Comp 790-184:
Hardware Security and Side-Channels

Introduction

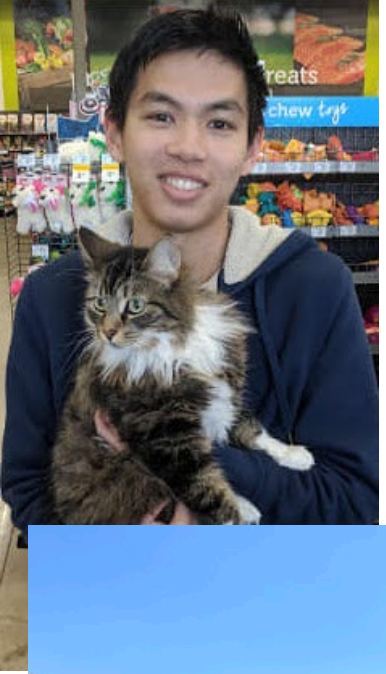
January 9, 2025
Andrew Kwong

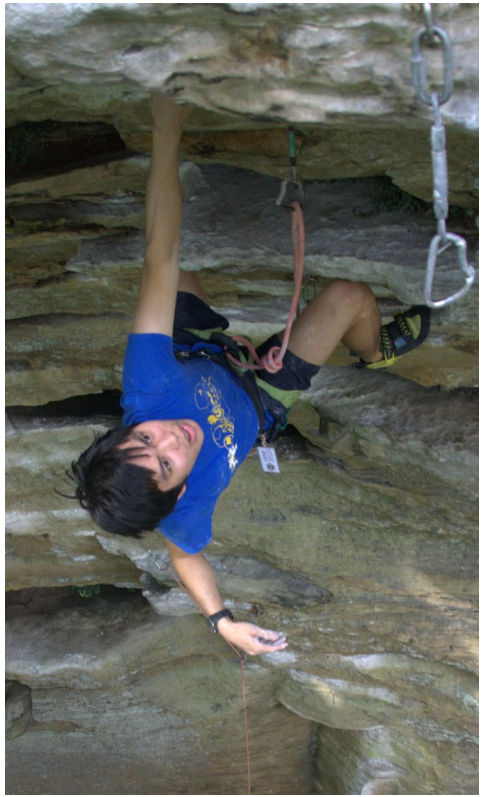
Department of Computer Science

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Today's Class

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

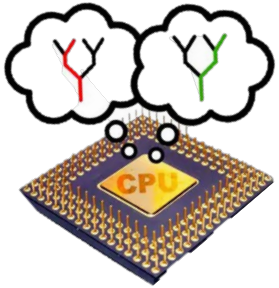




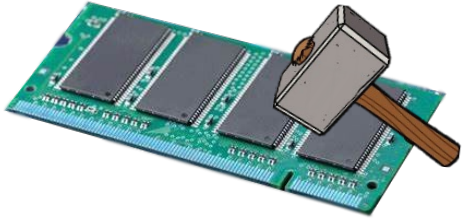
Who am I?

- Andrew Kwong
  - Assistant Professor

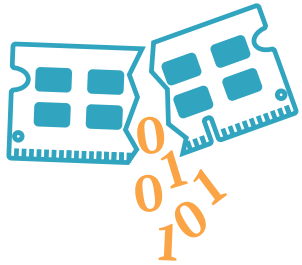
- Site: https://andrewkwong.org
- Email: andrew@cs.unc.edu
- Office: FB 340
- Office Hours: TBA



