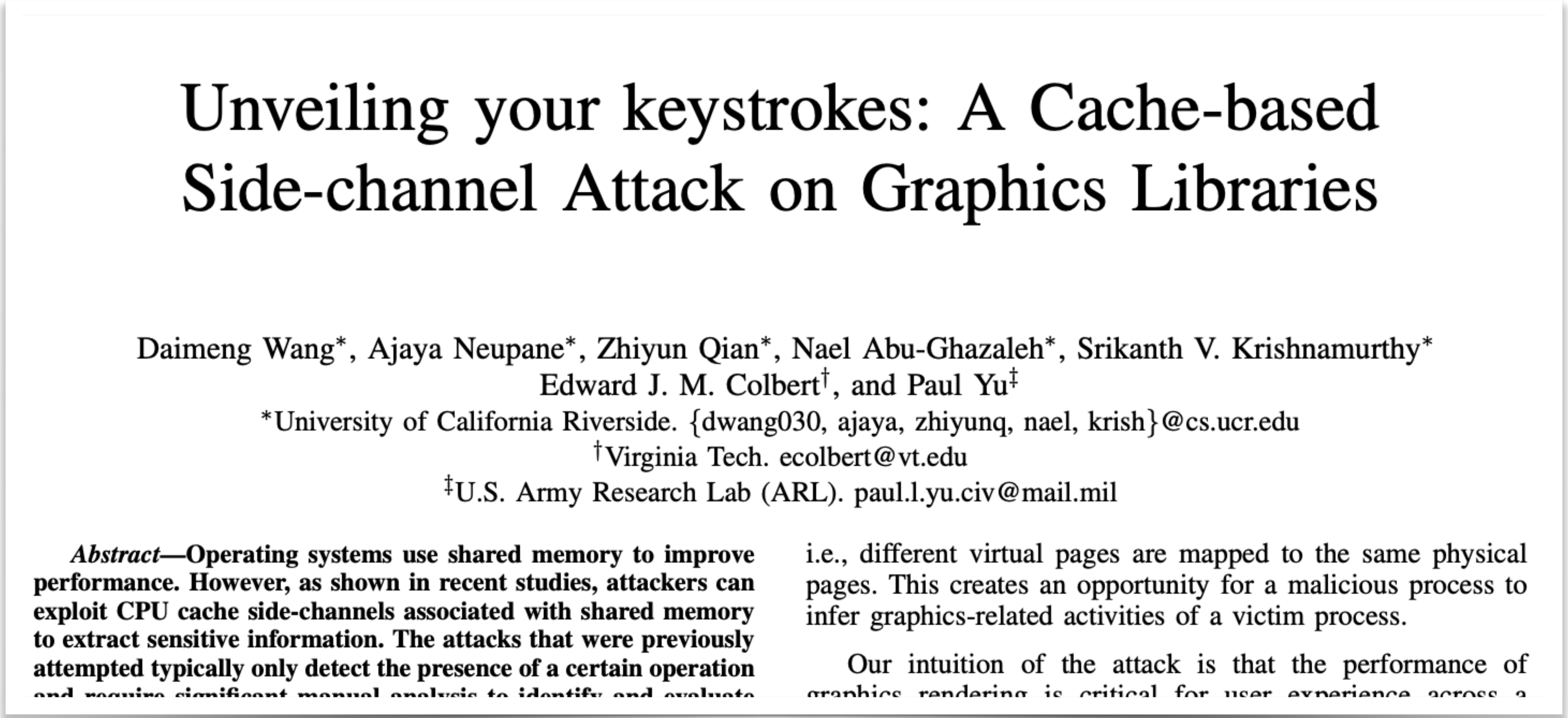
Introducing Architecture Security

Check In 3 in class;
HW2 due tonight!



Unveiling your keystrokes: A Cache-based Side-channel Attack on Graphics Libraries

Daimeng Wang[*], Ajaya Neupane[*], Zhiyun Qian[*], Nael Abu-Ghazaleh[*], Srikanth V. Krishnamurthy[*]
Edward J. M. Colbert[†], and Paul Yu[‡]
[*]University of California Riverside. {dwang030, ajaya, zhiyunq, nael, krish}@cs.ucr.edu
[†]Virginia Tech. ecolbert@vt.edu
[‡]U.S. Army Research Lab (ARL). paul.l.yu.civ@mail.mil

***Abstract*—Operating systems use shared memory to improve performance. However, as shown in recent studies, attackers can exploit CPU cache side-channels associated with shared memory to extract sensitive information. The attacks that were previously attempted typically only detect the presence of a certain operation and require significant manual analysis to identify and evaluate**

i.e., different virtual pages are mapped to the same physical pages. This creates an opportunity for a malicious process to infer graphics-related activities of a victim process.

Our intuition of the attack is that the performance of graphics rendering is critical for user experience across a

Image credit: https://www.ndss-symposium.org/ndss-paper/unveiling-your-keystrokes-a-cache-based-side-channel-attack-on-graphics-libraries/

Outline

- On studying attacks and security
- How to learn leaked information
- How to make sense of leaked information (after spring break)

Disclaimer on Teaching Attacks…

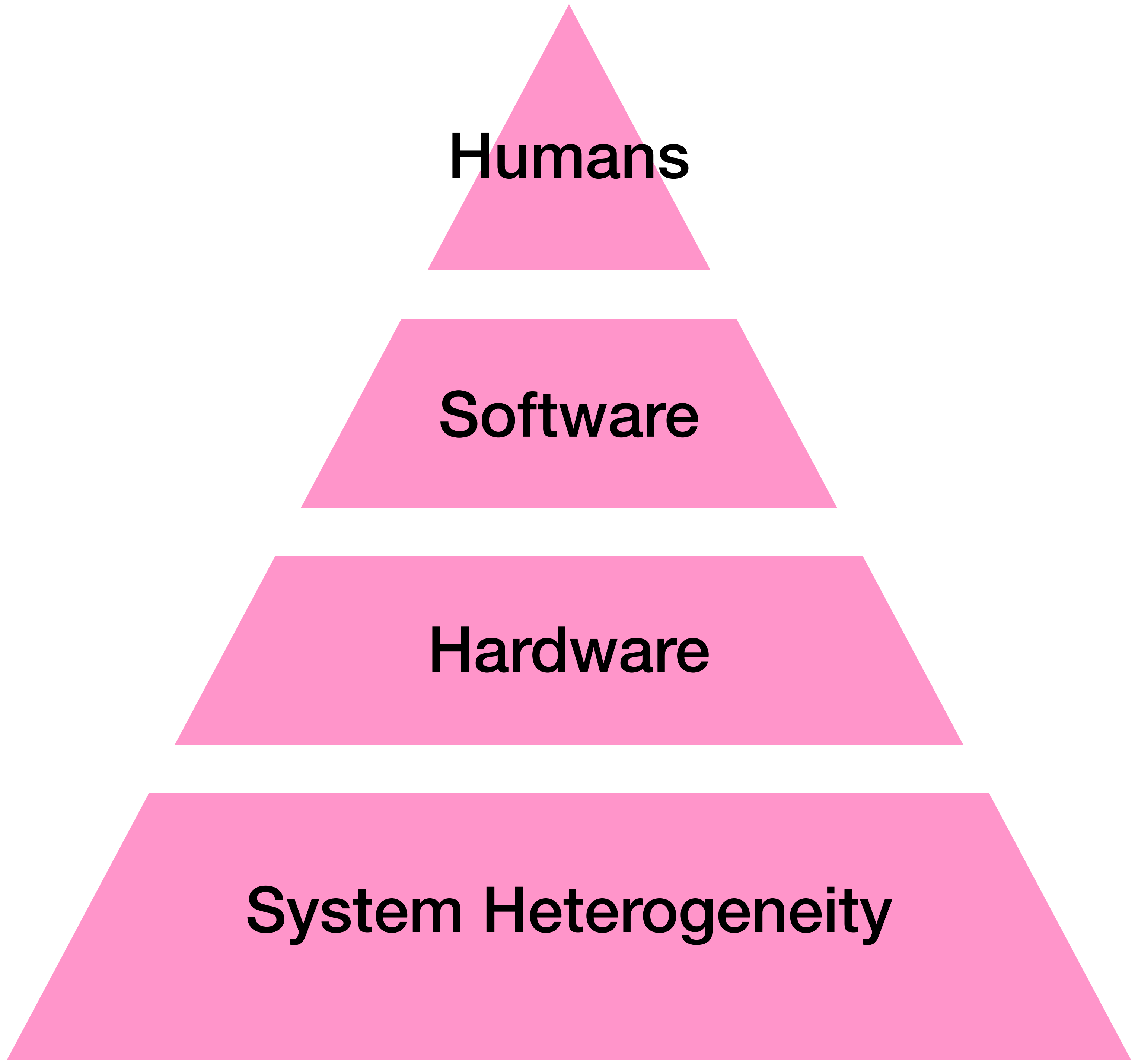
- We are going to describe published, well-studied literature about dangerous and powerful attacks
- These attacks are intuitive and easy to perform (they do not require high levels of privilege or complicated code to execute)
- One of the learning goals of this class is to study the trade-offs of design decisions made
  - ➡️ security is an often neglected component of this design space trade-off, so we will use it as a means to think deeply about the concepts that we have covered and learned thus far

Chat with your neighbor(s)!

Share your comfort levels of describing and learning about attacks.
1️⃣ How security conscious do you feel you are?
2️⃣ Do you feel like studying and publishing attacks should be encouraged (e.g., more awareness towards building defenses) or discouraged (e.g., don’t notify attackers of unknown vulnerabilities)?

