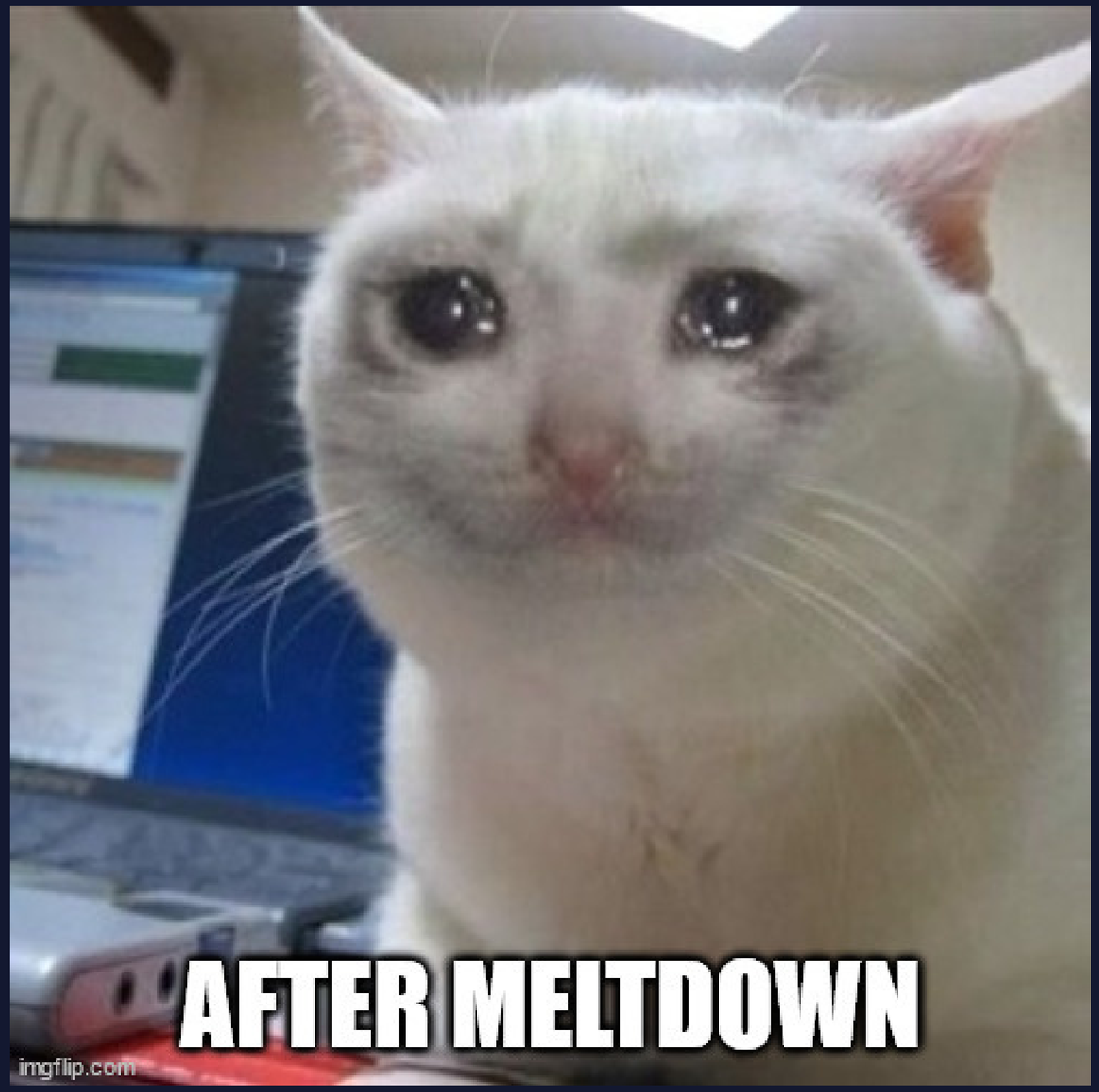
BEDOURET - CHAZOT - MOURGAND - REGNAULT - VERDIER

MELTDOWN

Présentation rapide



Comment ça marche ?

exec spéculative

Exécution séquentielle

```
public void Main()
{
    int a = 100000000;
    if (ReallyLongMethod(a))
    {
        a=10;
        AccessPrivateFile();
    }
}
```

1

2

3

4

Uniquement si ReallyLongMethod retourne “True”

