

Meltdown basically works like this:

1. READ secret from forbidden address

1. Check that program may read from address

2. Store the read value in register

2. Stash away secret

1. *Magic*

3. *Retrieve secret (later)*



MELTDOWN & SPECTRE FOR ARMED PEOPLE

MELTDOWN: READING FOR BEGINNERS

2

7

1

2







1

1

2

1

WORKS:

MELTDOWN: READING FORBIDDEN DATA



μOPs ordered by *instruction*

1 Check access

2 Read into register

1 *Magic*

μOPs ordered by *execution*

2 Read into register

1 *Magic*

1 Check access

The re-ordering on the right happens, when the “forbidden data” is already cached (because cache access is so fast).



MELTDOWN: READING FORBIDDEN DATA

Meltdown basically works like this:

- READ secret from forbidden address
 - 1 Check that program may read from address
 - 2 Store the read value in register
- Stash away secret
 - 1 *Magic*
- *Retrieve secret (later)*

μOPs:

