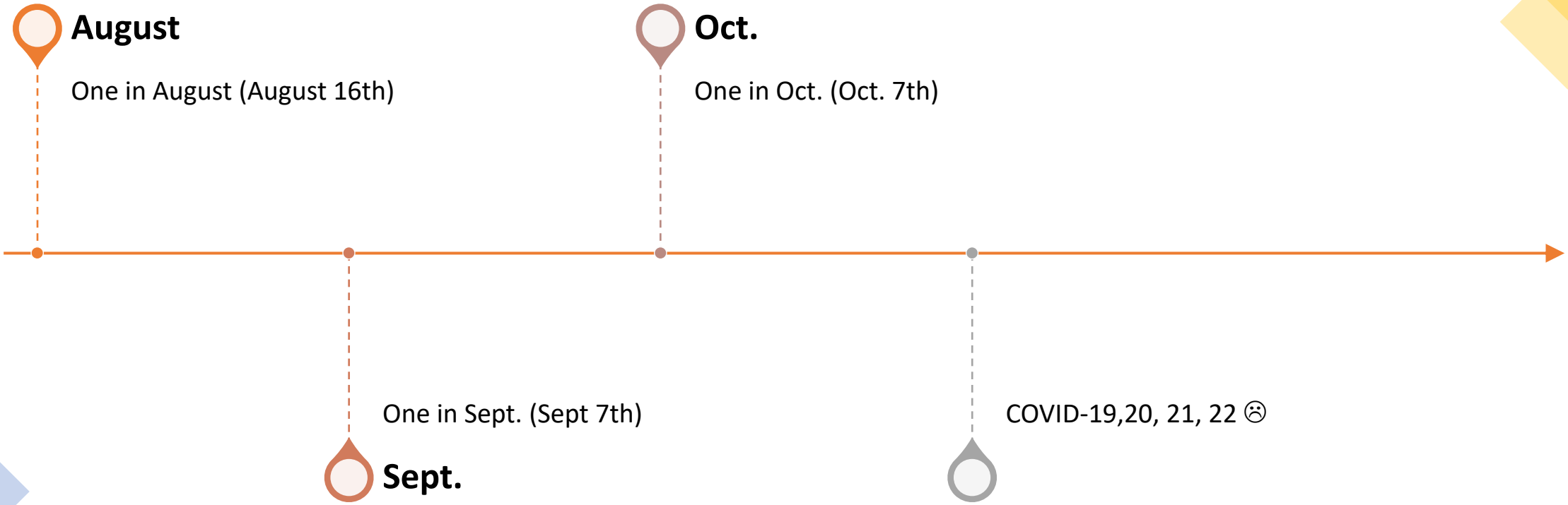
IITB Academic dishonesty protocol (go through it)

https://www.iitb.ac.in/newacadhome/punishments201521July.pdf

https://www.iitb.ac.in/newacadhome/procedures201521July.pdf

Assessment

Three Programming Assignments (individual, group of two): 3X10 (30) points



Bonus +5 points for the best assignment

Three Programming Assignments

1st Assignment: Simplest one. Solution available on web. Goal is to learn how to learn if something is available.

#Real system experiments

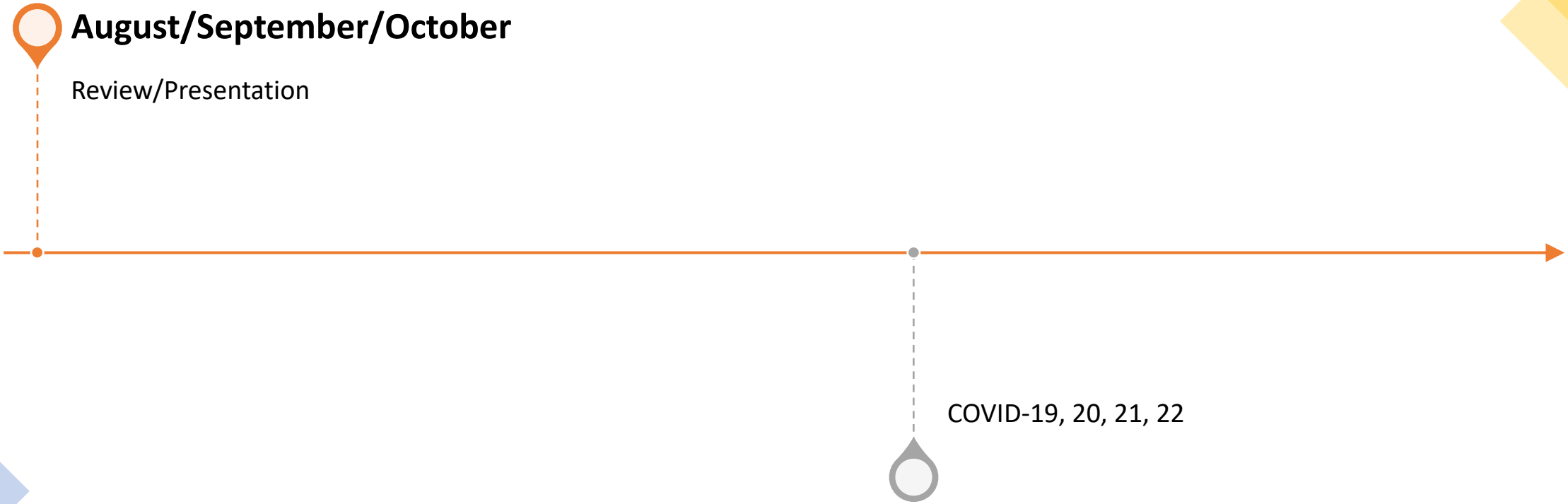
2nd Assignment: Simple one. Not available on web. Goal is to learn how to deliver what is expected with a bit of failure.

