









**SPECTRE: VARIANT 1 (CVE-2017-5753)**



- ▶ **x** is controlled by the attacker
- ▶ attacker wants to read **array1[x]** out of bounds
- ▶ **array2** is used to leak the value of y (like in Meltdown)

```
if (x < array1_size)  
    y = array2[array1[x] * 256];
```



1. Attacker manipulates branch prediction

2. `speculatively_runs` even when `x > array1_size`

3. The cache timing of `array2[..]` leaks the value `array1[x]`







## SPECTRE: VARIANT 1 (CVE-2017-5753)



```
if (x < array1_size)
    y = array2[array1[x] * 256];
```

- ▶ **x** is controlled by the attacker
  - ▶ attacker wants to read **array1**[**x**] out of bounds
  - ▶ **array2** is used to leak the value of y (like in Meltdown)
1. Attacker manipulates branch prediction
  2. speculatively runs even when  $x > \text{array1\_size}$
  3. The cache timing of **array2**[..] leaks the value **array1**[**x**]

# SPECTRE: VARIANT 2 (CVE-2017-5715)

