

Covert and Side Channels

Mengjia Yan

Spring 2025



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

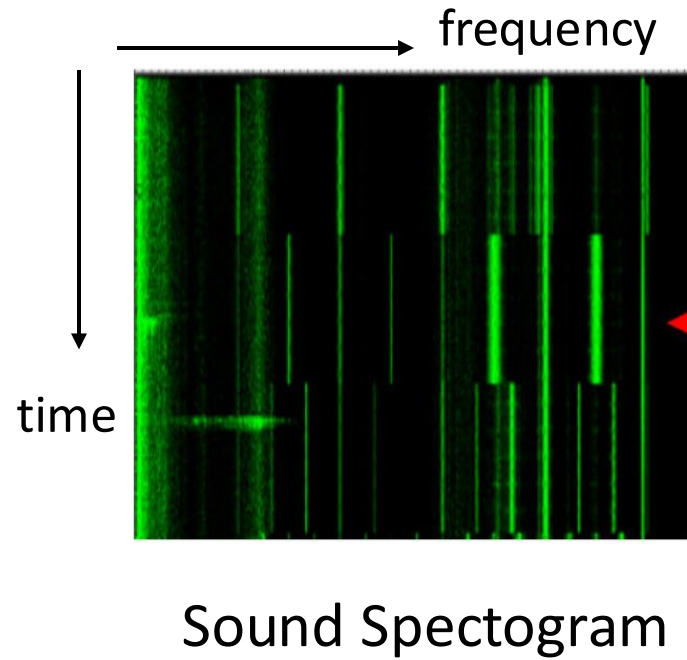
Other sources of acoustic side channels
inside a computer?