#Attack on a real system

3rd Assignment: Explore the unknowns with the hints from TAs/me.

#On tools/simulators

One Paper Presentation/Review Assignment (group of two or individual): 15 points

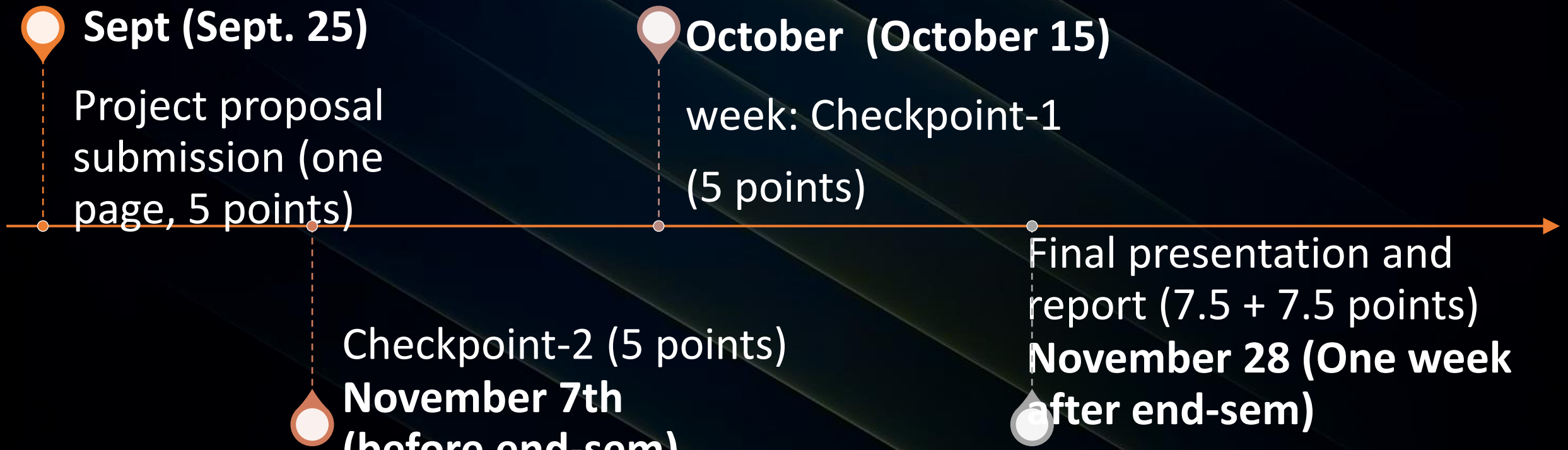


Bonus +5 points for the best group presentation and review. Note that you have to review/present only once in the entire semester

Explain more about this process

- Last week of every month
- Two presentations/lecture (tentative)
- TAs will upload your slides/reviews on Monday of last week of every month
- You need to go through it and participate during the lecture hours (at least two papers)
- 10 points for participating

One Project for Two months: 30 points



Project leading a workshop/conference submission (not acceptance): AA grade
Biweekly group meetings: To help you and your team reach the goal.

Does that happen? CS773-Spring22

Golmaal: Thanks to the Secure TimeCache for a Faster DRAM Covert Channel

Ajaykumar Kushwaha*, Ajay Jain†, Mahendra Patel‡, Biswabandan Panda§
* *Dept. of Computer Science and Engineering, Indian Institute of Technology Bombay, Email: ajaykushwaha@cse.iitb.ac.in*
† *Dept. of Computer Science and Engineering, Indian Institute of Technology Bombay, Email: ajayjain@cse.iitb.ac.in*
‡ *Dept. of Computer Science and Engineering, Indian Institute of Technology Bombay, Email: mahendrapatel@cse.iitb.ac.in*
§ *Dept. of Computer Science and Engineering, Indian Institute of Technology Bombay, Email: biswa@cse.iitb.ac.in*

