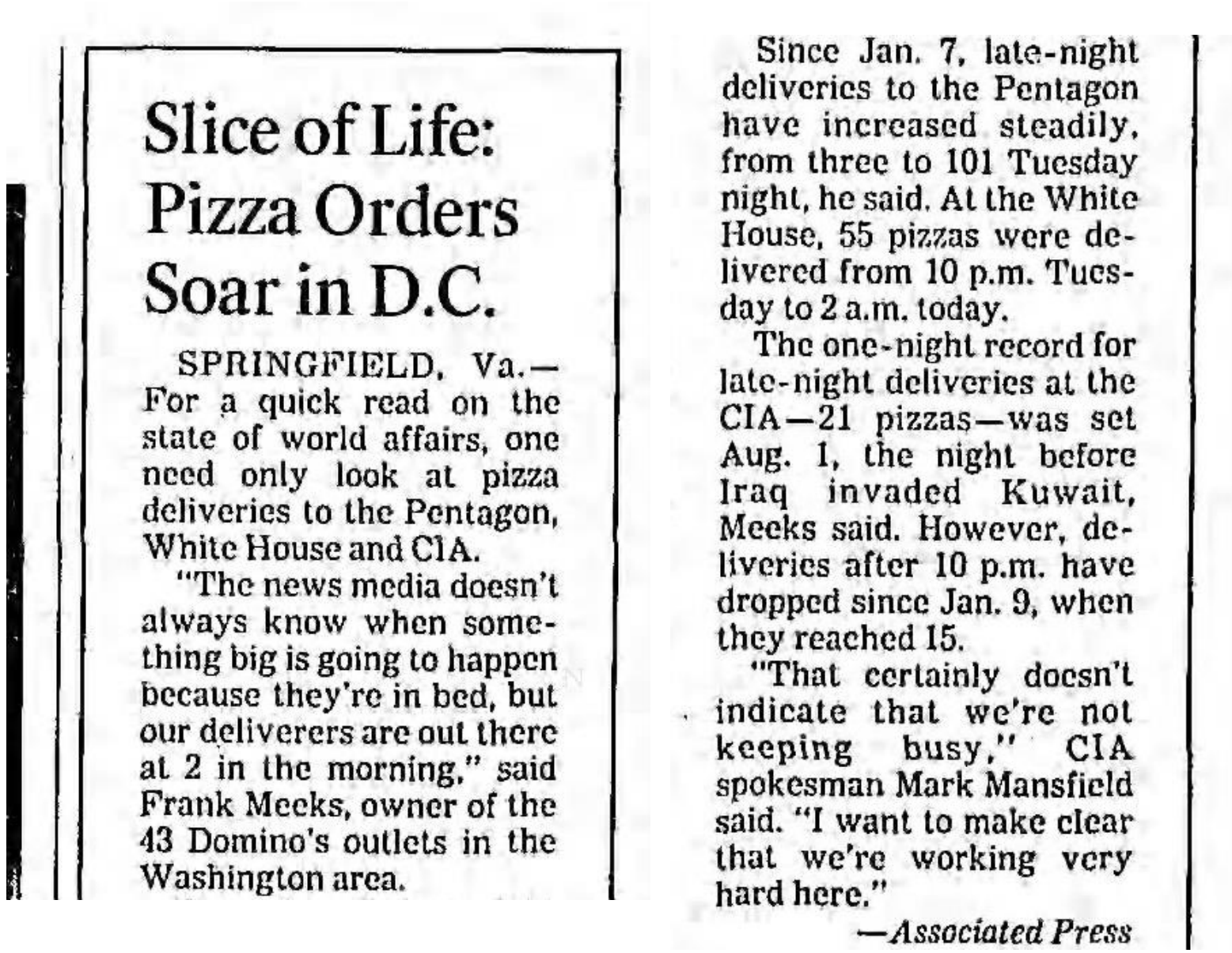
ECE 382N-Sec (FA26):

L1: Course Speedrun

Neil Zhao

neil.zhao@utexas.edu

Pentagon Pizza Theory



Slice of Life: Pizza Orders Soar in D.C.

SPRINGFIELD, Va.—For a quick read on the state of world affairs, one need only look at pizza deliveries to the Pentagon, White House and CIA.

"The news media doesn't always know when something big is going to happen because they're in bed, but our deliverers are out there at 2 in the morning," said Frank Meeks, owner of the 43 Domino's outlets in the Washington area.

Since Jan. 7, late-night deliveries to the Pentagon have increased steadily, from three to 101 Tuesday night, he said. At the White House, 55 pizzas were delivered from 10 p.m. Tuesday to 2 a.m. today.

The one-night record for late-night deliveries at the CIA—21 pizzas—was set Aug. 1, the night before Iraq invaded Kuwait, Meeks said. However, deliveries after 10 p.m. have dropped since Jan. 9, when they reached 15.

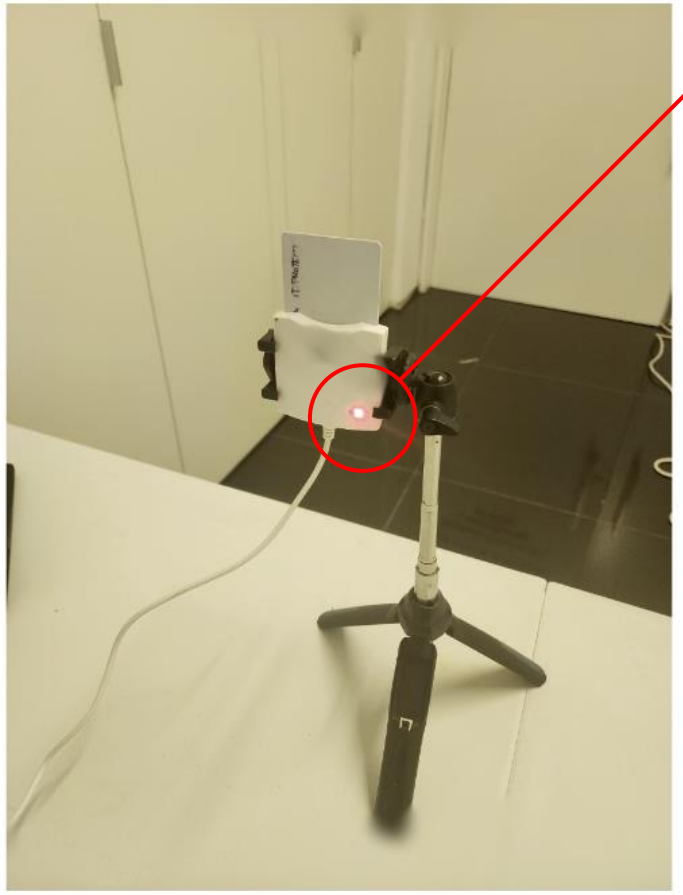
"That certainly doesn't indicate that we're not keeping busy," CIA spokesman Mark Mansfield said. "I want to make clear that we're working very hard here."

—Associated Press

Pizza deliveries to the CIA soared the night before Iraq invaded Kuwait

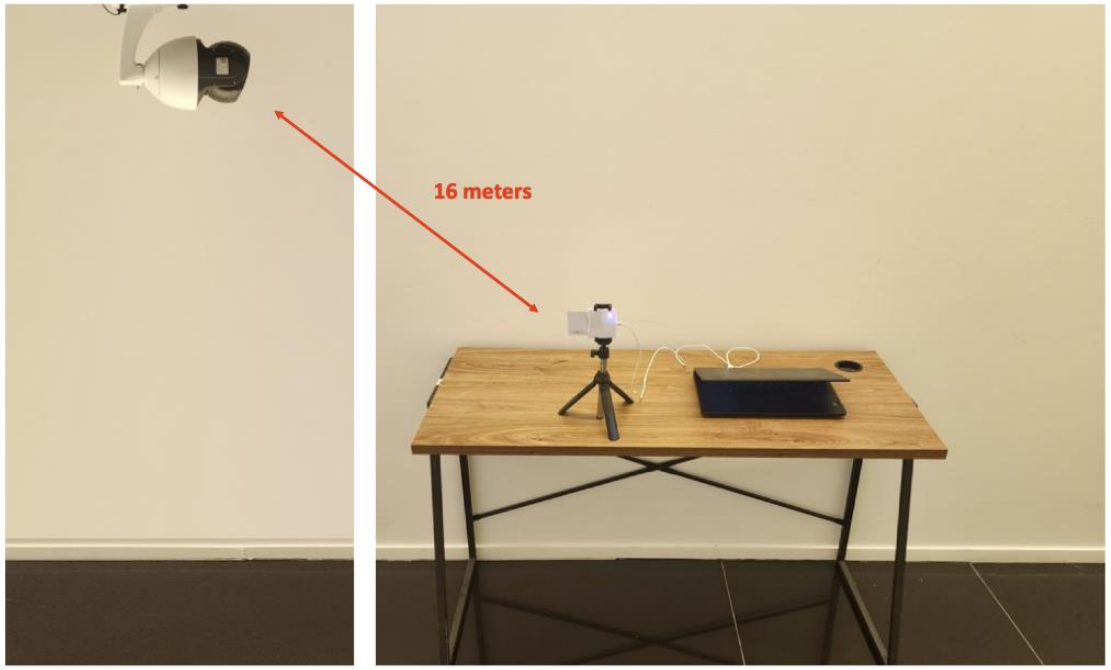
Source: The LA Times
Jan 16, 1991

Side Channel Example: Video-based Cryptanalysis



ECDSA operation ⇒ Higher power consumption
⇒ LED brightness changes ⇒ Captured by a security camera

End-to-end recovery of a 256-bit ECDSA private key from video footage



*Nassi et al., "Video-Based Cryptanalysis: Extracting Cryptographic Keys from Video Footage of a Device's Power LED Captured by Standard Video Cameras", IEEE S&P '24

Side Channel Example: Leaky String Comparison

A naïve implementation that compares strings s1 and s2

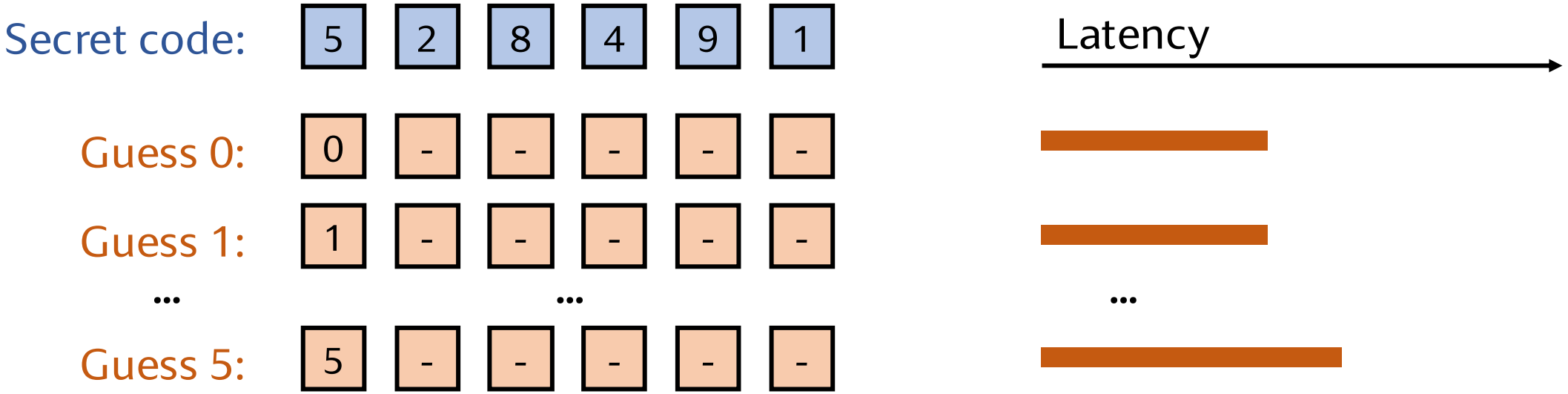
```
bool str_equal(const char *s1, const char *s2) {
    for (; *s1 && *s2; s1++, s2++) {
        if (*s1 != *s2) return false; // Early return
    }
    return *s1 == *s2;
}
```

More number of matching bytes between s1 and s2 → Longer execution time

Side Channel Example: Leaky String Comparison

Leaking a secret access code

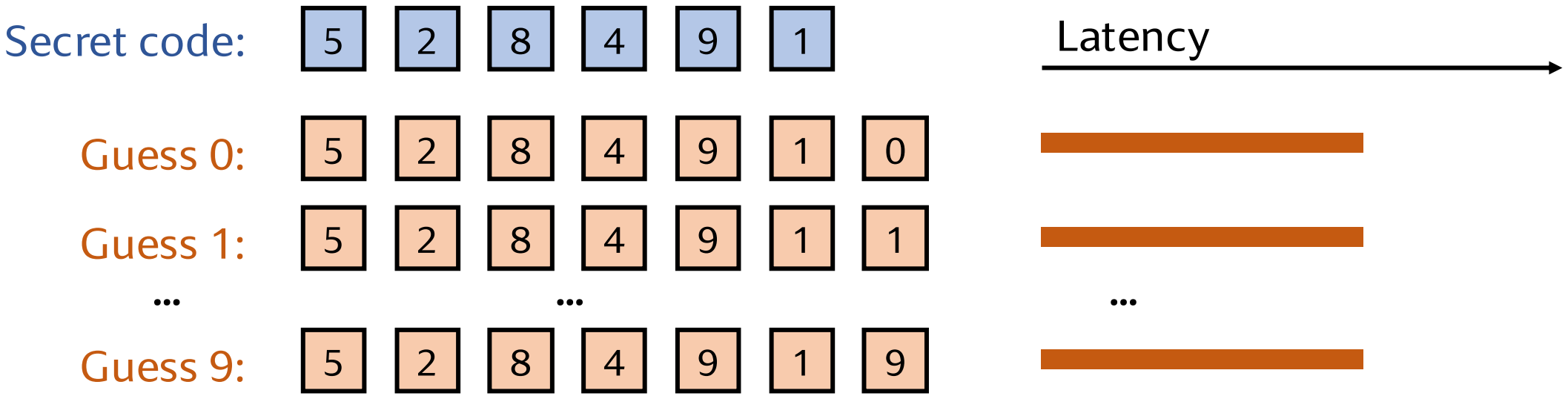
```
bool check_access_code(const char *user_input) {
    return str_equal(user_input, SECRET);
}
```



Side Channel Example: Leaky String Comparison

Leaking the length of the secret access code

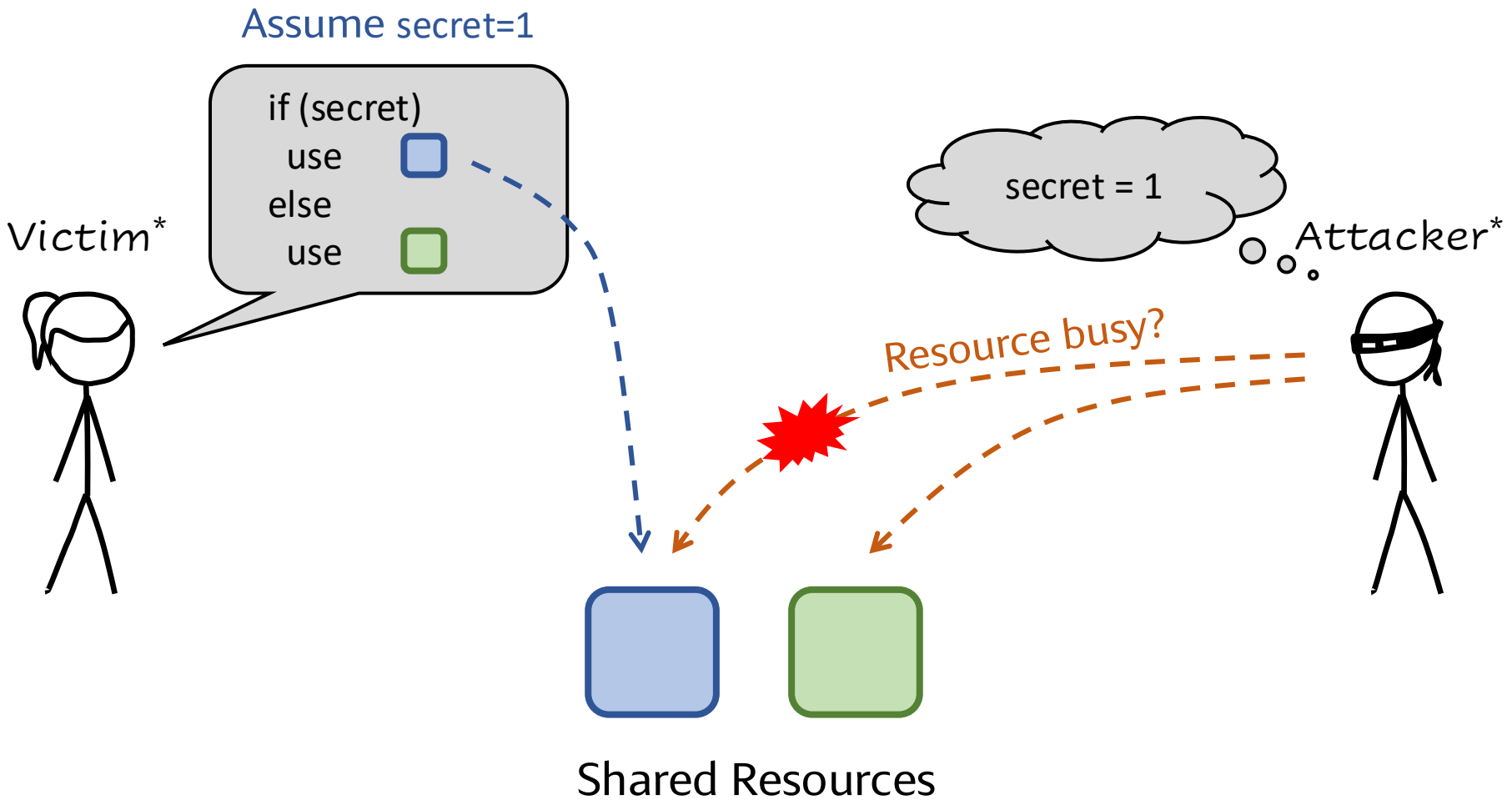
```
bool check_access_code(const char *user_input) {
    return str_equal(user_input, SECRET);
}
```



Launch Code Cracking in WarGames (1983)

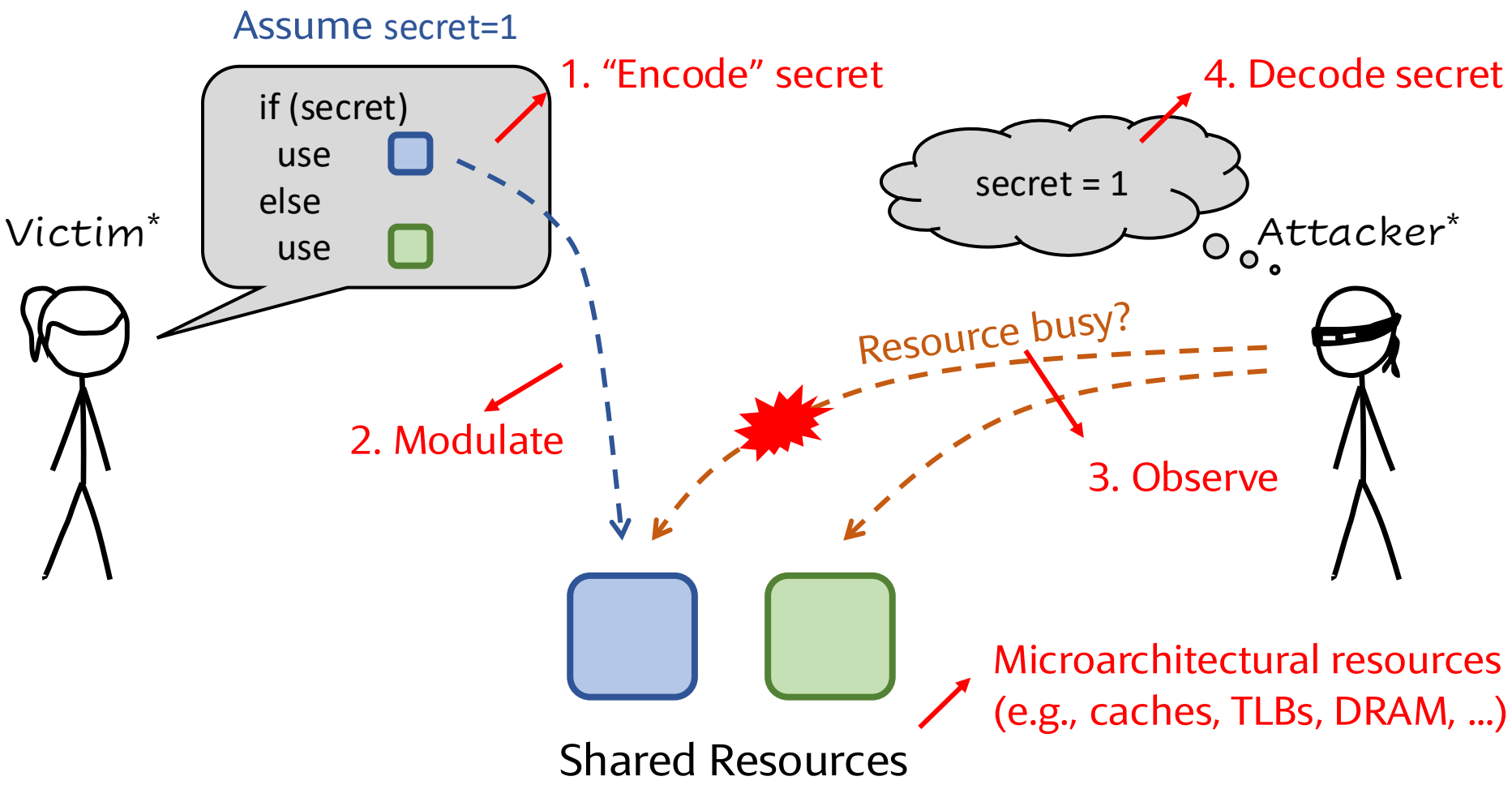
If the AI could validate each character of the launch code one-by-one (as shown in the movie):
36 possibilities x 10 characters => At most 360 attempts!
They won't have time to shut it down!

Side Channels based on Sharing



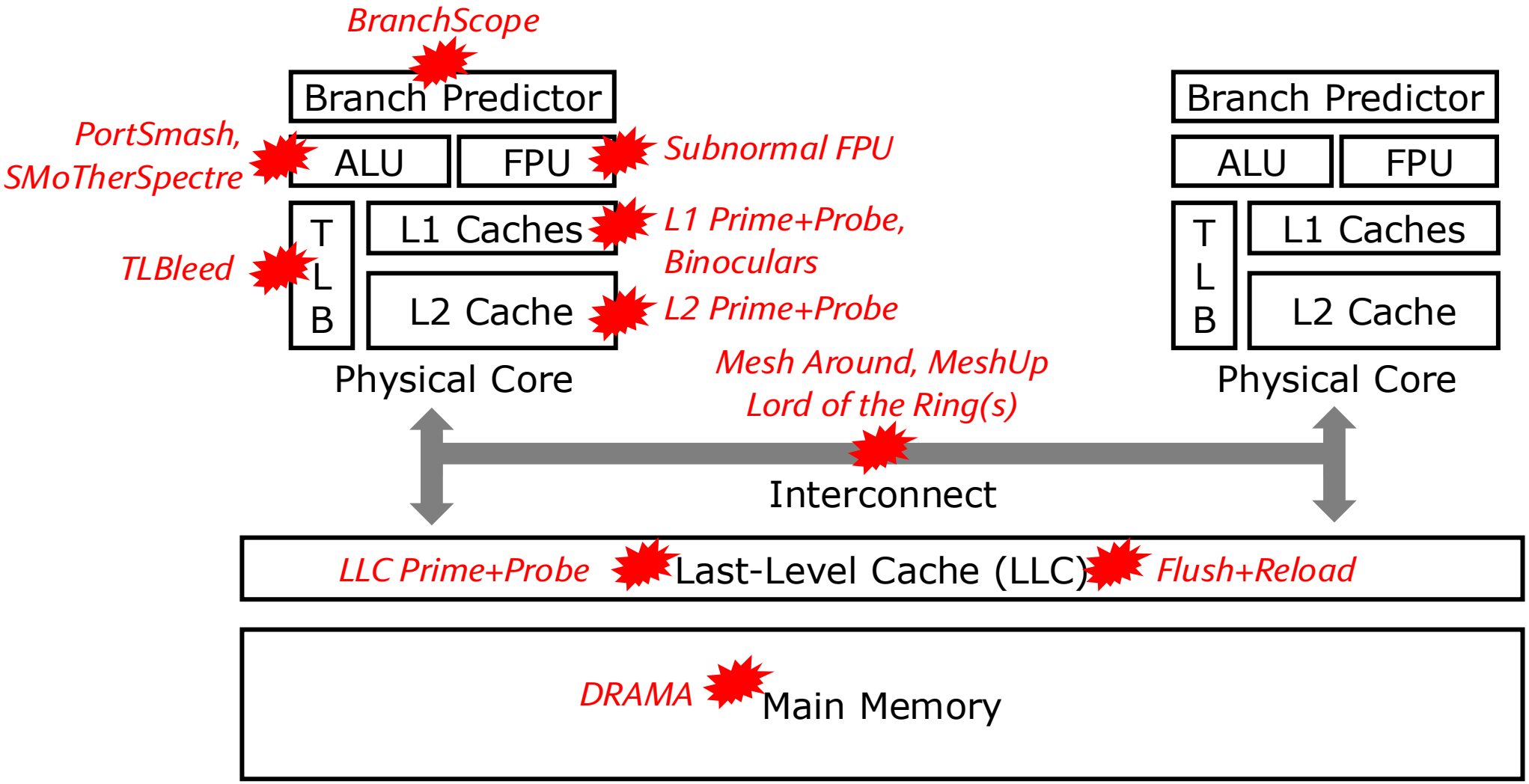
*Characters are based on https://xkcd.com/2176 and https://xkcd.com/1808 (under a CC Attribution-NonCommercial 2.5 License)

Side Channels based on Sharing

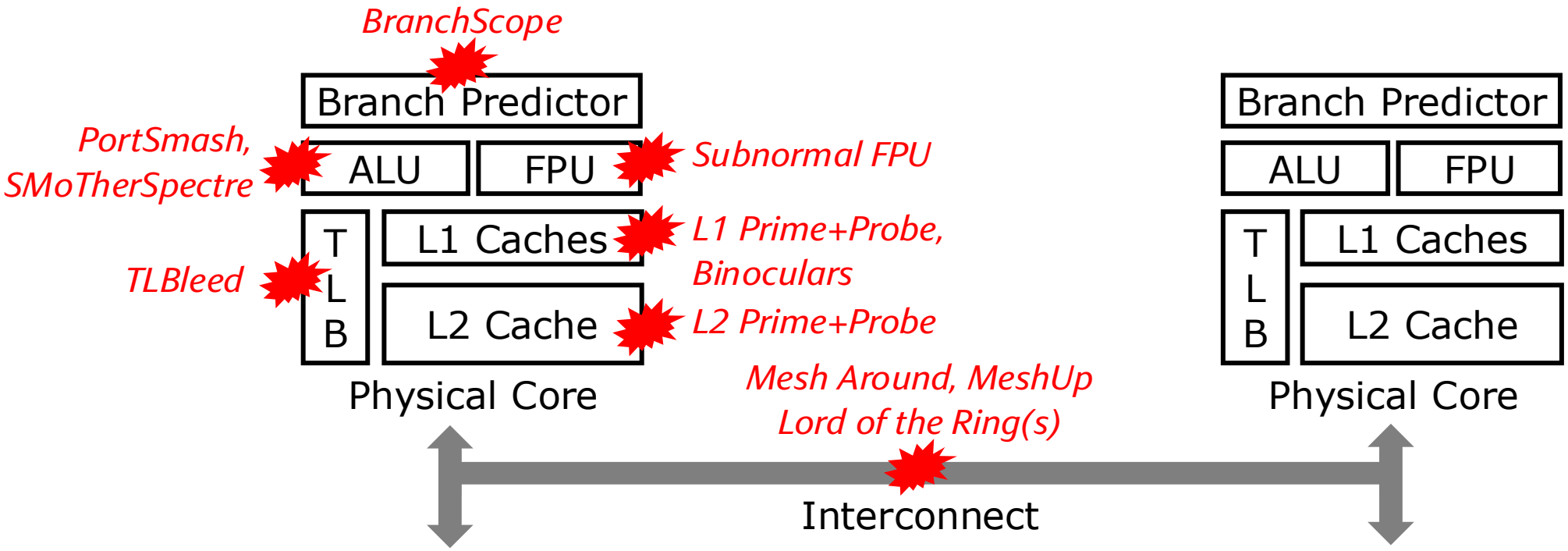


*Characters are based on https://xkcd.com/2176 and https://xkcd.com/1808 (under a CC Attribution-NonCommercial 2.5 License)

Many Microarchitectural Side-Channel Attacks



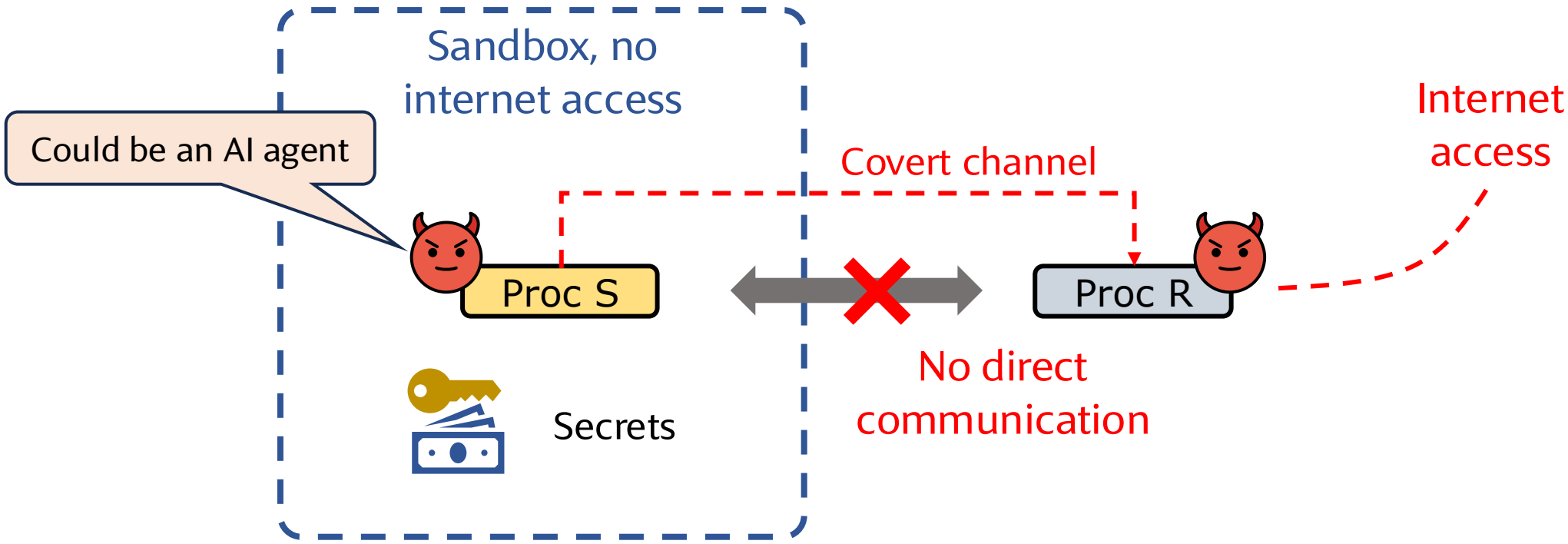
Many Microarchitectural Side-Channel Attacks



Term Project Directions:

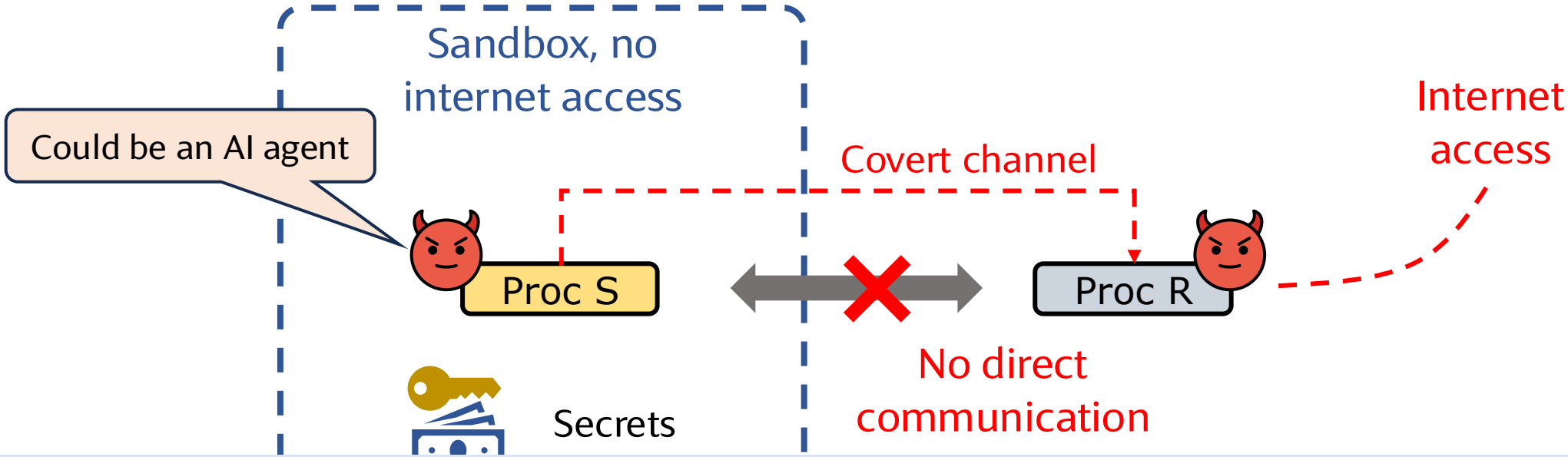
- Discover new microarchitectural or system-level side channels
- Reverse engineer CPU or GPU microarchitectures ⇒ Better attacks
- Efficient hardware designs to isolate resources among different security domains

Covert Channels



"A note on the confinement problem" by Butler W. Lampson, CACM, 1973

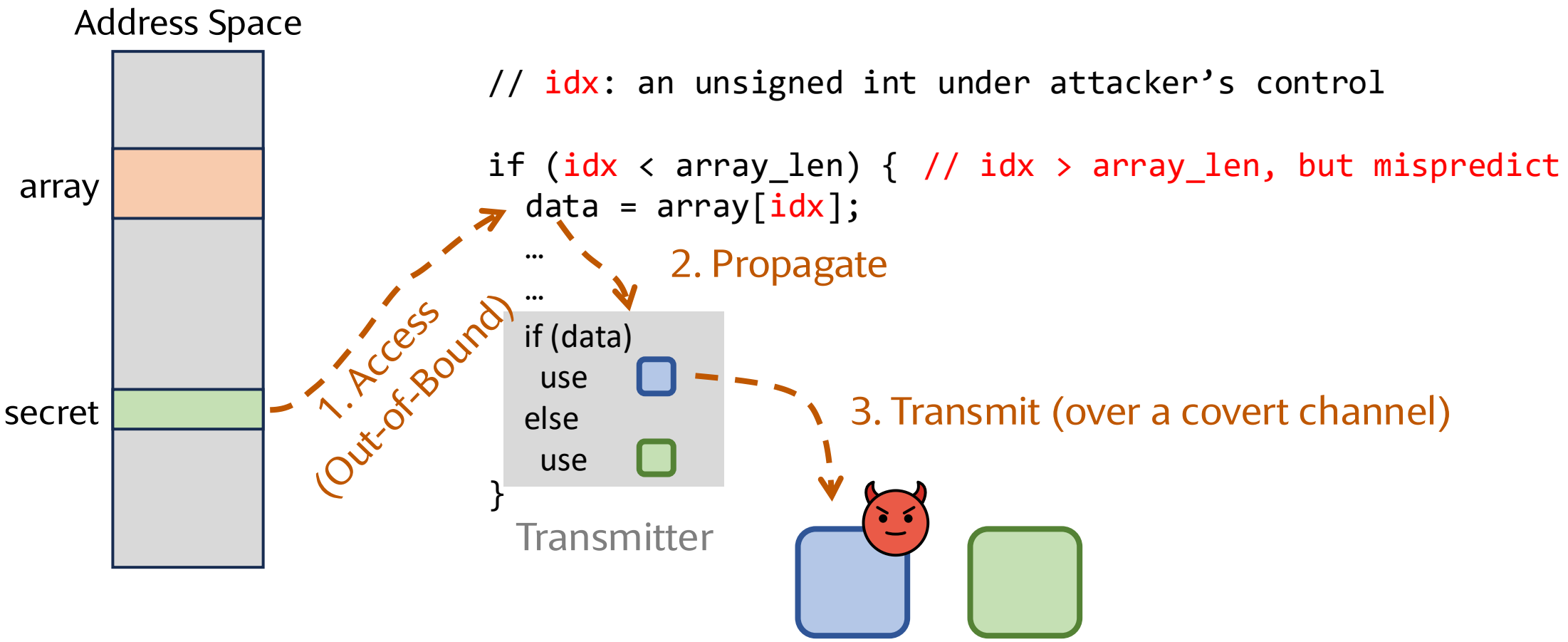
Covert Channels



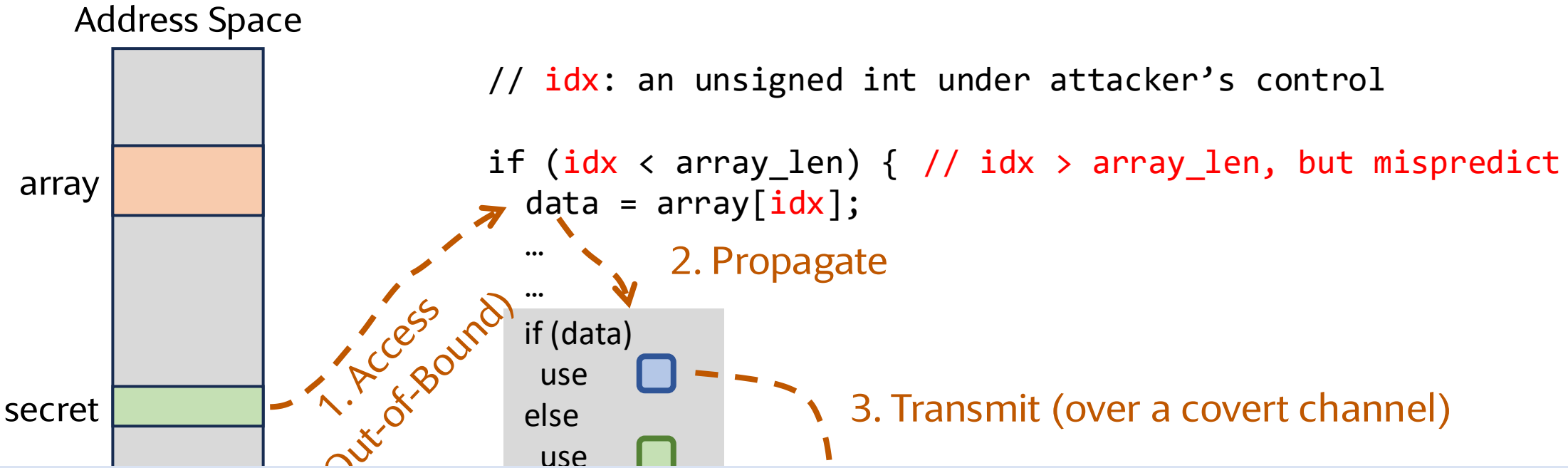
Term Project Directions:

- Faster and more noise-resilient covert channels
- Covert channel for triggering malware

Transient Execution Attacks



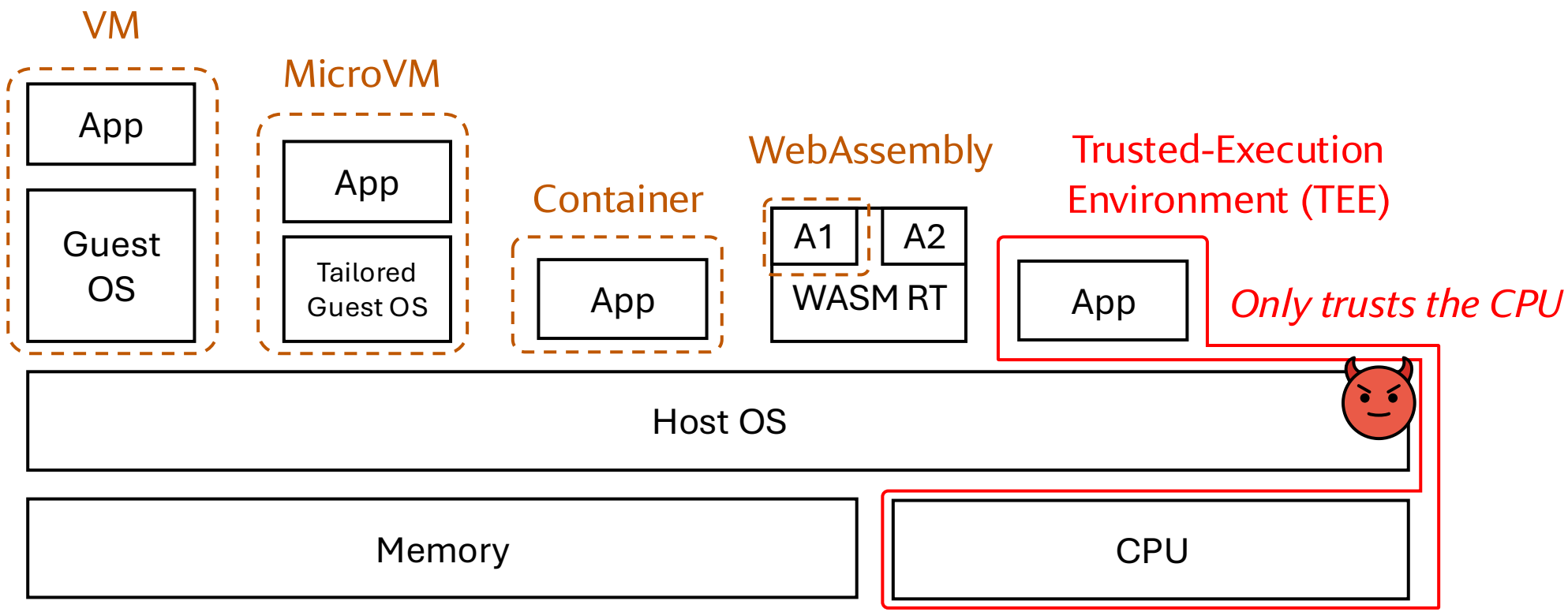
Transient Execution Attacks



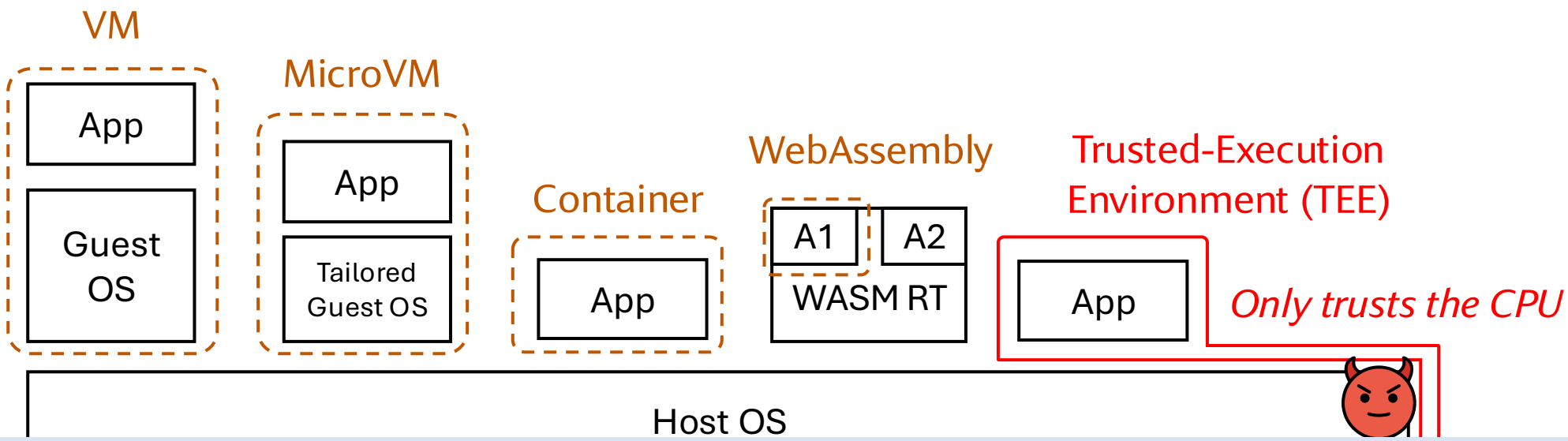
Term Project Directions:

- Automatic gadget discovery in high-value applications (Linux, web browsers, …)
- Improve the performance of transient execution defenses

Isolation


VM
App
Guest OS
MicroVM
App
Tailored Guest OS
Container
App
WebAssembly
A1
A2
WASM RT
Trusted-Execution Environment (TEE)
App
Only trusts the CPU
Host OS
Memory
CPU

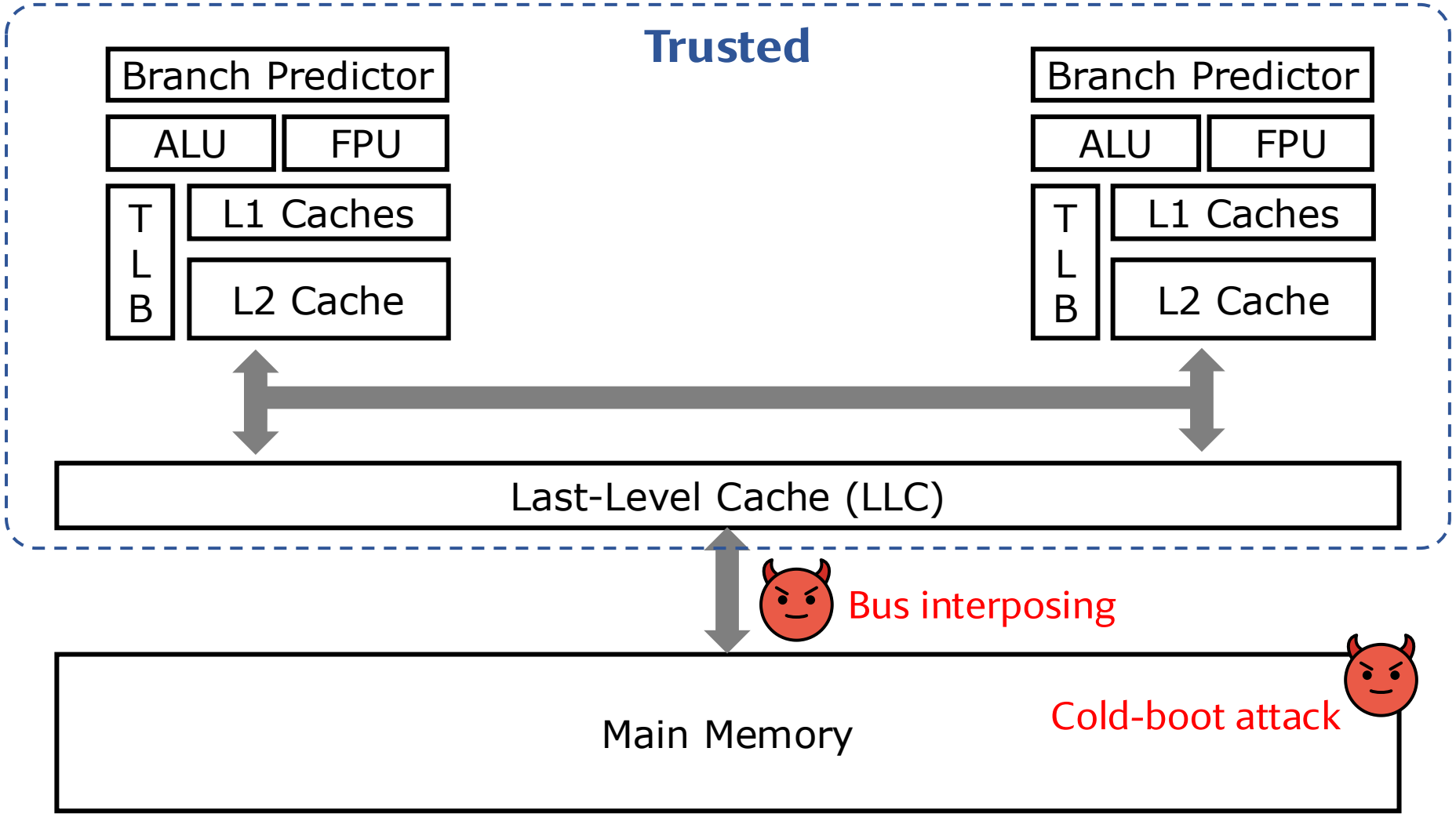
Isolation



Term Project Directions:

- Performance study of different isolation mechanisms (need to show why)
- New enclave design/implementation
- Attack these isolated environments (e.g., Spectre in WASM, sandbox escaping in OpenShell)

Memory Encryption and Integrity Protection



Memory Safety

De-referencing an out-of-bound pointer:

- Out-of-bound writes → Buffer overflow
  - Compromise program integrity
- Out-of-bound reads → Buffer over-read
  - Information leakage. Can lead to integrity attack
    - E.g., leaking the stack canary
  - Another high-profile example: Heartbleed

De-referencing a dangling pointer that points to a deleted object :

- Writes → Compromise code or data integrity
- Reads → Information leakage

Hardware Support for Memory Safety

- Hardware-enforced control-flow integrity
  - Example: Intel CET

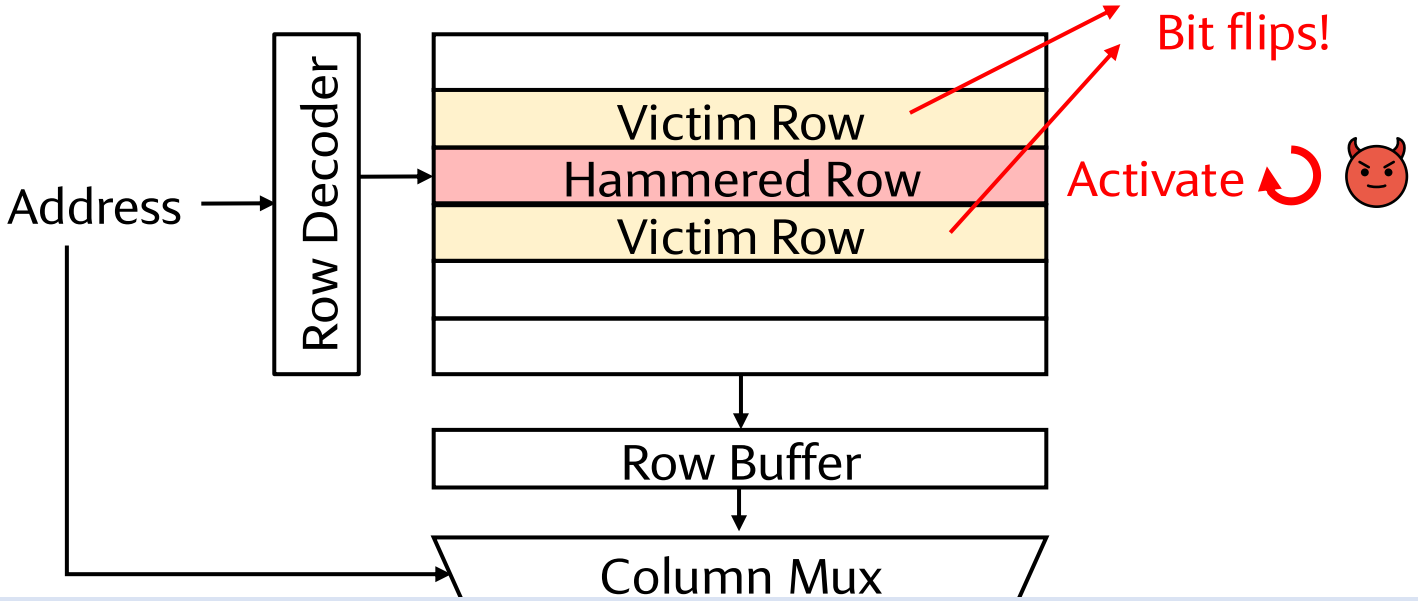
- Probabilistic hardware enforcement
  - ARM's Pointer authentication
  - ARM's Memory tag extension

- Hardware-enforced bounds check
  - Example: Capability Hardware Enhanced RISC Instructions (CHERI)

Term Project Directions:

- Compare the performance and protection tradeoffs of different protection mechanisms
- Attack these mechanisms (e.g., there was prior work that uses Spectre to attack them)

RowHammer



Term Project Directions:

- Evaluate the cost of the proposed RowHammer defenses (e.g., PRAC)
- Reduce the performance and storage overhead of RowHammer defenses