- Another example: “Hear” the screen



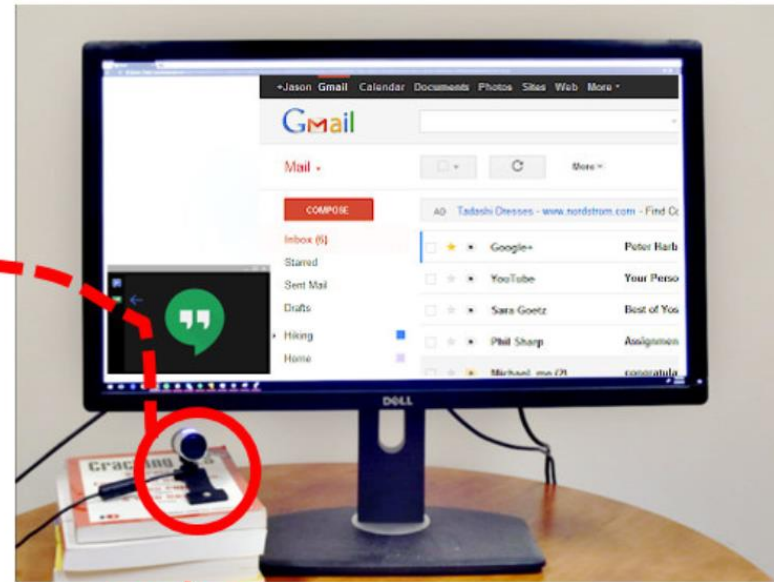
“Hear” The Screen



attacker

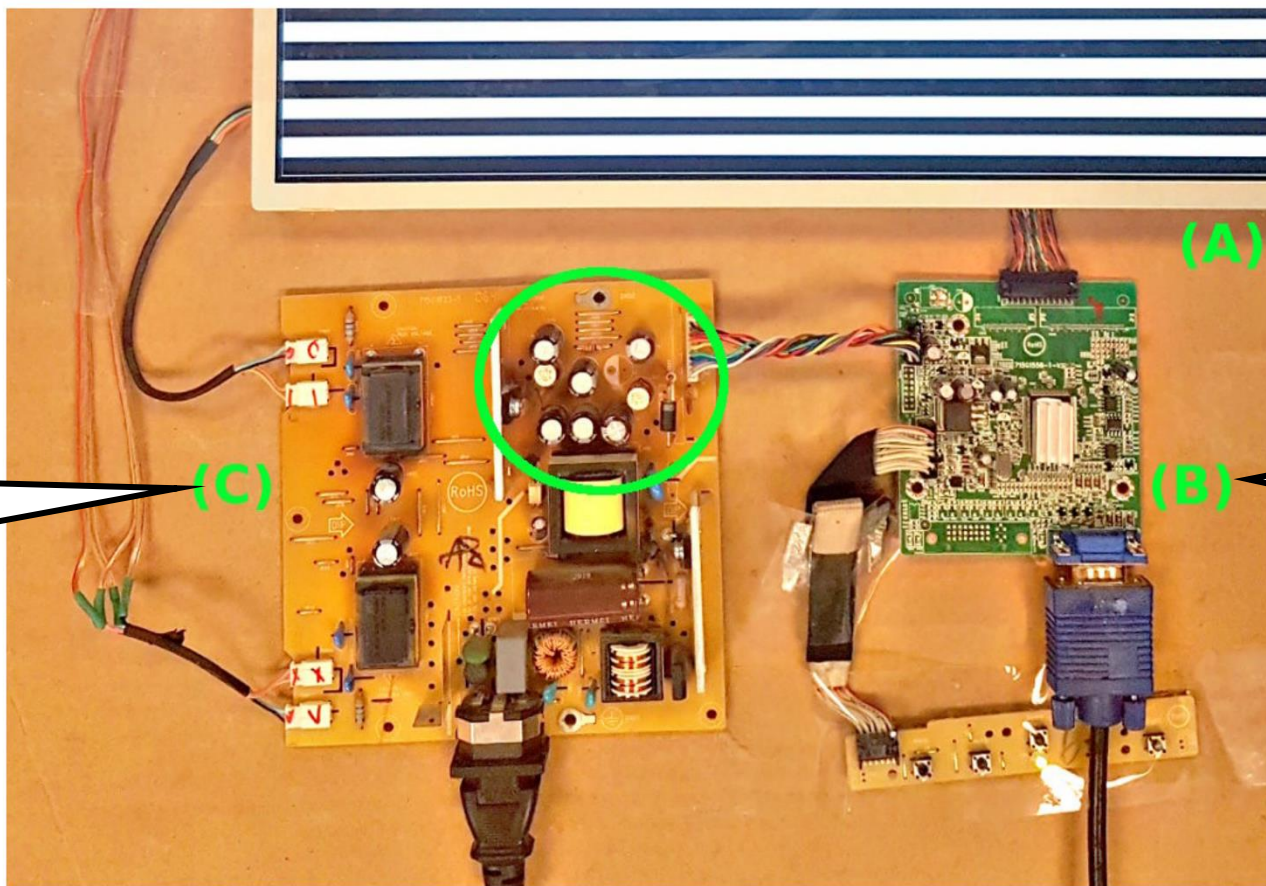


victim



webcam
microphone

“Hear” The Screen

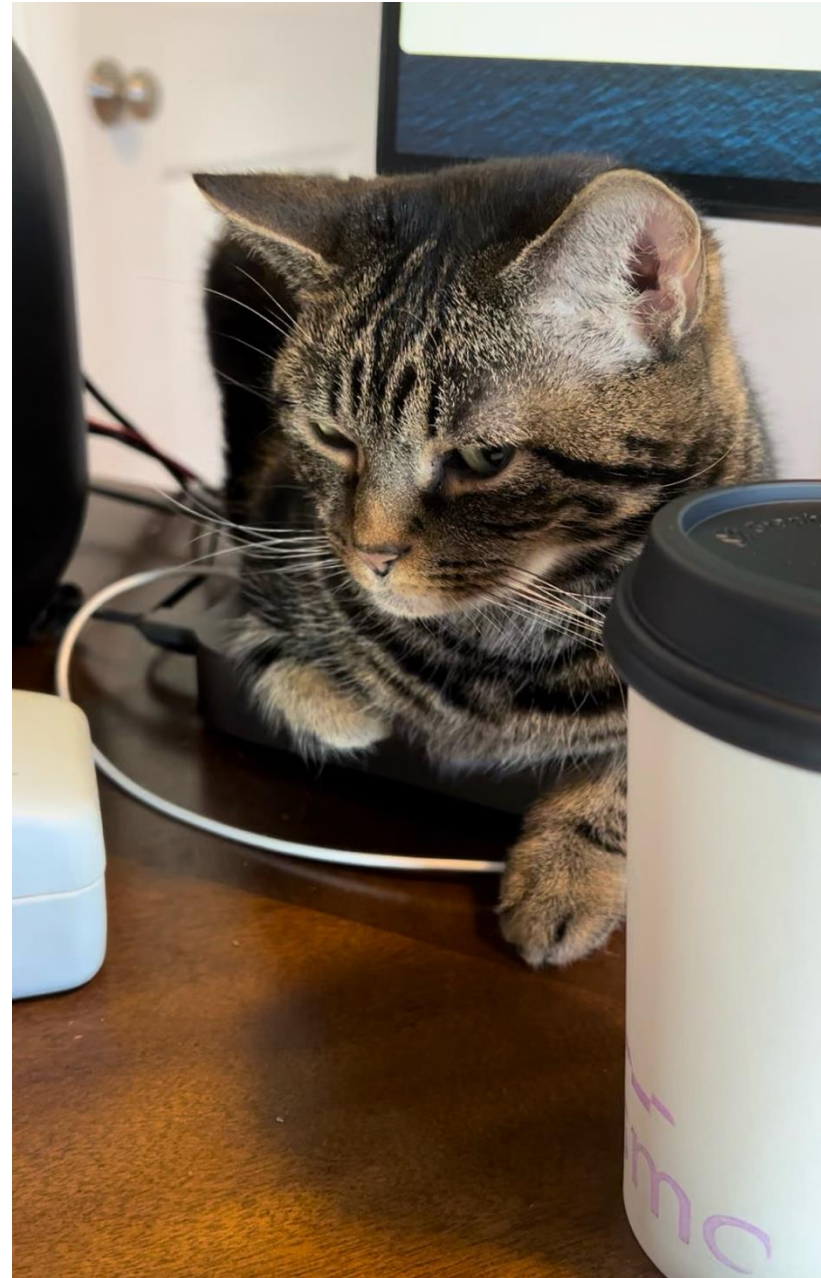


LCD panel

Power supply board

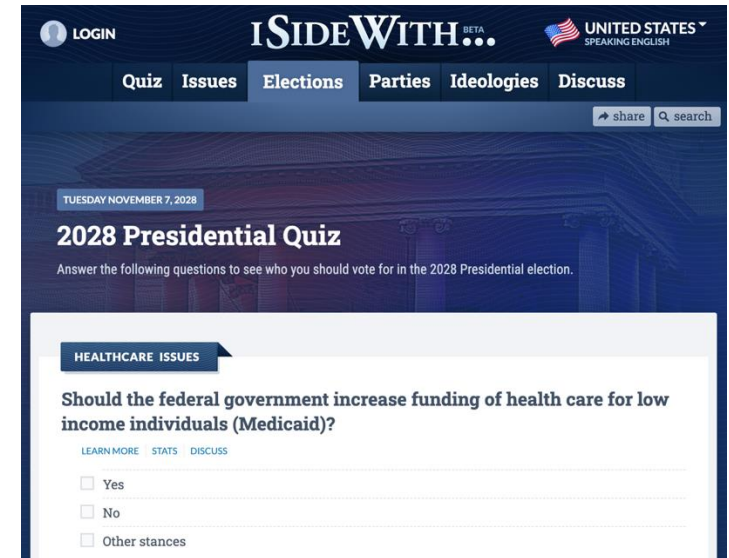
Digital logic and image rendering board

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



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

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

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