Exécution spéculative

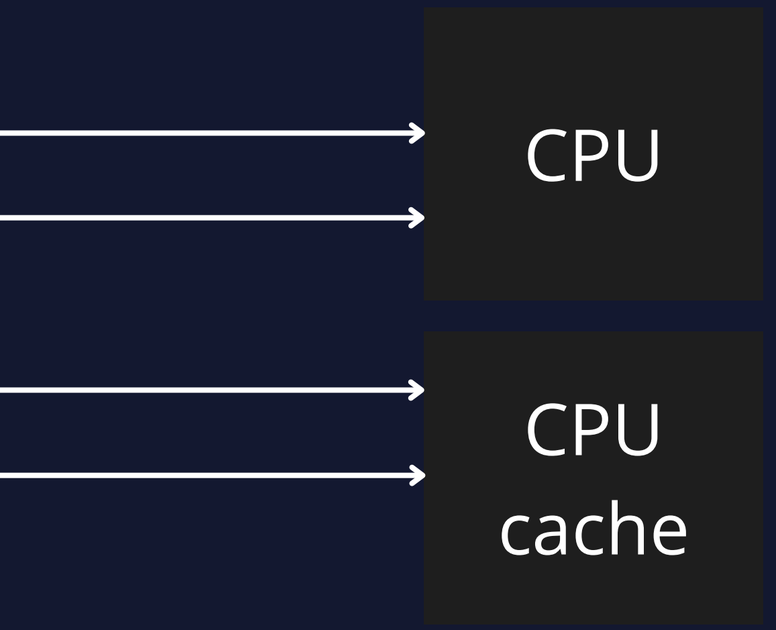
```
public void Main()
{
    int a = 100000000;
    if (ReallyLongMethod(a))
    {
        a=10;
        AccessMemorySpace();
    }
}
```

1
2
2
3

Le processeur va spéculer que ReallyLongMethod retourne “True”

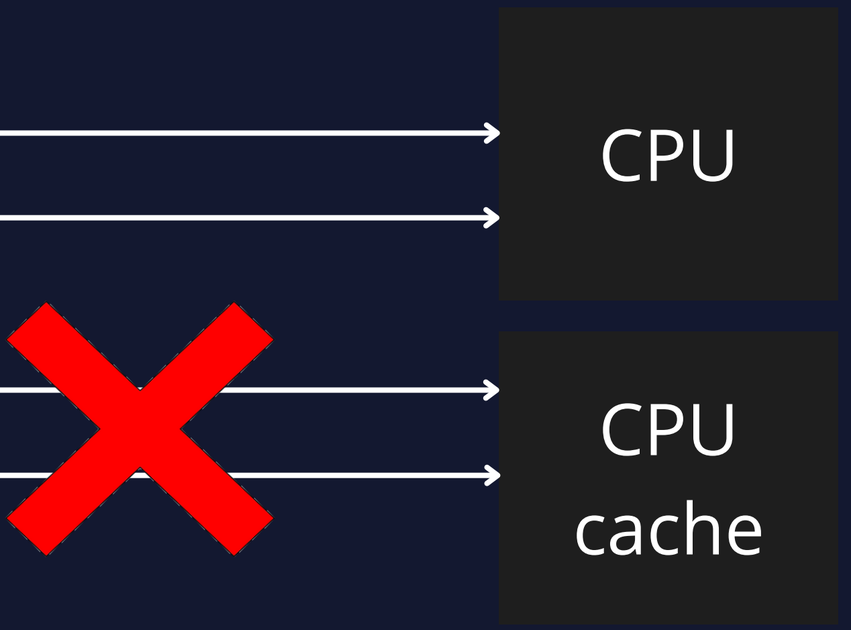
Exécution spéculative

```
public void Main()
{
    int a = 100000000;
    if (ReallyLongMethod(a))
    {
        a=10;
        AccessMemorySpace();
    }
}
```



Exécution spéculative

```
public void Main()
{
    int a = 100000000;
    if (ReallyLongMethod(a))
    {
        a=10;
        AccessMemorySpace();
    }
}
```



