Comp 590-184:
Hardware Security and Side-Channels

Introduction

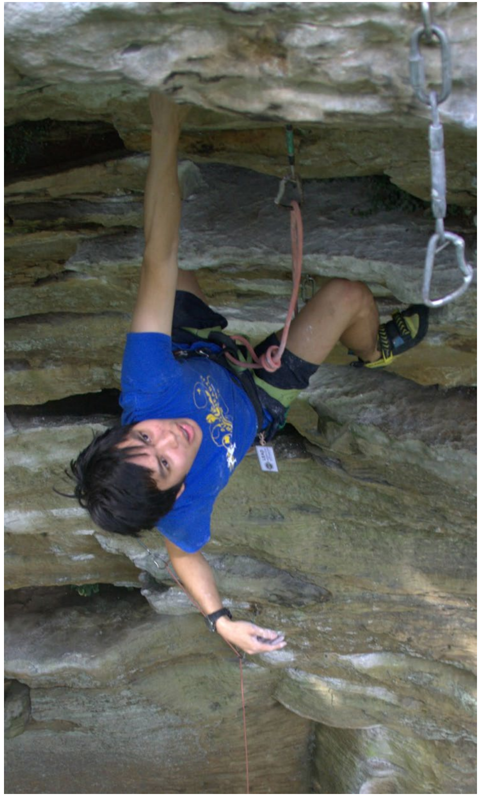
January 8, 2026
Andrew Kwong

Department of Computer Science

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Today’s Class

- Introductions
- Course Goals
- Course Structure
- Intro to Side-Channels



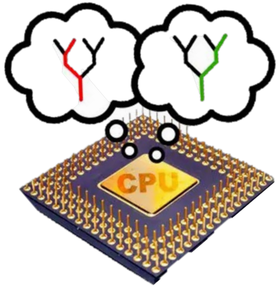
Who am I?

- Andrew Kwong
  - Assistant Professor

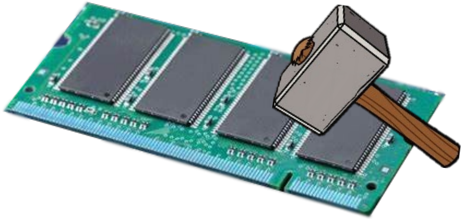
- Site: https://andrewkwong.org
- Email: andrew@cs.unc.edu
- Office: FB 340
- Office Hours: TBA

My Research

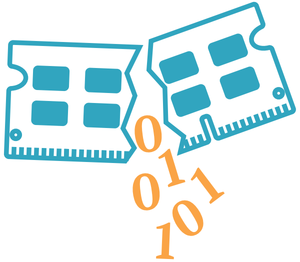
- Side-Channels:
  - Memory
  - CPU
  - Applied-crypto