CacheOut



Rowhammer



RAMBleed

My Research

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

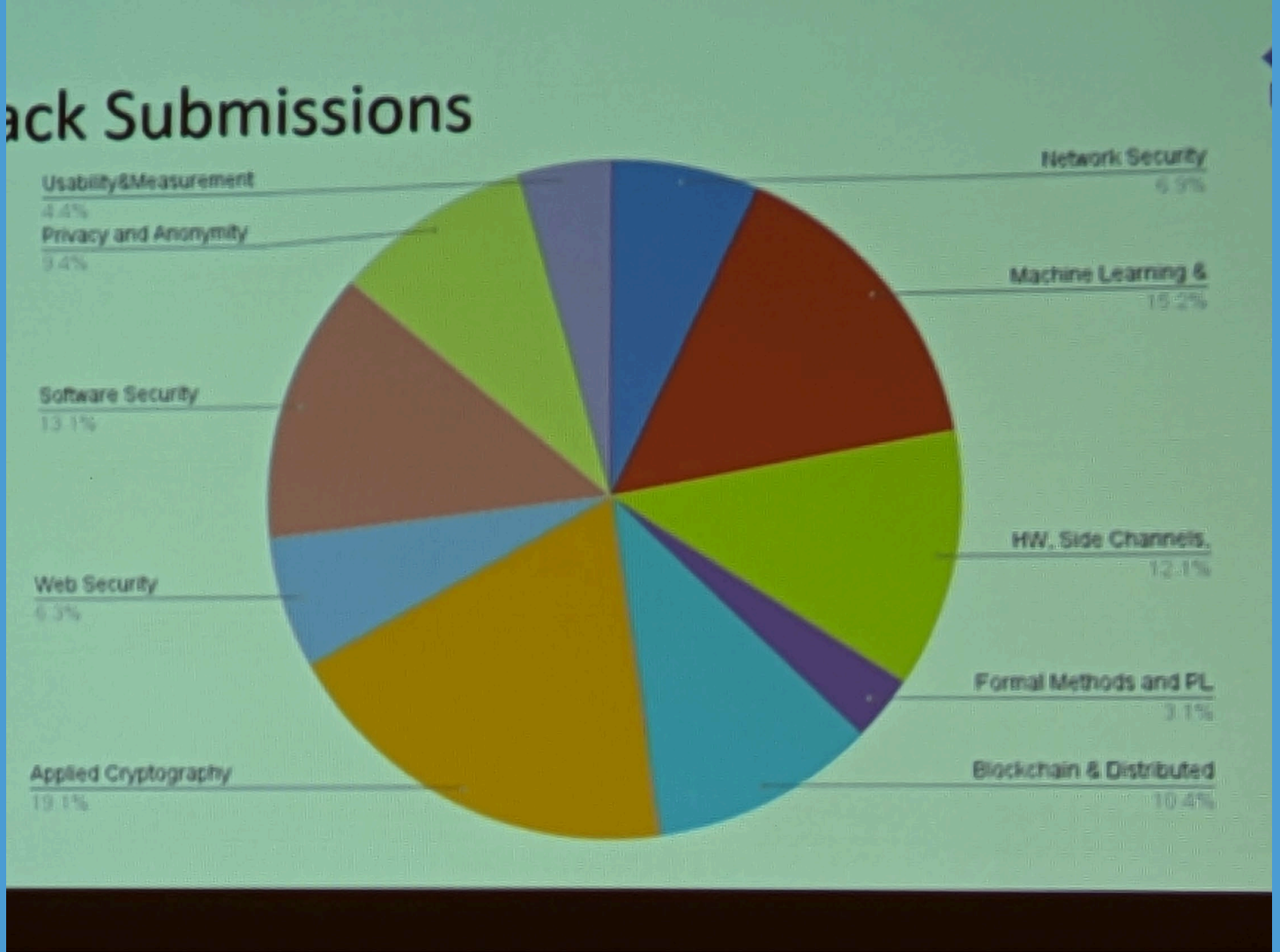
Who are you?

- Research Field
- Hobby/interesting fact
- Something you want to learn from this course.

