# MELTDOWN & SPECTRE FOR NORMAL PEOPLE

# MELTDOWN: READING FORBIDDEN DATA

28

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

Reordering is not a problem because the CPU will ensure that  is only seen *iff*  succeeds.

*Unless*  is able to hide the secret in such a way that the attacker can find it later.

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

# In our burger example:

1. Customer orders a burger
2. Customer gets his burger
3. Customer has not enough money
4. Customer runs away with burger

# MELTDOWN: READING FORBIDDEN DATA

| μOPs ordered by *instruction* | μOPs ordered by *execution* |
|---|---|
| 1 Check access | 2 Read into register |
| 2 Read into register | 1 *Magic* |
| 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).

Reordering is not a problem beca
that is only seen *iff* succe
*Unless* is able to hide the secre
attacker can find it later.

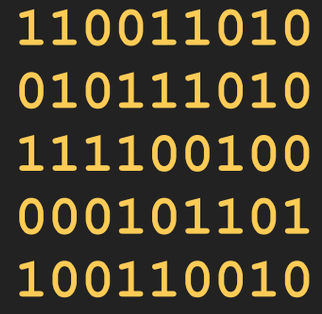
**In our burger example:**

1. **Customer orders a burger**
2. **Customer gets his burger**
3. **Customer has not enough money**
4. **Customer runs away with burger**

# MELTDOWN

For Meltdown two actors are needed

The a **spy** and a **collector**.




The **spy** will “steal” the secret and stash it away.

The CPU will kill him for accessing the secret information.

The **collector** will find the stashed away secret.