The Security Stack

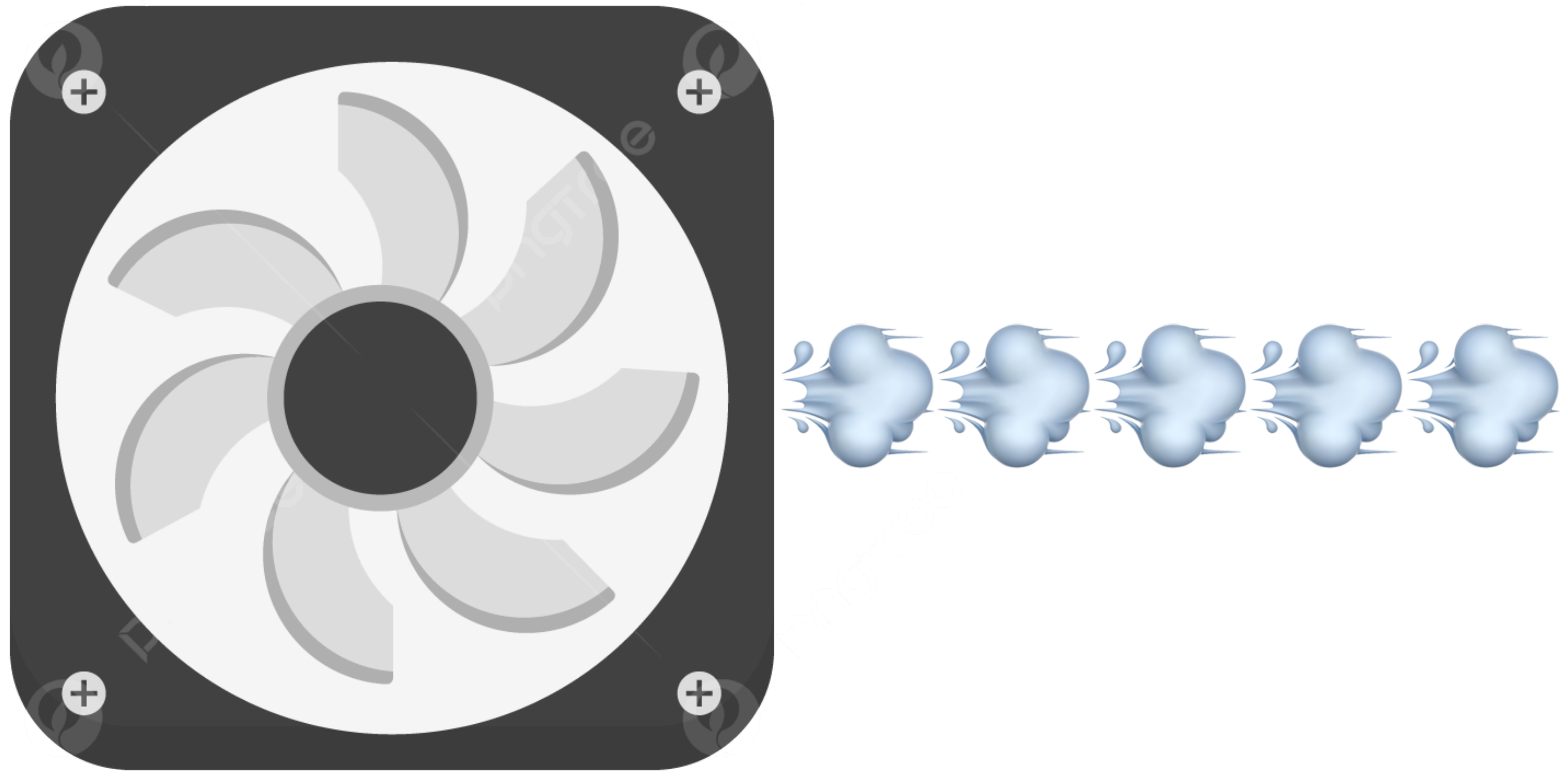
- In order to understand how to build secure systems, we should think about ways in which they are vulnerable
- Different levels of threat imply different degrees of defenses
- In general, defenses at one level of abstraction do not apply to the next level of vulnerability
- Different degrees of threat may apply to different computing contexts



Defining Side Channels

- A *side channel* describes incidental information leakage that can be inferred from observing normal execution
- How does hardware leak information?
  - Noise! 💃🕺
  - Heat (and power dissipation)! ☀️
  - Timing! ⏱️
- Adversaries need to have some notion of meaning associated with the information that is leaked by the behavior

```
for (;;) {
   // super intense computation!
}
```



Where we're going!

- If we run on multiprocessor systems where some cores might be running our programs and other cores may be running other programs…malicious guest code may be running in parallel with our current execution!
- We share hardware with all programs that run on our device, therefore the runtime behavior of my currently running programs is affected by other programs in the system
- If other programs are behaving maliciously, then they can use these shared components to create *covert channels* through which they can learn about the behavior of your program