Course Goals

- Get hands-on experience with side-channel attacks
  - Develop real-world attacks against real hardware
  - Learn how to defend against these attacks
  - Build toolkit for side-channel/hardware security research
- Gain high-level understand of the science
  - Discover where this newish field is going
  - Find out what problems are interesting

ack Submissions



ack Acceptance Rates

Course Structure

Structure

- Course meetings split 50-50 between lectures and paper discussions
- Lab Assignments
  - Programming based assignments leading towards real-world attacks on actual hardware
  - Putting theory into practice

Grading

- Class Participation – 10%
- Paper Presentations – 15%
- Paper Reviews – 15%
- Lab Assignments– 60%

Class Participation (10%)

- On Paper discussion days:
  - Ask insightful questions
    - No such thing as a dumb question
  - Discuss big picture ideas/future work
  - Participate in debates!
    - We will pretend that we are PC members arguing to accept or reject the paper
- On lecture days:
  - Show up ready to learn!

Paper Presentations (15%)

- Give conference style talk on assigned papers
- Can make or reuse/augment slides
- Roughly 20-30 minute presentation
  - High level advertisement for the paper
  - Impart the most important information
- Relate it to the most important recent related works
- Prepare discussion questions for the class

Paper Peviews (15%)

- Write down two strengths and two weaknesses of the paper
  - These shouldn’t just be a summary of the paper.
- Write down at least one insightful question (you may be asked to share!)

Lab Assignments(60%)

- 3-4 “CTF-style” labs
  - cache side-channels
  - Spectre attacks
  - Rowhammer
  - Speculative attack for ASLR break
- Discussing with classmates is allowed
  - Your team must write your own code
  - Allowed to work in pairs

What are Side-Channels?

Slides adapted from Mengjia Yan (shd.mit.edu)

And Bomb The Anchovies

By Paul Gray | Monday, Aug. 13, 1990

Like 0 Tweet Share Read Later

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.

Email Print
Share Reprints
Follow @TIME

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

Safe Cracking

- Should be secure, given enough combinations

Imperfections in the implementation indirectly leak information

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

EM Side-Channels

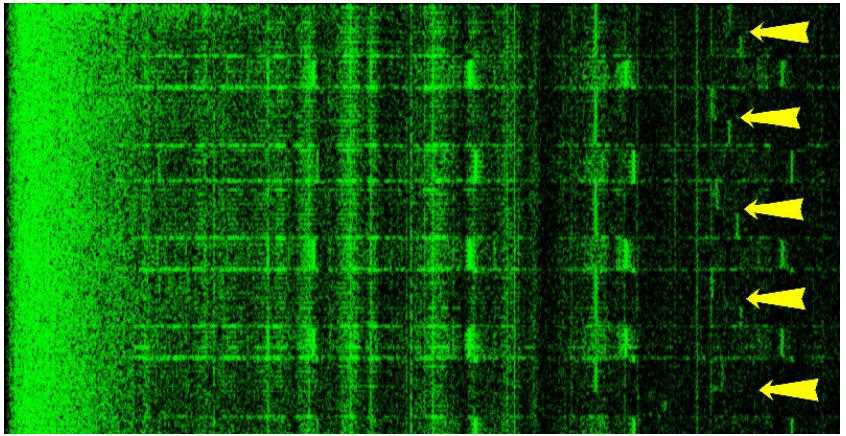
- Tempest paper written in 1972 (top secret)
- Standards for shielding sensitive equipment
  - Monitor contents can be recovered from EMR
- Researchers have demonstrated:
  - Stealing all kinds of cryptographic keys
  - fingerprinting

