Covert and Side Channels

Mengjia Yan

Spring 2026

What is a side channel?

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

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

What is Covert and Side Channel?

- Gather information by measuring or exploiting **indirect** effects of the system

- 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 does not follow the system specification
  - The communication medium is not designed to be a communication channel

Side Channels Are Almost Everywhere

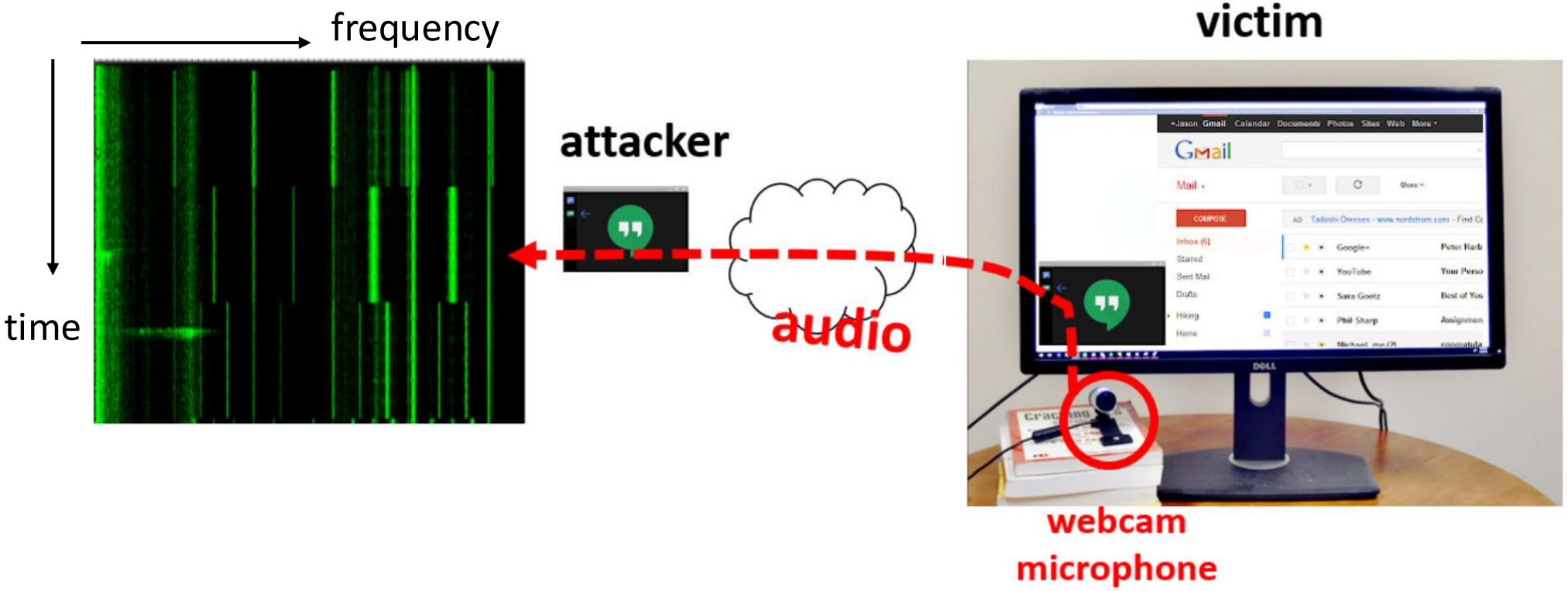
Example #1: Acoustic Side Channels

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

Other sources of acoustic side channels inside a computer?

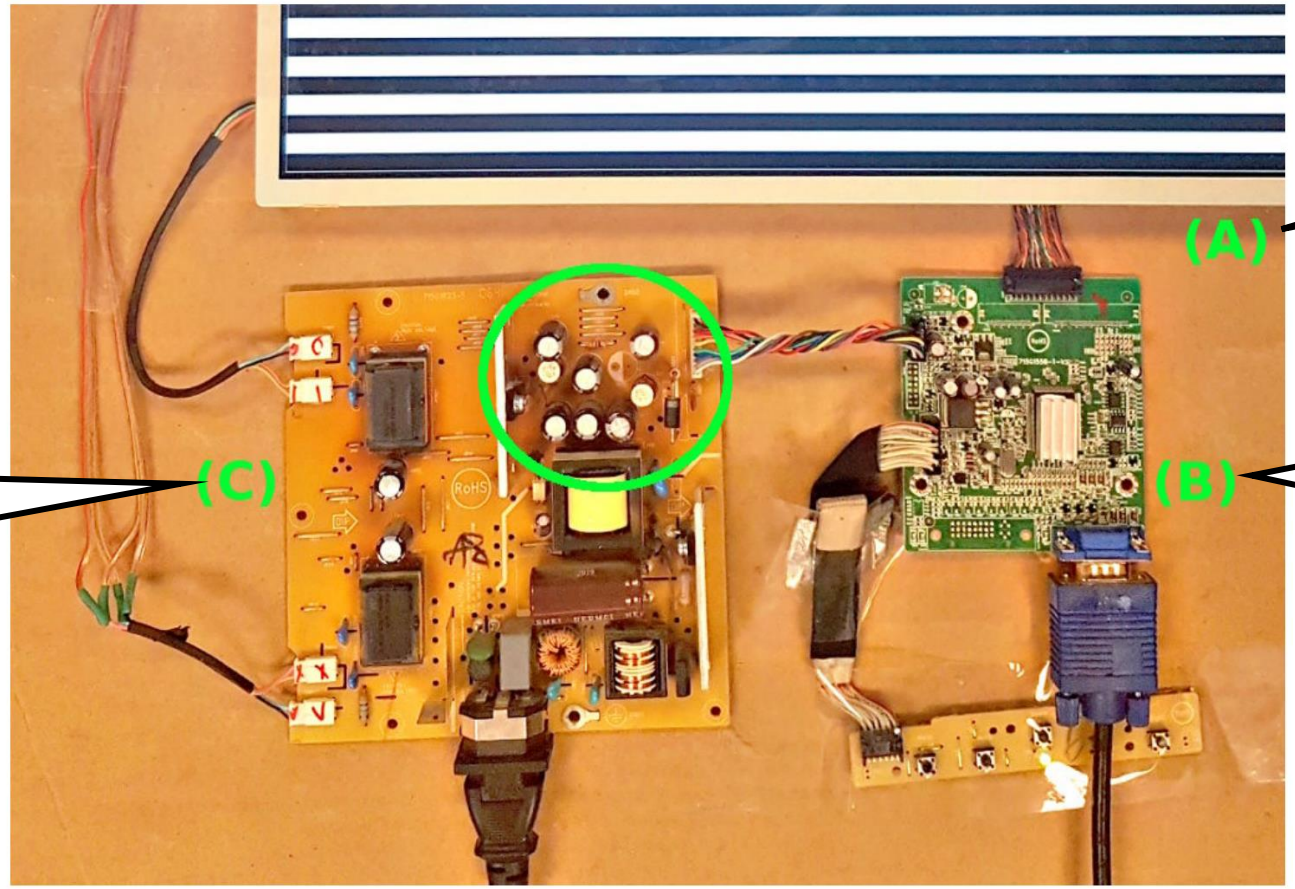
- Another example: “Hear” the screen

“Hear” The Screen



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

“Hear” The Screen

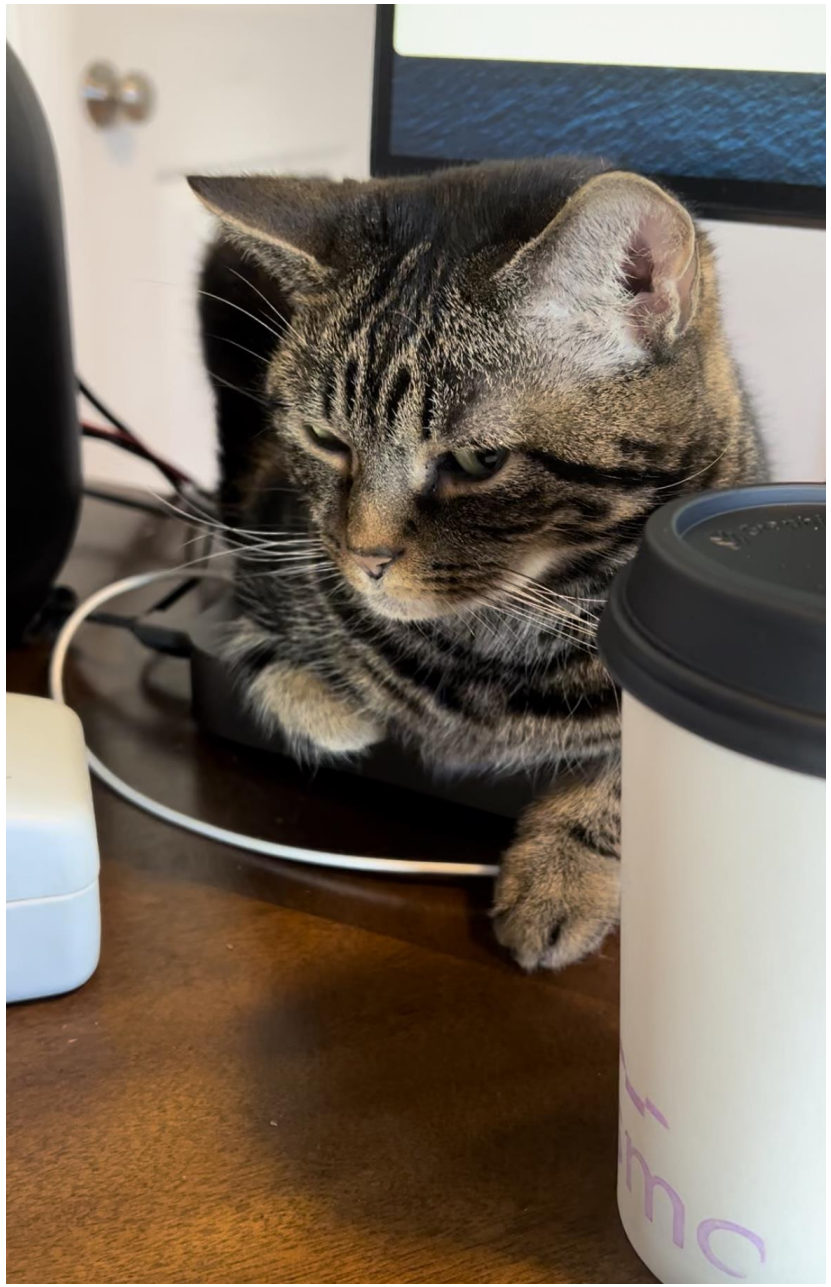


LCD panel

Digital logic and image rendering board

Power supply board

Even cats know side channels …



Example 2: Network Side Channels

- Website Fingerprinting
  - Frequency of packets, size of packets
  - Example: iSideWith.com

- Network traffic contention side channel

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):

  for i in range(0,128):
    if (input [i] != password[i]):
      return ("error");


  return (“success”);
```

Early termination

- Password: 128 digits
- How many attempts an attacker needs to brute force a password with **blind guess**?
- Consider the *check_password* program on the left. 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).

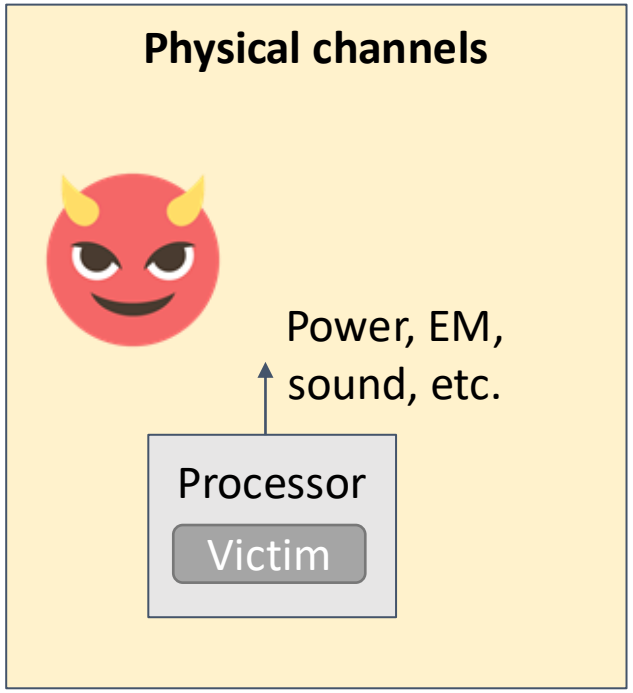
Input: Two integers x and m, represented as a sequence of limbs $x_0 \ldots x_{l-1}$ and $m_0 \ldots m_{k-1}$.
Output: x mod m.

```
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
```

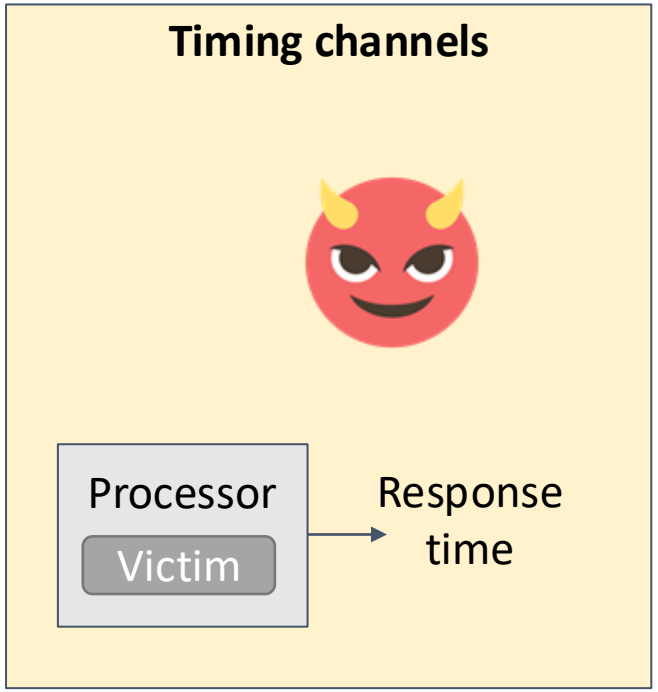
Vulnerability exists in a real-world implementation of Curve25519.

Genkin et al. May the Fourth Be With You: A Microarchitectural Side Channel Attack on Several Real-World Applications of Curve25519; CCS'17

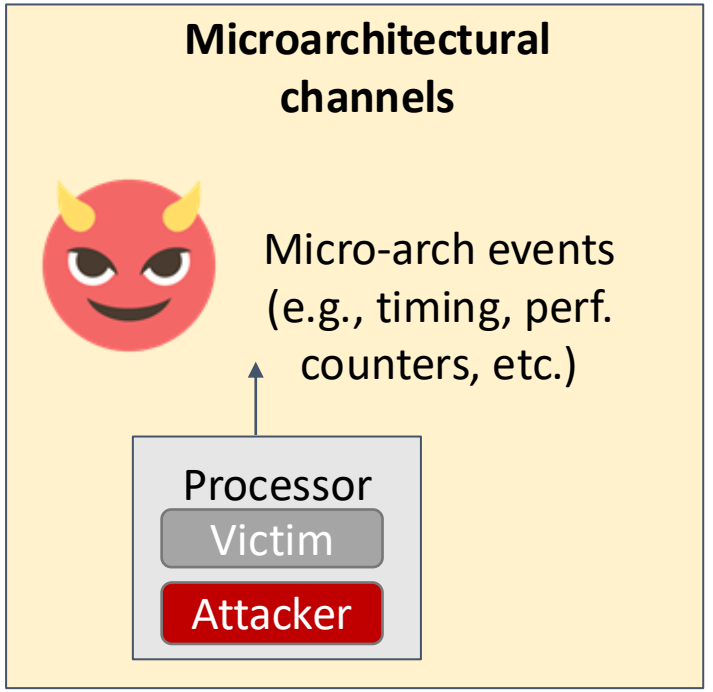
A Rough Classification based on What Attackers Can Observe



Attacker requires measurement equipment → physical access



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

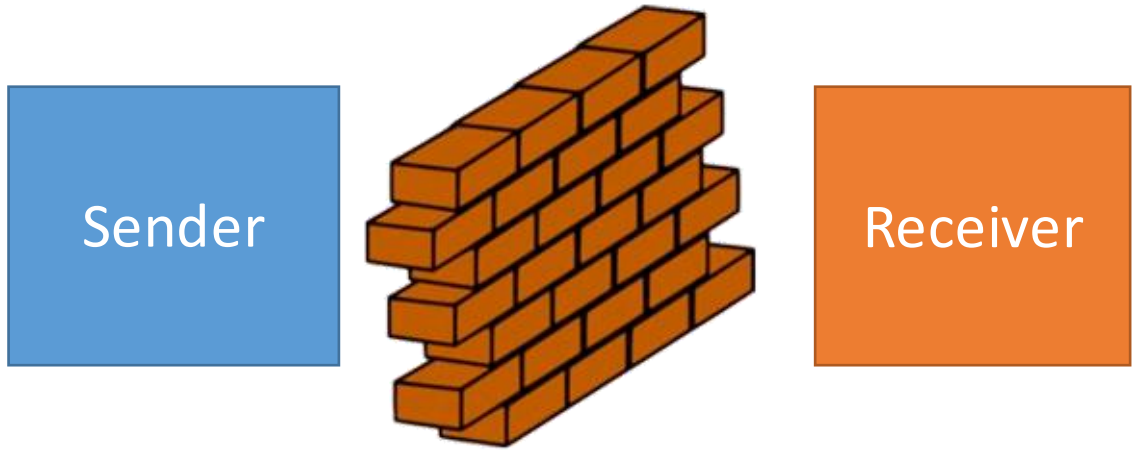


Attacker may be remote, or be co-located

Slides credit: Chris Fletcher

Microarchitecture (uArch) Side Channel

Side Channel Threat Model

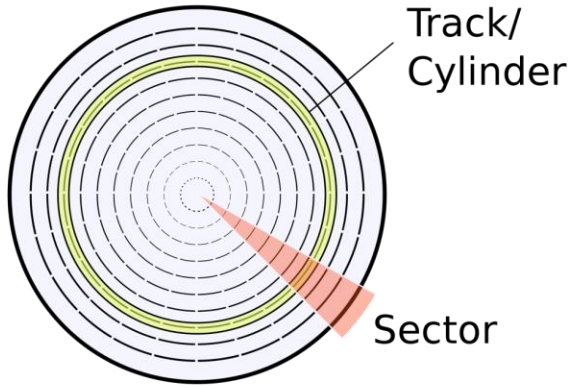


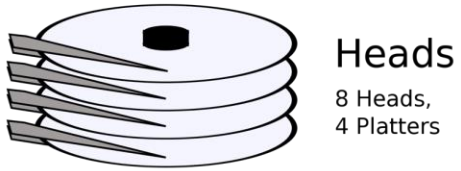
OS/Hypervisor enforced isolation

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

An Example Attack in 1977

- Disk arm optimization
  - Execute requests by the "elevator algorithm."
- Assume attacker's capability:
  - Can issue multiple requests to any tracks
  - Can measure request latency and the order of its own requests get processed by the disk
- Let's attack 

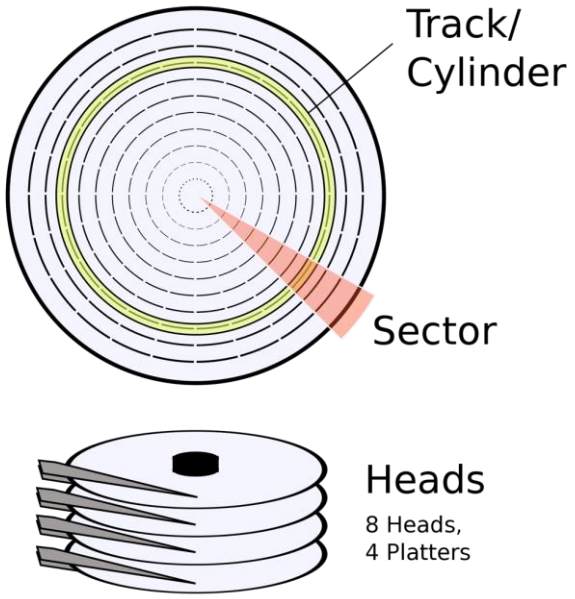




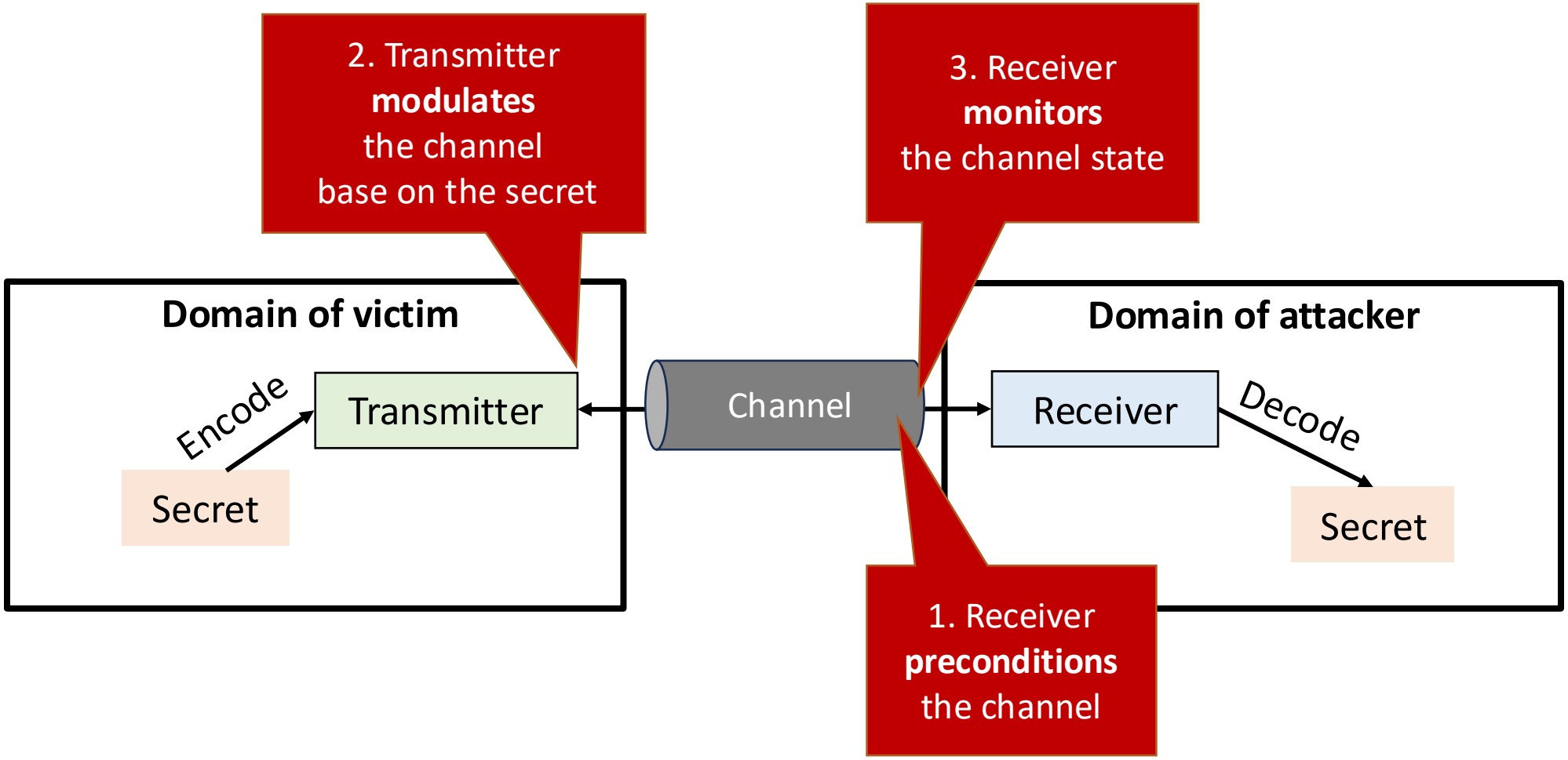
A retrospective on the VAX VMM security kernel, 1991

Victim Code:

```
if (secret_bit==1)
    access track 2;
else
    access track 8;
```

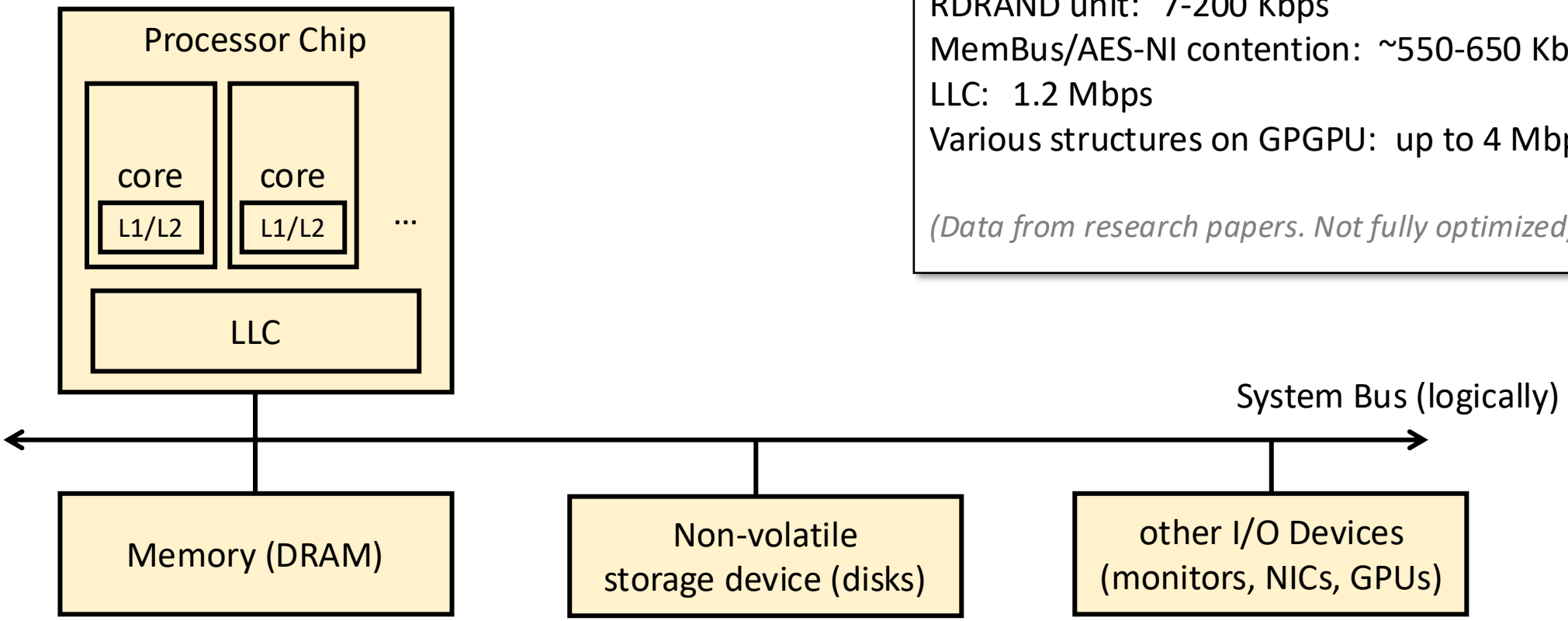


A Communication Model



Kiriansky et al; DAWG: A Defense Against Cache Timing Attacks in Speculative Execution Processors
Bourgeat et al; CaSA: End-to-end quantitative security analysis of randomly mapped caches

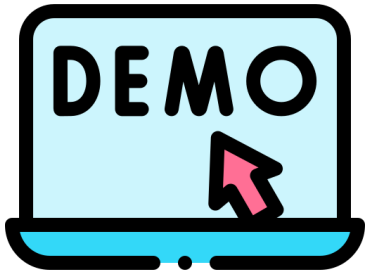
uArch Attacks Generalization



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)

Setup



- Sender: send a heartbeat every 5 seconds

```
while(1) {
    allocate a buffer;
    sleep(5);
    free the buffer;
}
```

- Receiver: sample system status every 1 second

```
allocate a buffer;
while(1) {
    latency = time(access the buffer);
    report latency;
    sleep(1);
}
```

Analyze The Demo

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

Next: Cache Side Channel Deep Dive