Looking Beyond Microarchitectural-Only Side Channels

Joseph Ravichandran, MIT

ZTHA @ ICCAD 2022

$whoami

Joseph Ravichandran
1st Year PhD Student, MIT
Twitter: @0xjprx

"Meltdown & Spectre: 'Worst Ever' CPU bugs affect virtually all computers"

The Guardian

THE UARCH ICEBERG

THE UARCH ICEBERG

CACHE MISSING FOR FUN AND PROFIT

Last-Level Cache Side-Channel Attacks are Practical

DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks

Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard,
Graz University of Technology

1 **Discrete, Stateful**

Port Contention for Fun and Profit

Don't Mesh Around: Side-Channel Attacks and Mitigations on Mesh Interconnects

Miles Dai, *MIT;* Riccardo Paccagnella, *University of Illinois at Urbana-Champaign;* Miguel Gomez-Garcia, *MIT;* John McCalpin, *Texas Advanced Computing Center;* Mengjia Yan, *MIT*

2 **Stateless, contention-based**

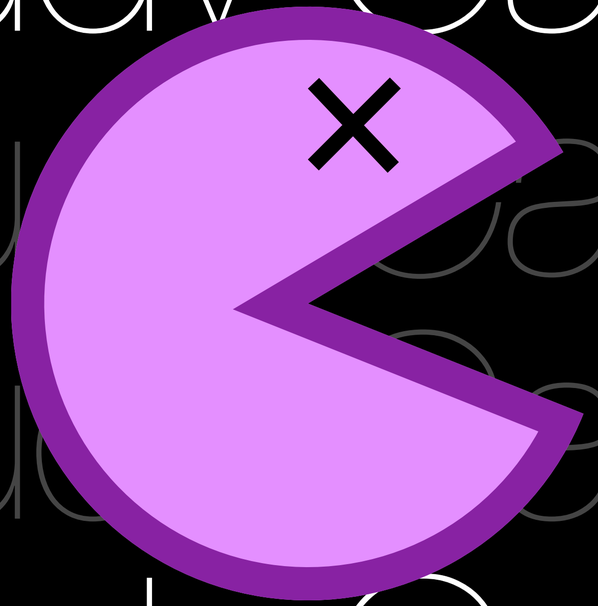
Hertzbleed: Turning Power Side-Channel Attacks Into Remote Timing Attacks on x86

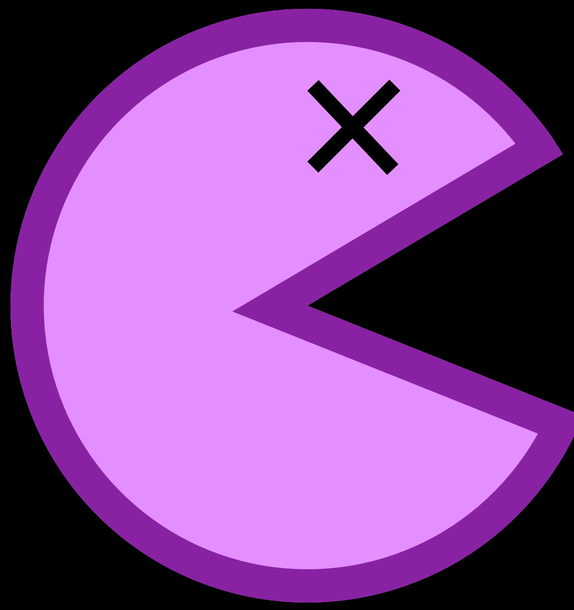
Yingchen Wang* *UT Austin*	Riccardo Paccagnella* *UIUC*	Elizabeth Tang He *UIUC*
Hovav Shacham *UT Austin*	Christopher W. Fletcher *UIUC*	David Kohlbrenner *UW*

3 **Analog**

TODAY'S LANDSCAPE

Case Study Case Study
Case Study Case Study
Case Study Case Study
Case Study Case Study
Case Study Case Study
Case Study Case Study