Acoustic Side Channels

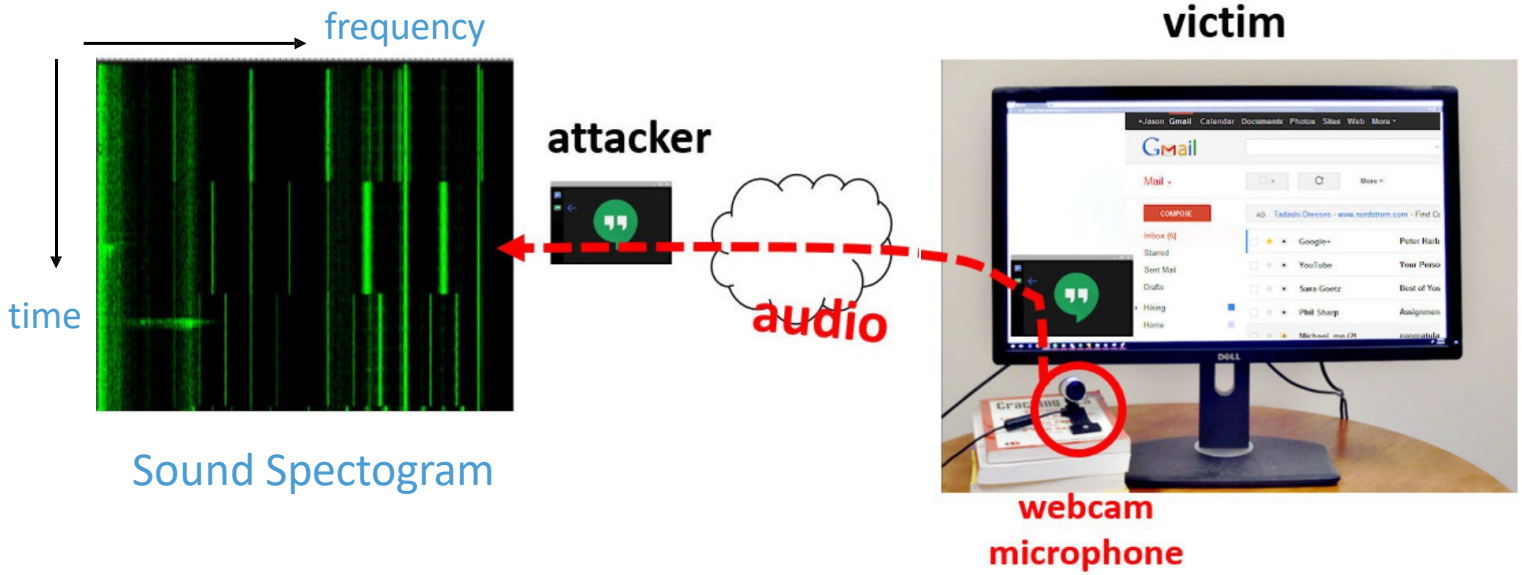
- Monitor keystroke
  - You only need: a cheap microphone + an ML model
- Other sources of acoustic side channels inside a computer?