CacheOut



Rowhammer



RAMBleed

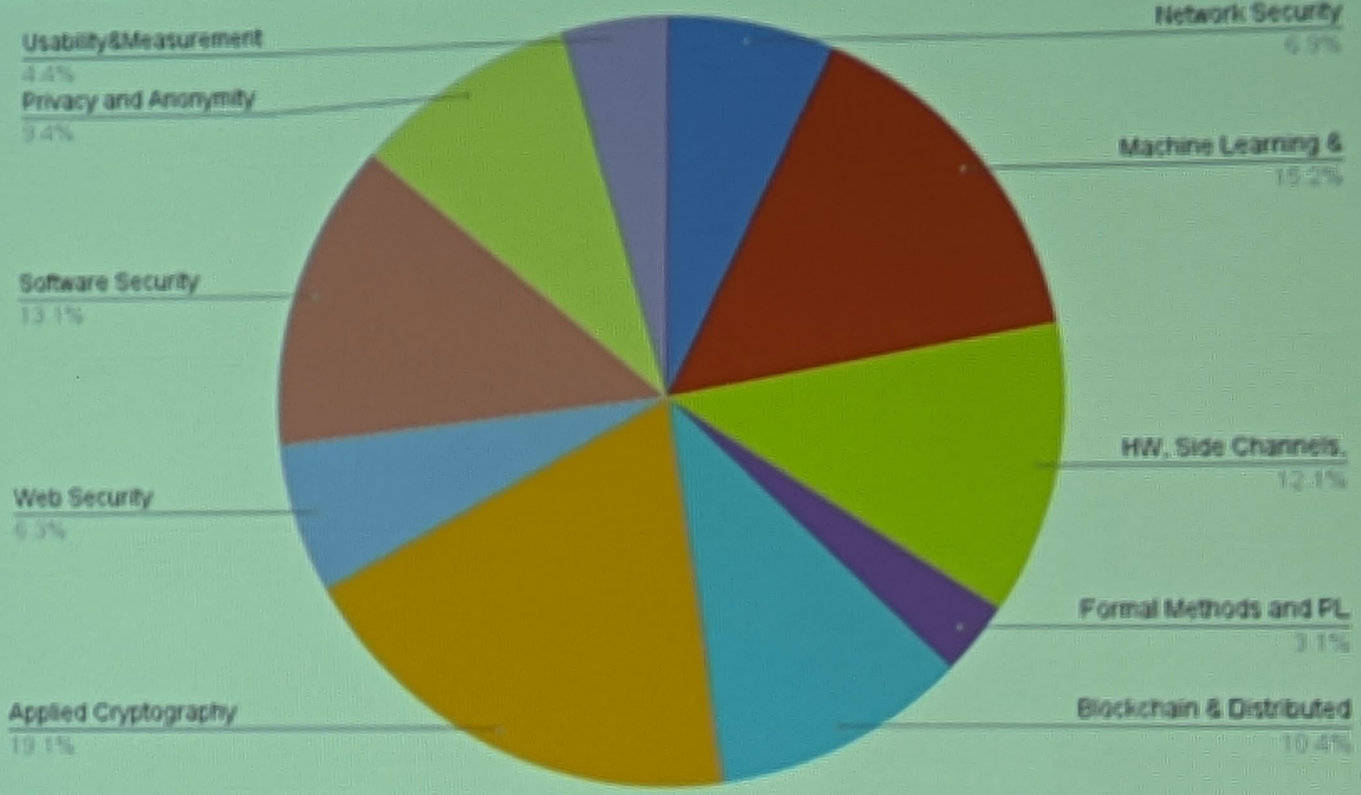
Your TA

- Yichang Hu
  - 3rd year PhD student
- Office Hours: TBA

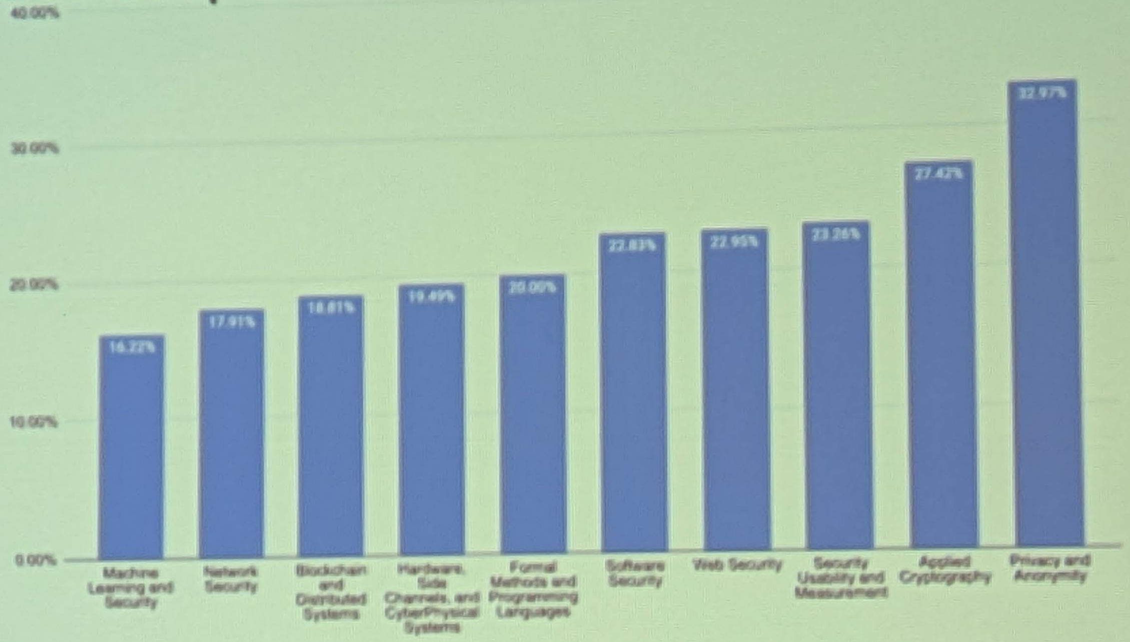
Course Goals

- Get hands-on experience with side-channel attacks
  - Develop real-world attacks against real hardware
    - No simulations
  - Learn how to defend against these attacks
  - Build toolkit for side-channel/hardware security research
  - Improve core CS skills
    - Architecture
    - Operating systems

ack Submissions



ack Acceptance Rates



Course Structure

Structure

- Course meetings will be lectures
- Lab Assignments
  - Programming based assignments leading towards real-world attacks on actual hardware
  - Putting theory into practice
- One final exam