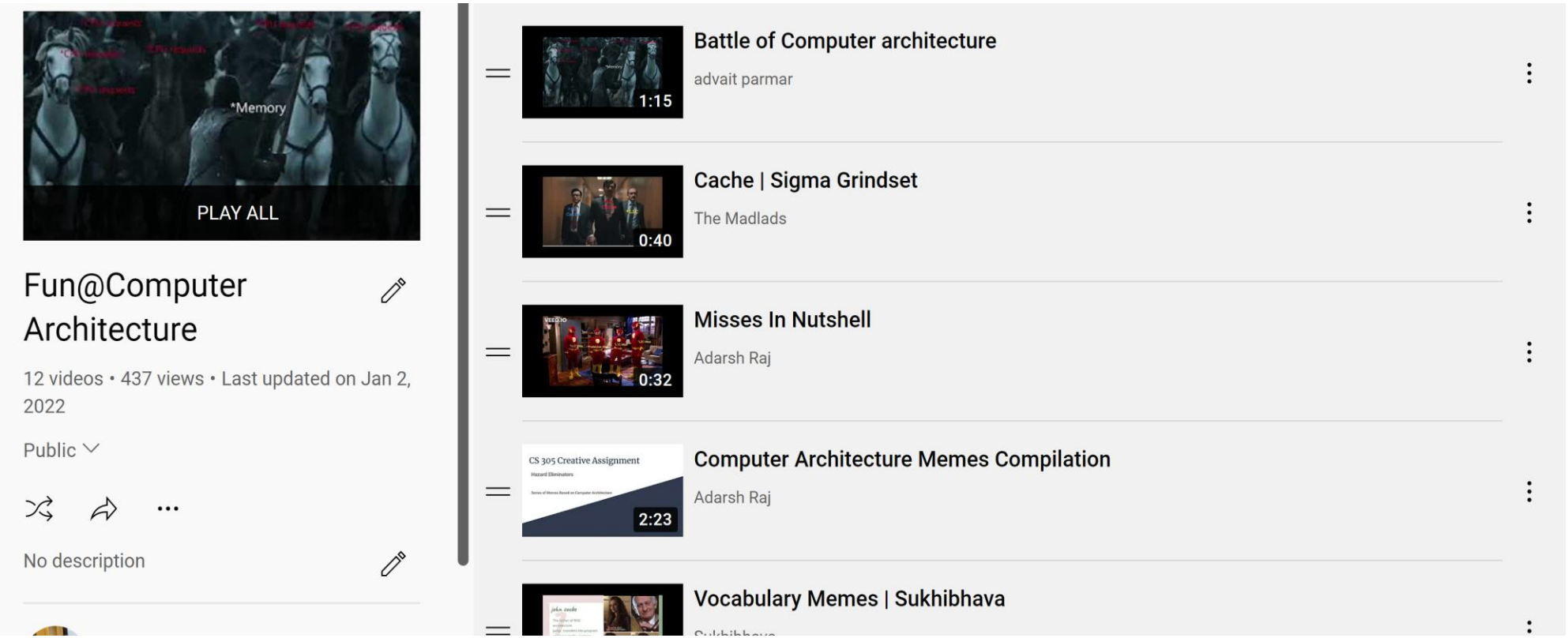
***Abstract*—Cache-based side-channels can cause information leakage thanks to the latency difference between a cache hit and a miss. One form of cache side channel is the shared memory channel that leading to attacks like Flush+Reload and Evict+Reload. A recent proposal in ISCA 2021 named TimeCache mitigates cache attacks that exploit the reuse of shared data and code between an attacker and the victim. With TimeCache, the first request to any memory address by a process is always a cache miss providing per-process cache line visibility, and it makes sure processes do not benefit from cached data brought in by another process until it pays the price of the corresponding cache miss penalty. Though TimeCache successfully mitigates cross-process shared memory**

A brief introduction to TimeCache. TimeCache eliminates reuse-based cache attacks that use shared data/code cache lines by providing per-process cache line visibility of a shared cache line. With TimeCache, accesses to a shared cache line by different processes are isolated in timing. For example, if an attacker core (core 0) and the victim core (core 1) share an LLC line L, then for a Flush+Reload attack, the following sequence of events will happen with TimeCache: (i) attacker core `flushes` the line L from LLC, (ii) victim core accesses the LLC line L and gets a response from DRAM, and (iii) then when the attacker core reloads the line L, it gets an LLC miss (thanks to per-process visibility cache lines with TimeCache).

TimeCache is implemented as a combination of both

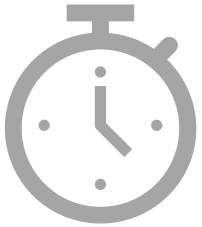
Finally, Memes/Songs/Videos (5 points)

https://www.youtube.com/playlist?list=PLw6vmiIQrilQL70KTTa4oljUYxmzGSgPp



And Teatime (Chai Pe Charcha): 10 points

Meet me once in k weeks for 20 mins over tea/coffee for “discussion”.



Completely informal. As per your timings.

2.5 points per CPC. If you do not attend, -2.5 points.

Late submissions/penalty

Programming assignments: -2 per day

Reviews/presentations:

-5 for no show

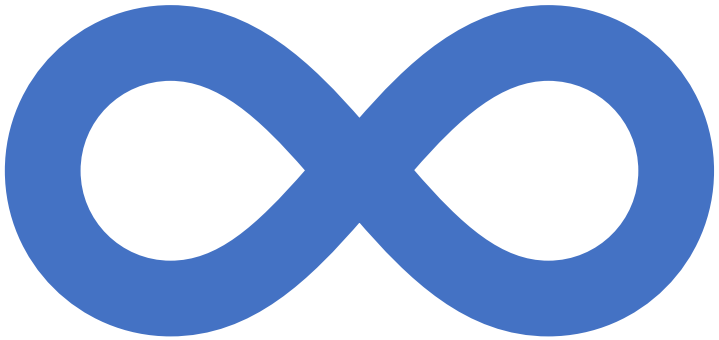
(Inform TAs at least a week before if there will be no-show)

Project checkpoints (I and II):

-2 per day

Infinity marks

Mid-sem and end-sem



Summary

Programming assignments:	30 (bonus +15)
Paper/review presentation:	15 (bonus +5)
Participation during presentation:	10 (bonus +5)
Memes:	5 (bonus +5), Teatime: minimum 10 (bonus +5)
Project:	30 (bonus AA grade)

You can do best in some and still get an AA

Bonus 35 points ☺ ☺ If you need a different way, please inform me/TAs

Grading

Won't be based on a curve.

If all learn well then, all AA grades.

So, focus on learning. Rest I will take care.

Changes from Spring-22

Spring 2022 (39 students)	Autumn 2022 (current semester)
Five paper reviews/presentations	One
Group of five	Group of two
No programming assignments	Three programming assignments
No Memes	Yes, to Memes
Lectures: Paper presentations	Lectures: lectures (discussions)
Online, boring TAs/Professor ☹ ☹	In-person, fun learning ☺
Online participation: Zero	Participation, CPC: 10+10 points

All Good. But you do not know…

How to read a top conference paper?

How to review a top conference paper?

How to approach a problem?

How to solve a problem?

How to think, how to question, how to convince, ….

CS773 will take care of that. We will discuss how to about everything ☺ but slowly not today

A few more

There won't be any deadlines on Saturday/Sundays.

