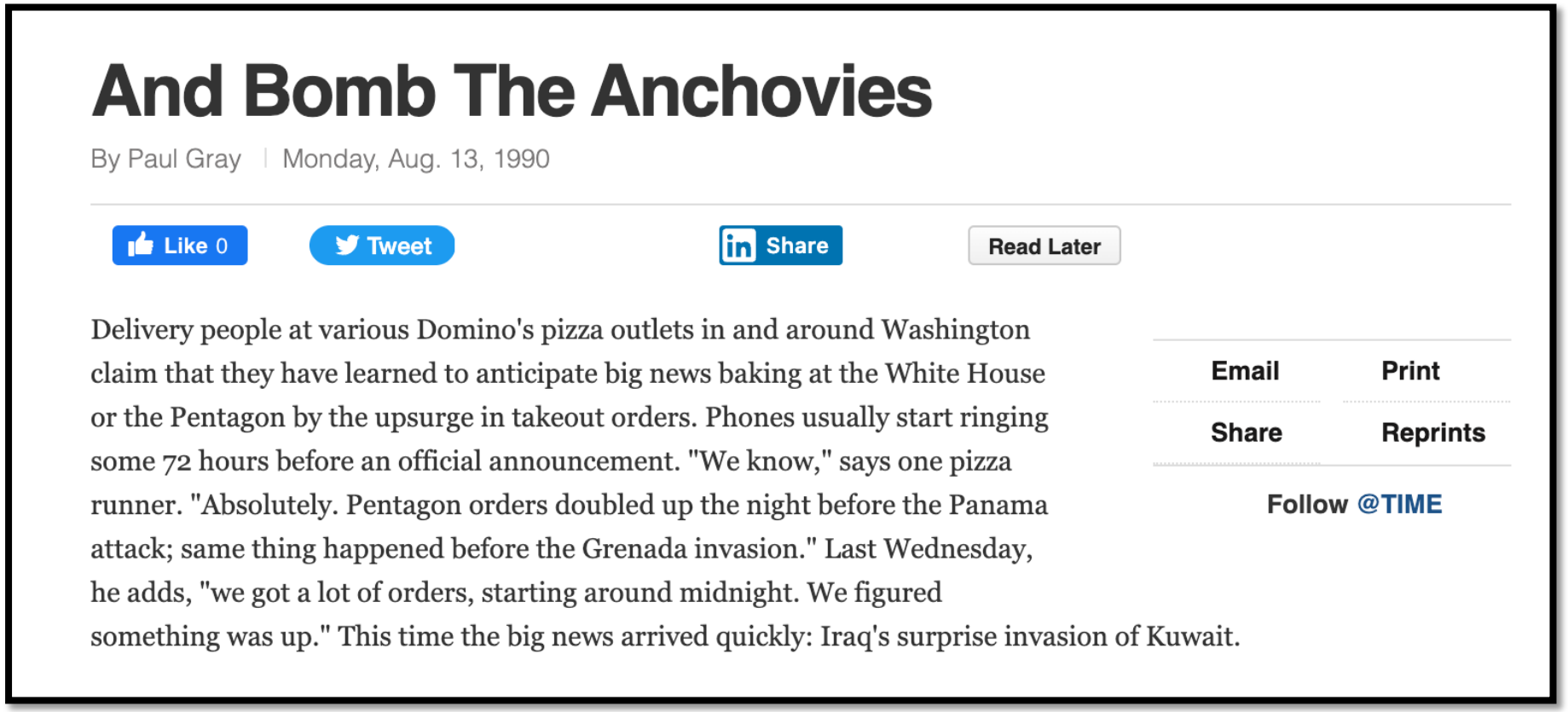
Covert and Side Channels

Mengjia Yan

Spring 2024

What is a side channel?



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

What is Covert and Side Channel?