Acoustic Cryptanalysis

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

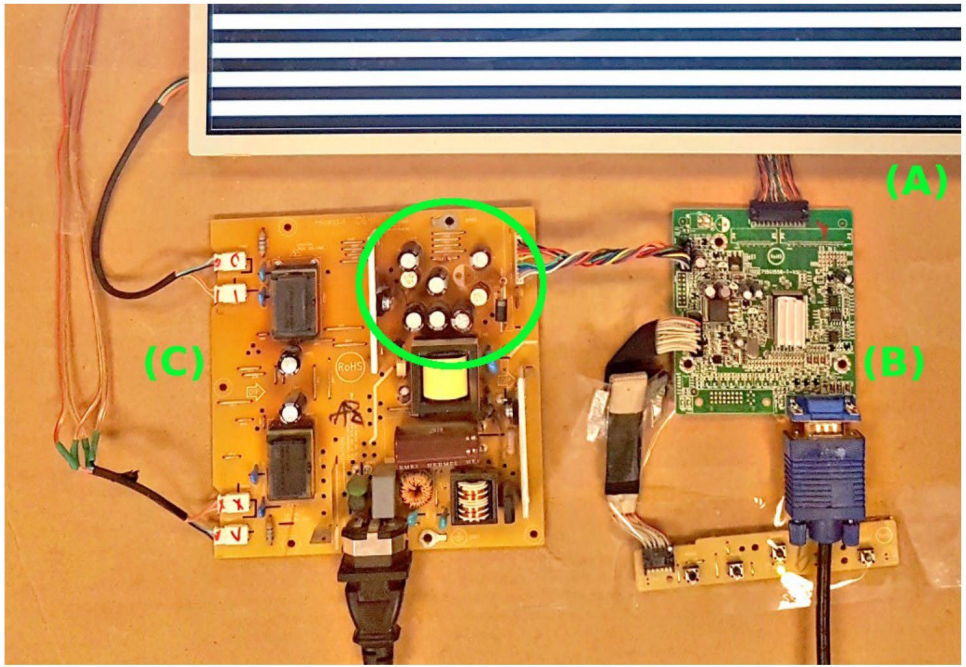


“Hear” The Screen



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

“Hear” The Screen



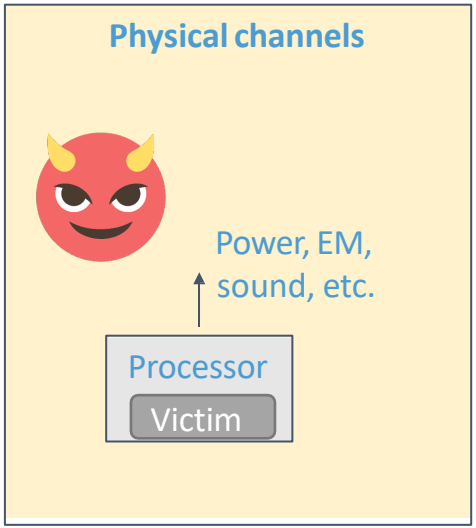
(A) is the LCD panel, (B) is the screen’s digital logic and image rendering board and, (C) is the screen’s power supply board.

