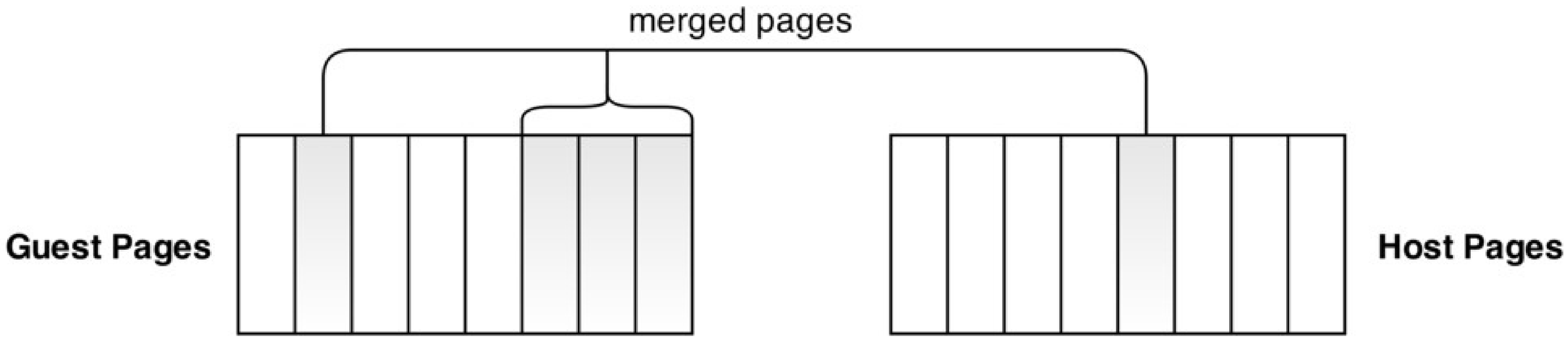
Timing Attacks on Memory Deduplication

David Bidner <david.bidner@student.tugraz.at>
Supervisor: Daniel Gruss

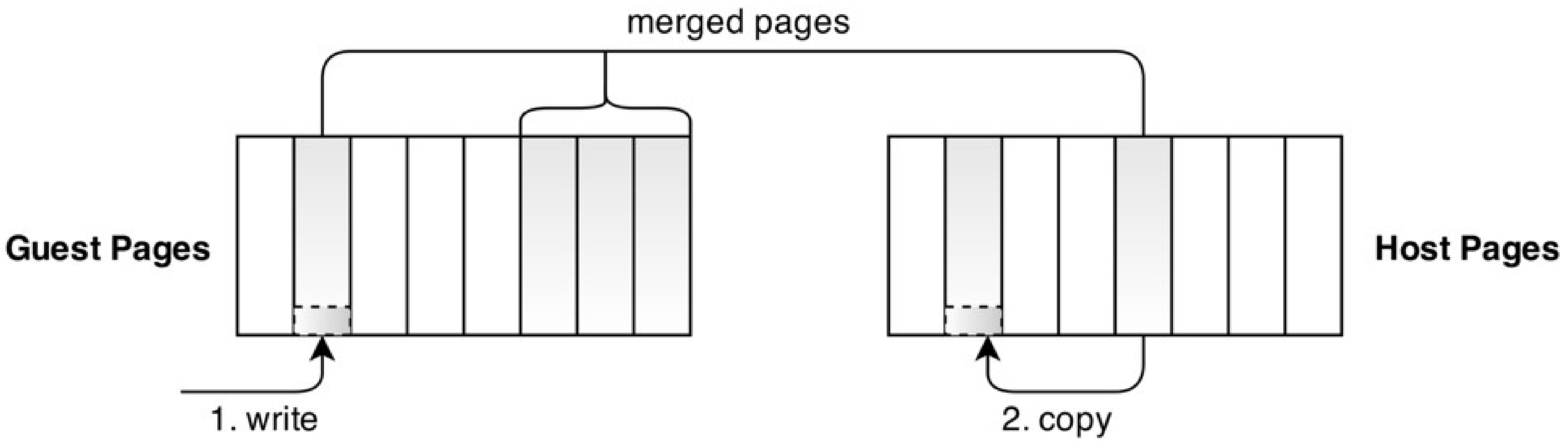
General Overview

- Background
- Attack
- Evaluation
- Conclusion

What is Memory Deduplication?