PA  MAN

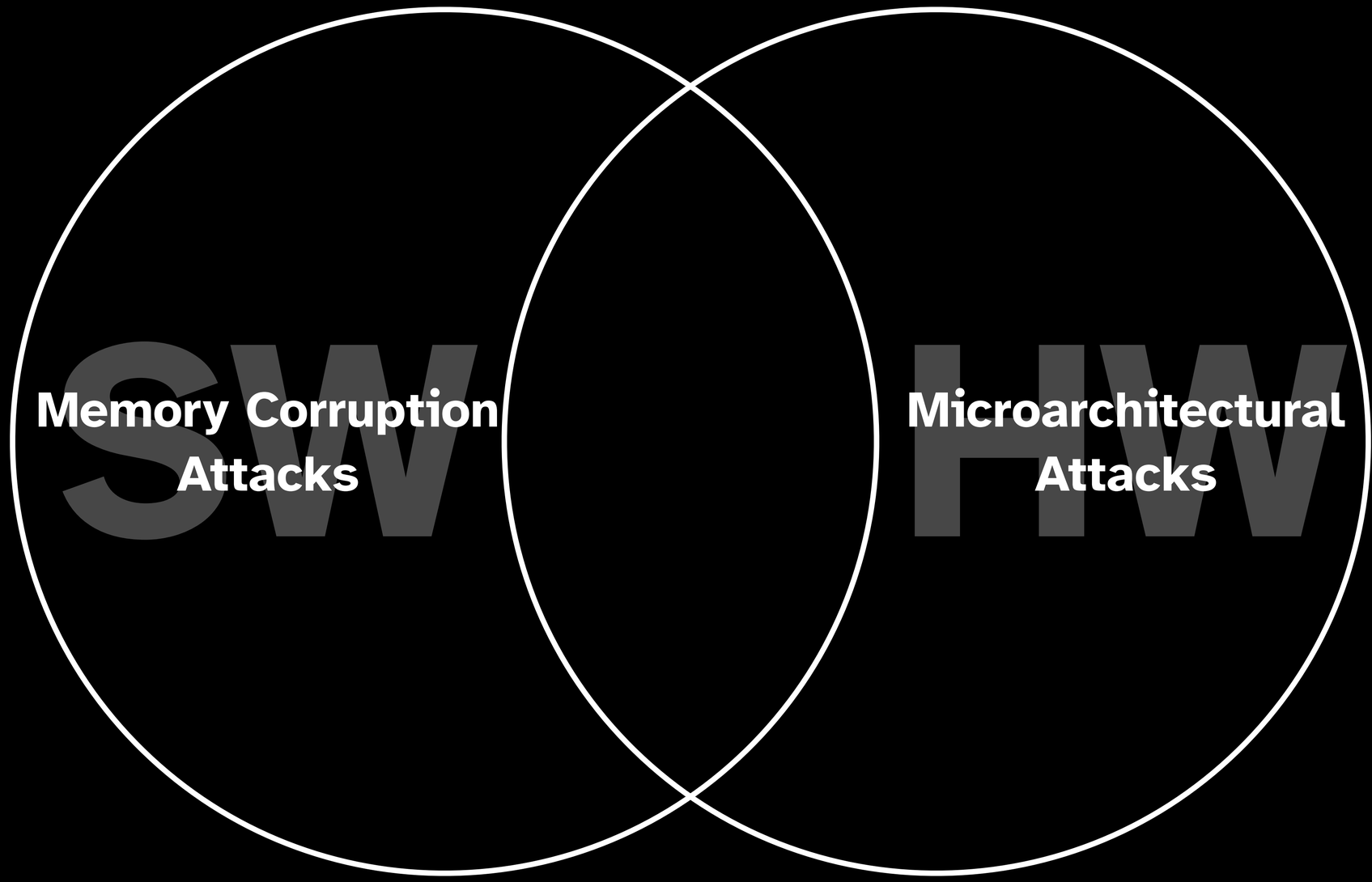
ATTACKING ARM POINTER AUTHENTICATION WITH SPECULATIVE EXECUTION

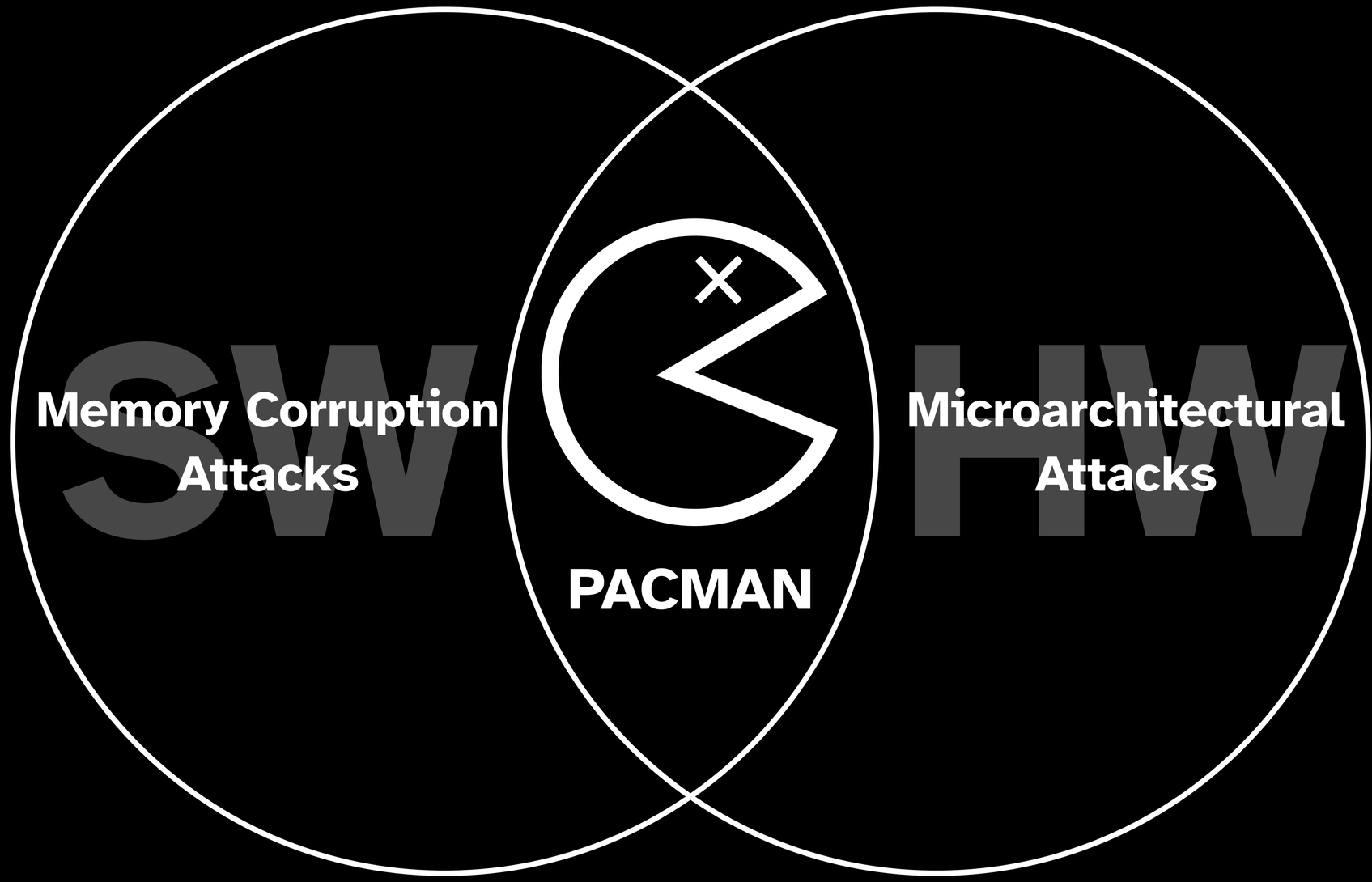
Joseph Ravichandran*, Weon Taek Na*, Jay Lang, Mengjia Yan

*Both authors contributed equally to this work.

MIT CSAIL

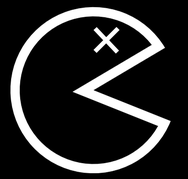
compute. collaborate. create.