Grading

- Lab Assignments– 80%
- Final Exam – 20%

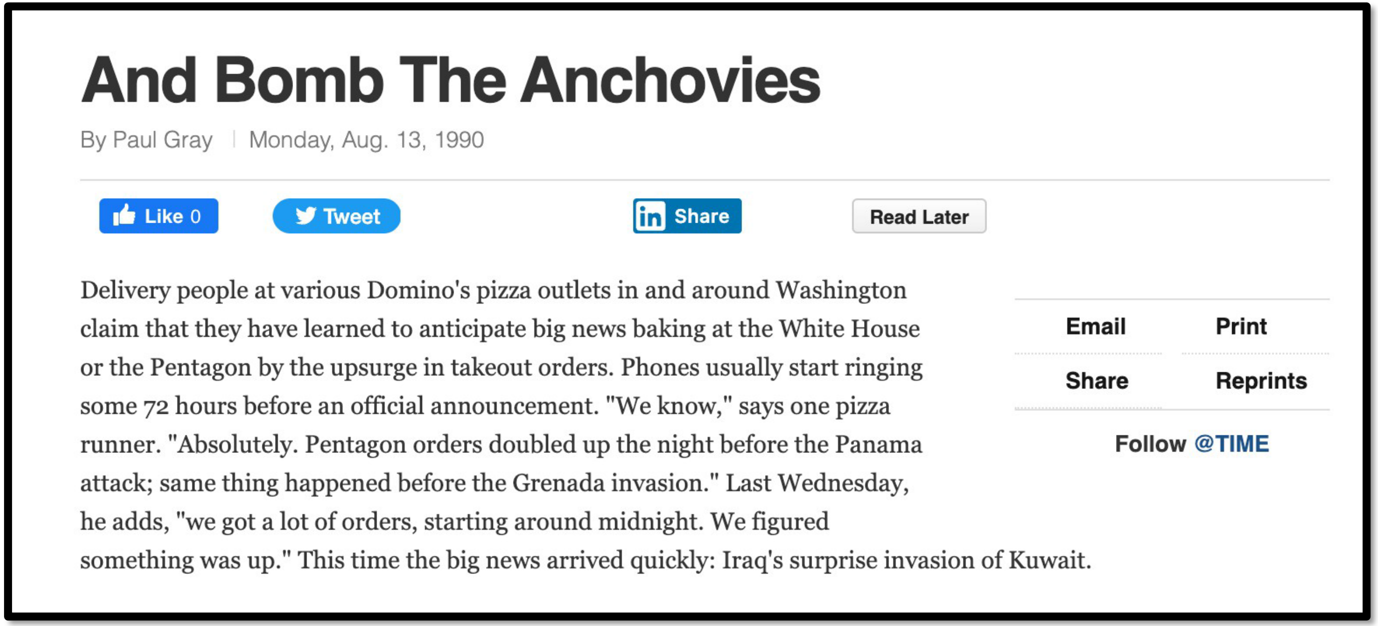
Lab Assignments(80%)

- 5-6 “CTF-style” labs
  - C crash course
  - Website fingerprinting
  - cache side-channels
  - Spectre attacks
  - Rowhammer
  - Speculative attack for ASLR break
- Work in teams of 3-4
- Discussing with classmates is allowed
  - Your team must write your own code
- AI is allowed!
  - Please include your prompts
- All assignments submitted on canvas
  - Late submissions lose 10% per day

Final Exam (20%)

- Test your understanding of the high level concepts
  - Lectures
  - Lab assignments

What are Side-Channels?