There won't be any midnight deadlines.

Working on weekend shows – incompetence

CS773 will be an incompetent course

Instructor and the TAs will be incompetent. I will not respond to queries on weekends/holidays.

PAUSE

Questions please

Hopefully, some course registrations/drops too ☺

Let’s get Started (Why CS773)

Hardware is new software

People who are really serious about software should make their own hardware - Alan Kay

And the trend ….

OPINION

Microsoft's Innovative 4-Processor PC

By Rob Enderle | May 30, 2022 4:00 AM PT | Email Article

Tweet 6 Share 0 Share 0 Share 6

Facebook is just crazy enough to make its own processors

Job listings for a chip design team have surfaced online.

Google Replaces Millions of Intel's CPUs With Its Own Homegrown Chips

By Anton Shilov published June 04, 2021

YouTube now uses homegrown Argos VCUs

HARDWARE INDUSTRY NETFLIX AMD EPYC

Netflix leverages AMD Epyc processors to achieve 400 Gbps video data flow per server

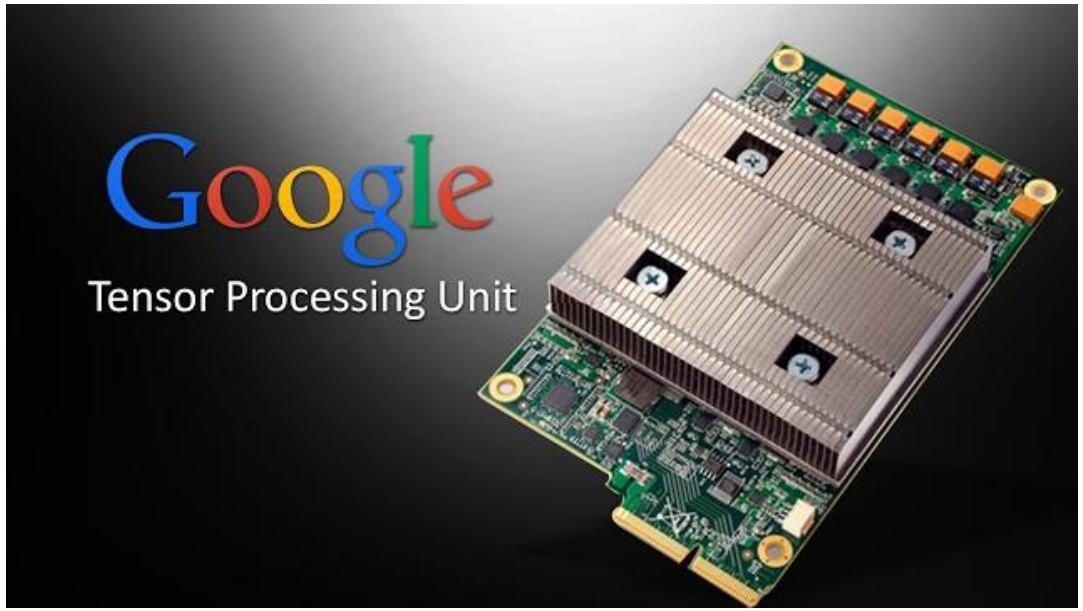
Epyc servers for epic streaming bandwidth

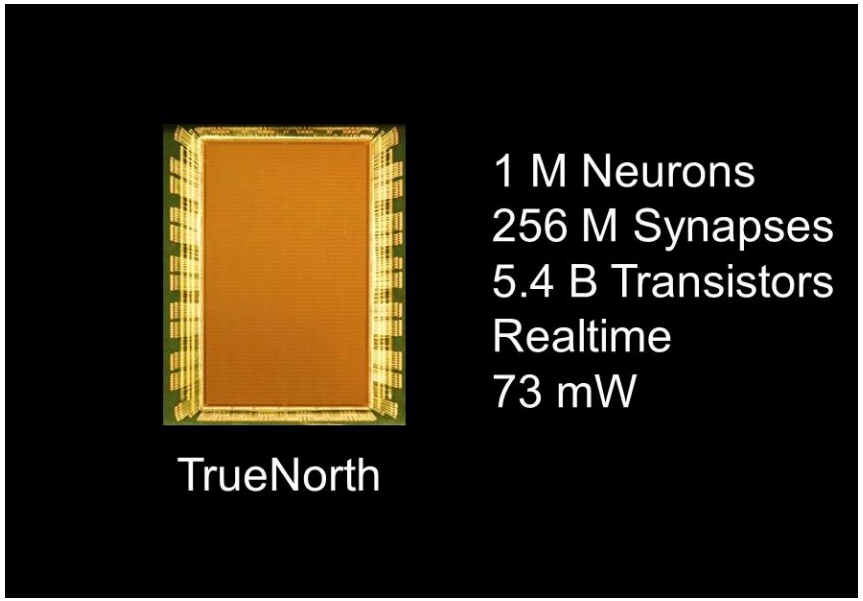
By Adrian Potoroaca September 21, 2021 at 9:10 AM

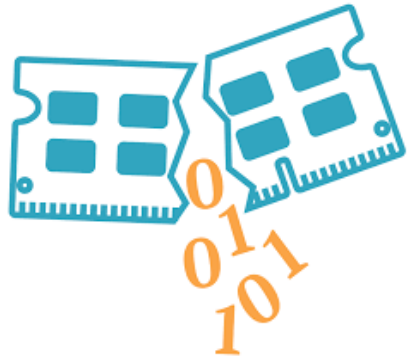
Application Specific

Intel launches crypto mining chip

By **Jonathan Spencer Jones** - Apr 12, 2022







But attacks everywhere
(These are not hardware attacks)
These are (micro)architecture attacks