Si ReallyLongMethod() retourne “False” → **Clean CPU cache**

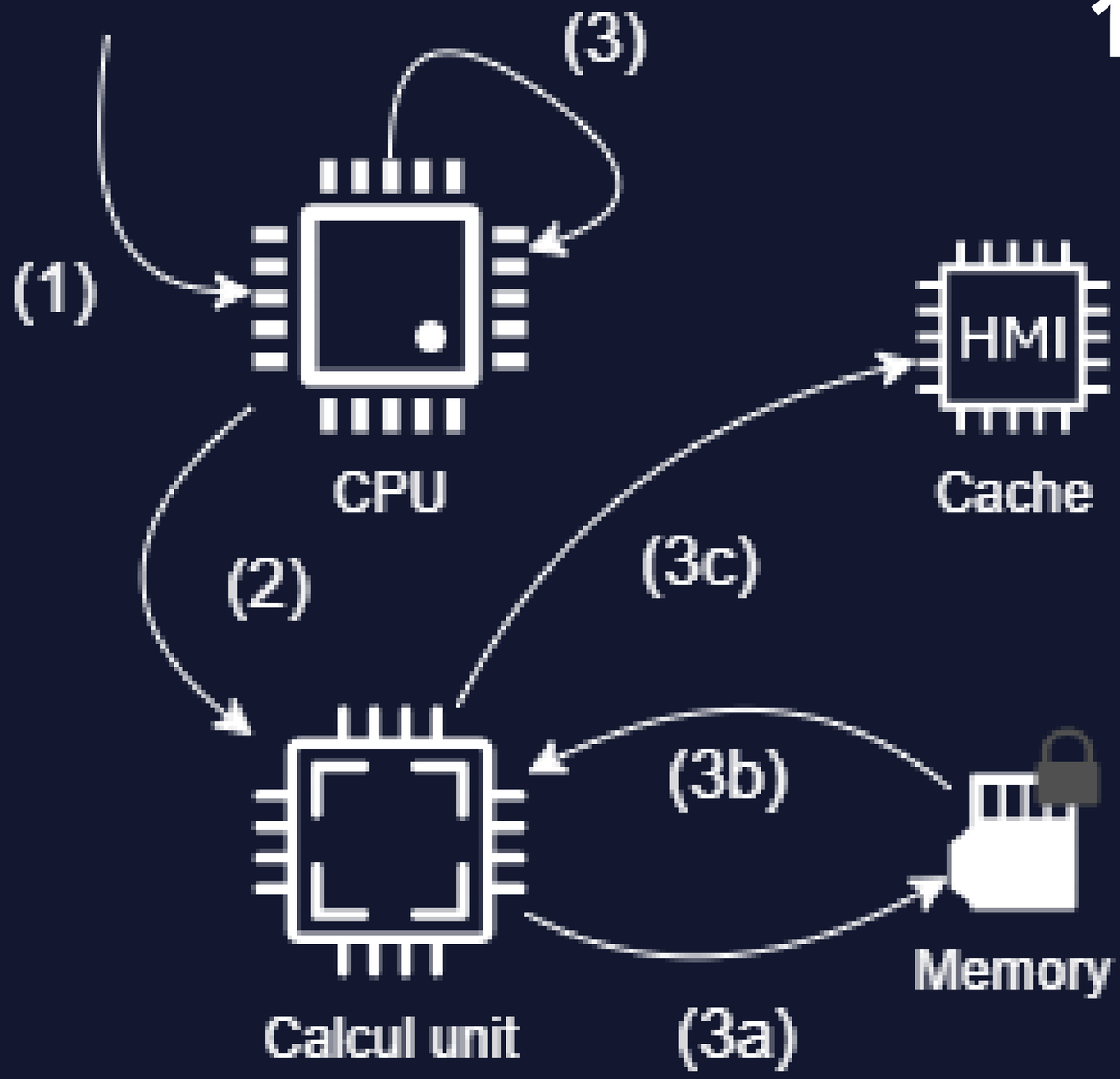
Exécution dans le désordre

```
public void Main()
{
    int a = 100000000;
    if (ReallyLongMethod(a))
    {
        a=10;
        AccessMemorySpace();
    }
}
```