SW
HW
Memory Corruption Attacks
Microarchitectural Attacks

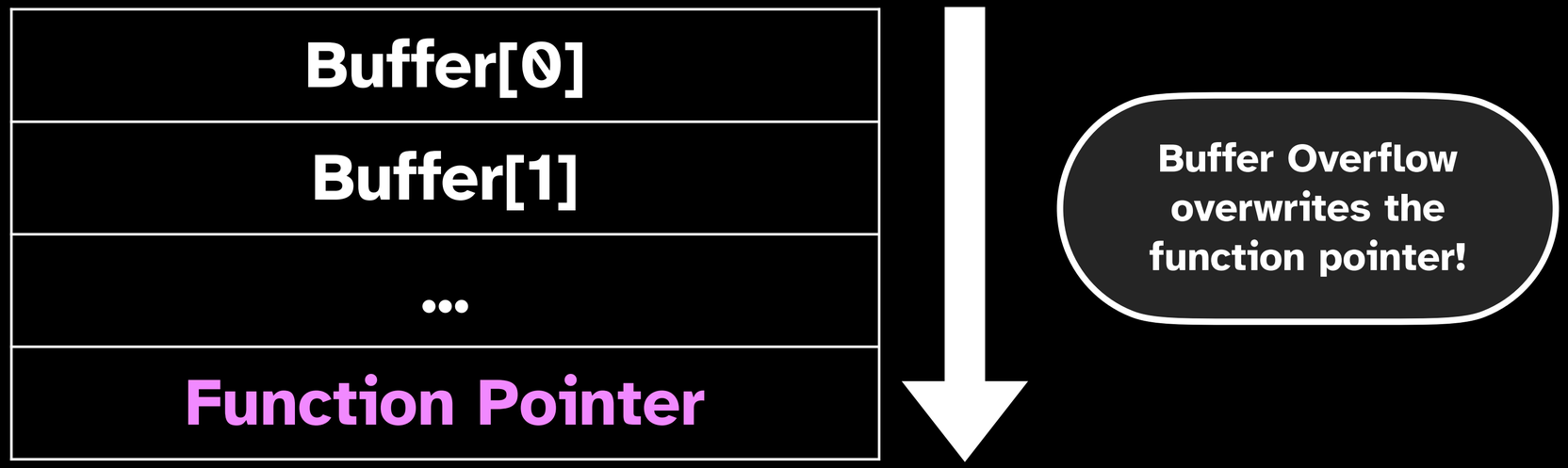

SW
HW
Memory Corruption Attacks
Microarchitectural Attacks
PACMAN

Buffer Overflow

Buffer[0]
Buffer[1]
...
Function Pointer



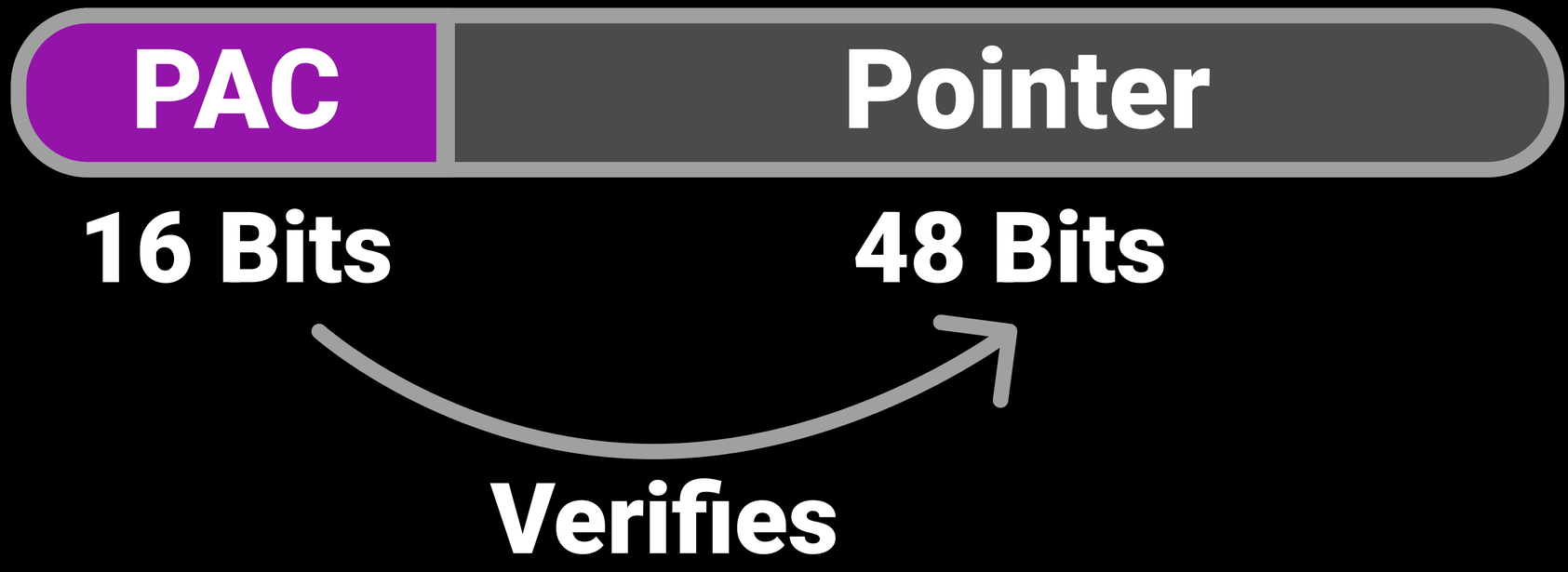
Buffer Overflow




Let's fix this bug with Pointer Authentication.

ARM Pointer Authentication

```
PAC = crypto_fn(pointer, salt, key)
```



Two Operations

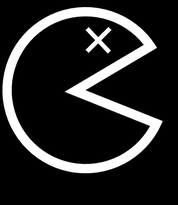
Sign

Before saving a pointer to memory, compute the PAC

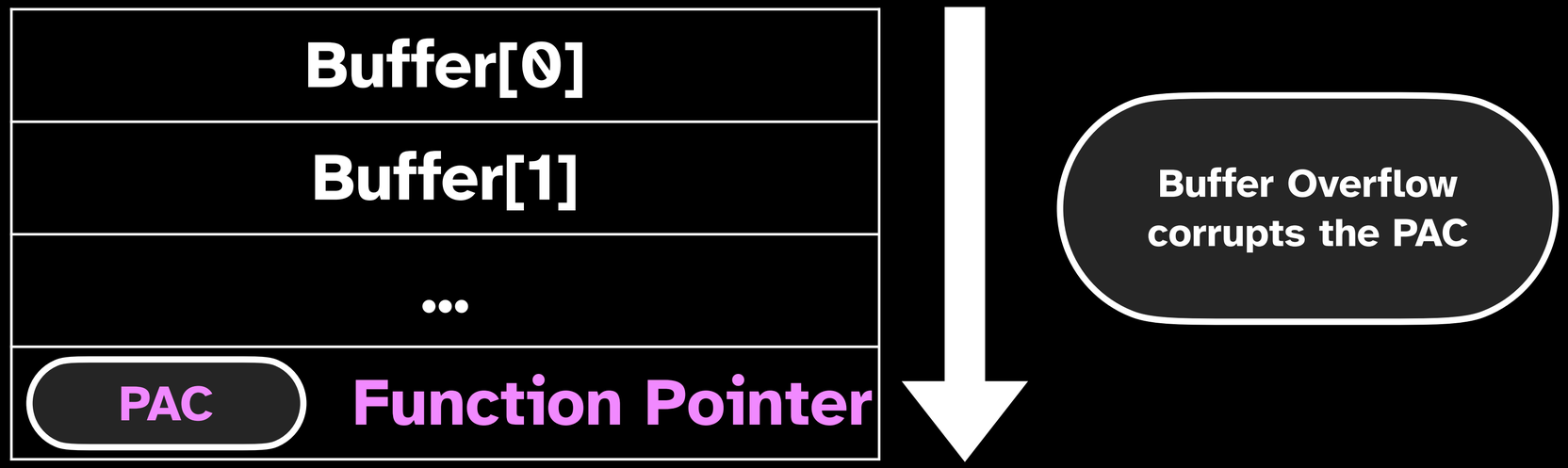
Verify

Before using a pointer, check the pointer's PAC

Buffer Overflow



Buffer Overflow



Invalid PAC means we crash!

Previous work **solely** considers memory safety threat model.

Previous work **solely** considers memory safety threat model.

PAC it up: Towards Pointer Integr
ARM Pointer Authenticati

Hans Liljestrand, *Aalto University, Huawei Technologies Oy;* Thomas Ny
Aalto University; Kui Wang, *Huawei Technologies Oy, Tampere University of T*
Carlos Chine

PTAuth: Temporal Memory
Robust Points-to Auther

Reza Mirzazade Farkhani, Mansour Ahmadi, and Long Lu, *Northeastern University*

Protecting Indirect Branches against Fault Attacks using ARM Pointer Authentication

Pascal Nasahl
Graz University of Technology
pascal.nasahl@iaik.tugraz.at

Robert Schilling
Graz University of Technology
robert.schilling@iaik.tugraz.at

Stefan Mangard
Graz University of Technology
Lamarr Security Research
stefan.mangard@iaik.tugraz.at