Input: Two integers x and m , represented as a sequence of limbs

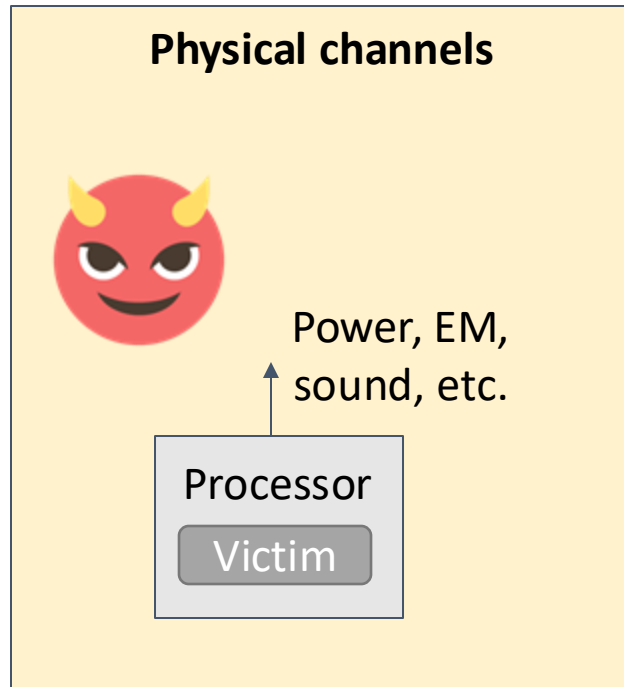
$x_0 \dots x_{l-1}$ and $m_0 \dots m_{k-1}$.

Output: $x \bmod m$.

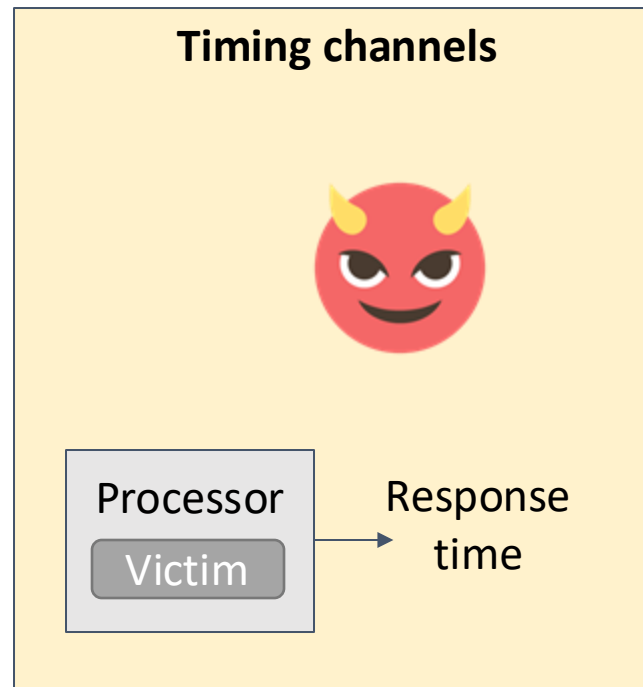
```
1: procedure MODULAR_REDUCTION( $x, m$ )
2:    $l \leftarrow \text{SIZE\_IN\_LIMBS}(x)$ 
3:    $k \leftarrow \text{SIZE\_IN\_LIMBS}(m)$ 
4:   if  $l < k$  then
5:     return  $x$             $\triangleright$  Early exit if  $x$  is smaller than  $m$ 
6:   for  $i \leftarrow l - 1$  downto  $k - 1$  do
7:      $q \leftarrow (x_i \cdot 2^{64} + x_{i-1}) / m_{k-1}$     $\triangleright$  Estimate quotient  $q$ 
8:     if  $q(m_{k-1} \cdot 2^{128} + m_{k-2}) > x_i \cdot 2^{128} + x_{i-1} \cdot 2^{64} + x_{i-2}$ 
9:       then
10:         $q \leftarrow q - 1$             $\triangleright$  If  $q$  is too large, adjust estimate
11:         $x \leftarrow x - q \cdot m \cdot 2^{64(i-k)}$     $\triangleright$  Subtract from  $x$ 
12:   return  $x$             $\triangleright$   $x$  holds the remainder
```

Vulnerability exists in a real-world implementation of Curve25519.