What does copy-on-write mean?



It needs more time!

Who uses Memory Deduplication?

- Hypervisors
- Android
- Windows

Attack Steps

- generate Code
- Run and Wait
- Measure Time

Code Comparison

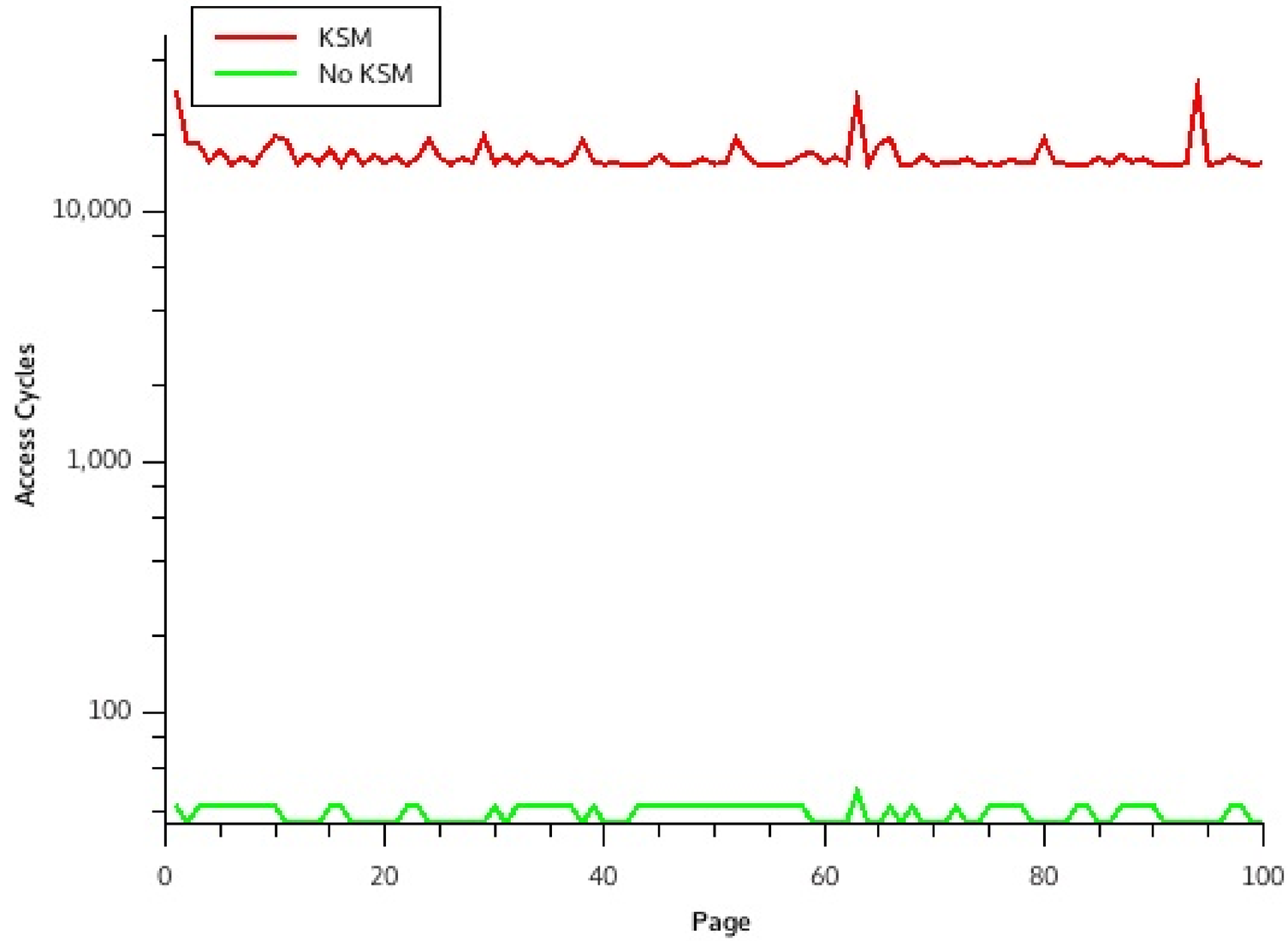
Native C Code

```
pages = (char*) mmap ( ... );
/* fill pages & wait */
for(i = 5; i < size; i+=4096)
{
        a = rdtsc();
        pages[i] ='a';
        b = rdtsc();
        result = b-a;
}
```

JavaScript Code

```
pages = new Uint8Array(size);
/* fill pages & wait */
for(var j = 5; j < size; j = j+4096)
{
        var t1 = window.performance.now();
        pages[j] = 10;
        var t2 = window.performance.now();
        result = t2 - t1;
}
```

Detect Memory Deduplication

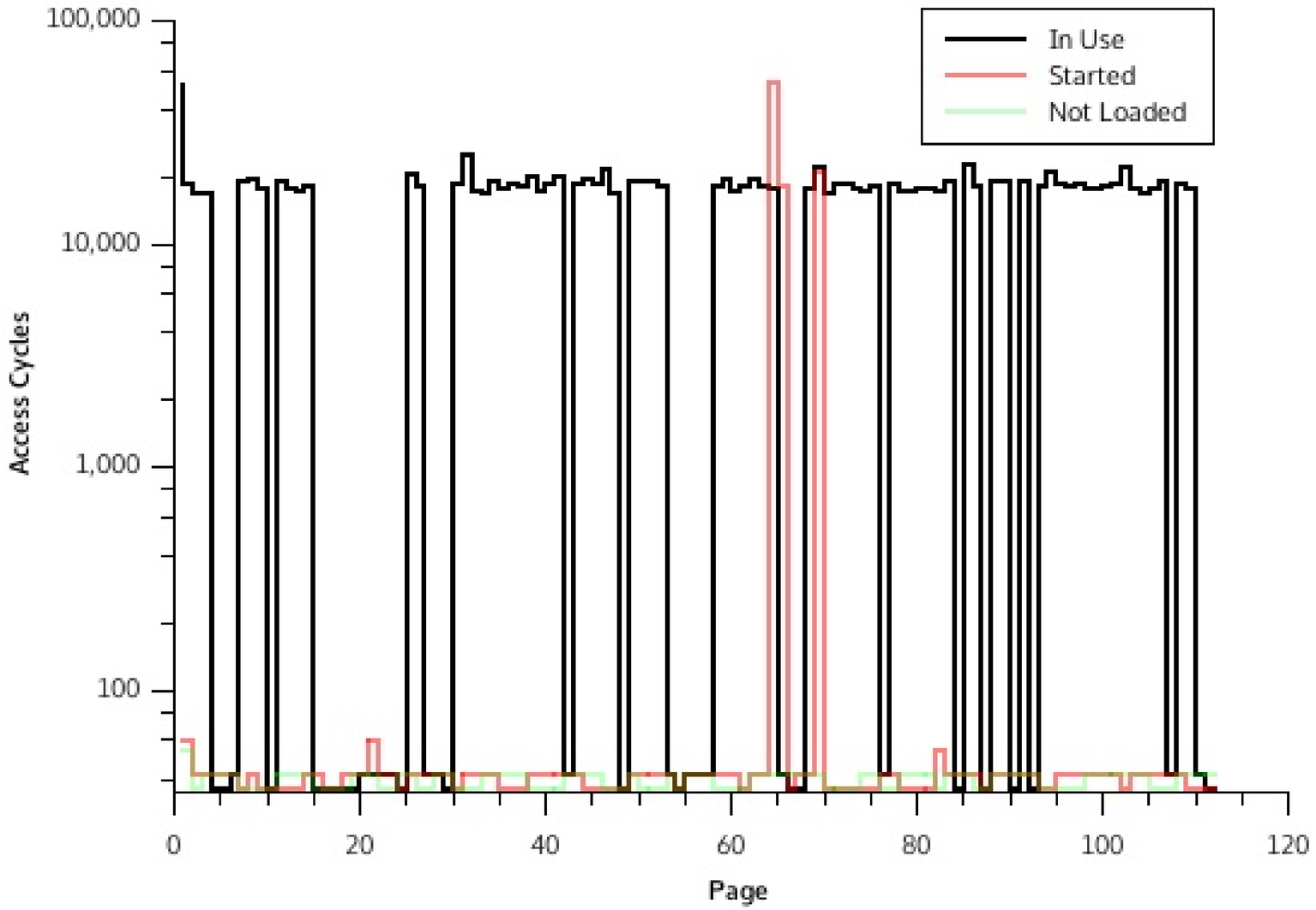


Access Time to Zero Pages in Memory (using RDTSC)

Evaluation based on:

- existing Attacks (native)
- Website detection (native)
- New Attacks (JavaScript)
- System Load Effects (JavaScript)

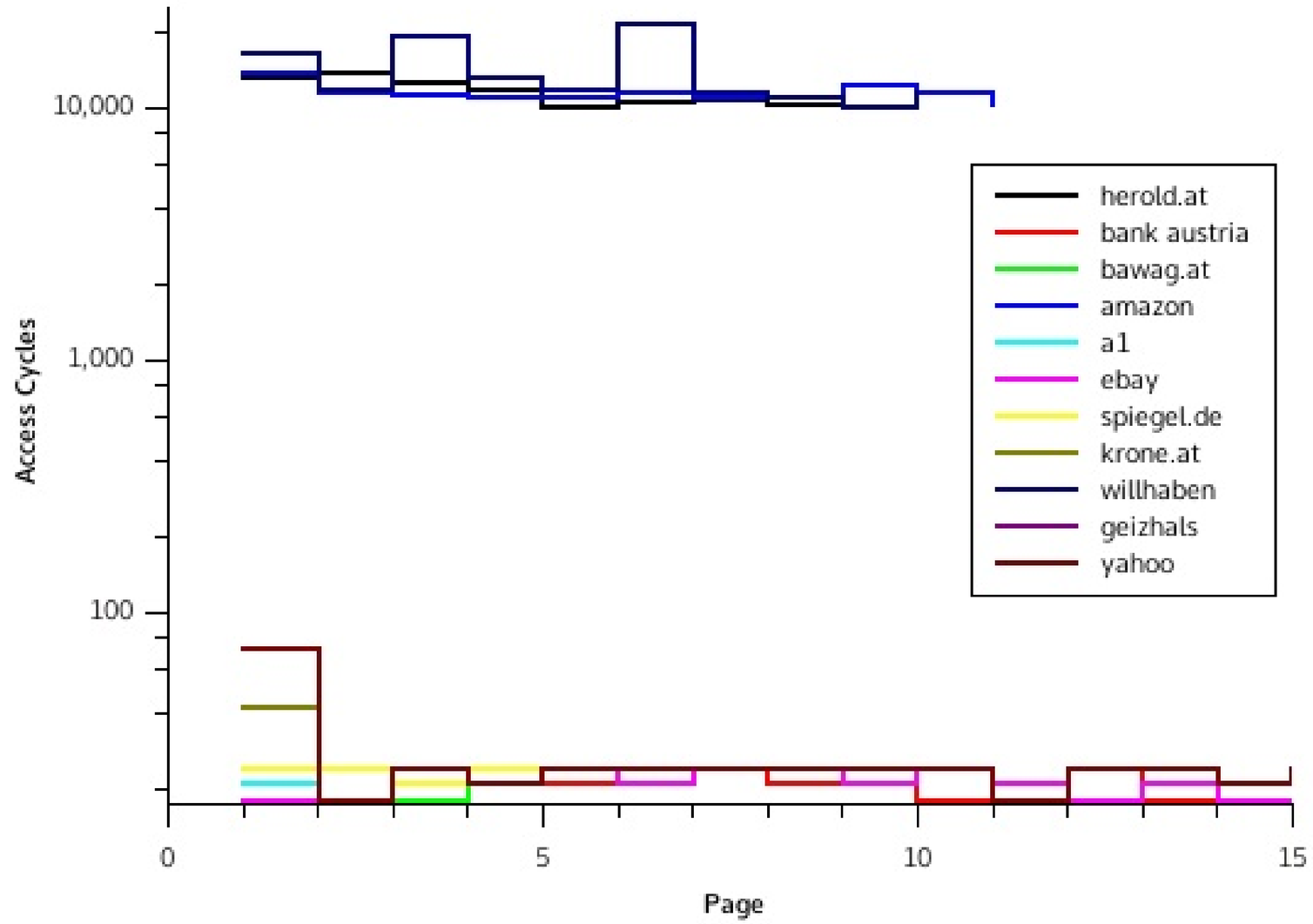
Existing Attack (native)



Implementing already known attacks:

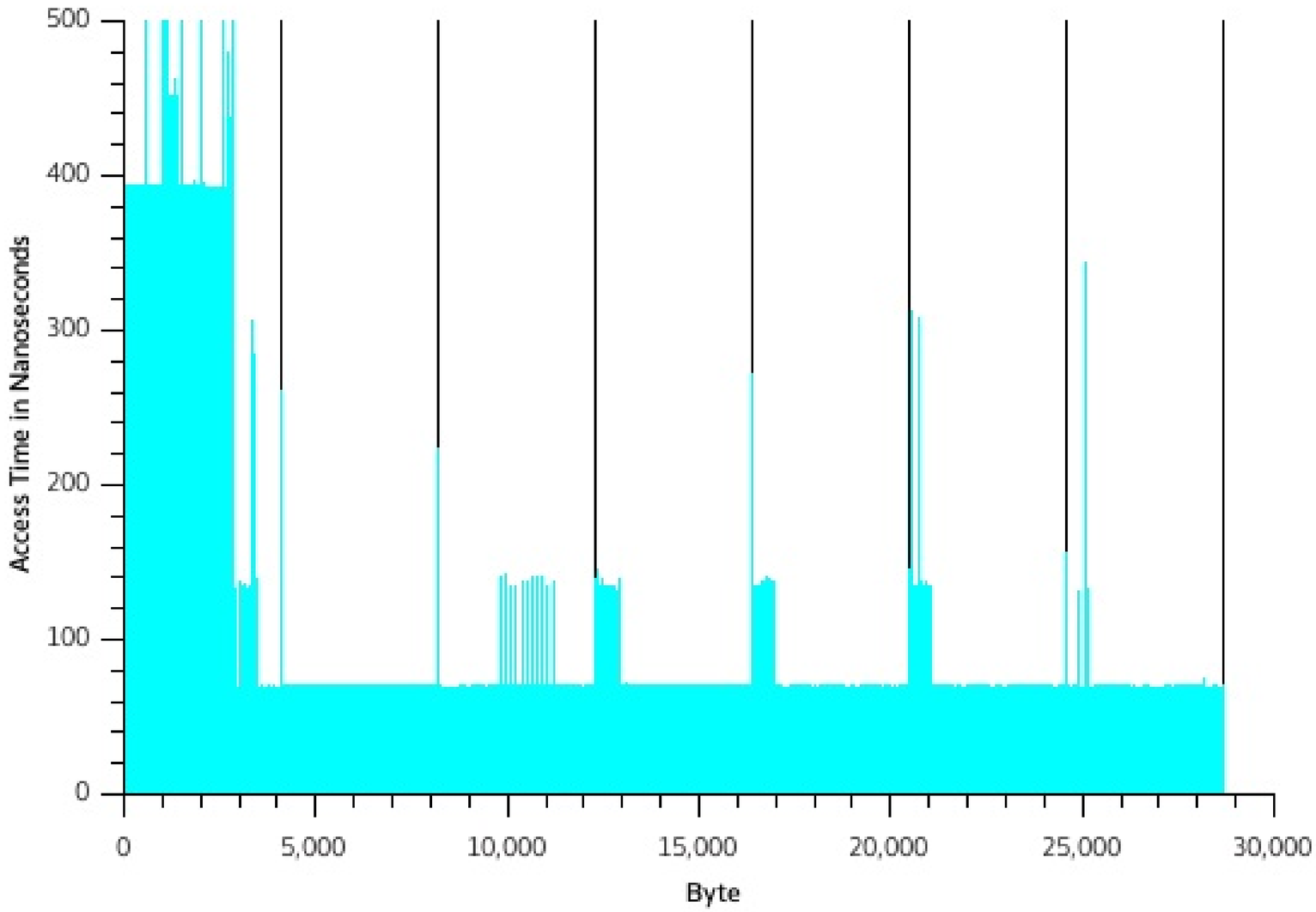
detect an Application in Memory

Detect Browser-Content (native)



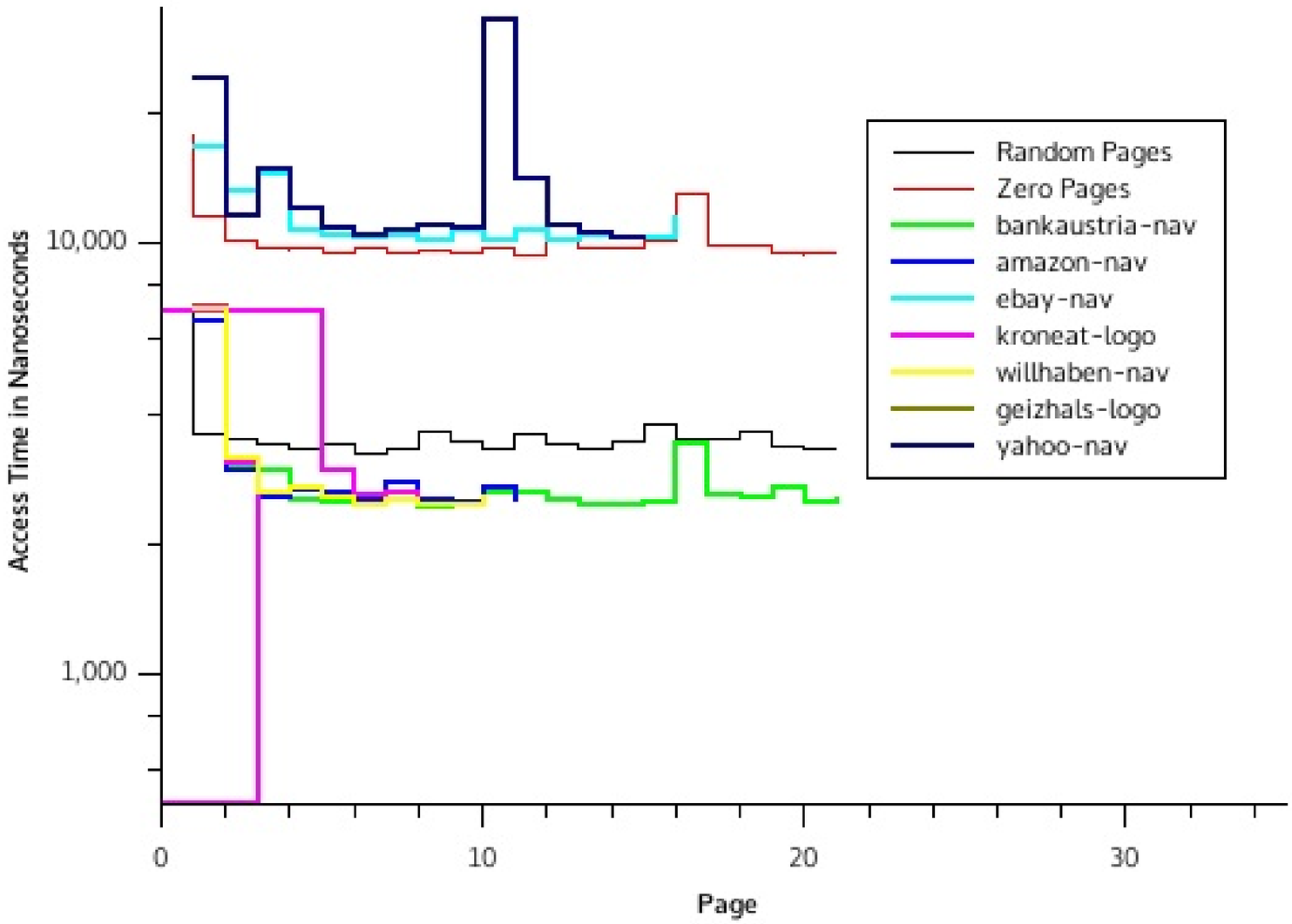
Which sites are open?

Bringing the Attack to the Web



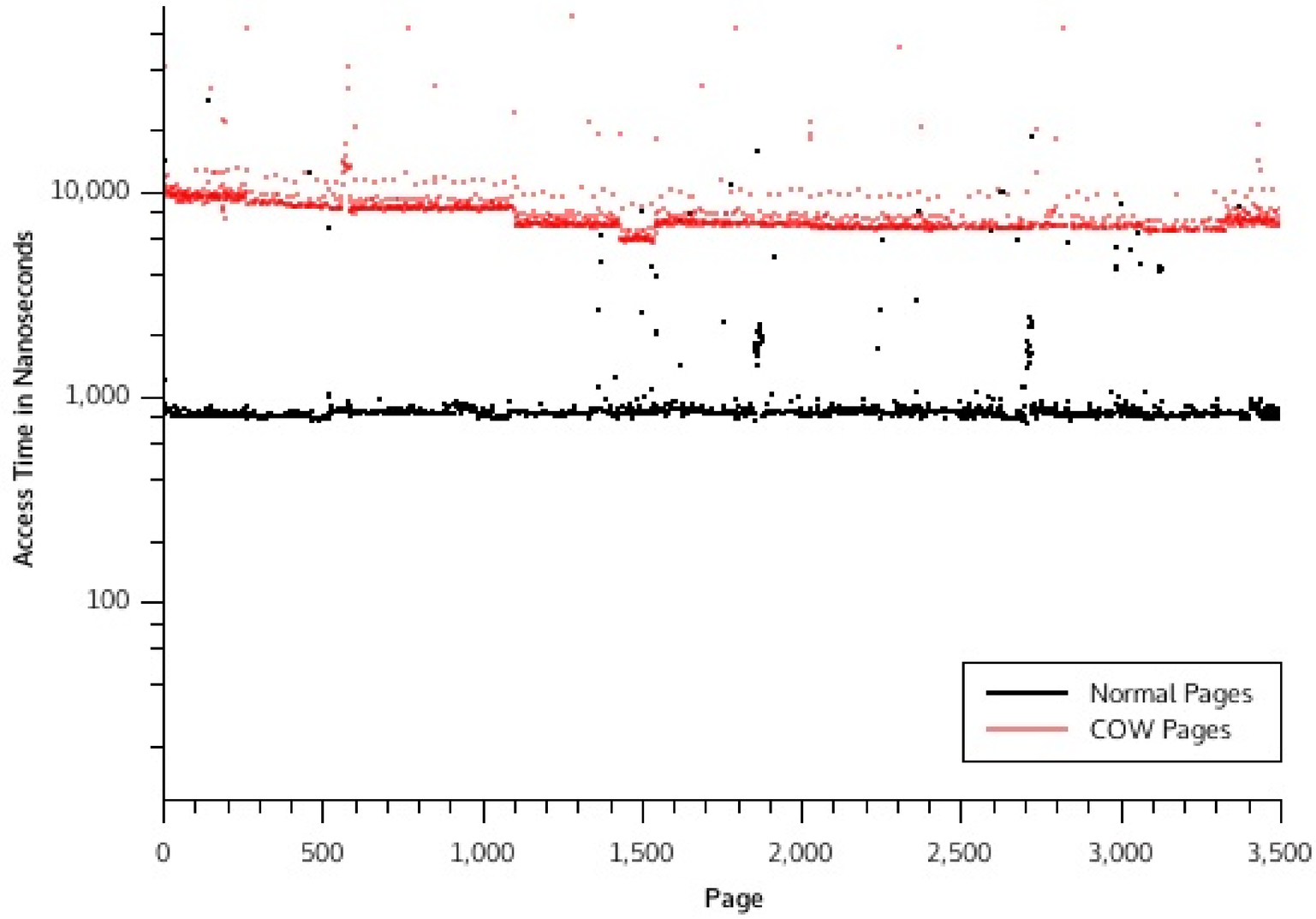
It is possible to measure time in JavaScript:
~100ns with performance.now() TimeStamp

What other sites are open? (JS)



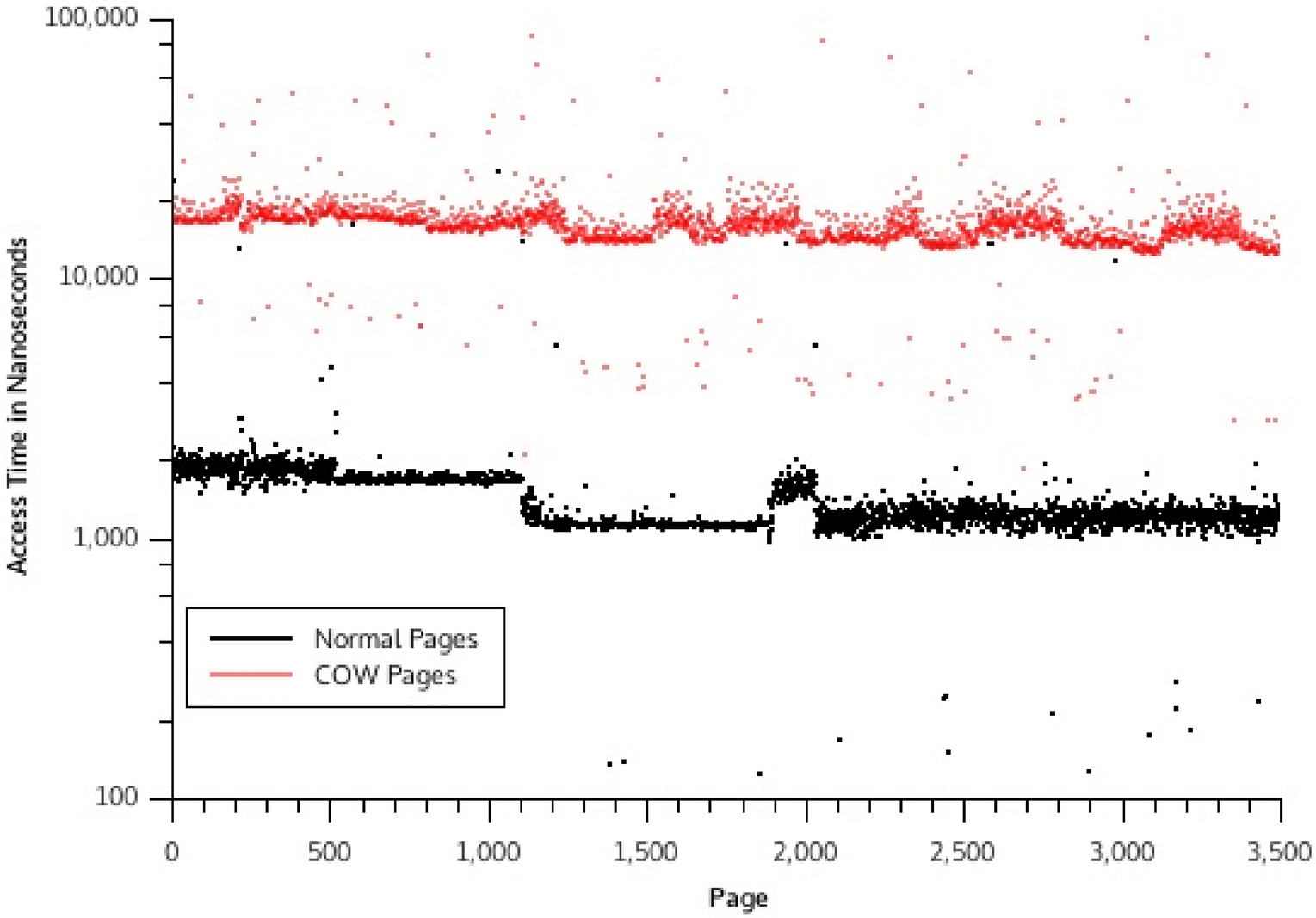
Not as accurate as native code, but accurate enough!

Does system load effect accurancy? (JS)



(Low-Load)

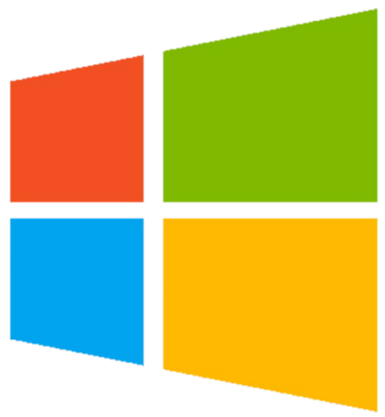
Does system load effect accurancy? (JS)



(high-load)

Countermeasures?

Disable Memory Deduplication.



Timing Attacks on Memory Deduplication

QUESTIONS?

David Bidner <david.bidner@student.tugraz.at>
Supervisor: Daniel Gruss