- 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
- Side channel:
  - **Unintended** communication between two or more security parties

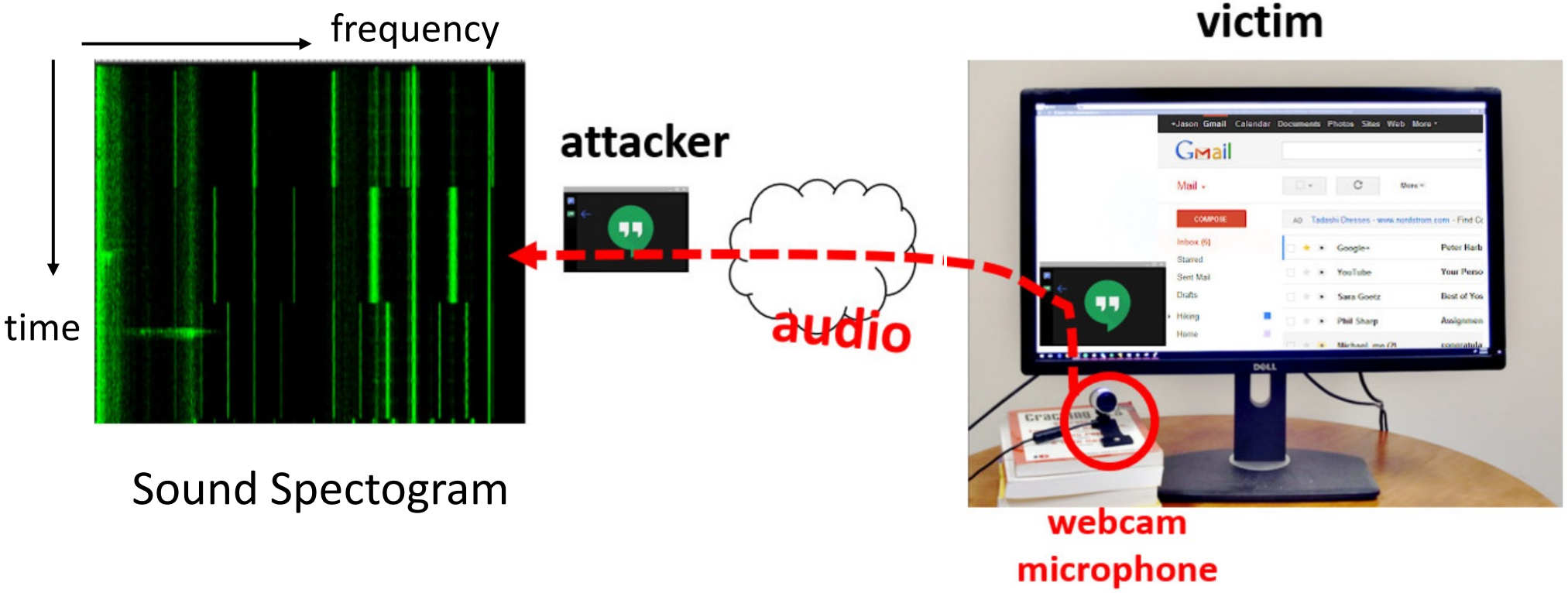
- In both cases:
  - Communication should not be possible, following system semantics
  - The communication medium is not designed to be a communication channel