Hardware-based Always-On Heap Memory Safety

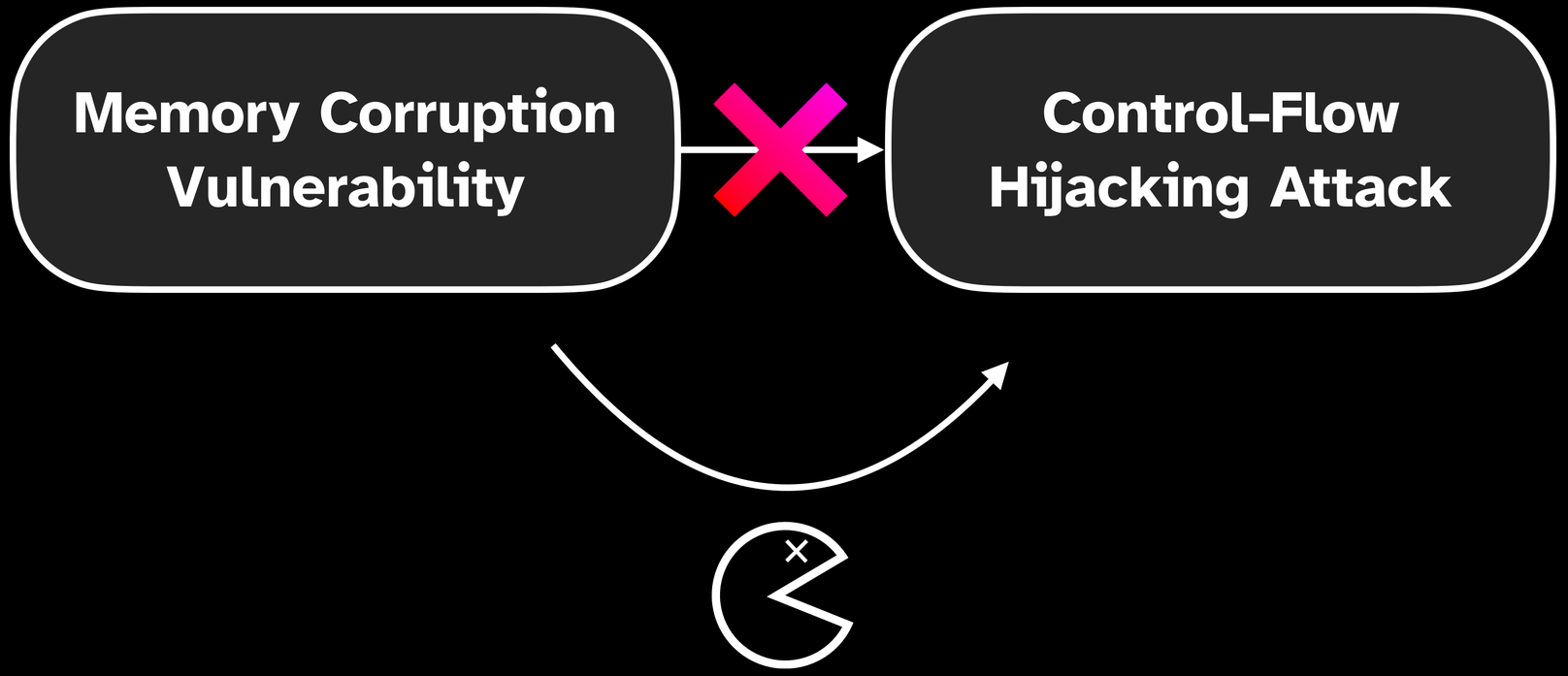
Yonghae Kim
Georgia Institute of Technology
yonghae@gatech.edu

Jaekyu Lee
Arm Research
jaekyu.lee@arm.com

Hyesoon Kim
Georgia Institute of Technology
hyesoon@cc.gatech.edu

Memory Corruption

Pointer Authentication
is the last line of defense

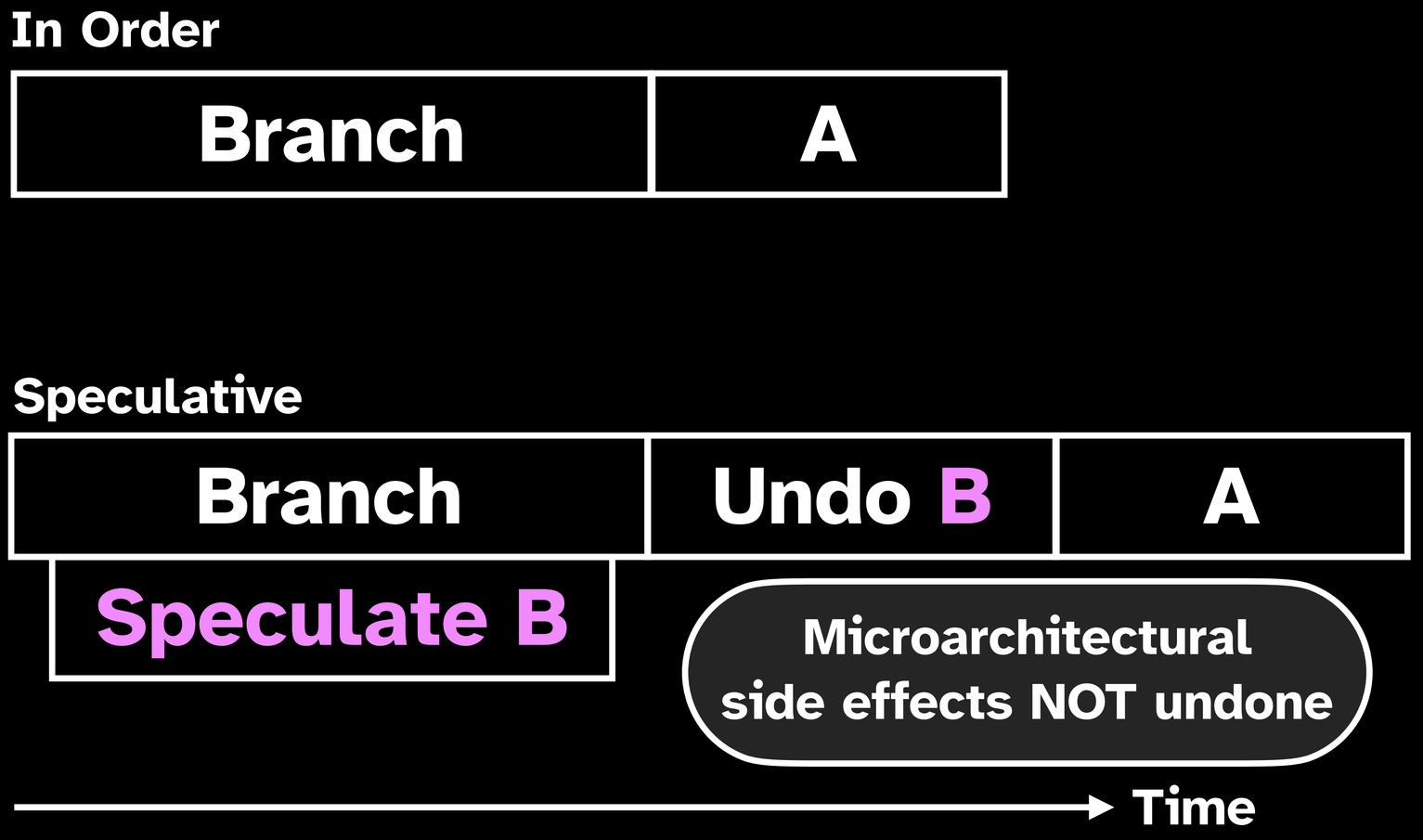


Break PAC with Hardware Attacks

- Guess a PAC **speculatively** to prevent crashes
- Leak verification results via side channel

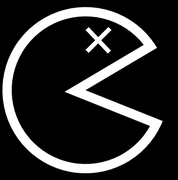
Speculative Execution

```
if (true)
    A
else
    B
```



Data Gadget

```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

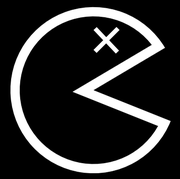


Data Attack

```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch →



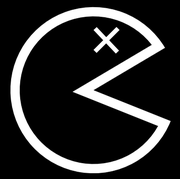
Data Attack

```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch →

PAC Check Succeeds

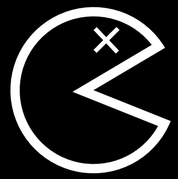


Data Attack

```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch → PAC Check Succeeds → Speculative **Load!** ✓



Data Attack

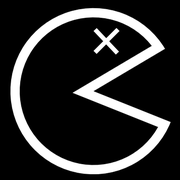
```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch → PAC Check Succeeds → Speculative Load!

Incorrect PAC

Mispredict Branch →



Data Attack

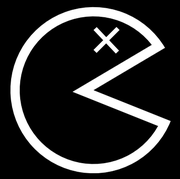
```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch → PAC Check Succeeds → Speculative **Load!** ✓

Incorrect PAC

Mispredict Branch → PAC Check Fails



Data Attack

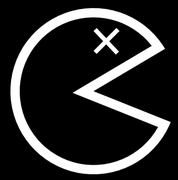
```
if (condition):
  verified_ptr = check_pac(guess_ptr)
  load(verified_ptr)
```

Correct PAC

Mispredict Branch → PAC Check Succeeds → Speculative **Load!** ✓

Incorrect PAC

Mispredict Branch → PAC Check Fails → Speculative **Exception** ✗



TARGET

The world's first desktop CPU
that supports Pointer Authentication.

