

# **The Sky is Falling!!!**

Architectural Vulnerabilities due to  
Speculative Execution

Discussion led by Gabe

# The Sky is Falling!!!

Architectural Vulnerabilities due to  
→ Speculative Execution

What is all of this about?

# The Sky is Falling!!!

Architectural Vulnerabilities due to  
Speculative Execution



What is all of this about?

# The Sky is Falling!!!

Architectural Vulnerabilities due to  
Speculative Execution



What is all of this about?

# The Sky is Falling!!!

Architectural Vulnerabilities due to  
Speculative Execution

Why is it important?





**MELTDOWN**



**SPECTRE**



# Outline for Today

- Architecture
  - Assembly
  - GHz and pipelines (MIPS 5 stage)
    - Parallelism – pipelined and data parallel
  - Branches and pipeline bubbles
- Speculation
  - *Fake it, and hope you make it:* branch prediction
  - ...but what happens when you *don't make it*?
- Side effects of speculation
  - *Visibility* of side-effects



array



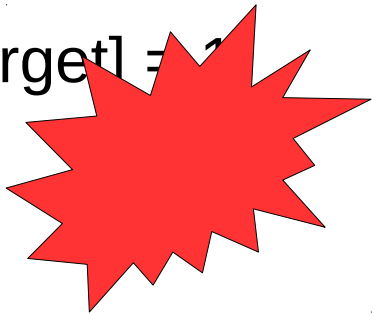
```
char *target = memory_address_i_shouldn't_be_able_to_access;
```

```
array[*target] = 1;
```



```
char *target = memory_address_i_shouldn't_be_able_to_access;
```

```
array[*target] = 1;
```



```
/* OS protection causes this to FAULT!!! */
```

array



```
char *target = memory_address_i_shouldn't_be_able_to_access;
```

```
if (<don't take this branch>) { /* prevents access so OK, right? */  
    array[*target] = 1;  
}
```

array



```
char *target = memory_address_i_shouldn't_be_able_to_access;
```

```
if (<don't take this branch>) { //..but can speculatively go into branch  
    array[*target] = 1;    // side-effect: brings array[] item into cache  
}
```