Les 3 étapes de l’attaque

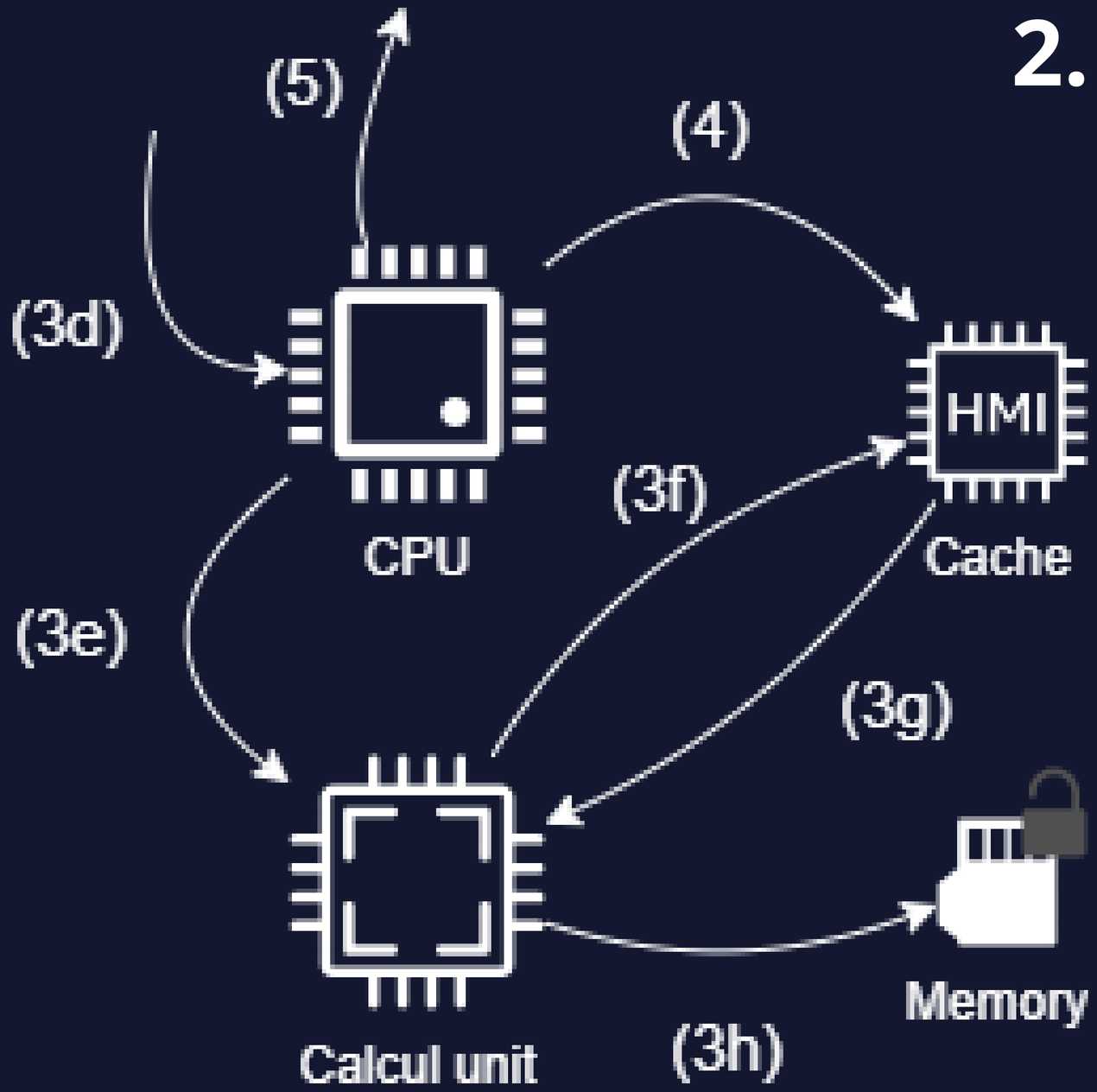
1. **Accès aux données**
2. **Déplacer les données**
3. **Récupération des données**

1. Accès aux données



1. Instruction sur la mémoire
2. Délègue l’exécution
3. Analyse des droits
    a. Accès mémoire
    b. Retour des résultats
    c. stockage dans le cache