Side Channels Are Almost Everywhere

Example #1: Acoustic Side Channels

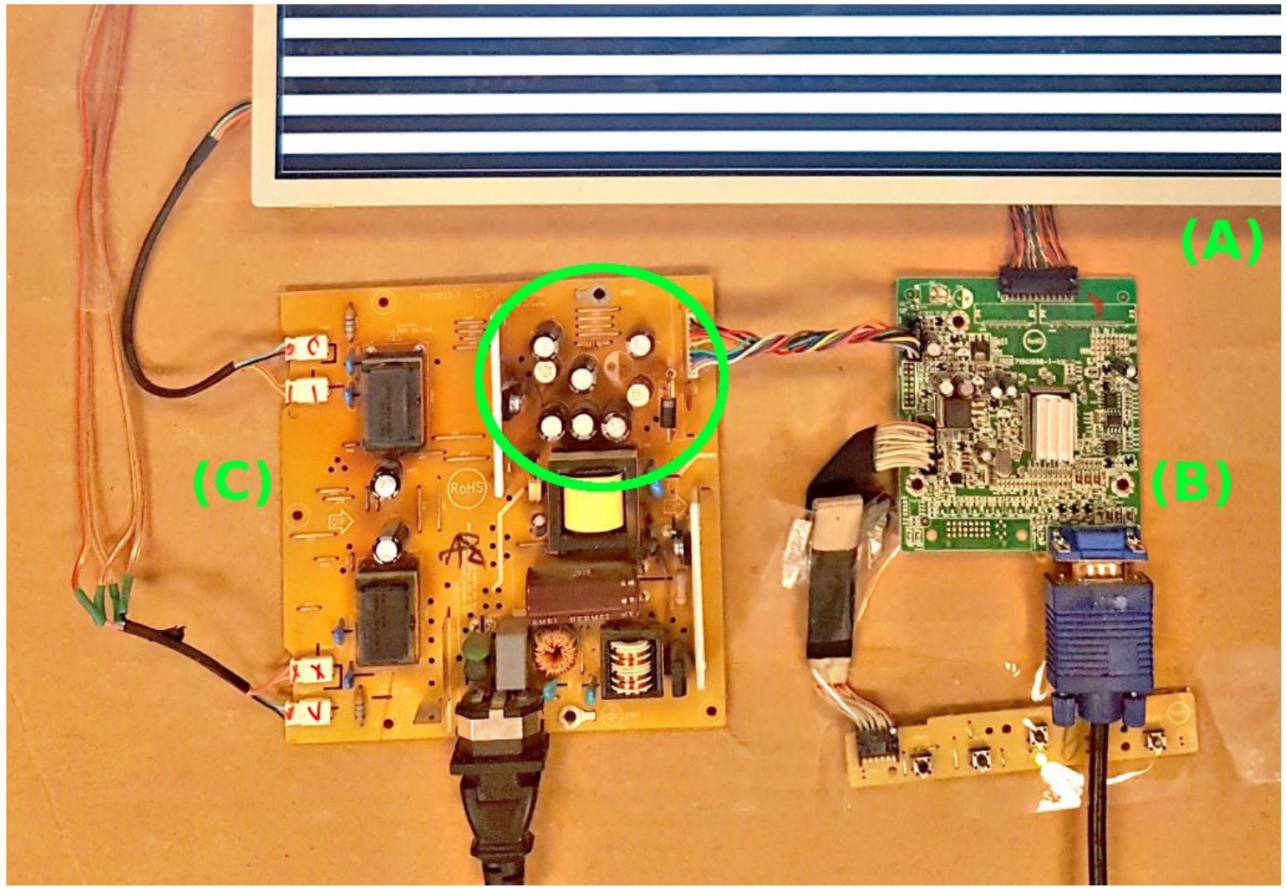
- Monitor keystroke
  - You only need: a cheap microphone + an ML model
- Other sources of acoustic side channels inside a computer?
- Another example: “Hear” the screen

“Hear” The Screen



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

“Hear” The Screen

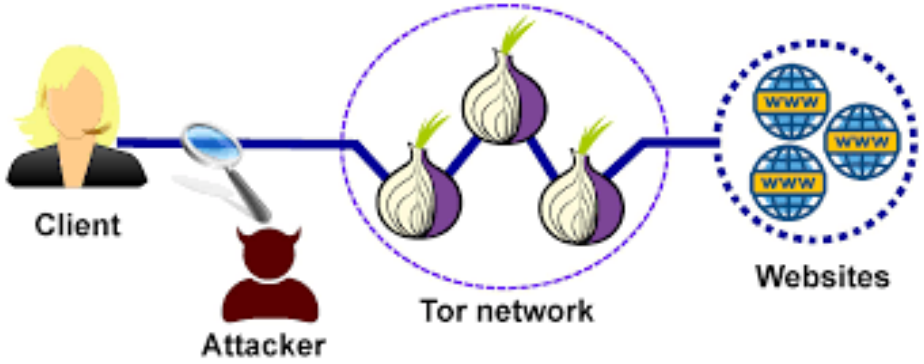


(A) is the LCD panel, (B) is the screen’s digital logic and image rendering board and, (C) is the screen’s power supply board.

Even cats know side channels …

Example 2: Network Side Channels

- Website Fingerprinting
  - Frequency of packets, size of packets
  - Response dependent:
    - iSideWith.com
  - Real-time feedback:
    - Google Search auto-complete
- Network traffic contention side channel
  - Active attacker: try stress test



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.

Example 3: 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 the attacker needs to crack the password?
- Can we reduce the number of attempts? How?

Vulnerabilities in Real-world Crypto

- Libgcrypt's Montgomery ladder scalar-by-point multiplication routine

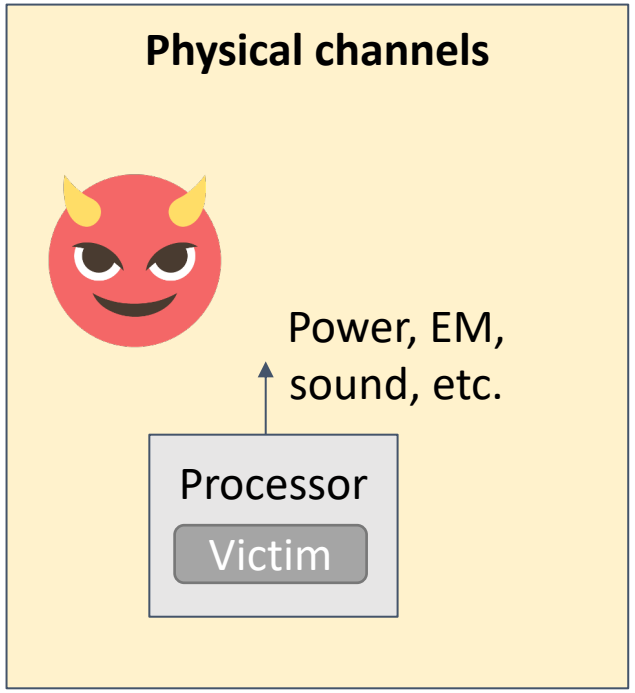
Algorithm 3 Libgcrypt's modular reduction operation (simplified).

Input: Two integers x and m, represented as a sequence of limbs $x_0 \dots x_{l-1}$ and $m_0 \dots m_{k-1}$.
Output: x mod m.

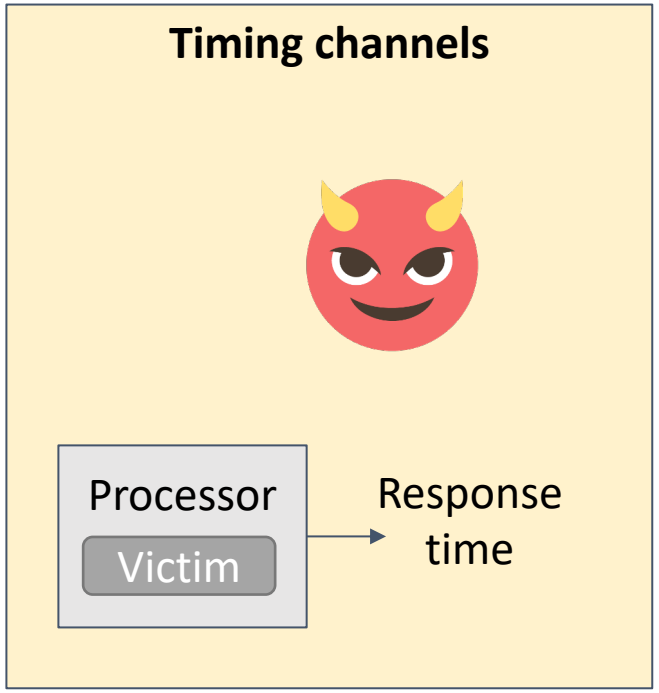
```
1:  procedure MODULAR_REDUCTION(x, m)
2:      l ← SIZE_IN_LIMBS(x)
3:      k ← SIZE_IN_LIMBS(m)
4:      if l < k then
5:          return x                          ▷ Early exit if x is smaller than m
6:      for i ← l − 1 downto k − 1 do
7:          q ← (x_i · 2^64 + x_{i−1})/m_{k−1}        ▷ Estimate quotient q
8:          if q(m_{k−1} · 2^128 + m_{k−2}) > x_i · 2^128 + x_{i−1} · 2^64 + x_{i−2}
    then
9:              q ← q − 1                     ▷ If q is too large, adjust estimate
10:         x ← x − q · m · 2^{64(i−k)}               ▷ Subtract from x
11:     return x                              ▷ x holds the remainder
```

Vulnerability exists in a highly-regular real-world implementation of Curve25519.

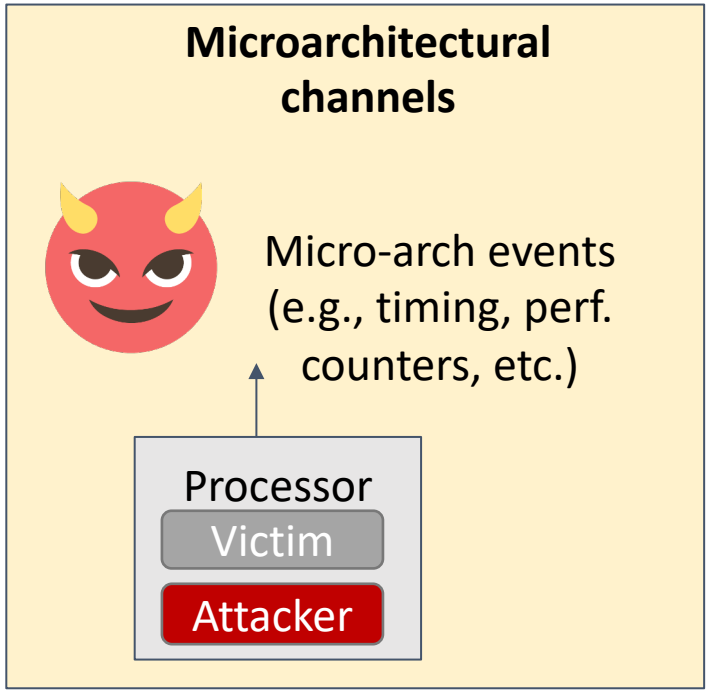
A Rough Classification based on What Attackers Can Observe



Attacker requires measurement equipment → physical access



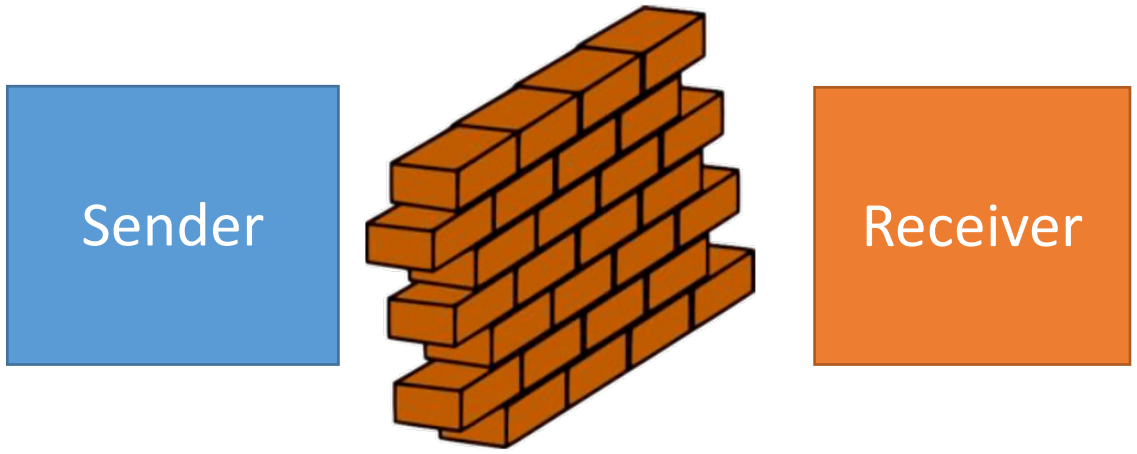
Attacker may be remote (e.g., over an internet connection)



Attacker may be remote, or be co-located

Microarchitecture (uArch) Side Channel

Threat Model



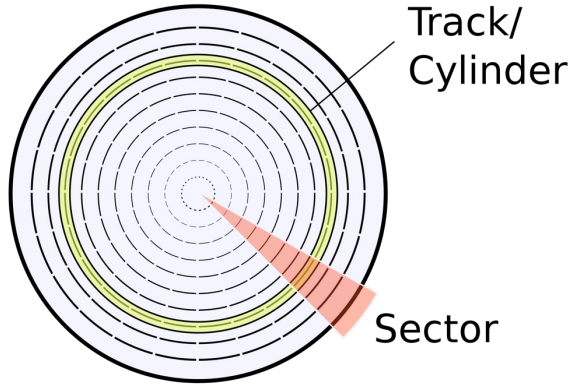
OS/Hypervisor enforced isolation

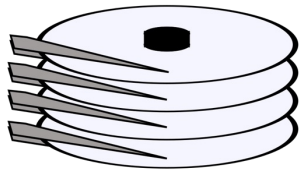
File, Socket, Pipe, Shared memory (shm in Linux) …

An Example Attack in 1977

- Disk arm optimization
  - Enqueues requests by ascending cylinder number and dequeues (executes) them by the "elevator algorithm."

- Come up with an attack strategy to leak which track a neighboring application accesses.

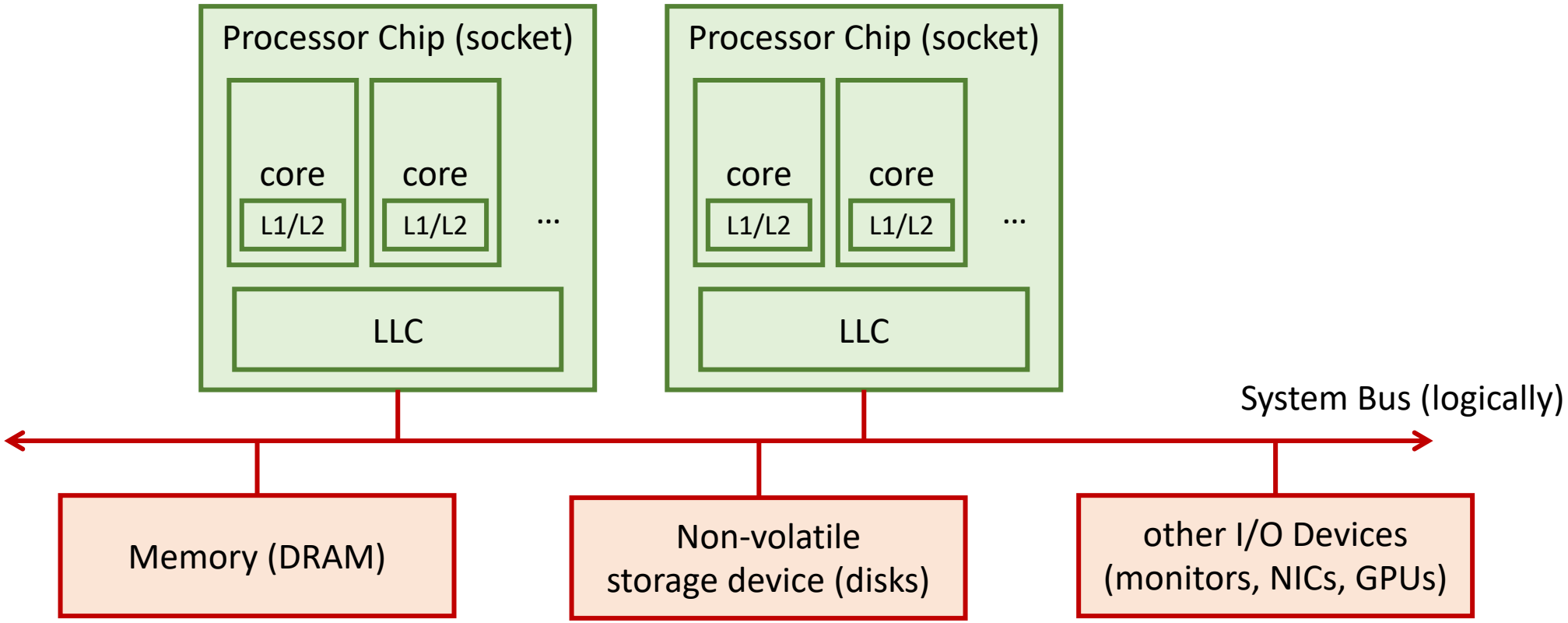




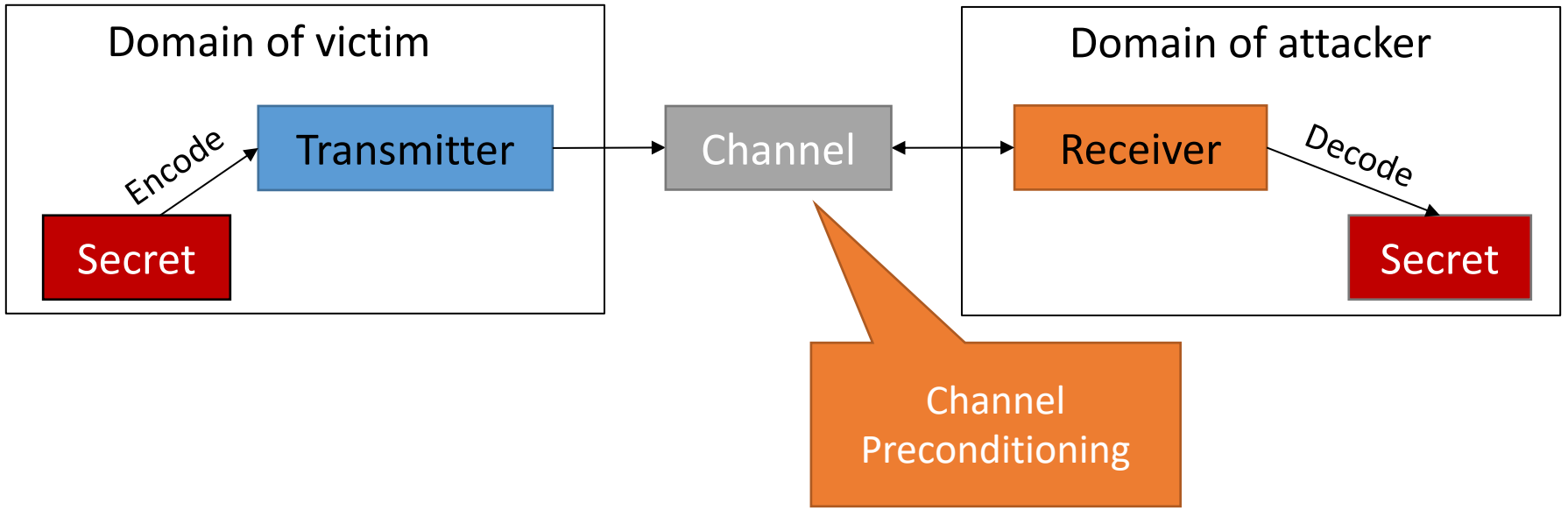
Heads

8 Heads,
4 Platters

uArch Attacks Generalization



A Communication Model



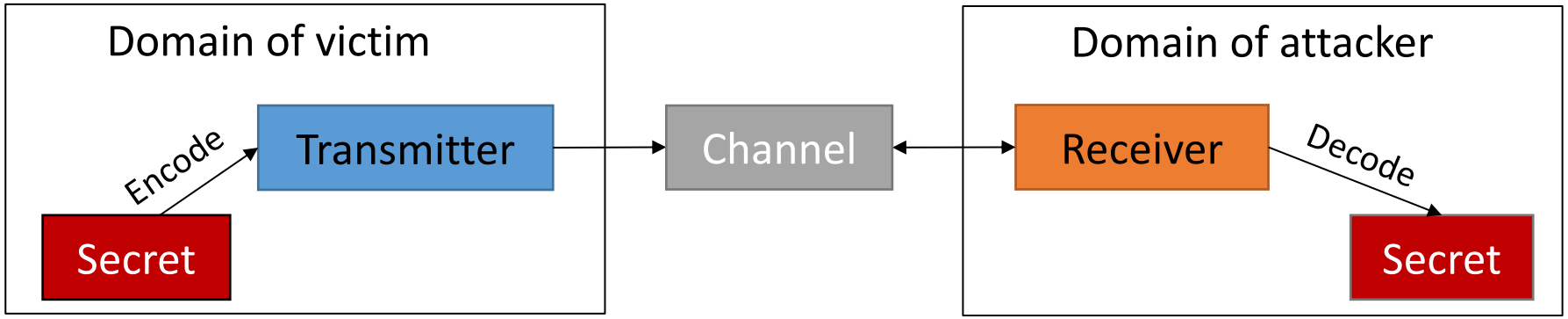
Communication Protocols

- 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 L05)*
- Making disjoint channels makes communication impossible.
- Add noise.

Analyze A Demo

How difficult is it to figure out the **root cause** of a covert/side channel?

Next: Cache Side Channel Deep Dive