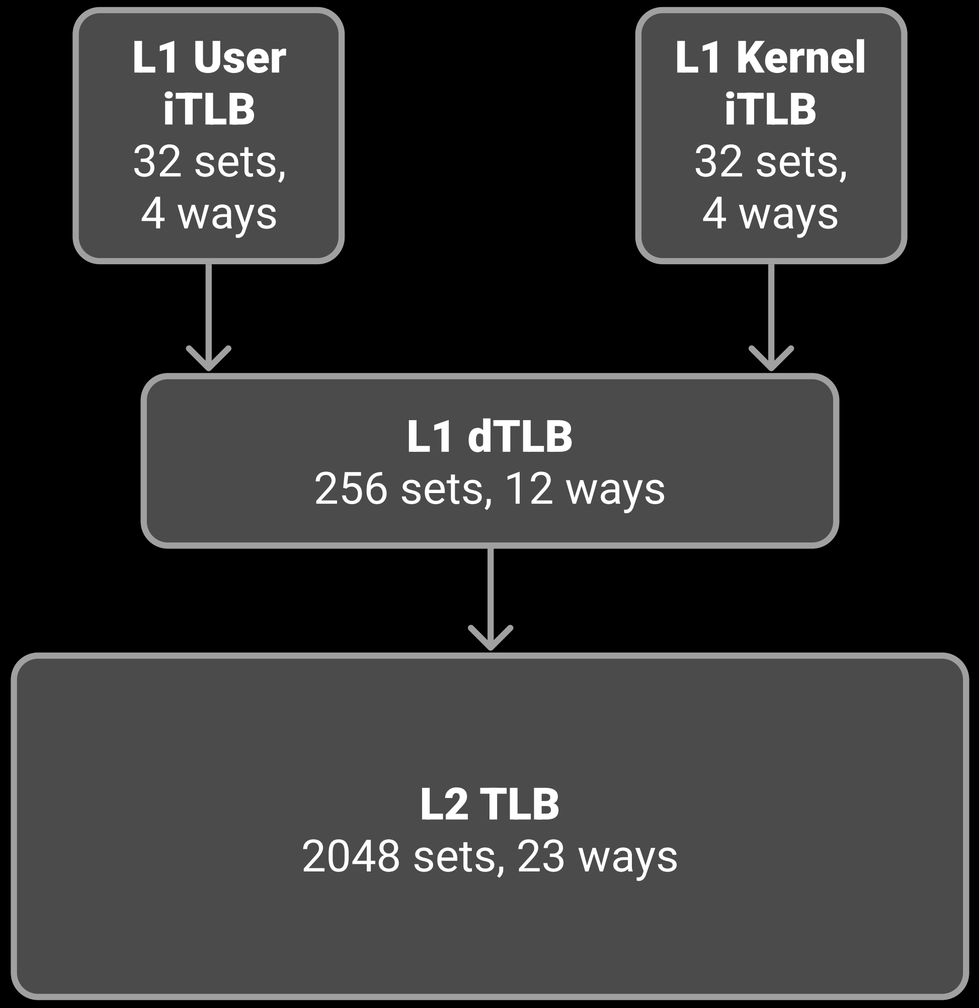
Image: Apple ("Apple Unleashes M1")

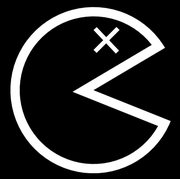
Challenges of Real World HW

- No documentation of microarchitectural details.
- No high resolution timer.
- macOS is a difficult system to integrate attacks on.

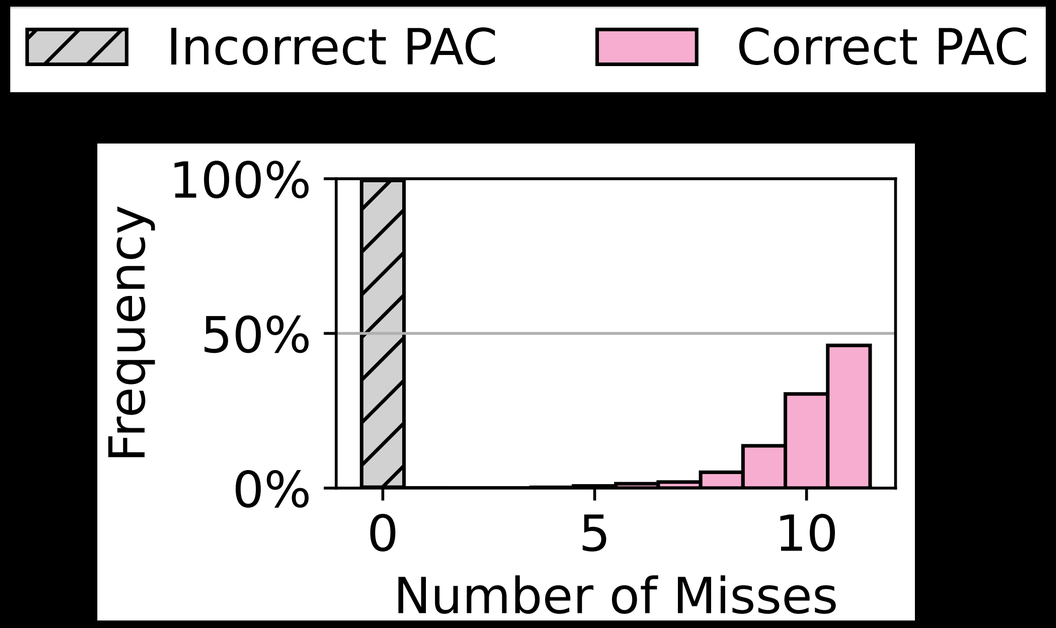
Essentially, we had to reinvent the wheel.