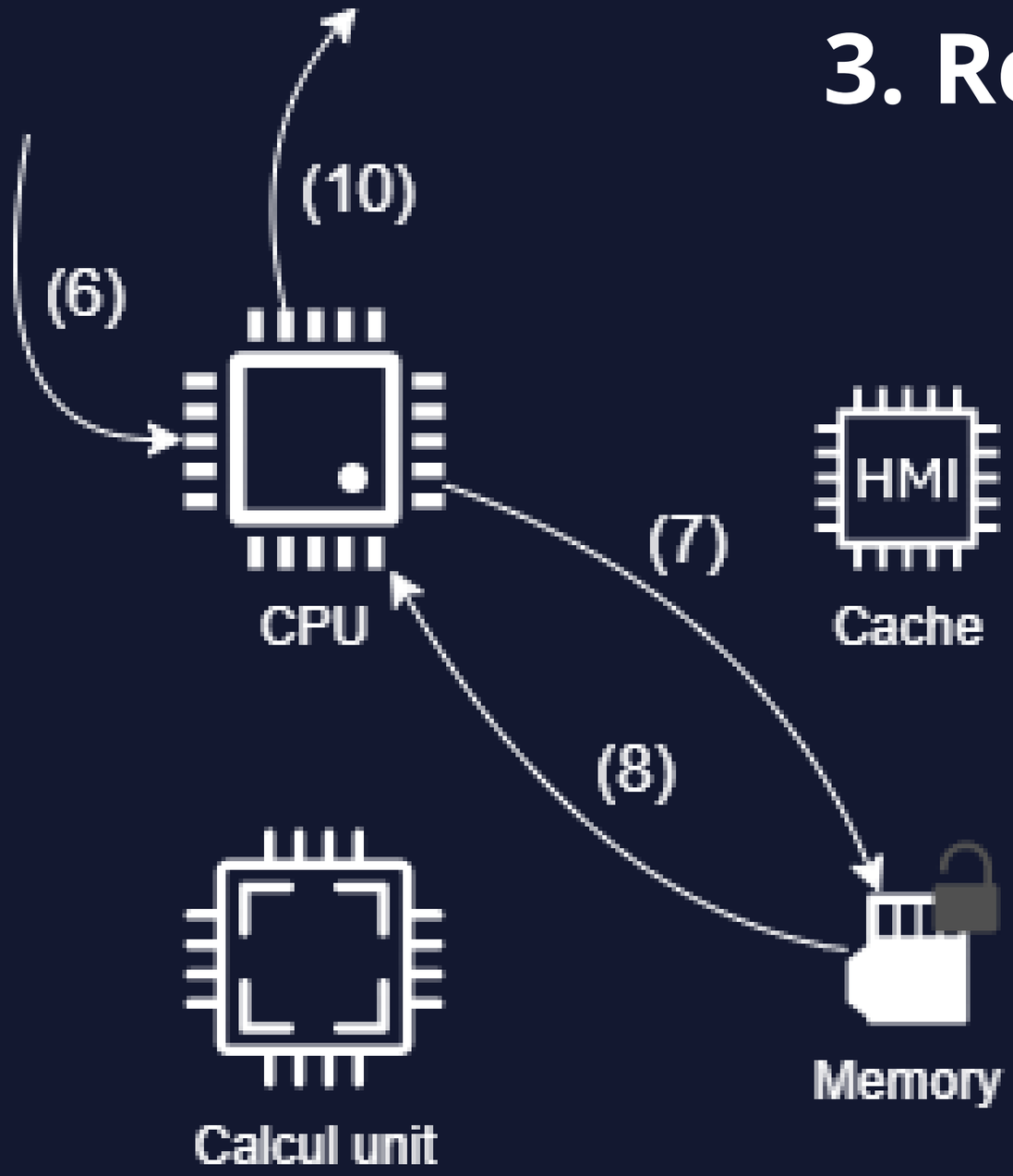
2. Déplacer les données



d. nouvelle instruction
e. délèguation
f. accès aux données
g. récupération
h. stockage

4. Reset du cache
5. Renvoie une exception

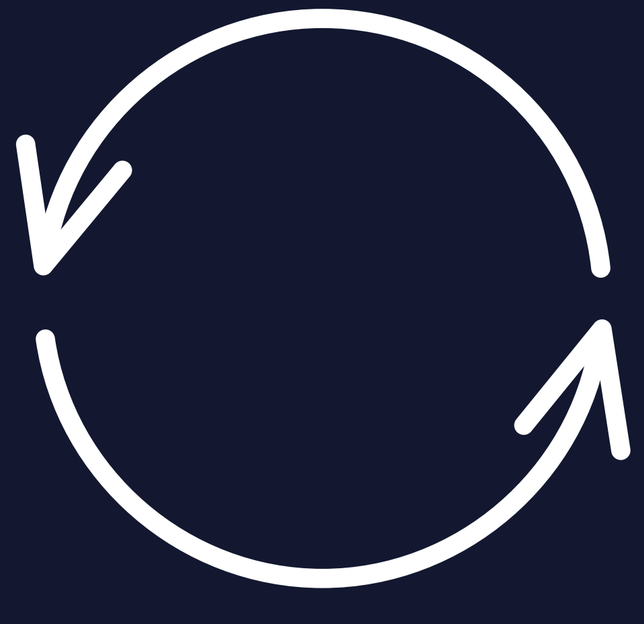
3. Récupération des données



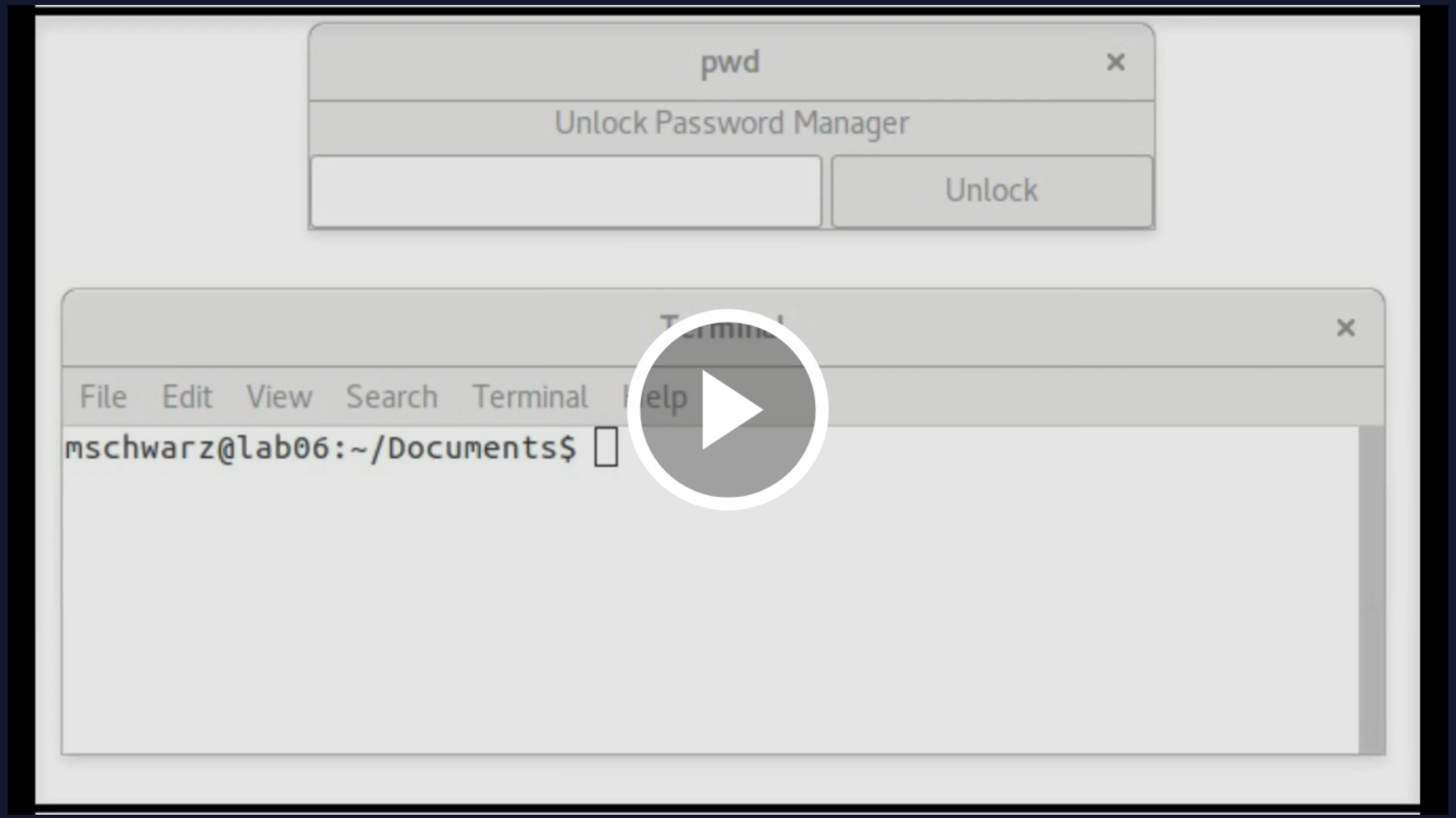
6. Nouvelle instruction
7. Cherche l’adresse
8. Récupère les données
10. Renvoie du résultat

Les 3 étapes de l’attaque

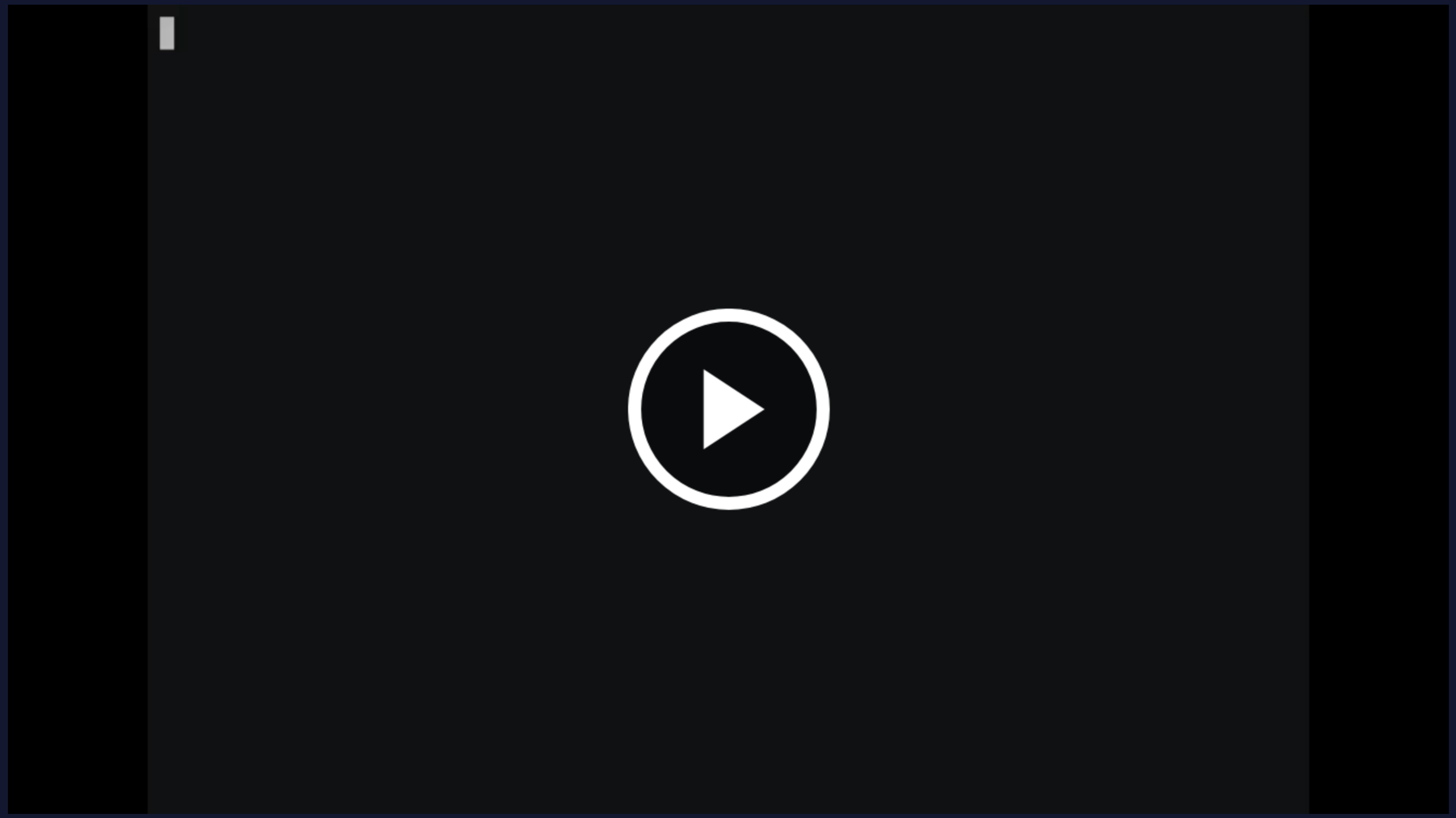
1. **Accès aux données**
2. **Déplacer les données**
3. **Récupération des données**