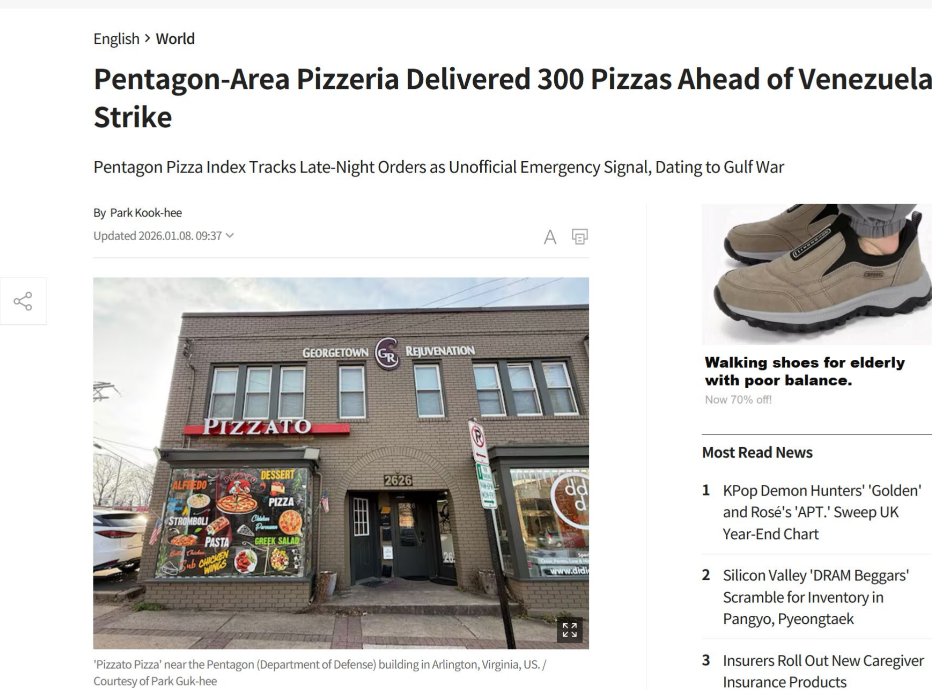


And Bomb The Anchovies

By Paul Gray | Monday, Aug. 13, 1990

Delivery people at various Domino's pizza outlets in and around Washington claim that they have learned to anticipate big news baking at the White House or the Pentagon by the upsurge in takeout orders. Phones usually start ringing some 72 hours before an official announcement. "We know," says one pizza runner. "Absolutely. Pentagon orders doubled up the night before the Panama attack; same thing happened before the Grenada invasion." Last Wednesday, he adds, "we got a lot of orders, starting around midnight. We figured something was up." This time the big news arrived quickly: Iraq's surprise invasion of Kuwait.

By making indirect observations (the number of pizzas ordered), one is able to infer partial information



English > World

Pentagon-Area Pizzeria Delivered 300 Pizzas Ahead of Venezuela Strike

Pentagon Pizza Index Tracks Late-Night Orders as Unofficial Emergency Signal, Dating to Gulf War

By Park Kook-hee

Updated 2026.01.08. 09:37

'Pizzato Pizza' near the Pentagon (Department of Defense) building in Arlington, Virginia, US. / Courtesy of Park Guk-hee

Most Read News

1 KPop Demon Hunters' 'Golden' and Rosé's 'APT.' Sweep UK Year-End Chart

2 Silicon Valley 'DRAM Beggars' Scramble for Inventory in Pangyo, Pyeongtaek

3 Insurers Roll Out New Caregiver Insurance Products

Safe Cracking

- Should be secure, given enough combinations

Imperfections in the implementation indirectly leak information

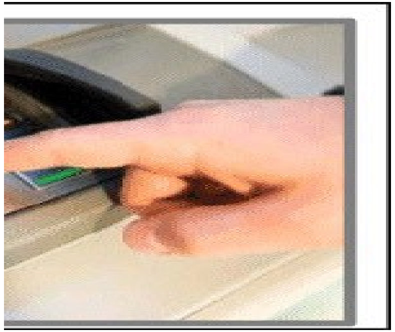
EM Side-Channels

- Tempest paper written in 1972 (top secret)
- Standards for shielding sensitive equipment
  - Monitor contents can be recovered from EMR
- Researchers have demonstrated:
  - Stealing all kinds of cryptographic keys
  - fingerprinting

Acoustic Side Channels

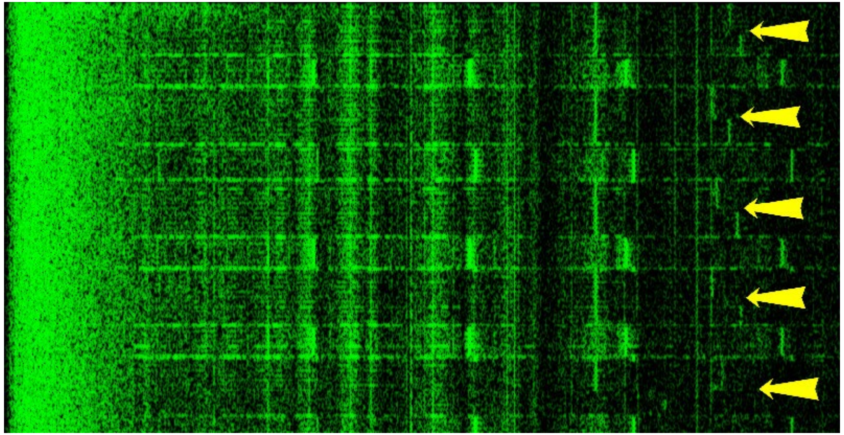
- Monitor keystroke
  - You only need: a cheap microphone + an ML model

- Other sources of acoustic side channels inside a computer?