Desi Attacks

DABANGG: A Case for Noise Resilient Flush-Based Cache Attacks

Anish Saxena
School of Computer Science
Georgia Institute of Technology[§]
anish.saxena@cc.gatech.edu

Biswabandan Panda
Department of CSE
Indian Institute of Technology Bombay
biswa@cse.iitb.ac.in

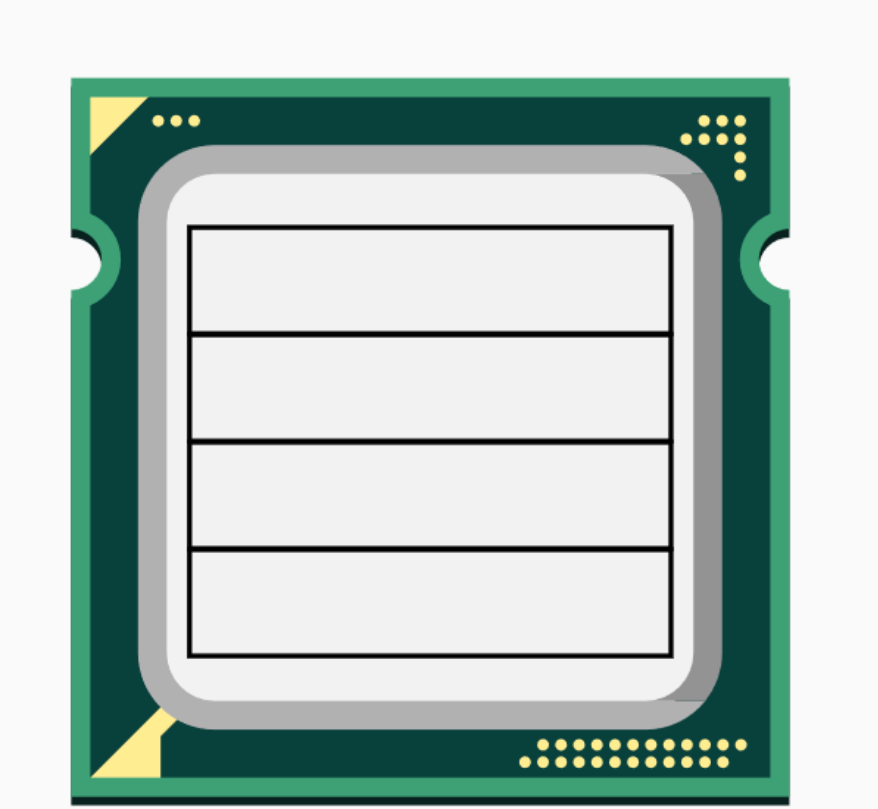
Golmaal: Thanks to the Secure TimeCache for a Faster DRAM Covert Channel

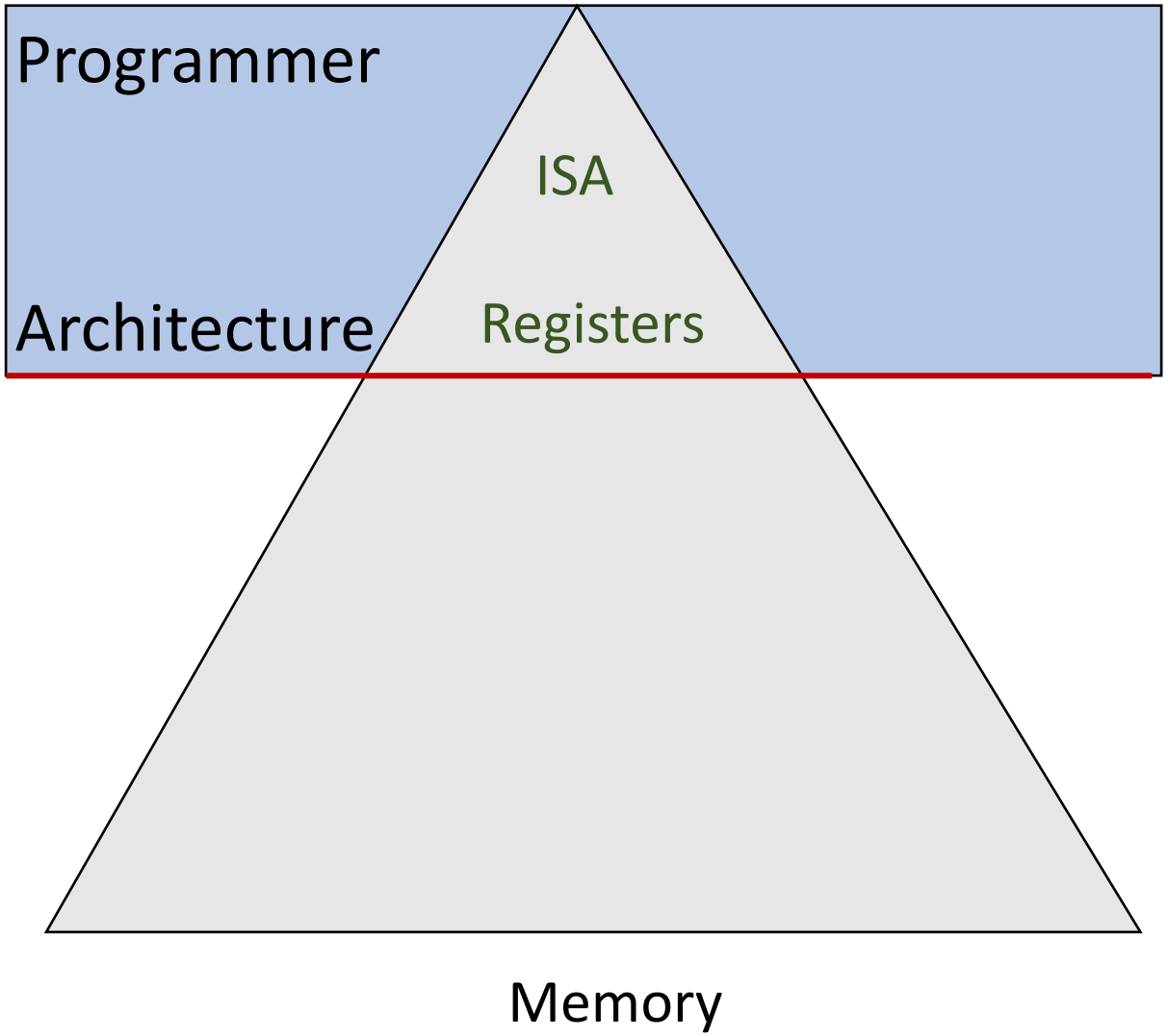
Ajaykumar Kushwaha*, Ajay Jain†, Mahendra Patel‡, Biswabandan Panda§