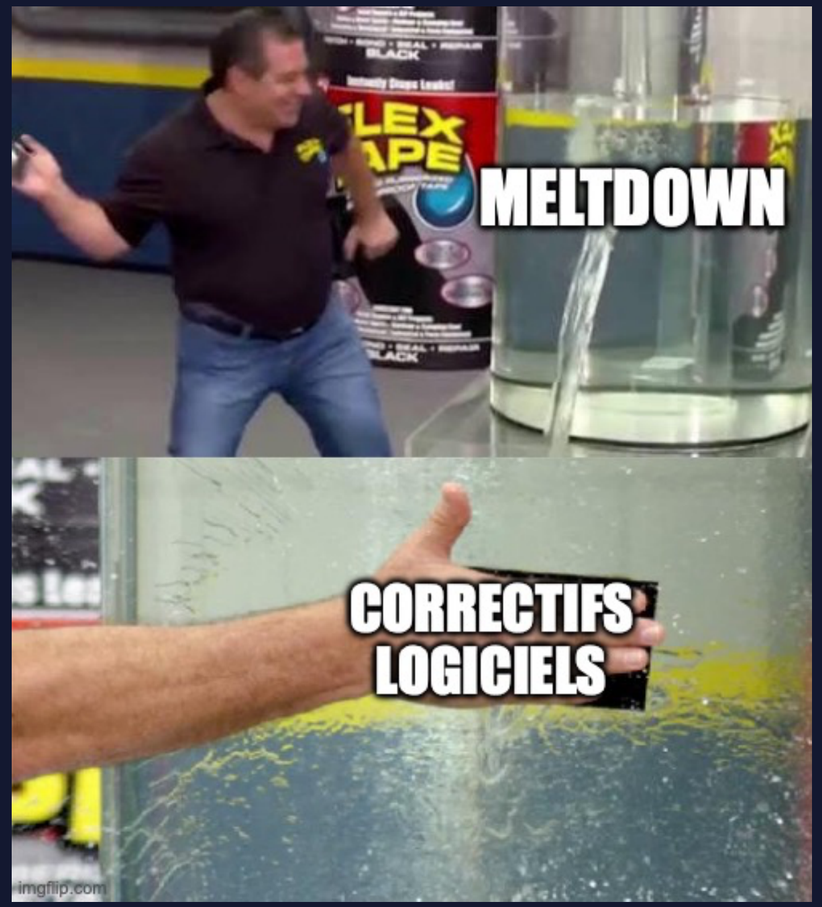
Exemples :


pwd
Unlock Password Manager
Unlock
File Edit View Search Terminal Help
mschwarz@lab06:~/Documents$

Exemples :