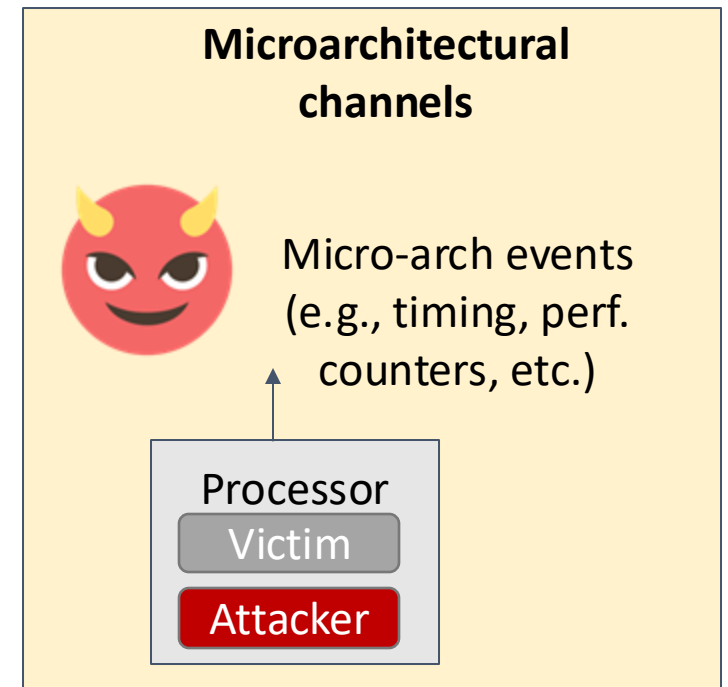
A Rough Classification based on What Attackers Can Observe



Attacker requires measurement equipment → physical access



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

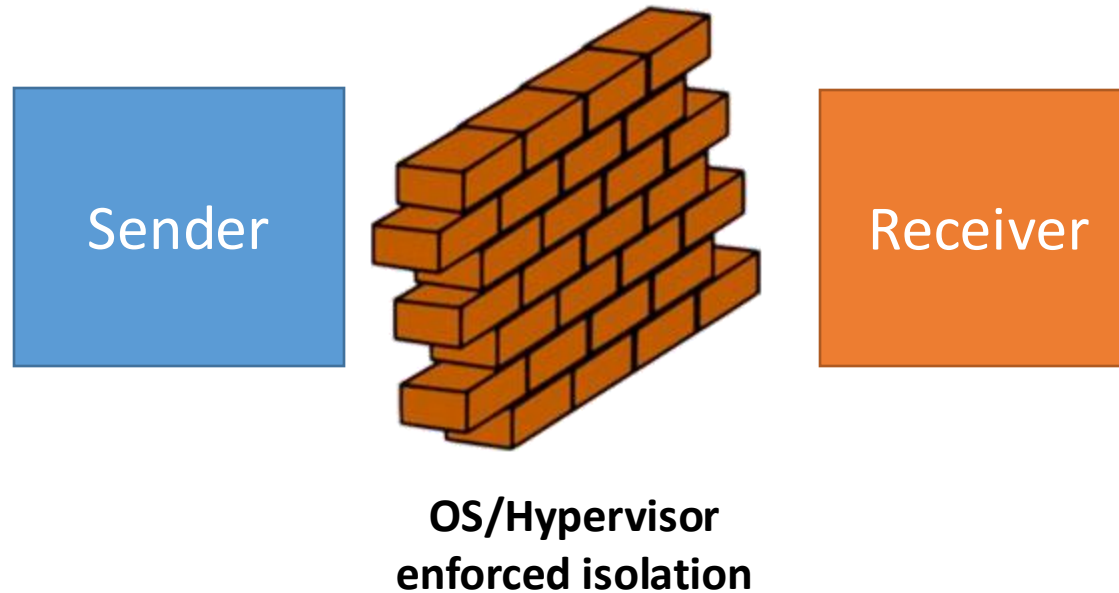


Attacker may be remote, or be co-located

Microarchitecture (uArch) Side Channel



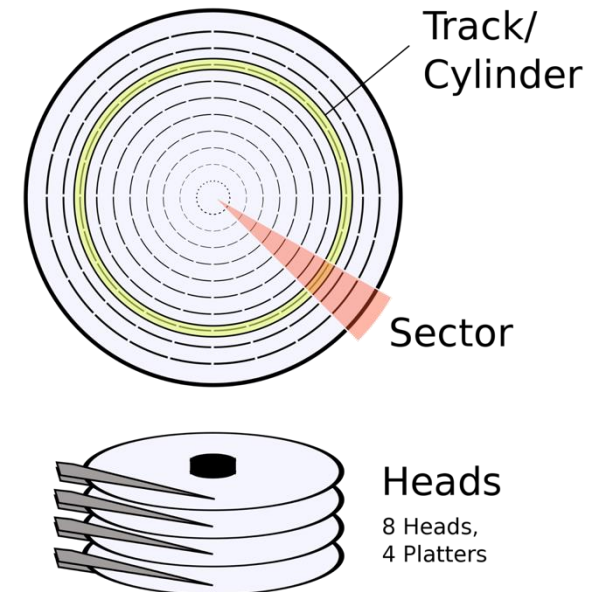
Side Channel Threat Model



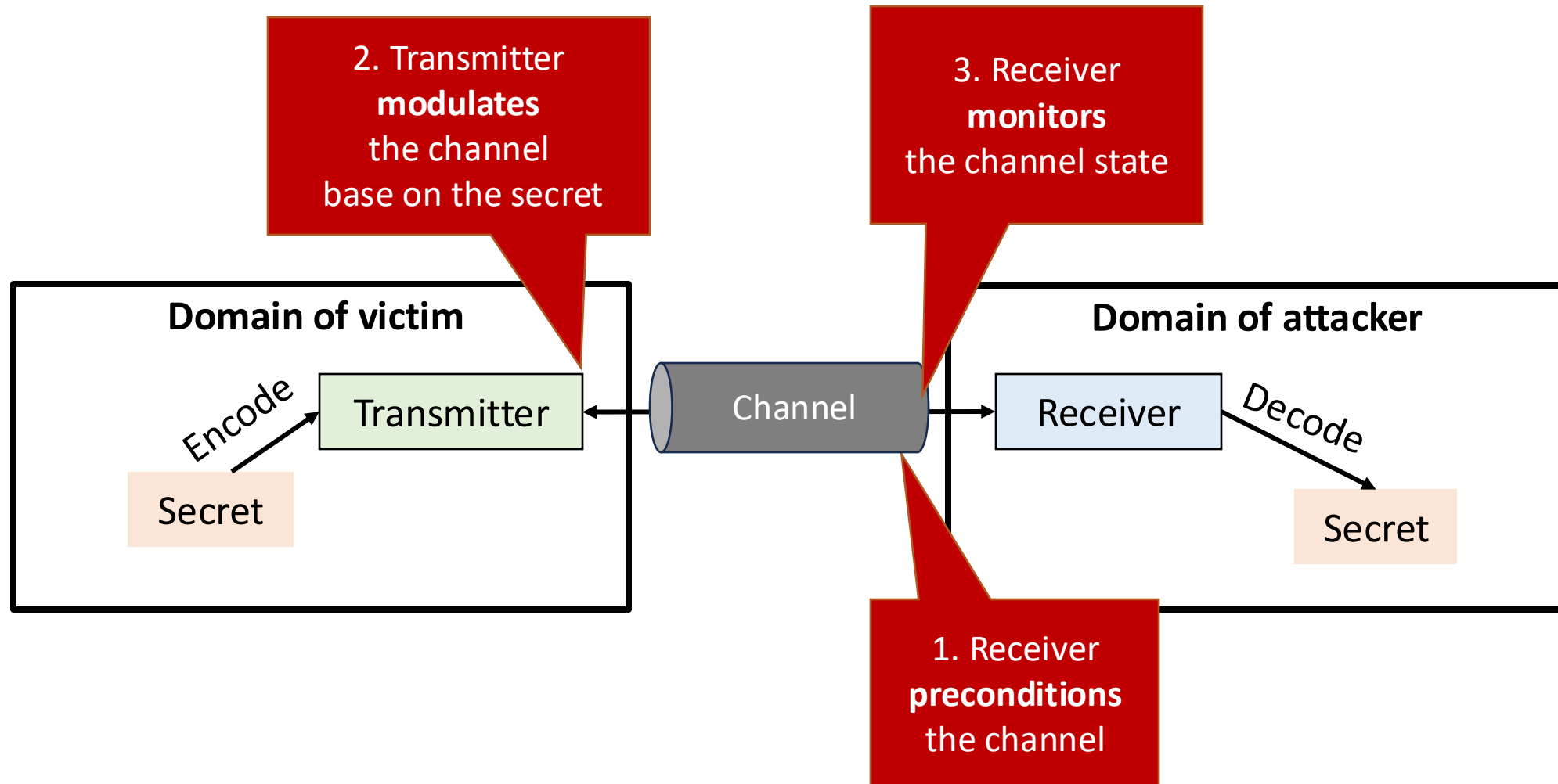
X File, Socket, Pipe, Shared memory (shm in Linux) ...

An Example Attack in 1977

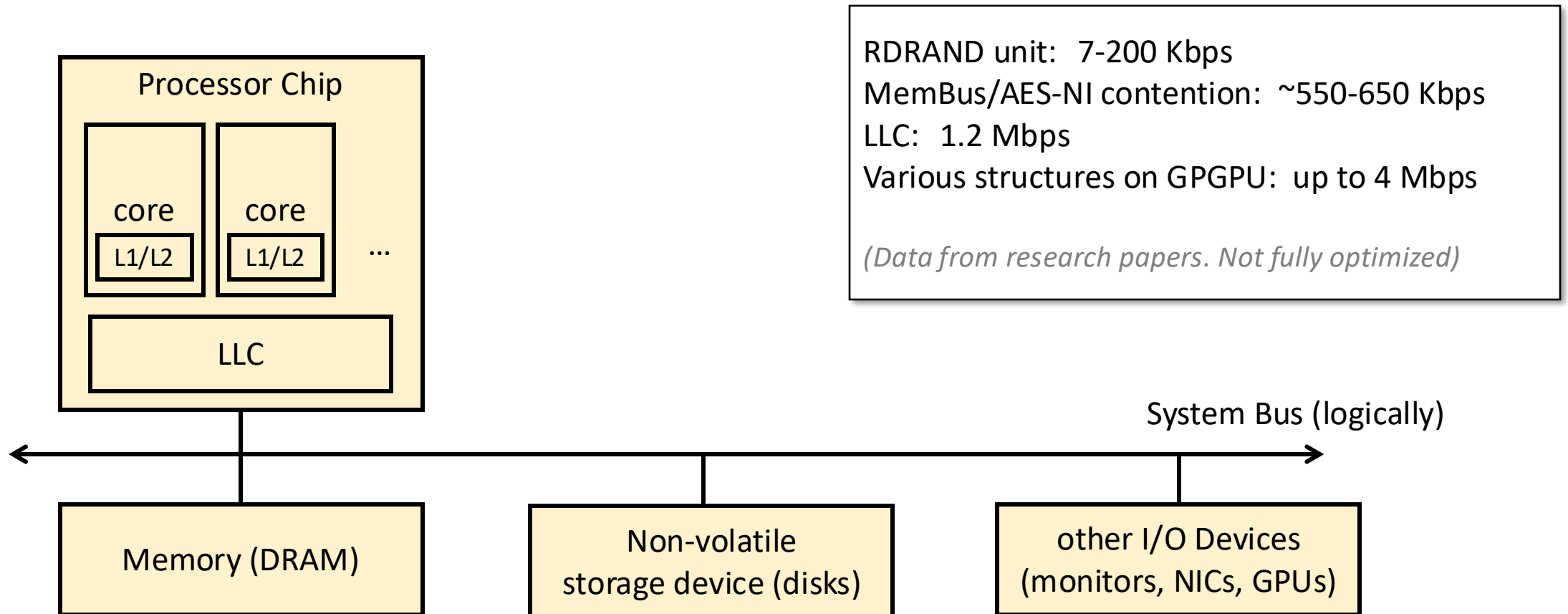
- Disk arm optimization
 - Execute requests by the "elevator algorithm."
- Assume attacker's capability:
 - Can issue multiple requests to any tracks
 - Can measure request latency and the order of its own requests get processed by the disk
- Let's attack 🤖



A Communication Model



uArch Attacks Generalization



Analyze A Demo

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



Next: Cache Side Channel Deep Dive