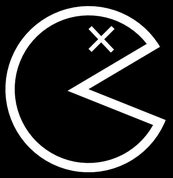
Conjectured TLB Hierarchy





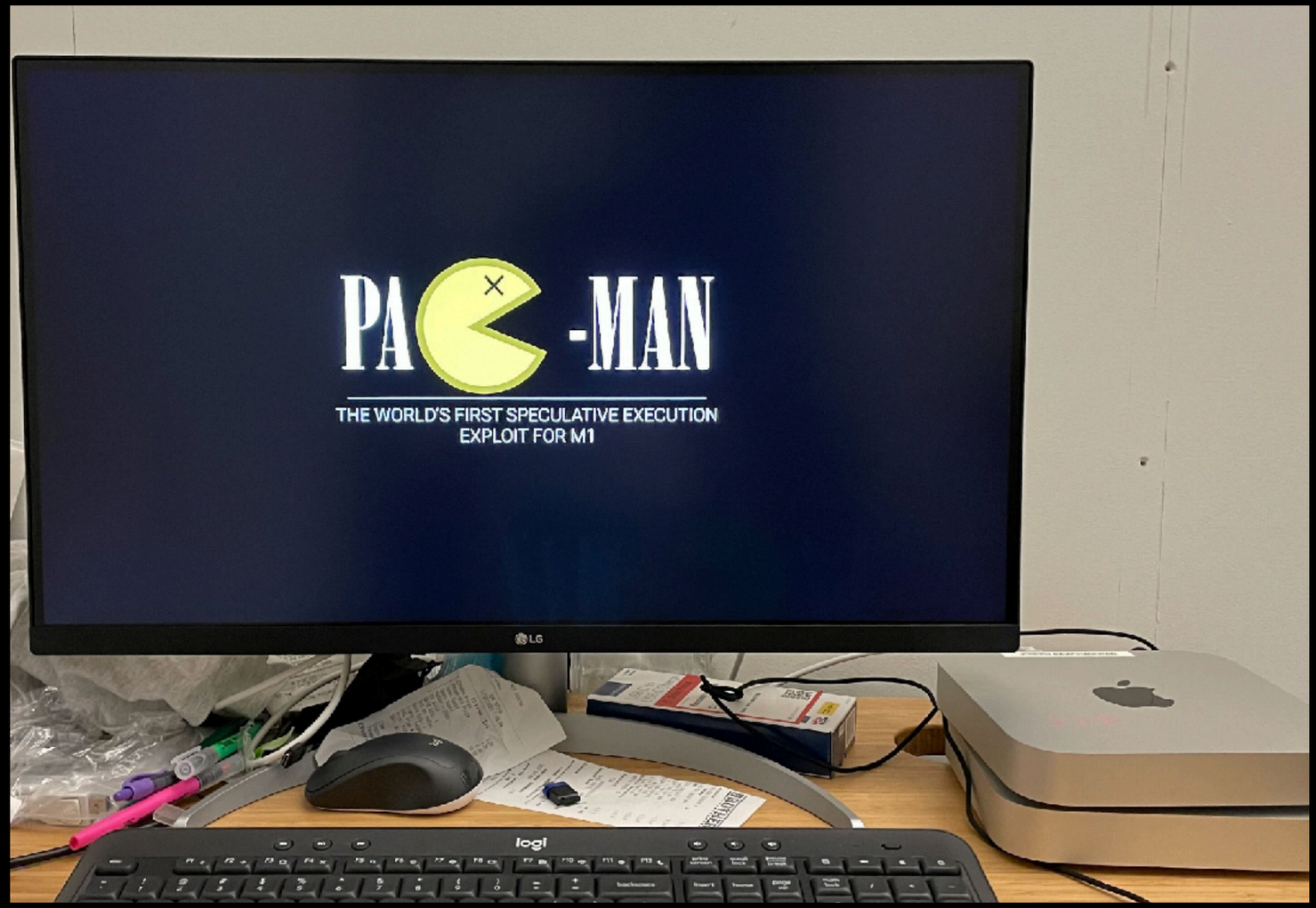
PAC Oracle Accuracy

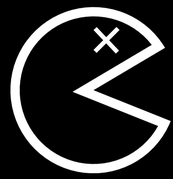




PacmanOS

A Rust-based bare metal
environment for performing experiments.





Top news

digitaltrends

The M1 has a big security loophole, and Apple can't patch it

4 hours ago

TechCrunch

MIT researchers uncover 'unpatchable' flaw in Apple M1 chips

51 minutes ago

HARDWARE

MIT Finds New Arm Vulnerability Present in Apple M1, Demos PACMAN Attack

4 hours ago

9TO5Mac

PACMAN M1 chip attack defeats 'the last line of security' – but requires physical access

2 hours ago

All coverage

Phoronix

Apple M1 Affected By "PACMAN" Hardware Vulnerability In Arm Pointer Authentication

4 hours ago

VentureBeat

MIT researchers discover Apple M1 chip vulnerability

3 hours ago

The Register

Apple M1 chip contains hardware vulnerability that bypasses memory defense

4 hours ago

DARKReading

Design Weakness Discovered in Apple M1 Kernel Protections

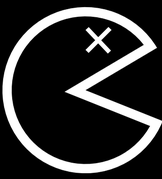
3 hours ago

Macworld

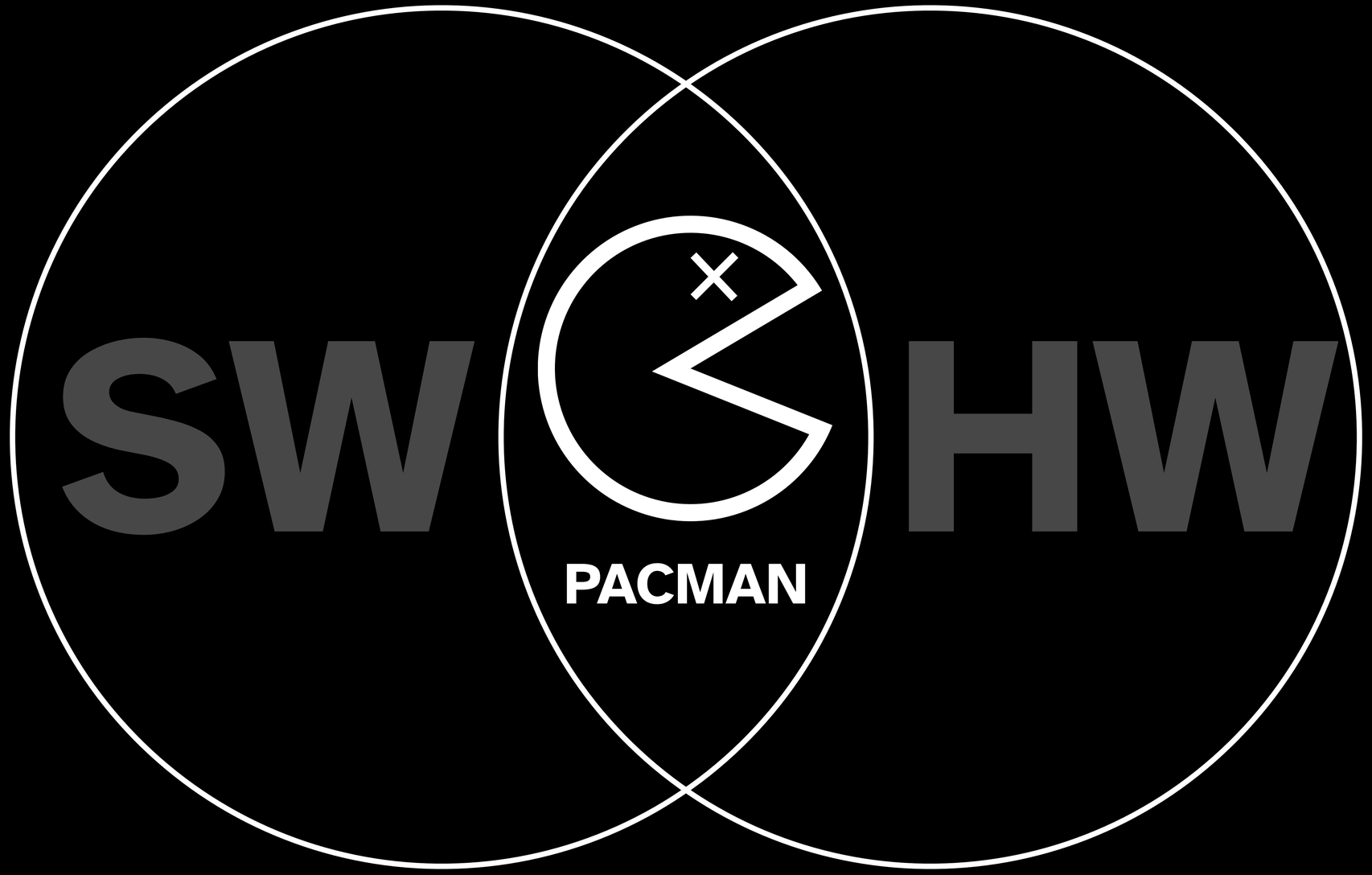
Experts warn of 'PACMAN' flaw in M1 chip that can't be patched