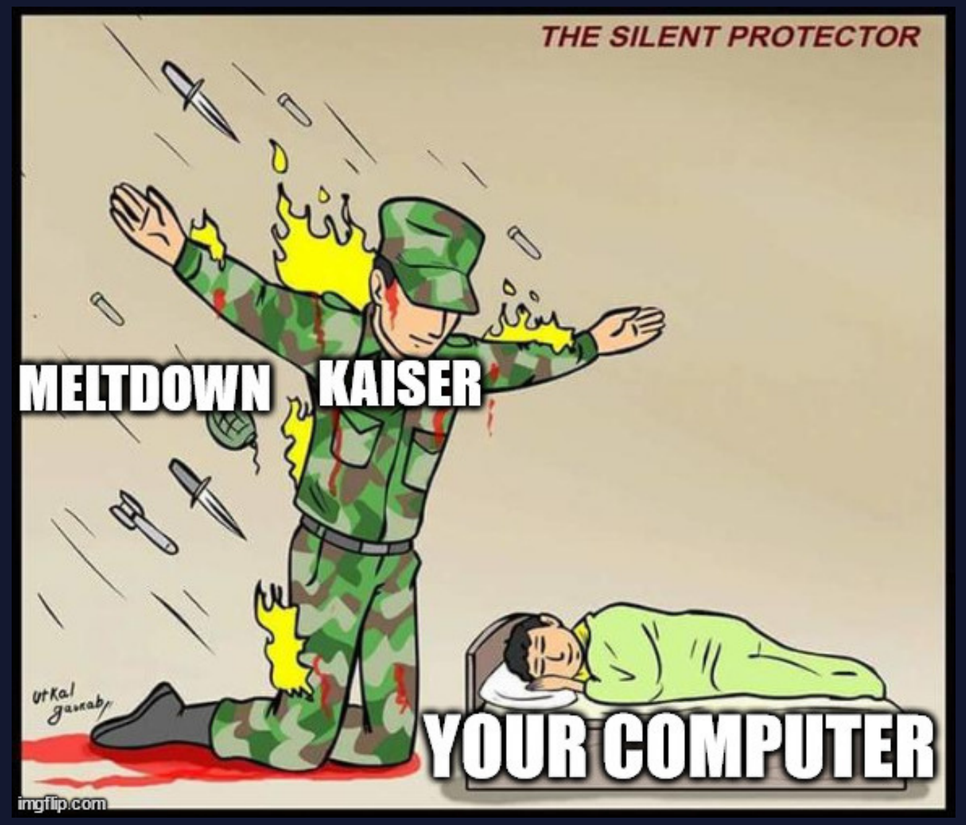
Comment se protéger de l’attaque Meltdown



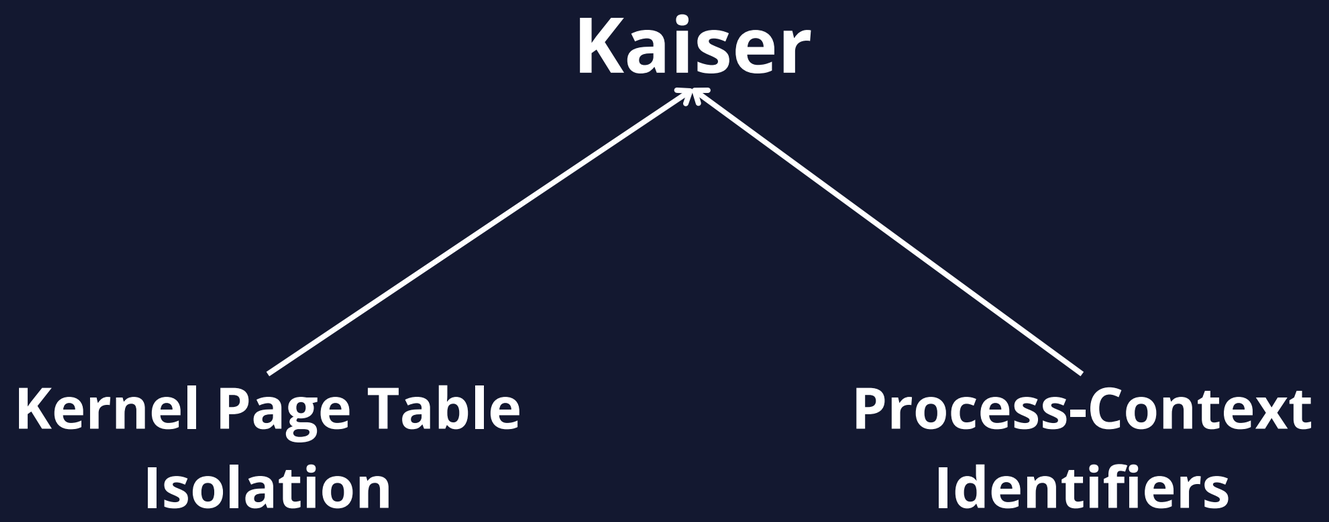
intel ⟶ Isolation du noyau (Kaiser)

⟶ Correctifs

KAISER : Qu’est-ce que c’est ?



Coté matériel :



Le petit frère : Spectre

Différences Meltdown / Spectre

Meltdown se repose sur Spectre

Spectre accès cache / Meltdown mémoire utilisateur

Spectre affecte plus de processeurs

Correctifs différents

Conclusion

Affecte les processeurs Intel

Récupère les données de la mémoire utilisateur

Correctifs logiciels et matériels

Merci de votre attention