Timing Side Channel

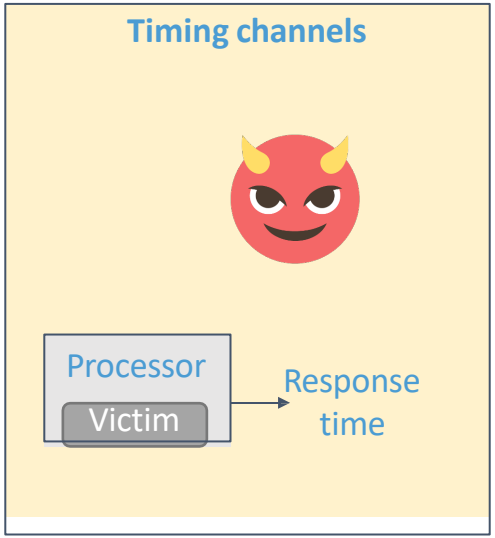
```
def check_password(input):

  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

A Rough Classification based on What Attackers Can Observe

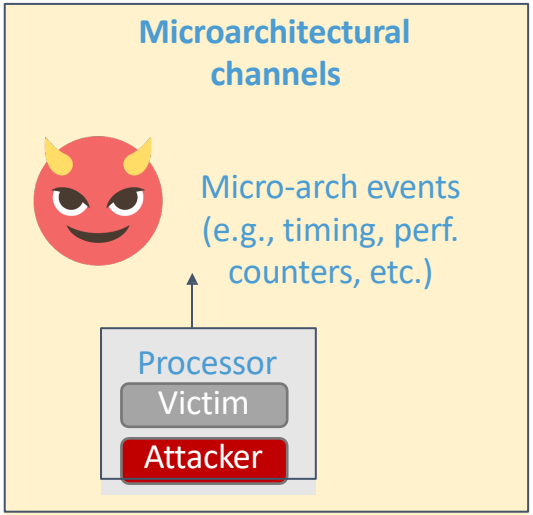


Attacker requires measurement equipment ➔ physical access



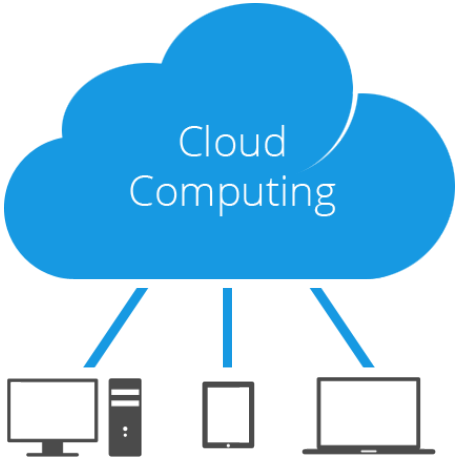
Attacker may be remote (e.g., over an internet connection)

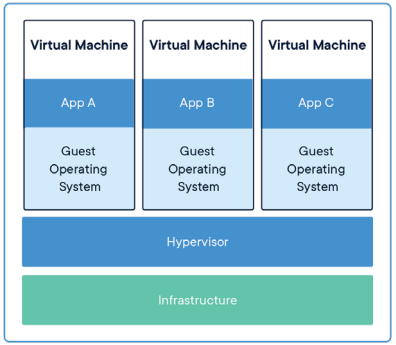
Requires shared hardware



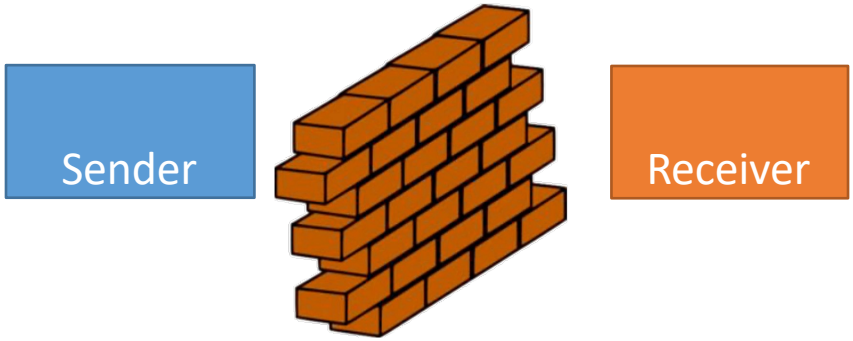
Attacker may be remote, typically co-located

Where is hardware shared?





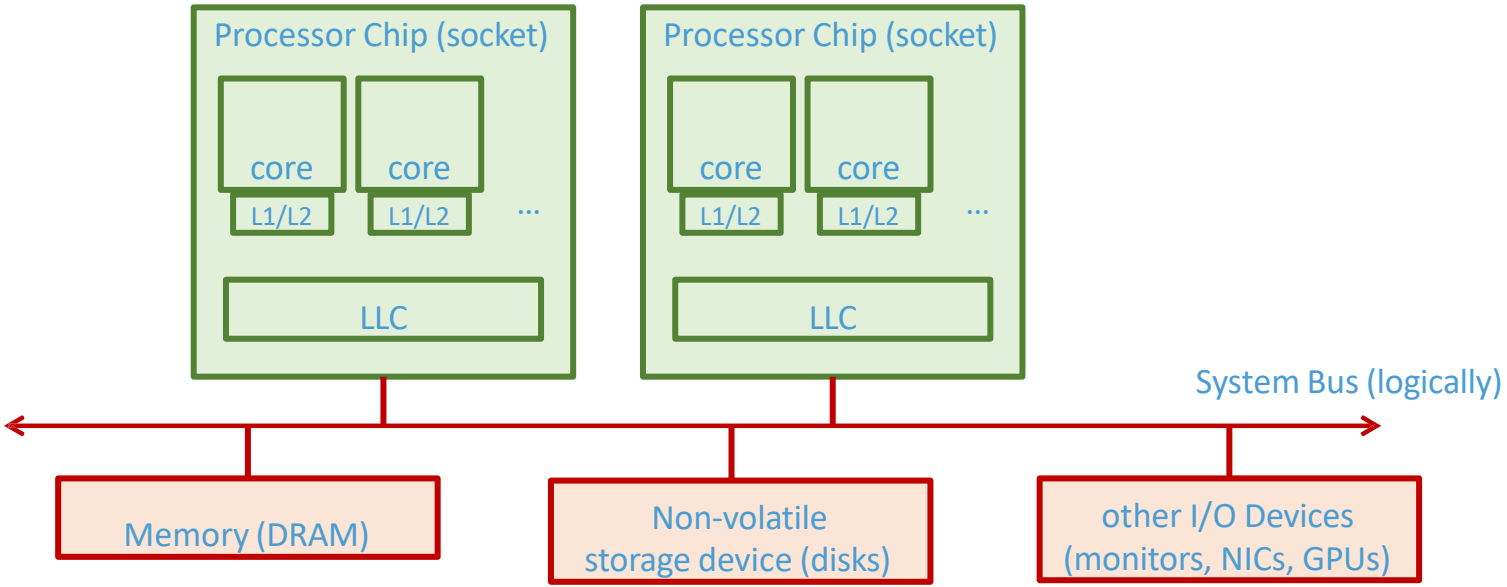
Threat Model



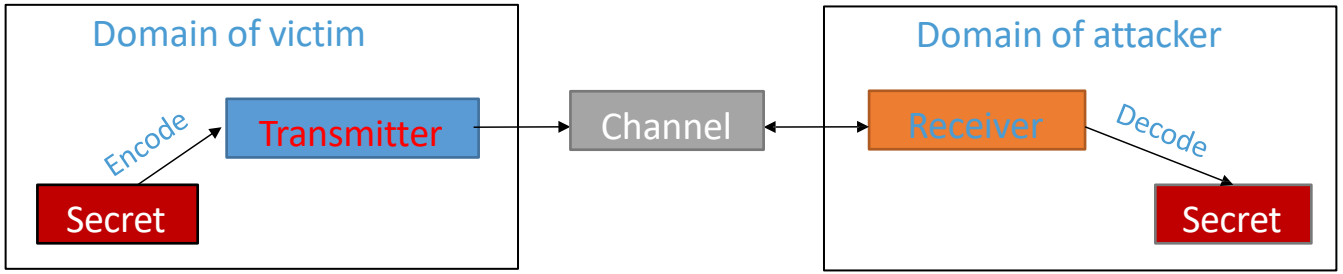
OS/Hypervisor enforced isolation

File, Socket, Pipe, Shared memory (shm in Linux) …

uArch Attacks Generalization



A Communication Model



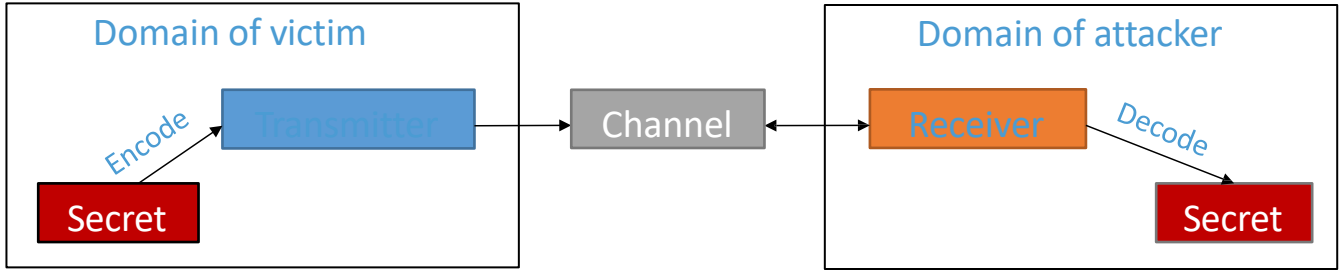
Communication Protocols

- How to encode?
  - Encode secrets via time or space
- How to coordinate between the sender and receiver?
  - Synchronization
- Bandwidth

RDRAND unit: 7-200 Kbps
MemBus/AES-NI contention: ~550-650 Kbps
LLC: 1.2 Mbps
Various structures on GPGPU: up to 4 Mbps

(Data from research papers. Not fully optimized)

Mitigations



- Sender does not use the channel -> ”data-oblivious execution” or “constant-time programming”. *(more in a later lecture)*
- Making disjoint channels makes communication impossible.
- Add noise.

To be continued…

Your Assignments

- First paper discussion Tuesday (the 21st)
  - Write down two strengths and two weaknesses of the paper
  - Write down at least one insightful question (you may be asked to share!)
- Rate preferences for paper presentations (let me know if you have a preference for presenting twice for extra credit)

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL