Comp 590-184:
Hardware Security and Side-Channels

Lecture 6: ML-assisted Browser attacks

January 29, 2026

Andrew Kwong

Slides adapted from Jack Cook
(https://jackcook.github.io/bigger-fish/)

Overview

- Super brief ML tutorial
- Lab Discussion

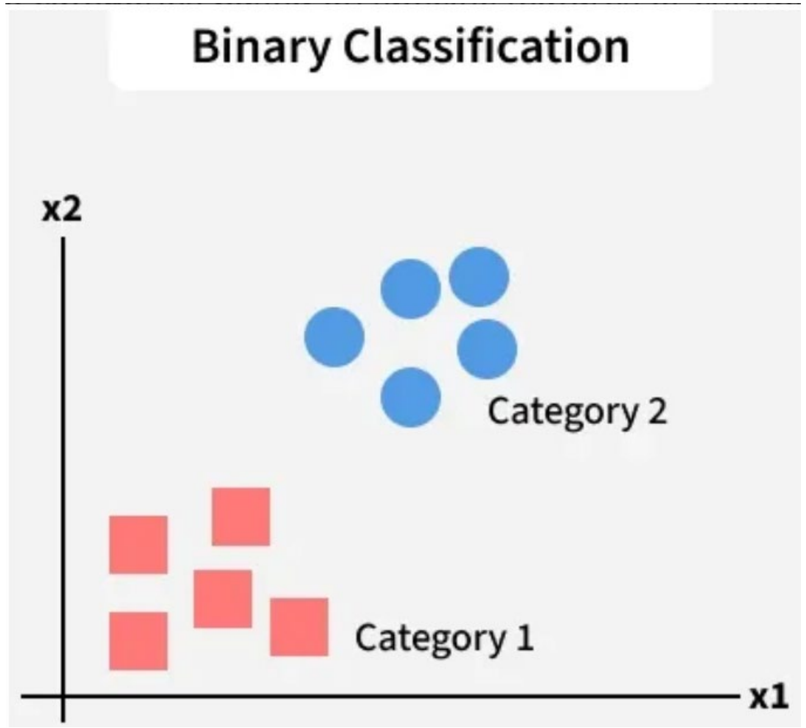
Classification

$$h: X \rightarrow Y$$

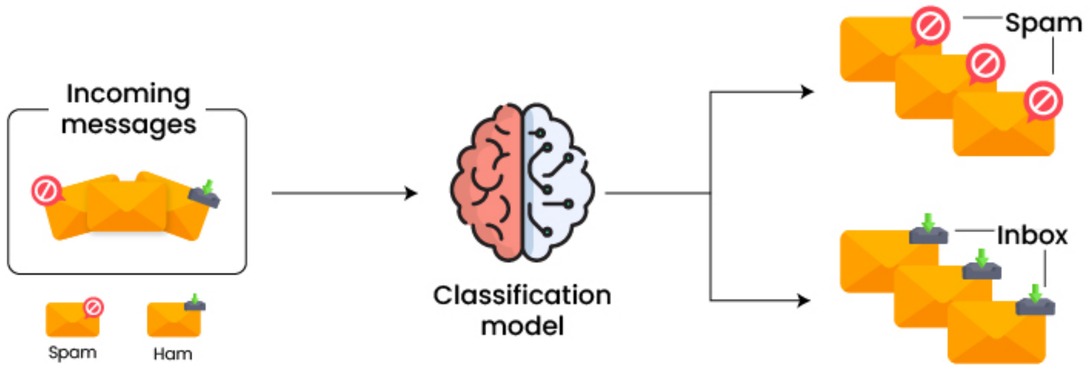
- input: data points, or feature vectors ($\mathbb{R}^d$)
- output: A finite, unordered set of labels

Classification

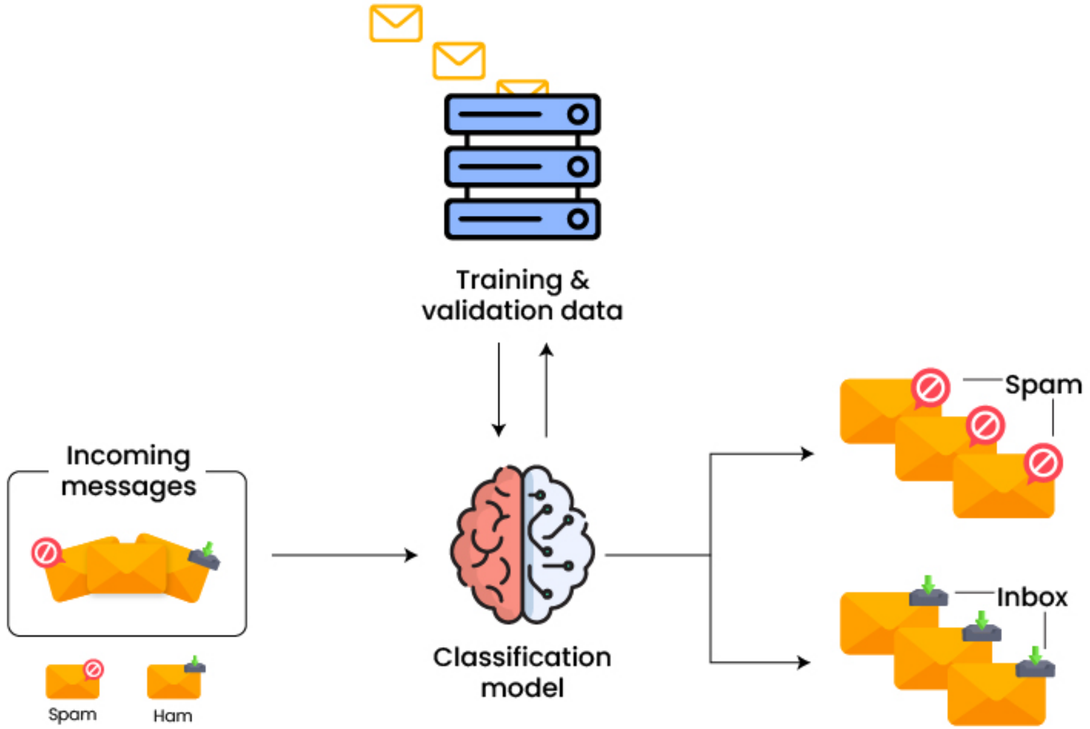
$$h: X \rightarrow Y$$



Spam Classification



Spam Classification

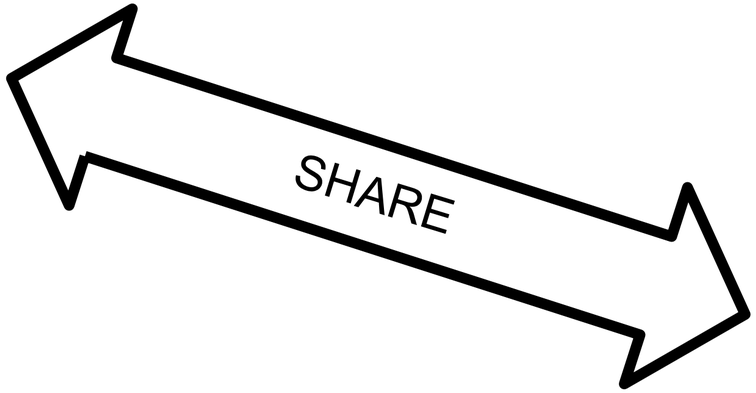


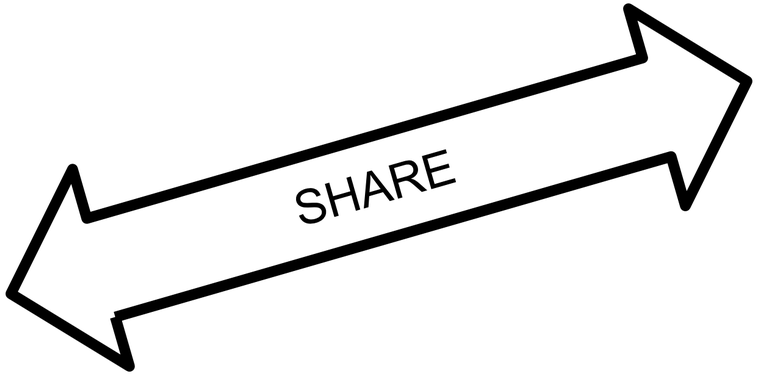
There’s Always a Bigger Fish: A Clarifying Analysis of a Machine-Learning-Assisted Side-Channel Attack (ISCA `22)

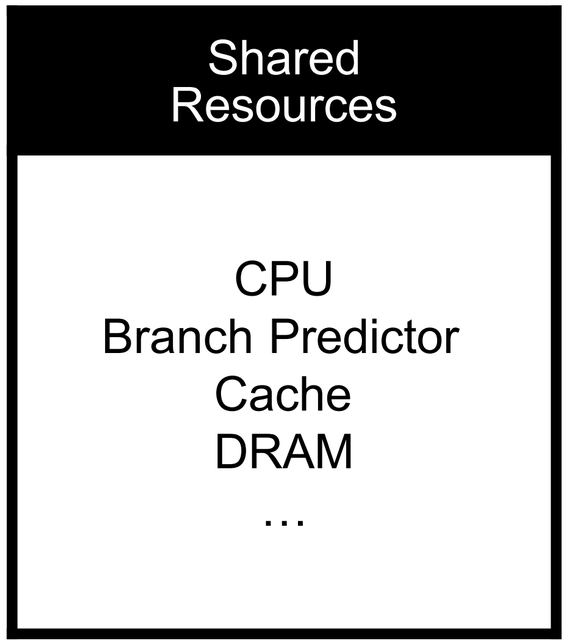
- Sweep-counting attacks (USENIX Security `21)
- ML assisted side-channel attacks are highly effective and even work with noise
- Work as a black box and **are hard to interpret**

Bigger Fish is a detailed analysis of a misunderstood side-channel attack

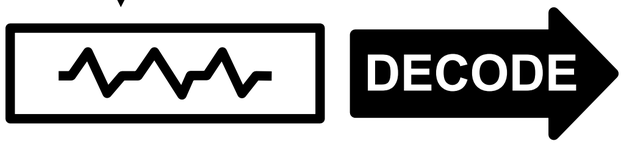
Browser-based Timing Side Channels







Signal

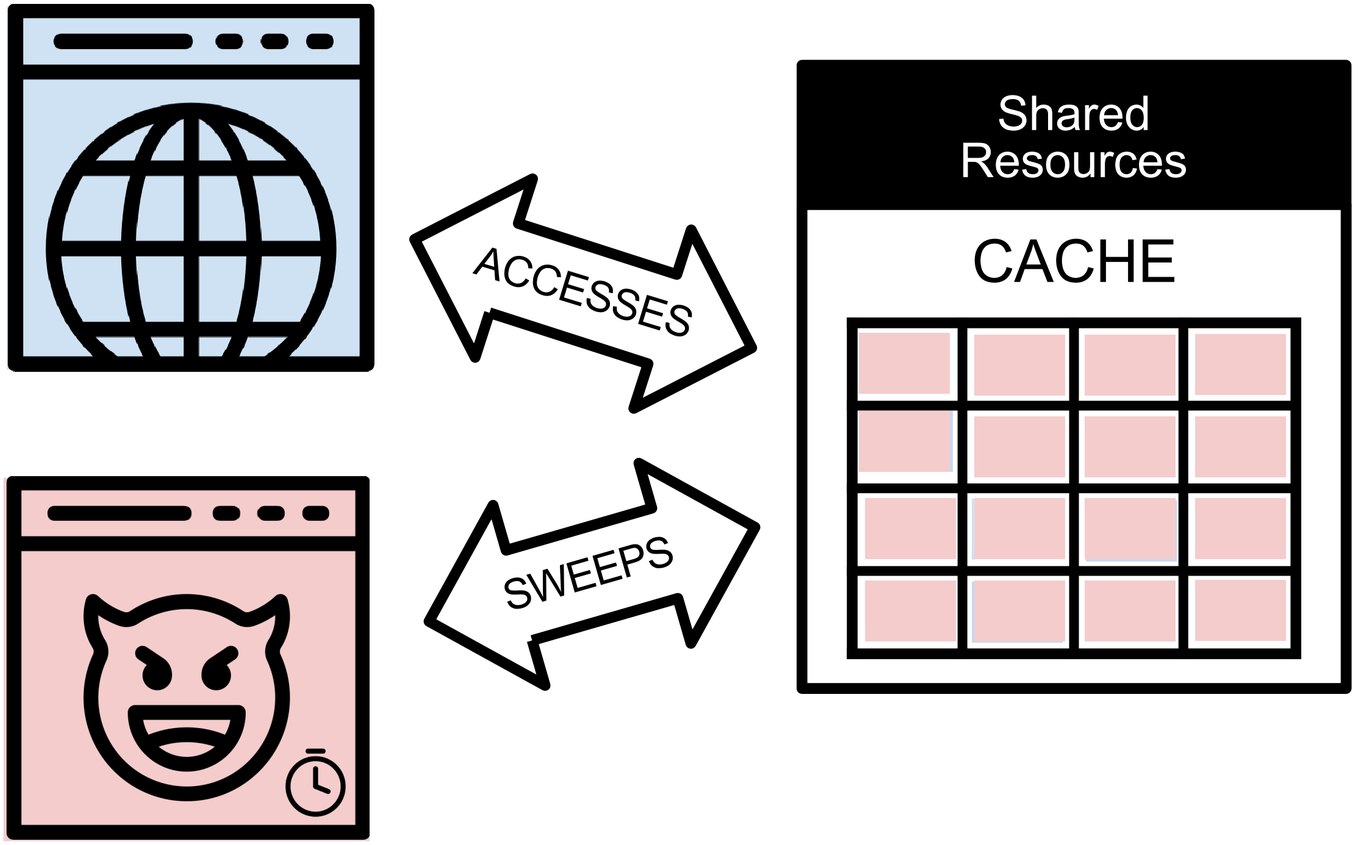


"Victim Secret"

A Cache-Occupancy Attack*

ATTACKER'S CODE

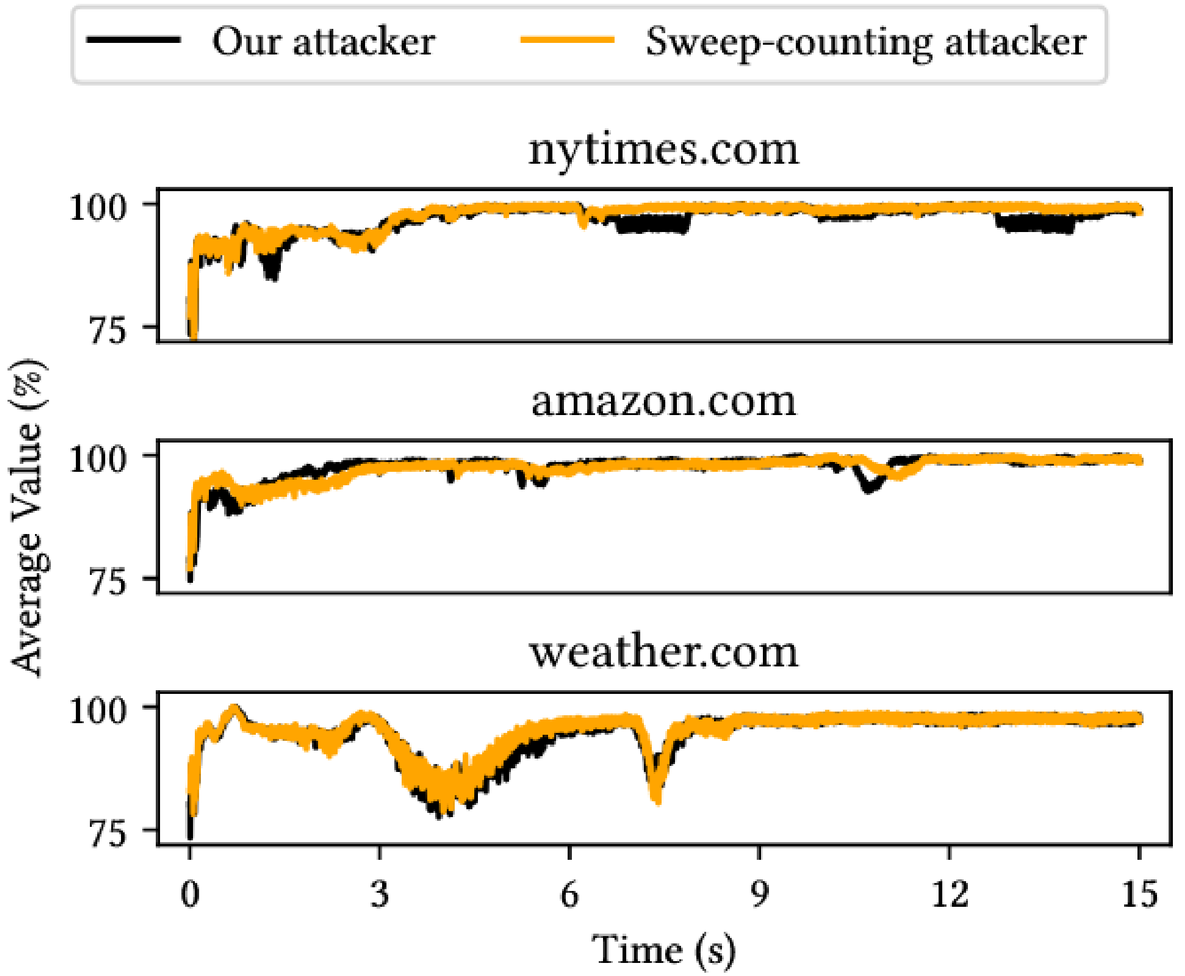
```
loop {
  start = time()
  counter = 0;
  while(time() - start < 5ms) {
    counter++;
    SWEEP_CACHE();
  }
  Trace[start] = counter;
}
```



* Shusterman, et al. "Prime+Probe 1,JavaScript 0: Overcoming Browser-based Side-Channel Defenses." *30th USENIX Security Symposium (USENIX Security 21)*. 2021.

Website Fingerprinting Attacks

- Very serious privacy implications
- Can be mounted from JavaScript
- Good benchmark for side channels


Our attacker
Sweep-counting attacker
nytimes.com
amazon.com
weather.com
Average Value (%)
100
75
0
3
6
9
12
15
Time (s)

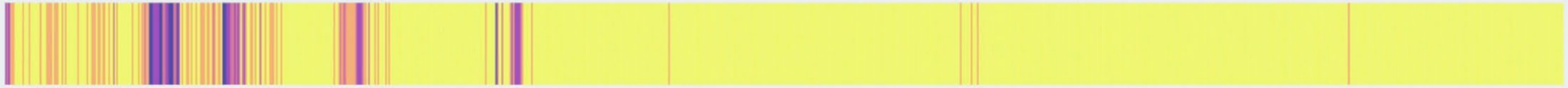
Chrome File Edit View History Bookmarks Profiles Tab Window Help Wed Jun 15 9:01 AM

There's Always a Bigger Fish

jackcook.github.io/bigger-fish/

Collect trace | Download traces

#1: amazon.com, 5 seconds

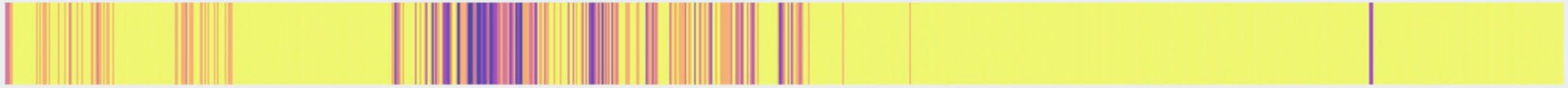


#2: amazon.com, 5 seconds

#3: amazon.com, 5 seconds

#4: weather.com, 5 seconds

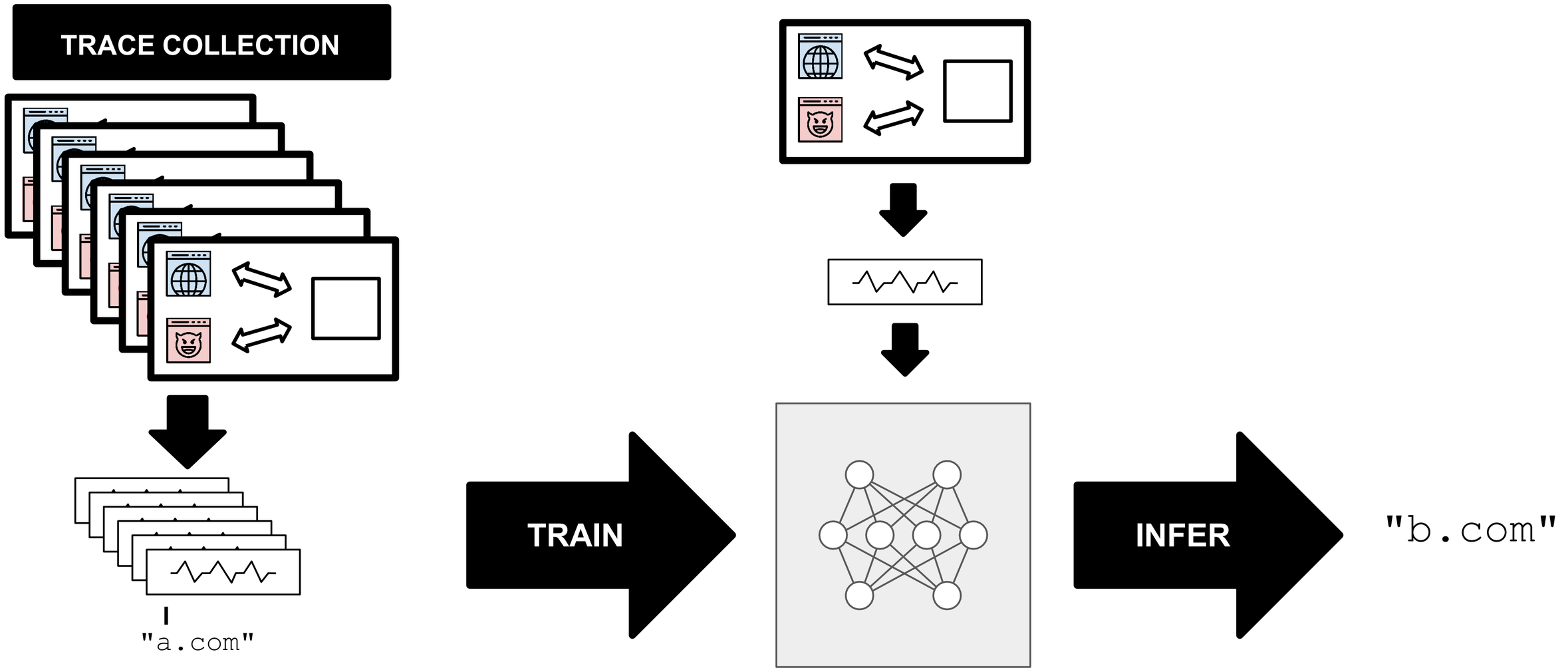
#5: weather.com, 5 seconds



#6: weather.com, 5 seconds

Key Takeaways

Website Fingerprinting: Machine-Learning Classifier



	Top-1 Accuracy (%)				Top-5 Accuracy (%)			
Attack Technique	Intel i5-3470	AMD Ryzen 9 3900X	Apple M1	Samsung Exynos 2100	Intel i5-3470	AMD Ryzen 9 3900X	Apple M1	Samsung Exynos 2100
Cache Occupancy	87.5	69.1	89.7	84.5	97.0	91.4	97.8	95.3
Sweep Counting	45.8	54.9	90.5	69.7	74.3	82.9	98.1	91.5
DNS Racing	50.8	5.4	48.2	5.8	78.5	16.3	83.5	37.1
String and Sock	72.0	53.9	90.6	60.2	90.6	85.5	97.9	85.5
CSS Prime+Probe	50.1	—	15.7	—	78.6	—	32.6	—

Table 2: Closed-world accuracy (percent) across different microarchitectures.

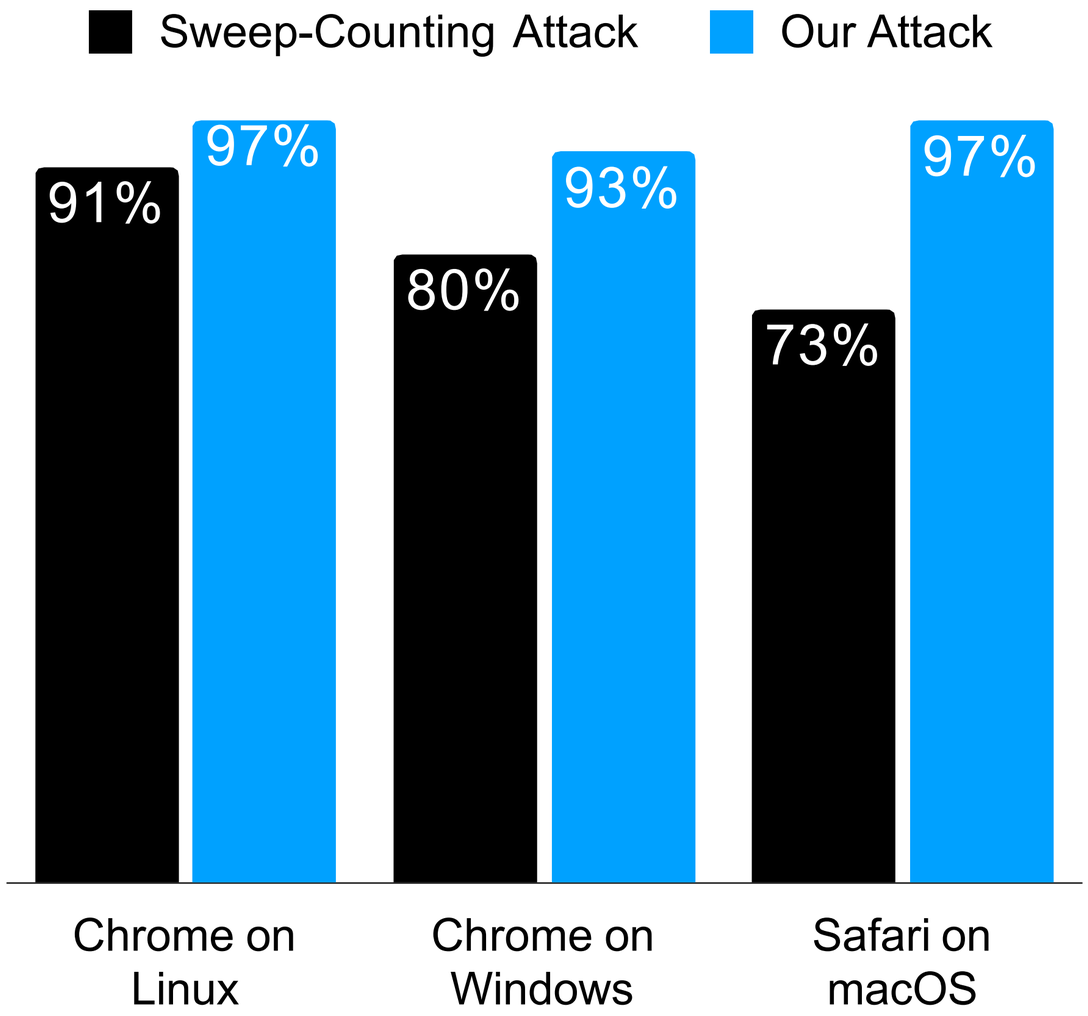
- Sweep-counting understood to be a powerful cache side-channel
- Defeated modern day browser defenses
  - didn’t require any fine-grained timing primitives
  - Didn’t require flushing
  - Didn’t require shared memory
  - Didn’t require eviction sets
- Demonstrated the power of cache side-channels on browsers
  - Or did it?

A Surprising Experiment

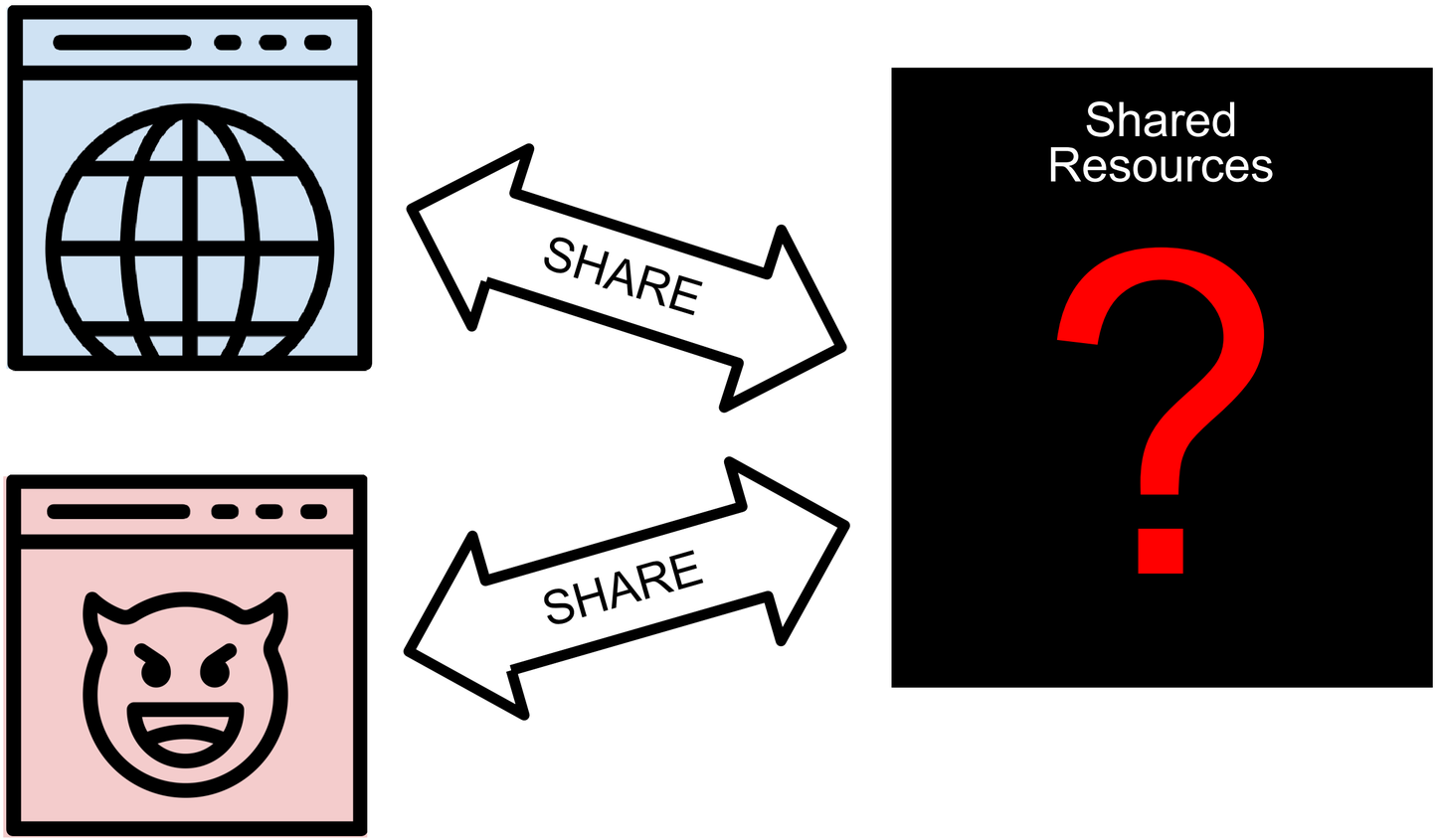
ATTACKER'S CODE

```
loop {
  start = time()
  counter = 0;
  while(time() - start < 5ms) {
    counter++;
  }
  Trace[start] = counter;
}
```

REMOVE MEMORY ACCESSES



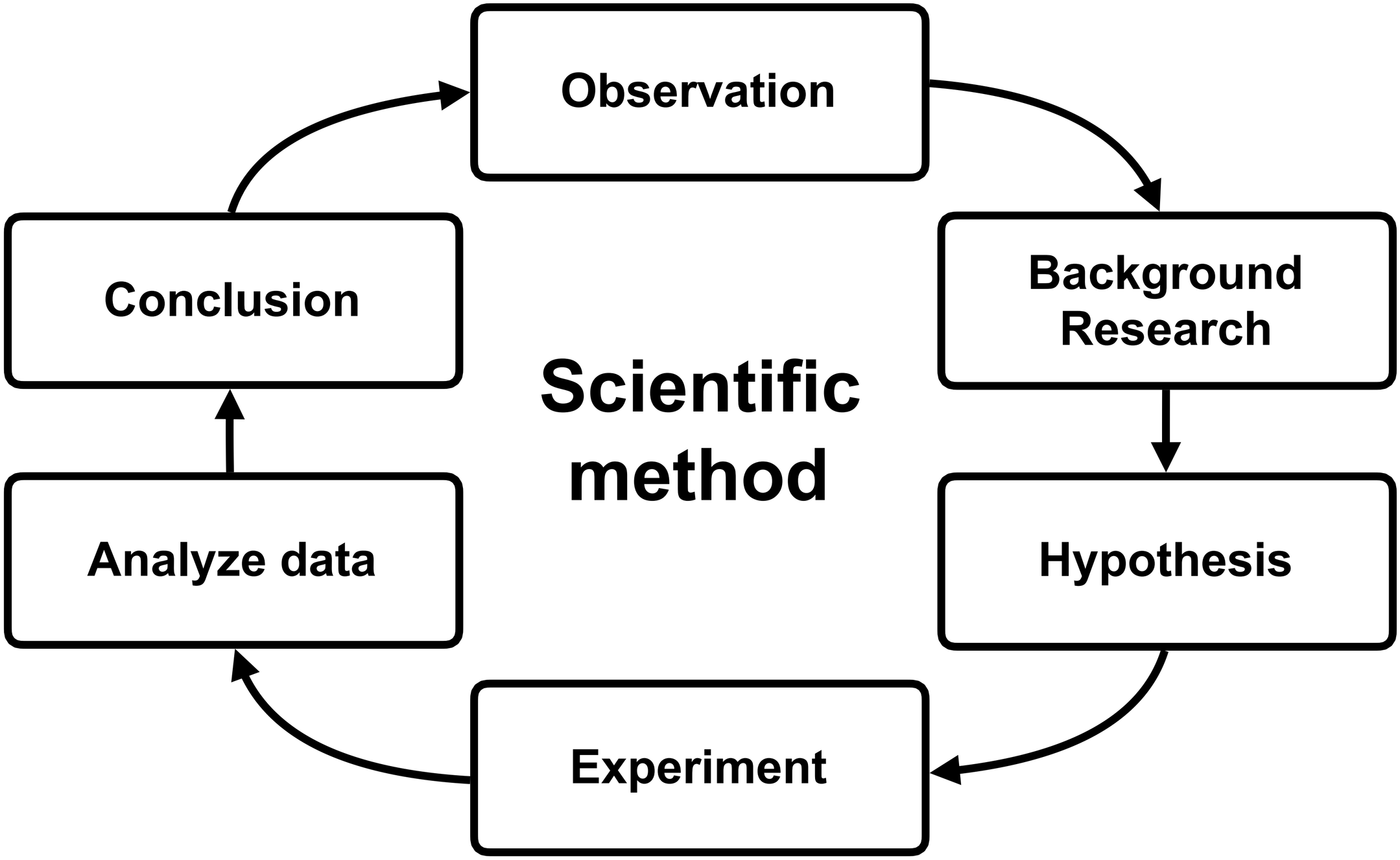
What is the primary side channel?



ML-Assisted Side-Channel Attacks

- Work as a black box and **are hard to interpret**

Bigger Fish is a detailed analysis of a misunderstood side-channel attack


Observation
Background Research
Hypothesis
Experiment
Analyze data
Conclusion
Scientific method

DVFS?

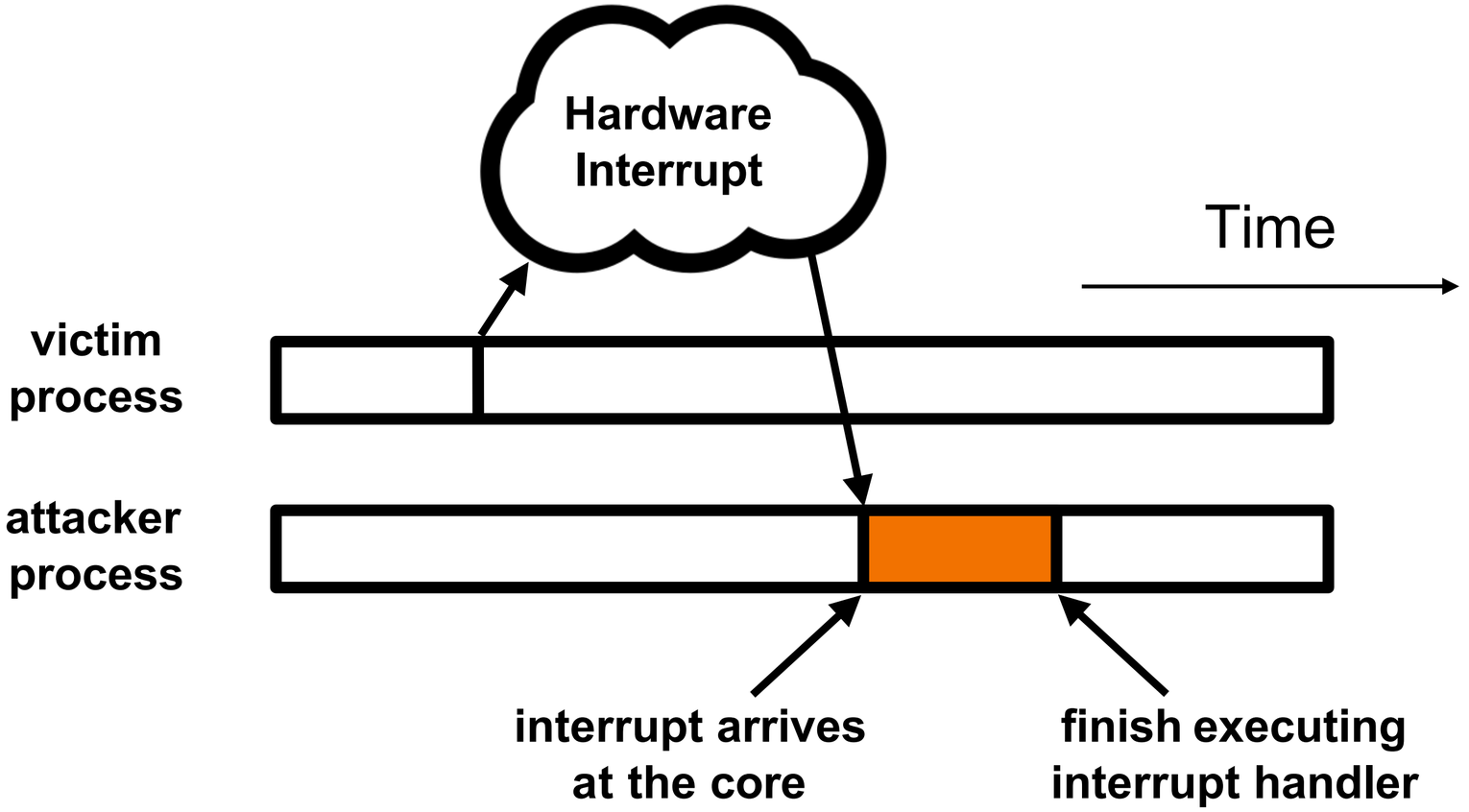
- 94.2% accuracy

Core Contention

- 94.0% accuracy

System Interrupts

- Used to deal with asynchronous events
  - e.g. Graphics interrupts render content on a display
- Some can be “pinned” to specific cores, some can’t

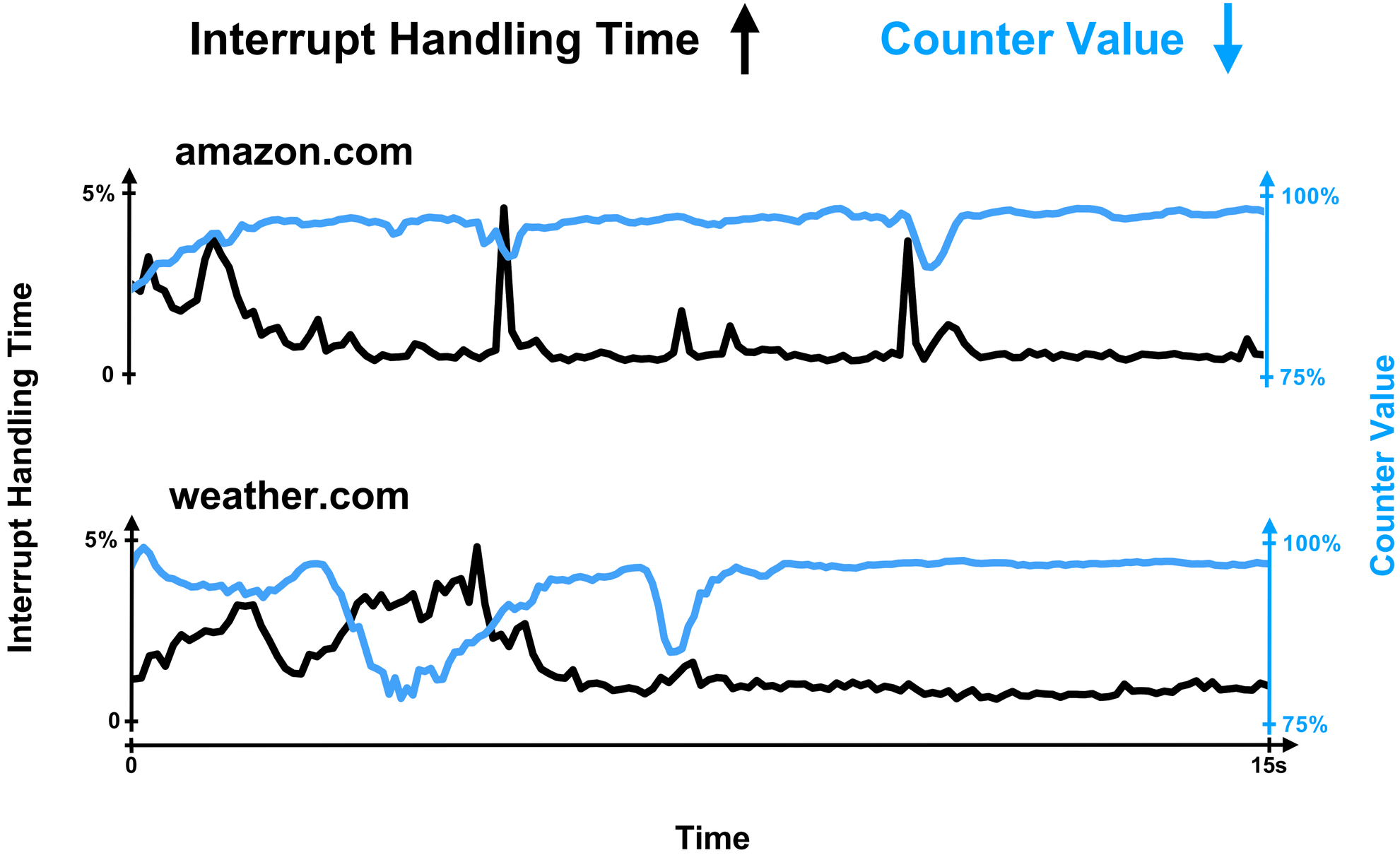


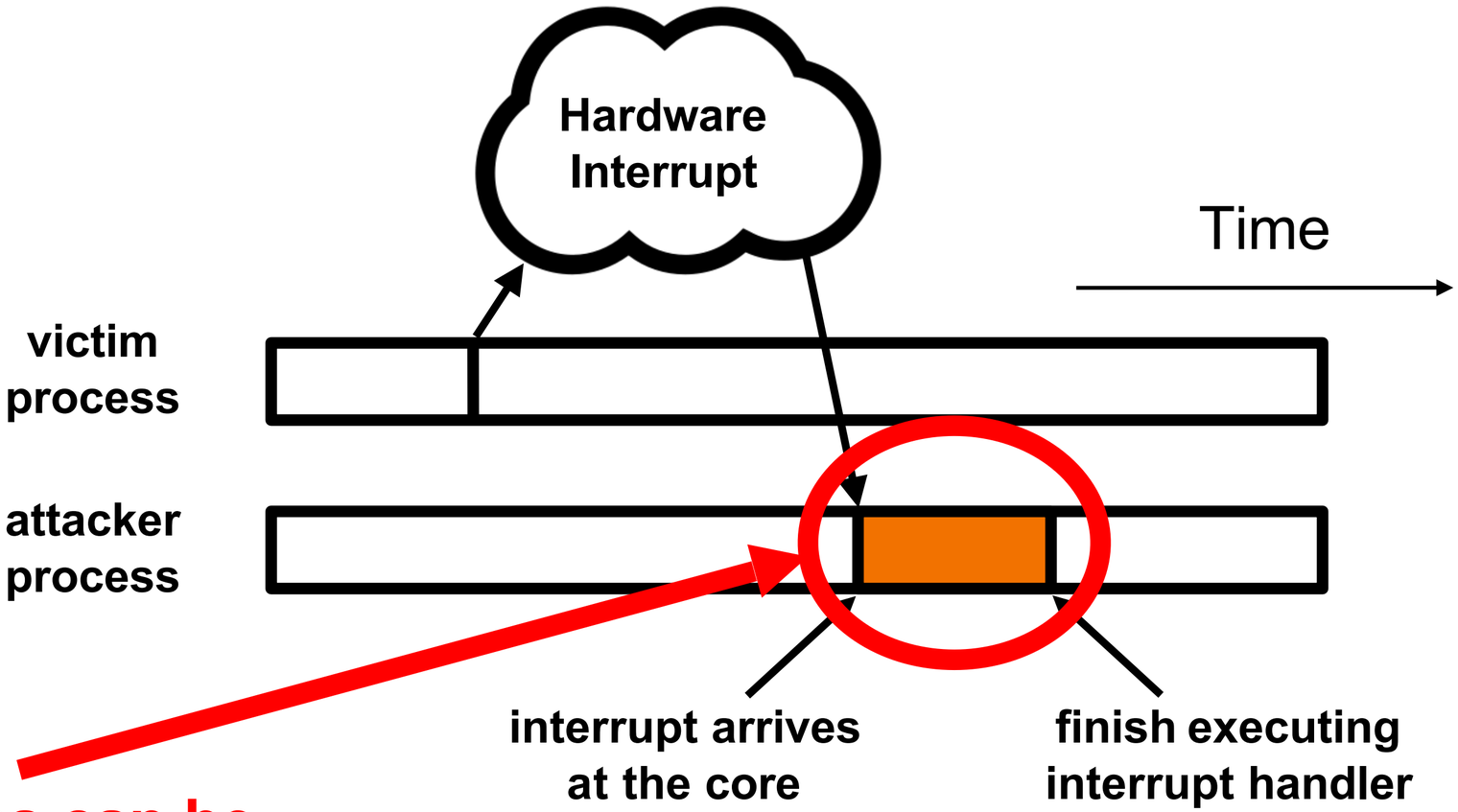
Interrupts?

- Can’t remove them

eBPF

- Allows instrumentation of the Linux kernel at runtime
- They developed a tool to monitor interrupt characteristics
- Records time at beginning and end of interrupt handlers


Interrupt Handling Time
Counter Value
amazon.com
5%
0
100%
75%
weather.com
5%
0
100%
75%
0
15s
Interrupt Handling Time
Counter Value
Time



99% of gaps can be explained by the presence of interrupts

Findings and Conclusions

- Machine-learning-assisted attacks are powerful but hard to interpret
- Sweep-counting “cache-occupancy” attack* primarily exploits system interrupts
- Non-movable interrupts have strong security implications