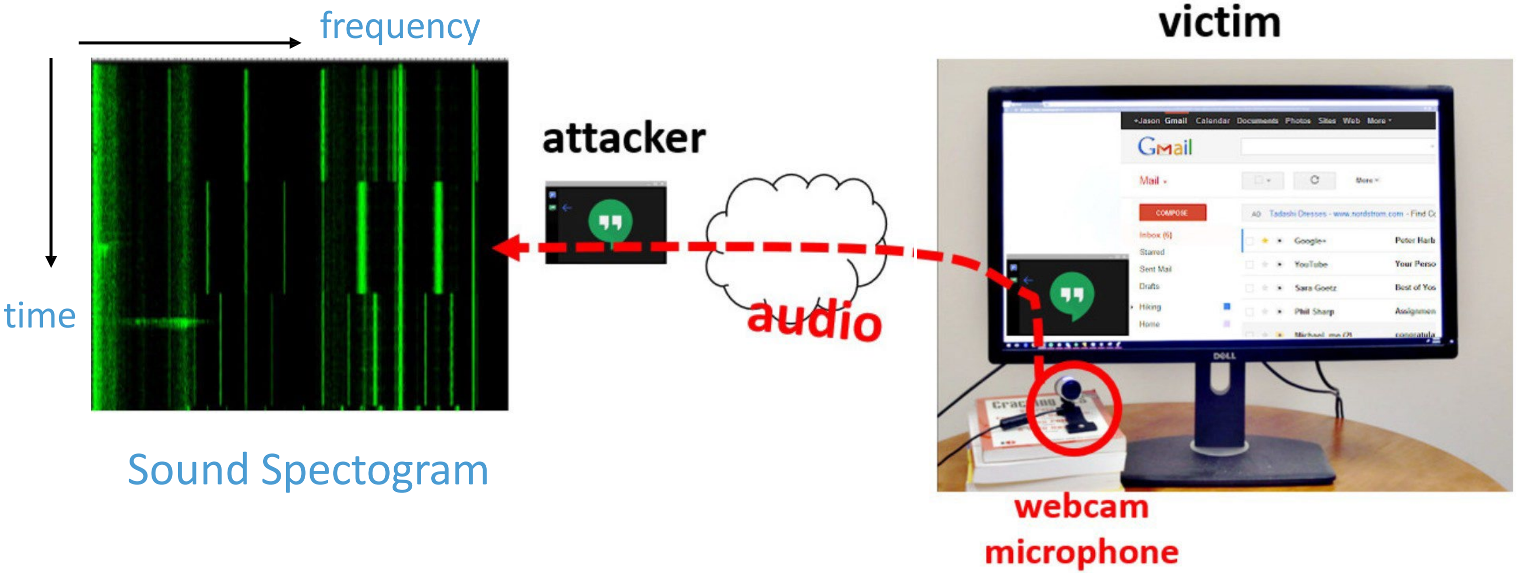


Acoustic Cryptanalysis

- Ceramic capacitors also leak
- Different operations on the CPU create different sounds
- Can extract RSA key from GPG!