DAMARU: A Denial-of-Service Attack on Randomized Last-Level Caches

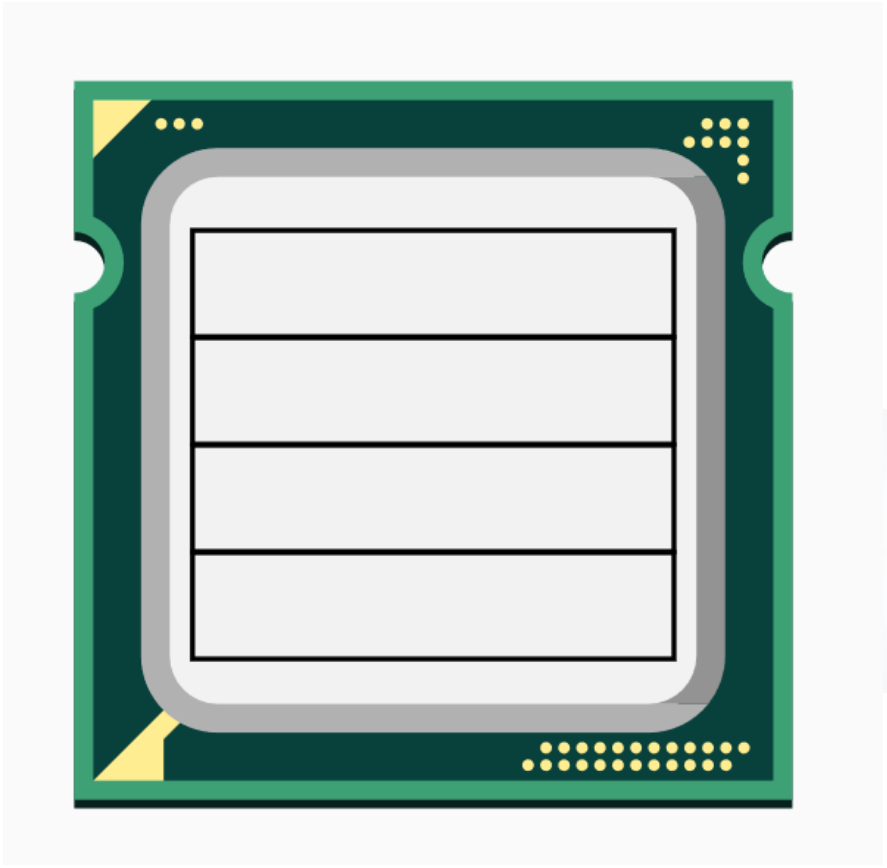
Pratik Kumar, Chavhan Sujeet Yashavant, and Biswabandan Panda