1 hour ago

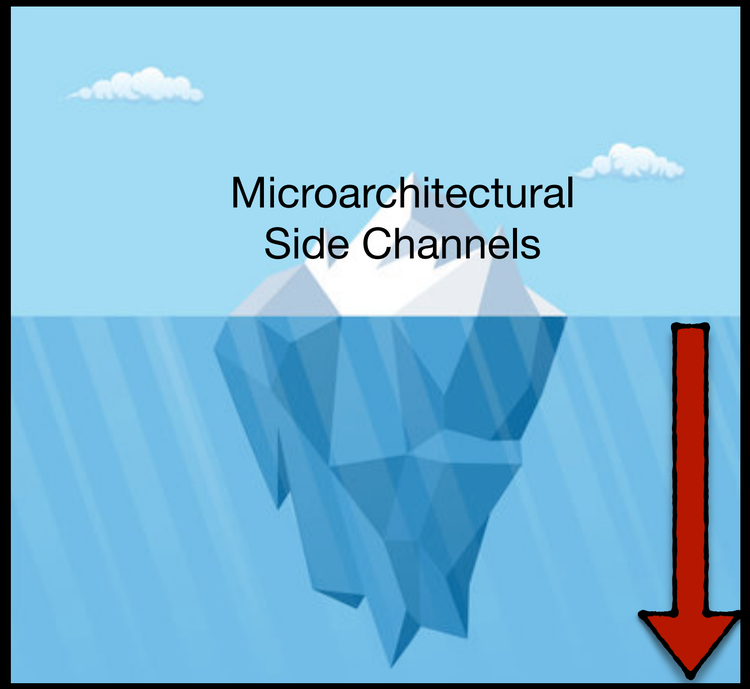
PACMAN @ DEF CON 30

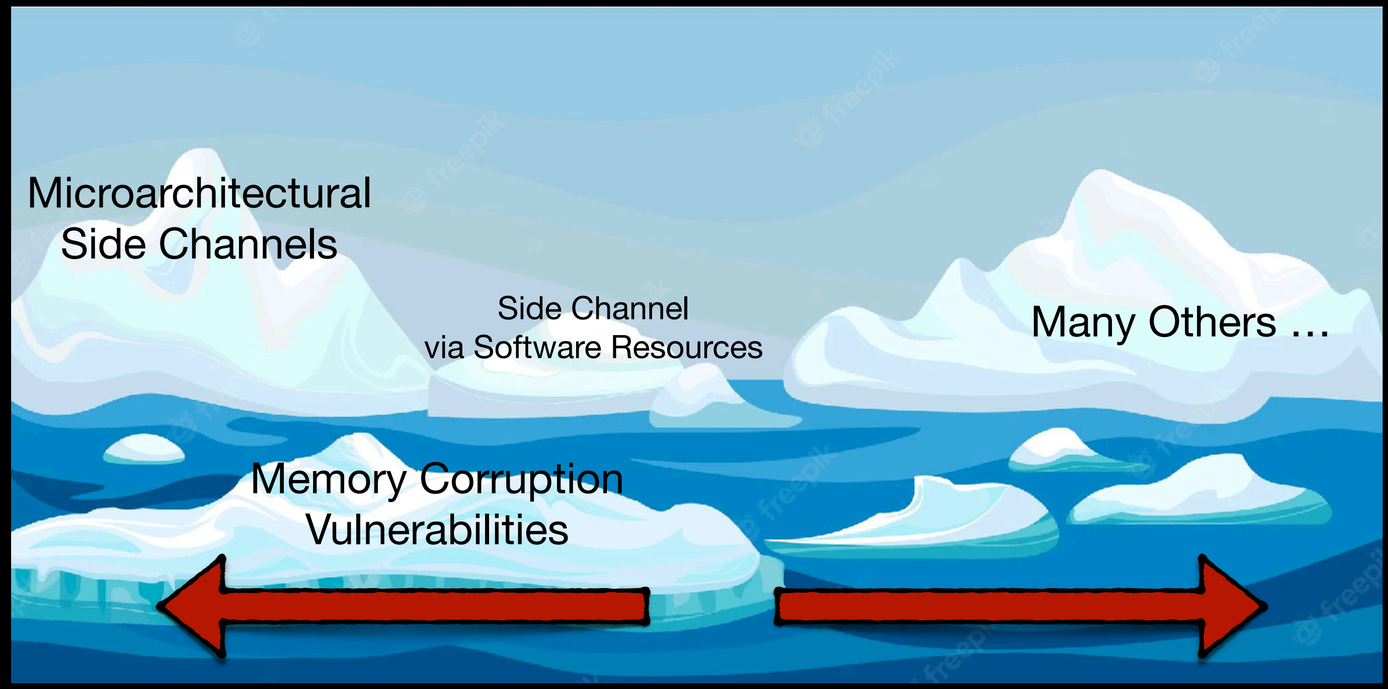


PACMAN: Attacking ARM Pointer Authentication with Speculative Execution



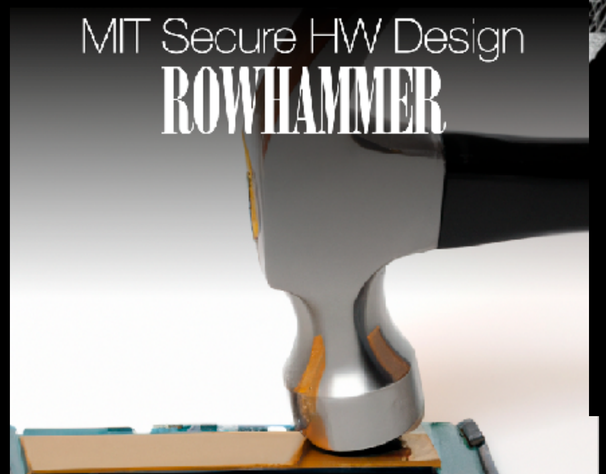
Takeaway: **New threats** arising from compound threat models