“Hear” The Screen



frequency

time

attacker

audio

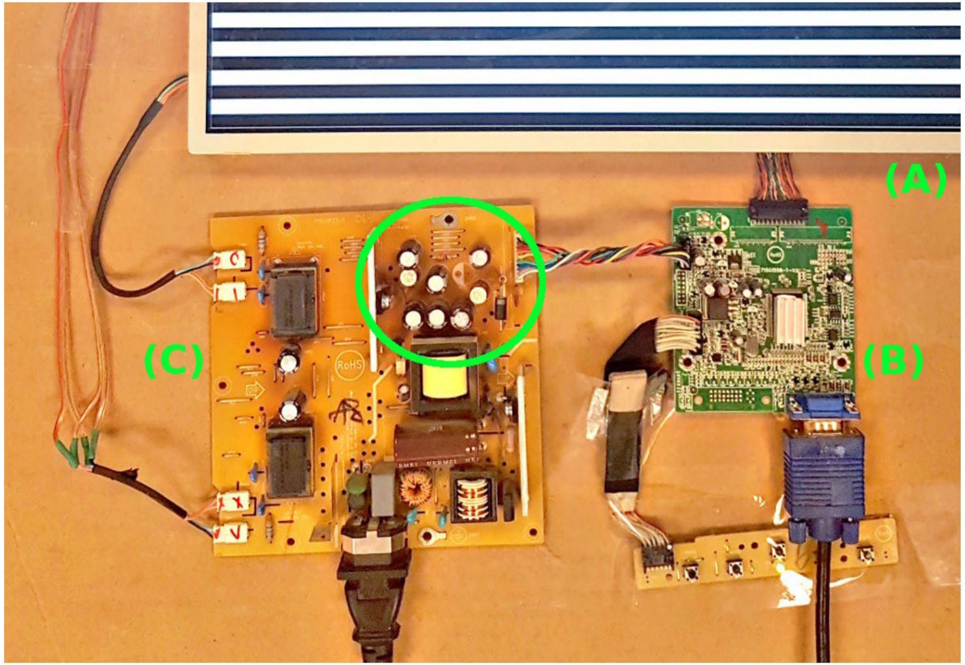
victim

webcam
microphone

Sound Spectogram

Genkin et. al. Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels. S&P’19

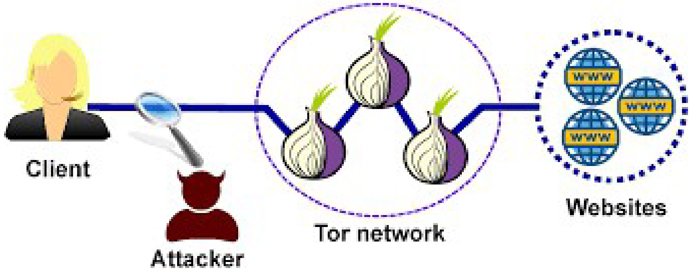
“Hear” The Screen



(A) is the LCD panel, (B) is the screen’s digital logic and image rendering board and, (C) is the screen’s power supply board.

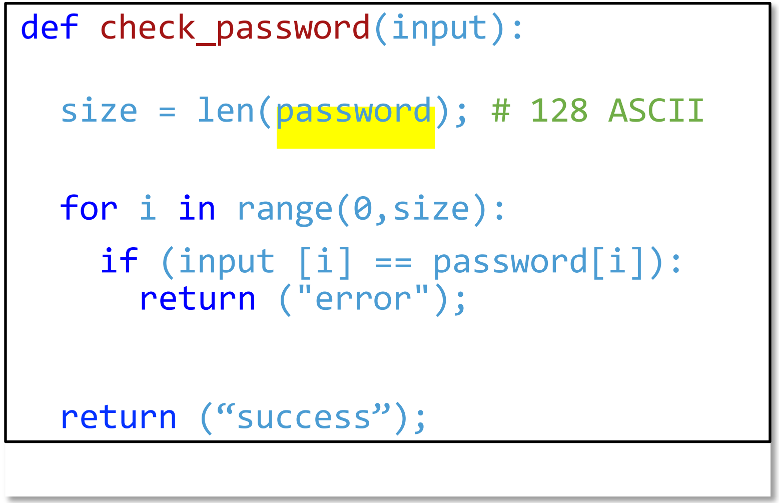
Network Side Channels

- Website Fingerprinting
  - Frequency of packets, size of packets
  - Response dependent:
    - iSideWith.com
  - Real-time feedback:
    - Google Search auto-complete



Lescisin et. al. Tools for Active and Passive Network Side-Channel Detection for Web Applications. WOOT'18
Cai et. al. Touching from a distance: Website fingerprinting attacks and defenses. CCS'12.

Timing Side Channel



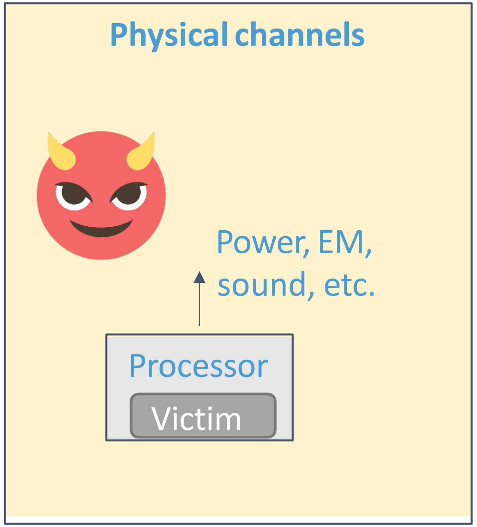
```
def check_password(input):

  size = len(password); # 128 ASCII

  for i in range(0,size):
    if (input [i] == password[i]):
      return ("error");


  return (“success”);
```

- How many attempts does the attacker need to crack the password?
- Can we reduce the number of attempts? How?
- Numerous timing side-channels have also been demonstrated against cryptographic algorithms

Covert Channels vs Side Channels

- Gather information by measuring or exploiting **indirect** effects of the system or its hardware -- rather than targeting the program or its code directly.
- Covert channel:
  - **Cooperated/Intended** communication between two or more security parties
  - Sender and receiver are cooperating
- Side channel:
  - **Unintended** communication between two or more security parties
  - Receiver is not cooperating
- In both cases:
  - Communication should not be possible, following system semantics
  - The communication medium is not designed to be a communication channel
  - Imperfection in the *implementation* leaks information