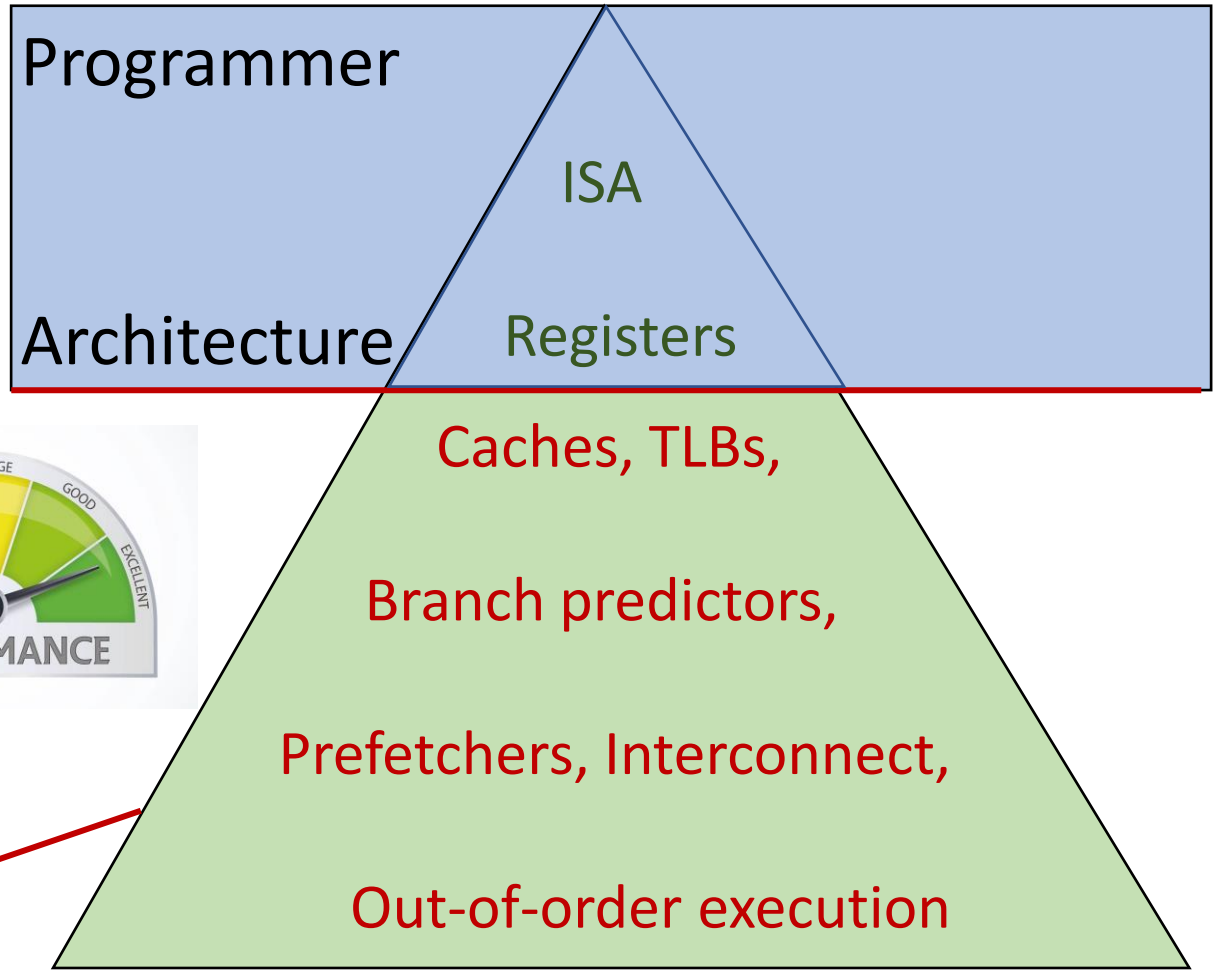
CS773:101





CS773:101





Not exposed to programmer

Performance (faster the better): 100K Feet View

Better Cache Hierarchy

Better Processors for AI/ML

Better OS-architecture interaction

Better Network-architecture interaction

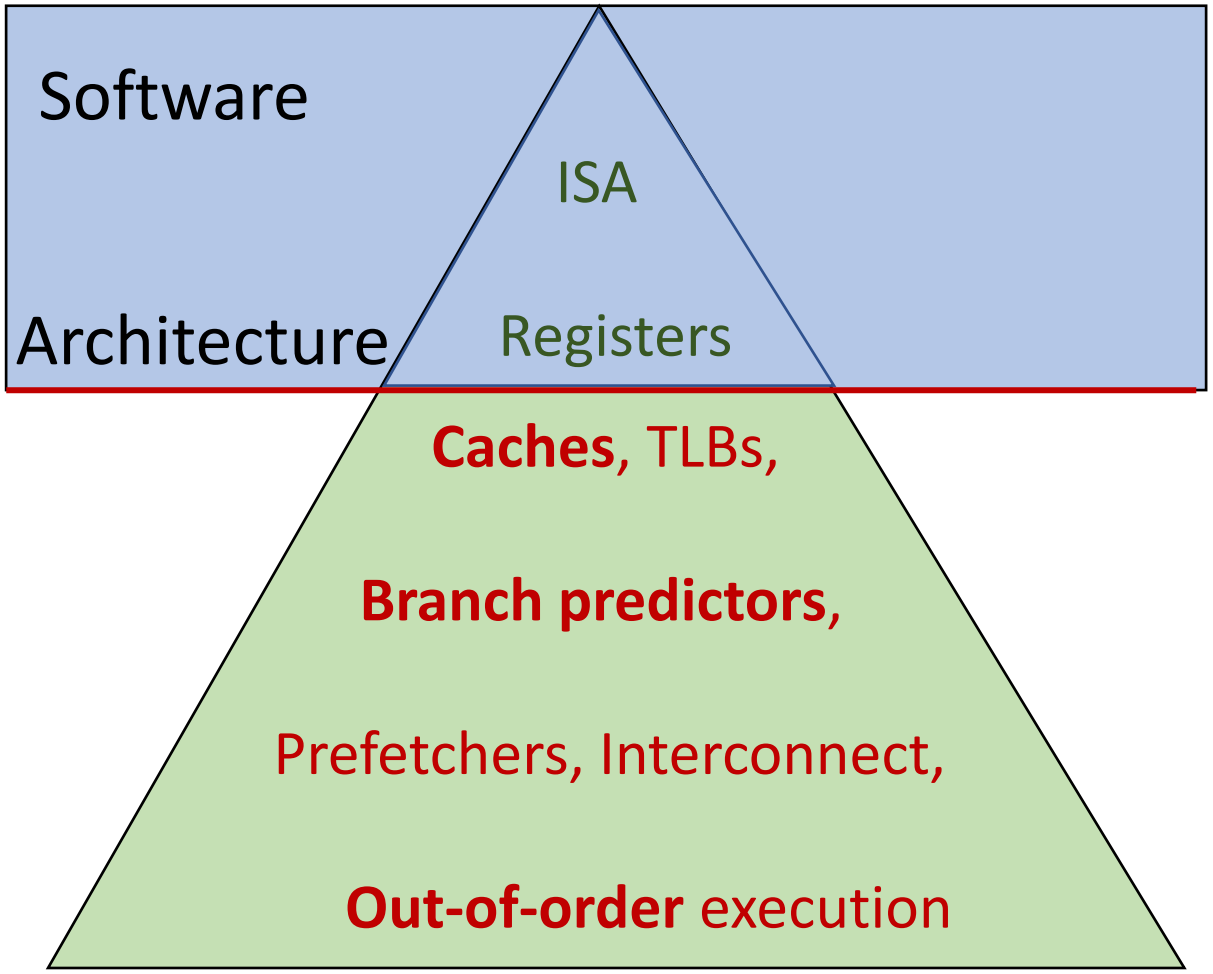
Microarchitecture for cloud, servers, virtualized environments

Memory hierarchy for persistent memory

Performance/Power tradeoffs

We won't cover all. Depending on your interests, we will jump into these topics, again slowly

From Performance to Security



Security (not privacy)

Confidentiality	*You do not **see** **(READ)** what you are not supposed to see*
Integrity	*You do not **change** **(WRITE)** what you are not supposed to see*
Availability	*You do not **affect** **(DELAY)** others (un)intentionally*

Intel Inside; NO; attacks inside ☺

Security: 100K Feet View

Secure Cache Hierarchy

Secure Processors

Secure OS-architecture interaction

Microarchitecture for security and performance

Offensive side: More attacks, attacking mitigations

Defensive side: More mitigations

We won't cover all. Depending on your interests, we will jump into these topics, again slowly

Projects

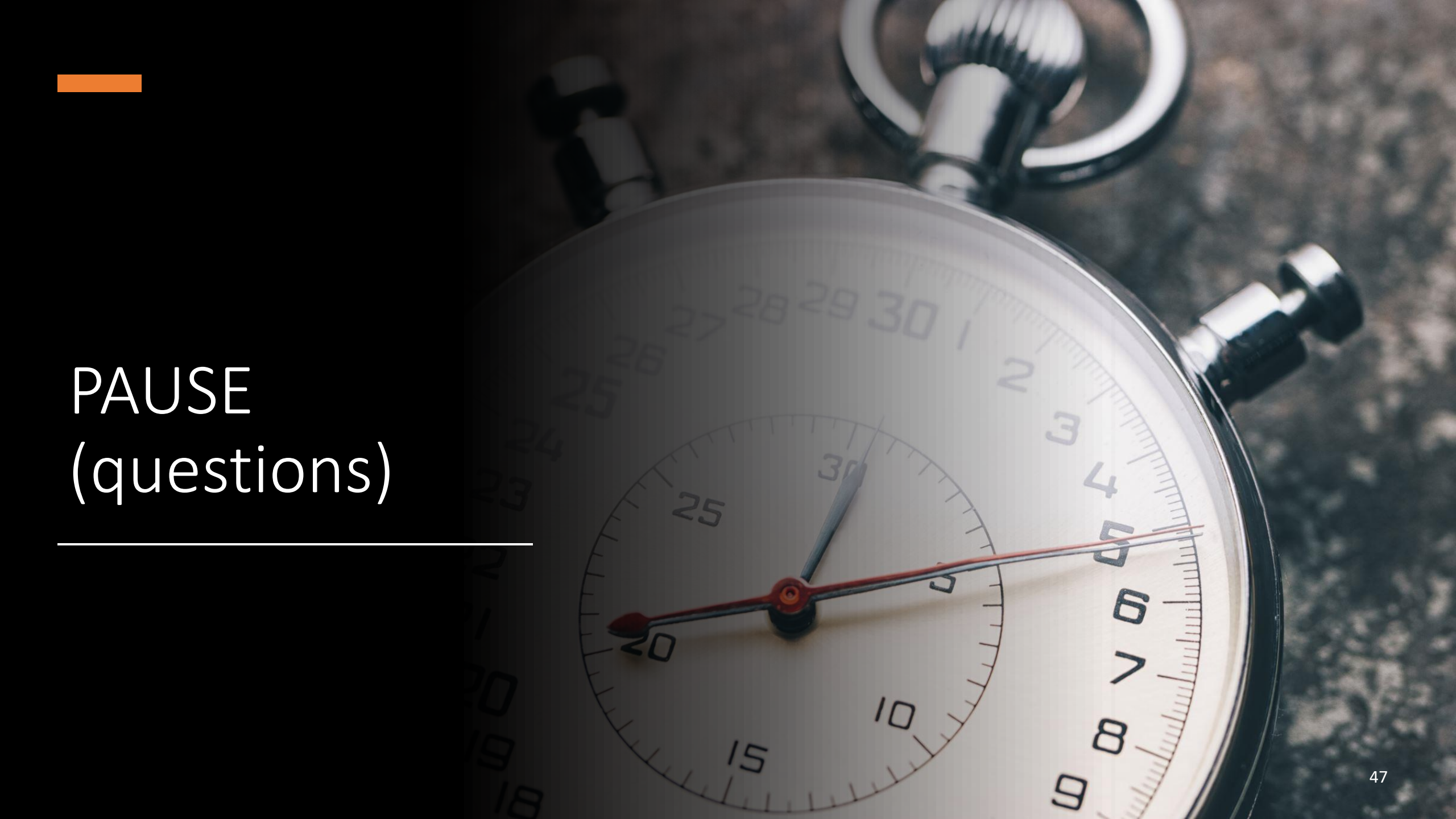
PERFORMANCE

SECURITY

PERFORMANCE AND SECURITY

On real systems, simulators, other tools. We will go through it slowly.
No need to learn all. Depending on your interests, you should learn one (not all)

PAUSE (questions)



Drop the Course

It is not a core course. So, no compulsion.

Lesser the number of the students the better (max. 25 around). I am happy, it is less than 20 so far ☺

By dropping the course, you will help your friends/me who are really interested in this course.

Fill the Form (before next lecture) so that we will know you better

Feel free to speak now so that we can make the course better

Form link: [Hello CS773 Autumn 2022 (google.com)]

Thanks

Next Lecture

Brushing up computer architecture-101