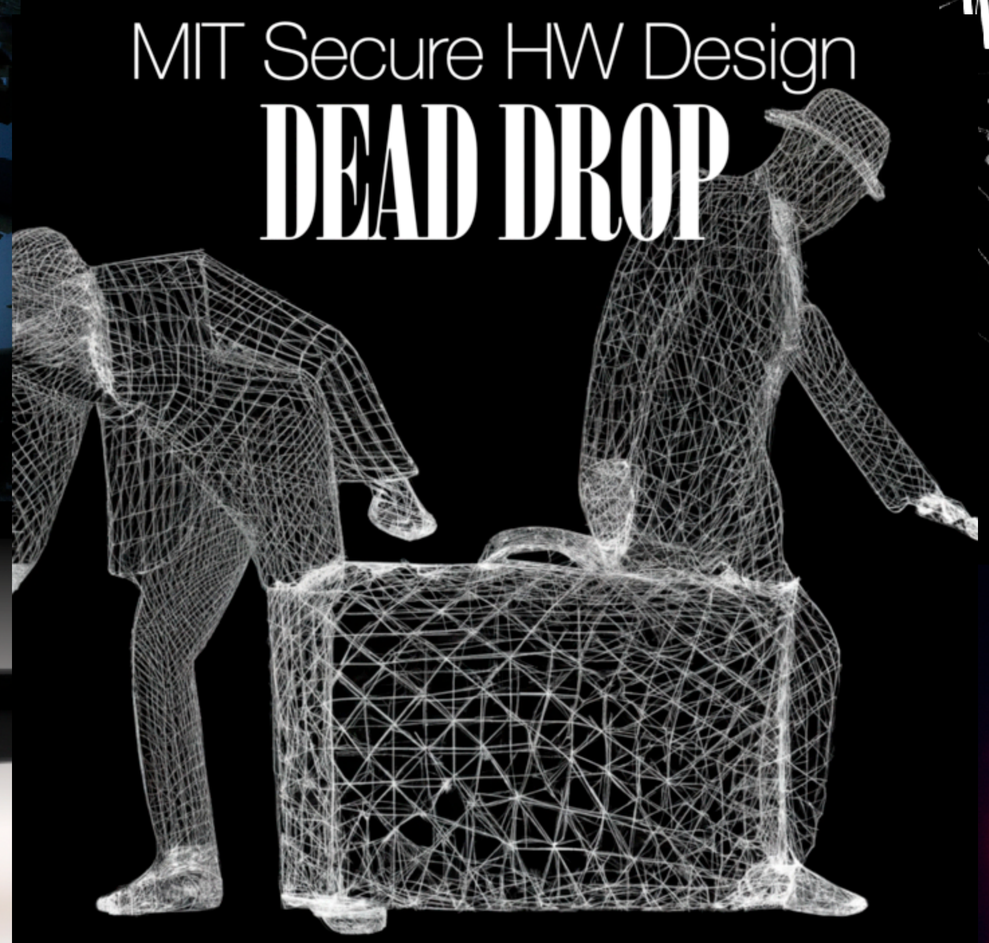


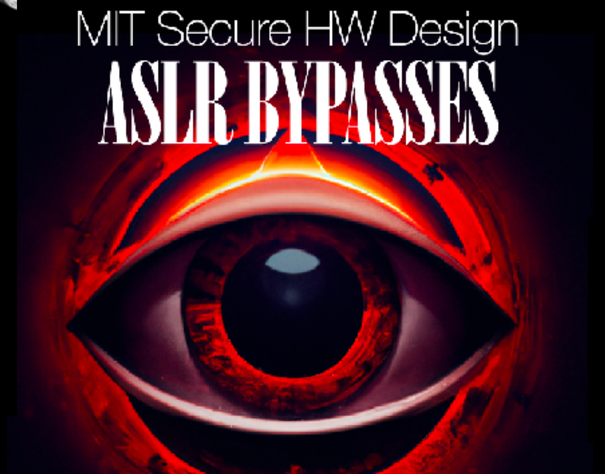


Learning CPU Architecture for fun

http://csg.csail.mit.edu/6.888Yan/for_instructors/

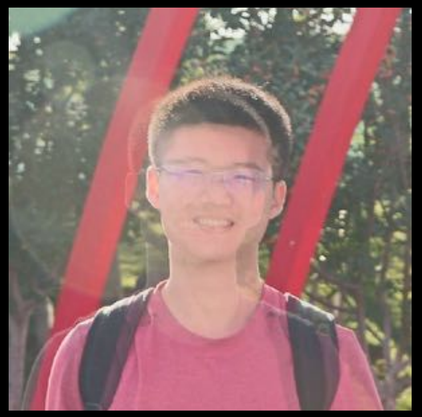






The **Dream Team**

Peter Deutsch



Yuheng Yang

Joseph Ravichandran

Mengyuan Li

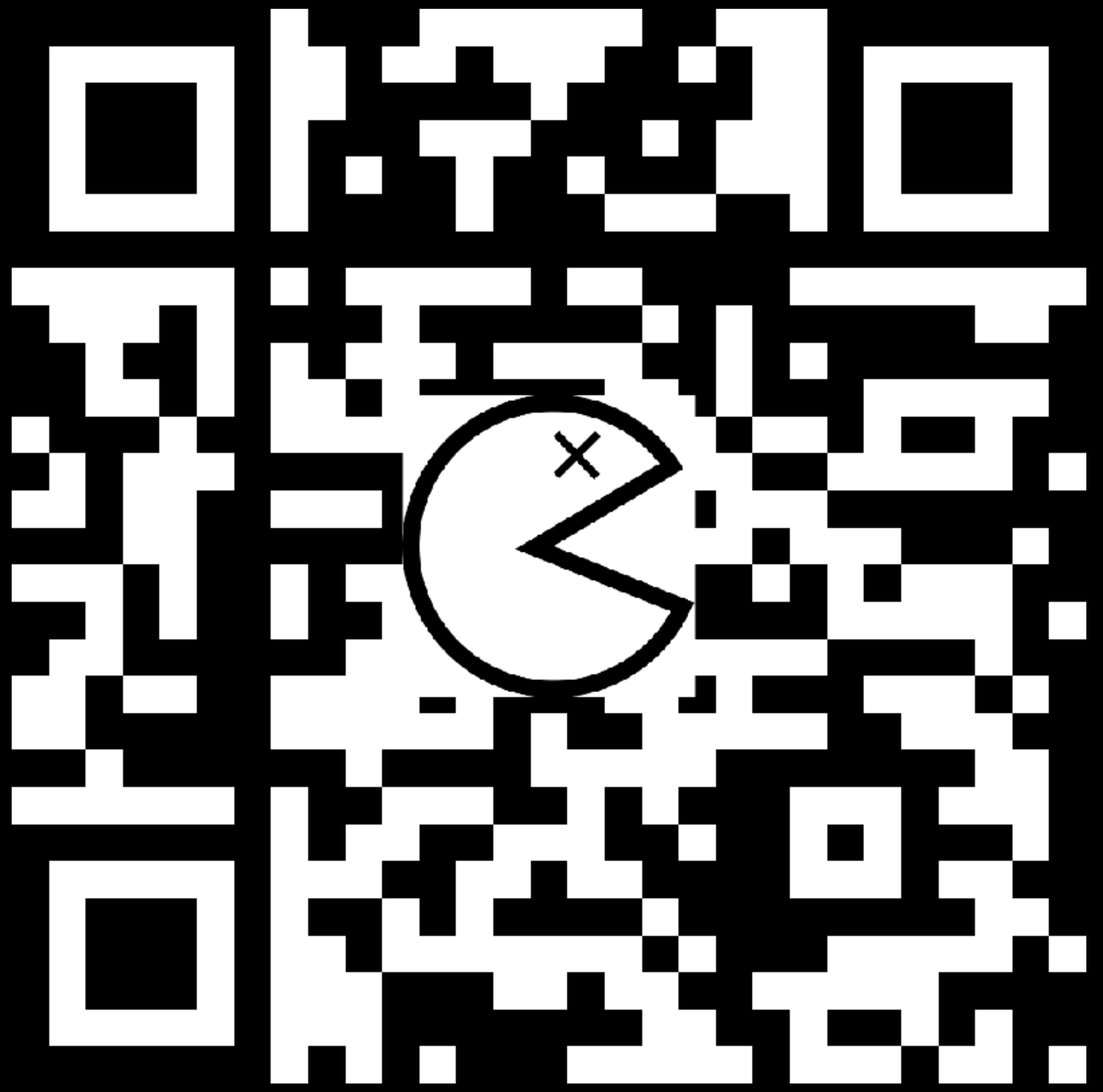
Jules Drean

Shixin Song

Jack Cook

Miguel Gomez-Garcia

Follow me on Twitter!



PACMANATTACK.COM

MIT CSAIL

compute. collaborate. create.