A Rough Classification based on What Attackers Can Observe



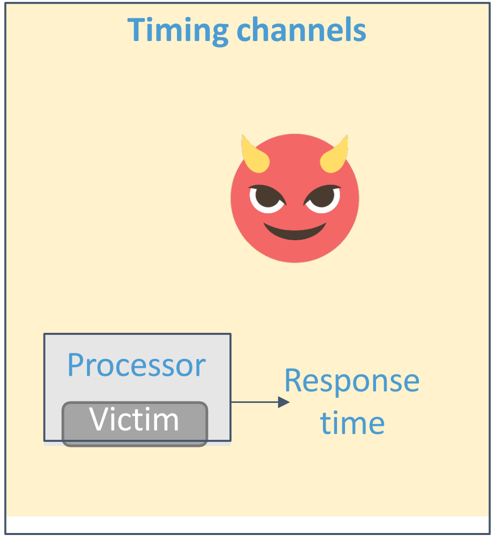
Physical channels

Power, EM, sound, etc.

Processor

Victim

Attacker requires measurement equipment ➔ physical access



Timing channels

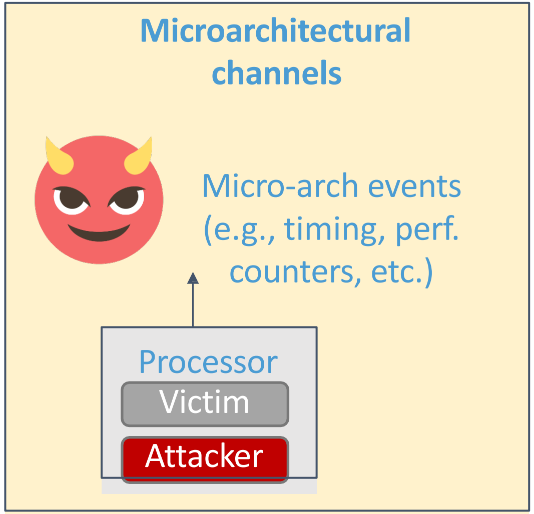
Processor

Victim

Response time

Attacker may be remote (e.g., over an internet connection)

Requires shared hardware



Microarchitectural channels

Micro-arch events (e.g., timing, perf. counters, etc.)

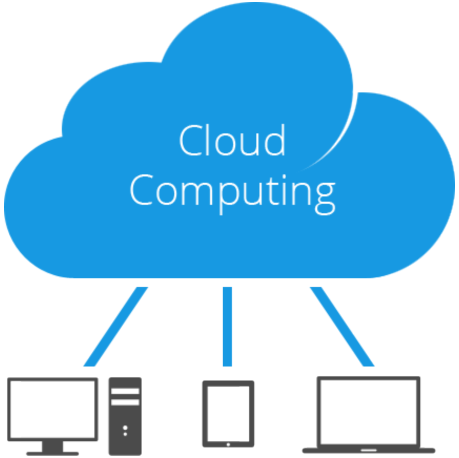
Processor

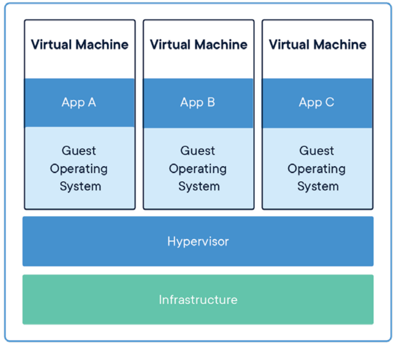
Victim

Attacker

Attacker may be remote, typically co-located

Where is hardware shared?



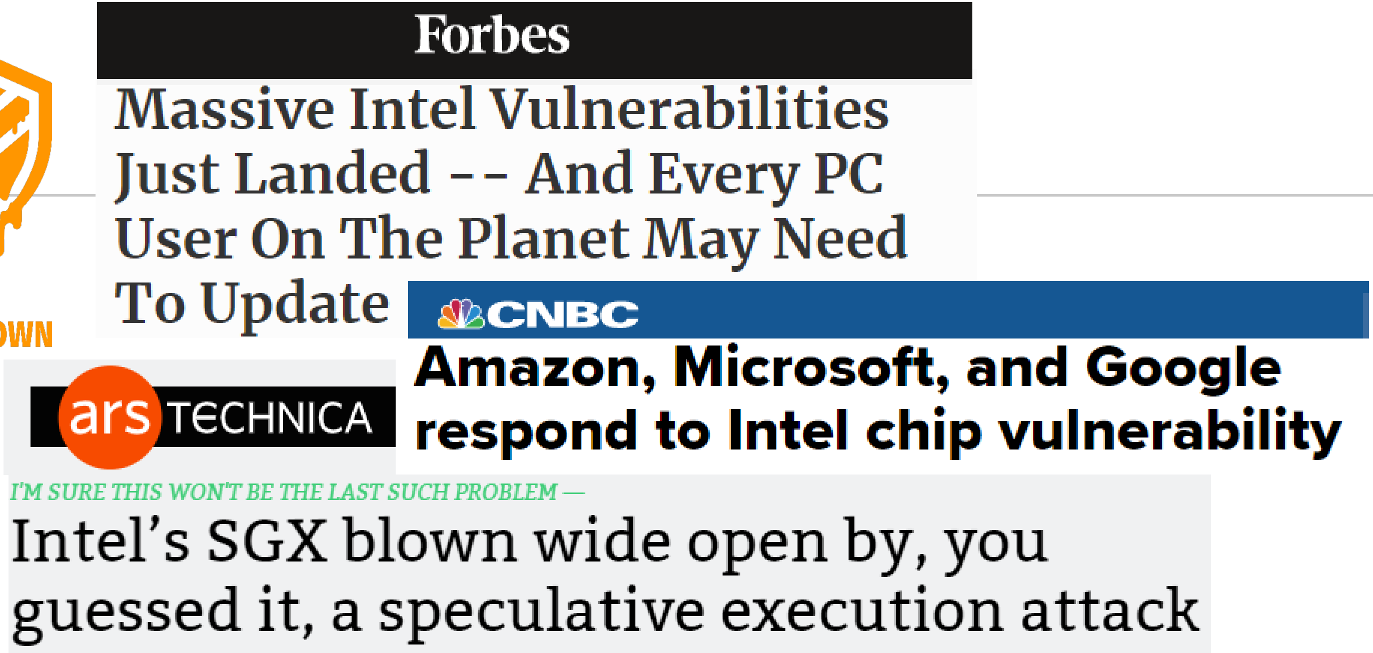

Virtual Machine | Virtual Machine | Virtual Machine

App A | App B | App C

Guest Operating System | Guest Operating System | Guest Operating System

Hypervisor

Infrastructure


Forbes

Massive Intel Vulnerabilities Just Landed -- And Every PC User On The Planet May Need To Update

CNBC

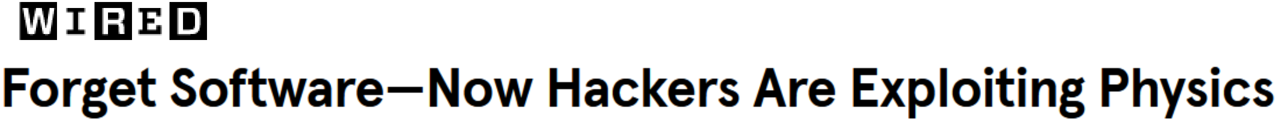
Amazon, Microsoft, and Google respond to Intel chip vulnerability

ars TECHNICA

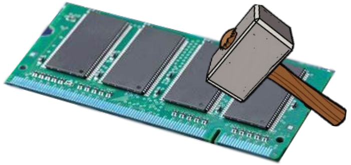
I'M SURE THIS WON'T BE THE LAST SUCH PROBLEM —

Intel's SGX blown wide open by, you guessed it, a speculative execution attack

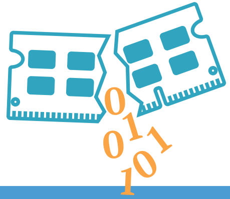
CacheOut


WIRED

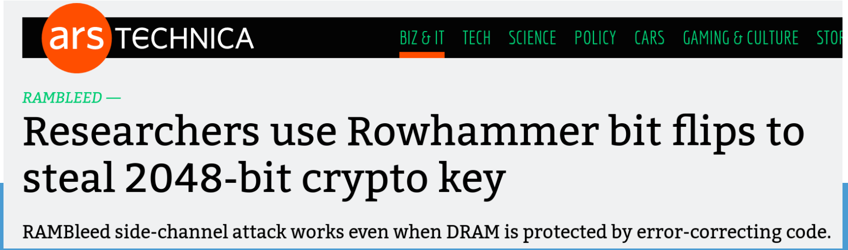
Forget Software—Now Hackers Are Exploiting Physics



Rowhammer



RAMBleed


ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STOR

RAMBLEED —

Researchers use Rowhammer bit flips to steal 2048-bit crypto key

RAMBleed side-channel attack works even when DRAM is protected by error-correcting code.

To be continued…

Your Assignments

- Send me group info
- If you don’t have a team, let me know and I’ll make on for you

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL