

# Spectre & Meltdown

Revue technique

# Qui suis-je ?



Romain BENTZ `pixis`

Consultant **pentester**  
**Sogeti ESEC**

Auteur de **beta.hackndo.com**



@hackanddo



# 0b00 Plan



0b01

Origine

0b10

Mécanismes

0b11

Meltdown & Spectre

# 0b00 Plan



0b01

Origine

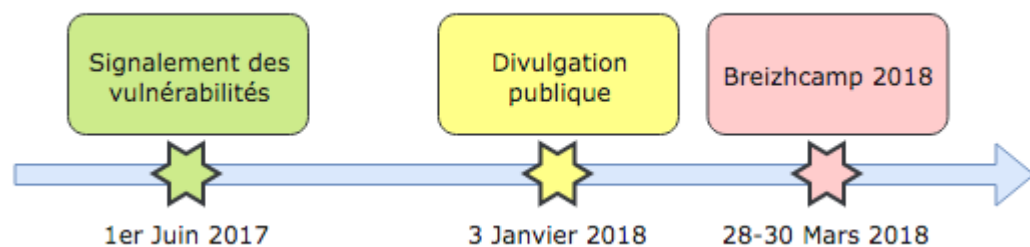
0b10

Mécanismes

0b11

Meltdown & Spectre

# Origine



Google « Project Zero »

Jann Horn (@tehjh)



# 0b00 Plan



0b01

Origine

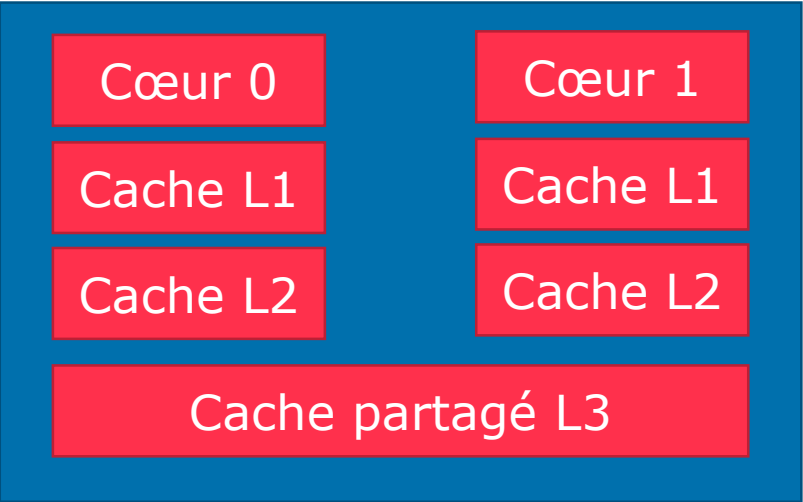
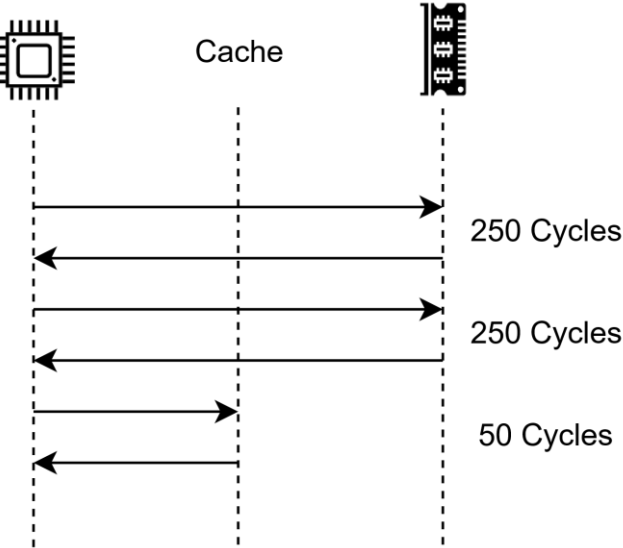
0b10

Mécanismes

0b11

Meltdown & Spectre

# Cache



CPU

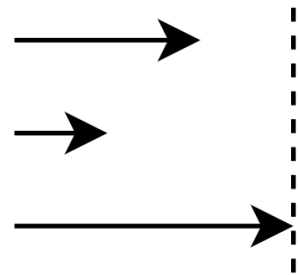
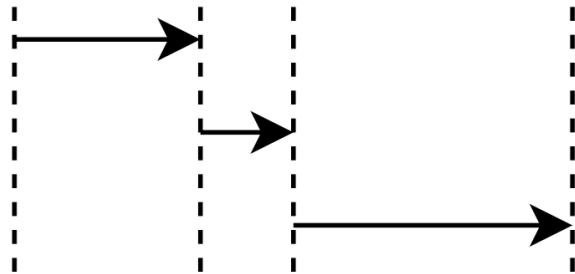


# Out of Order

```
var_A = function()  
var_B = calcul()  
var_C = lecture()
```



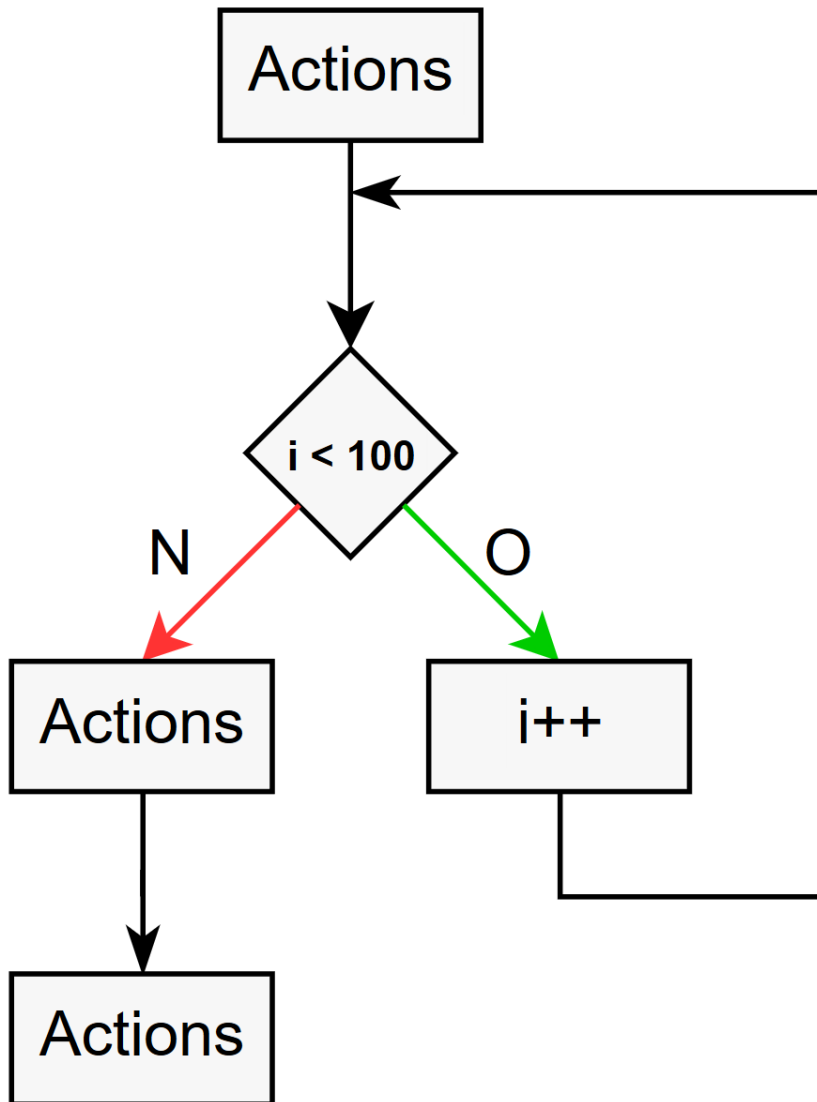
```
var_C, var_A, var_B = lecture(), function(), calcul()
```



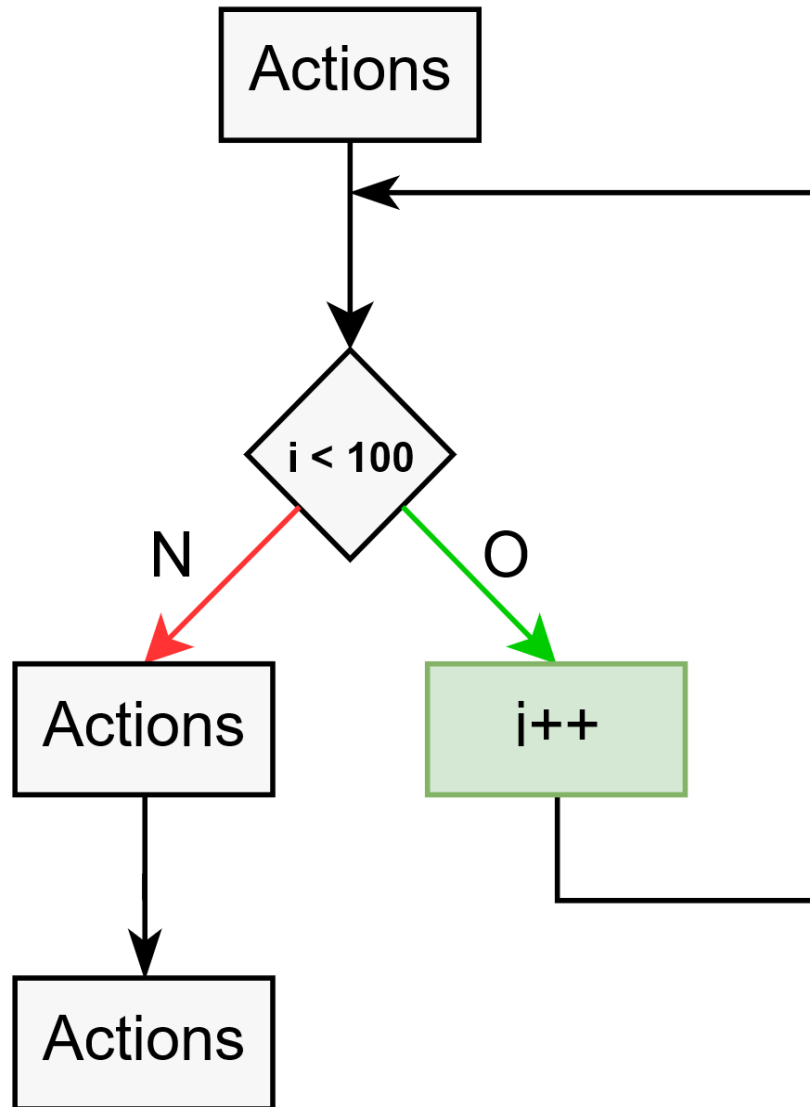
Assignations  
dans l'ordre



# Prédiction



# Prédiction



# 0b00 Plan



0b01

Origine

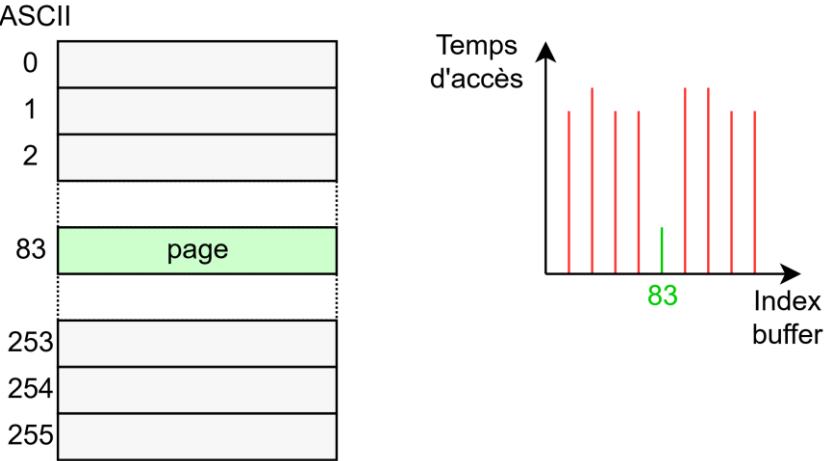
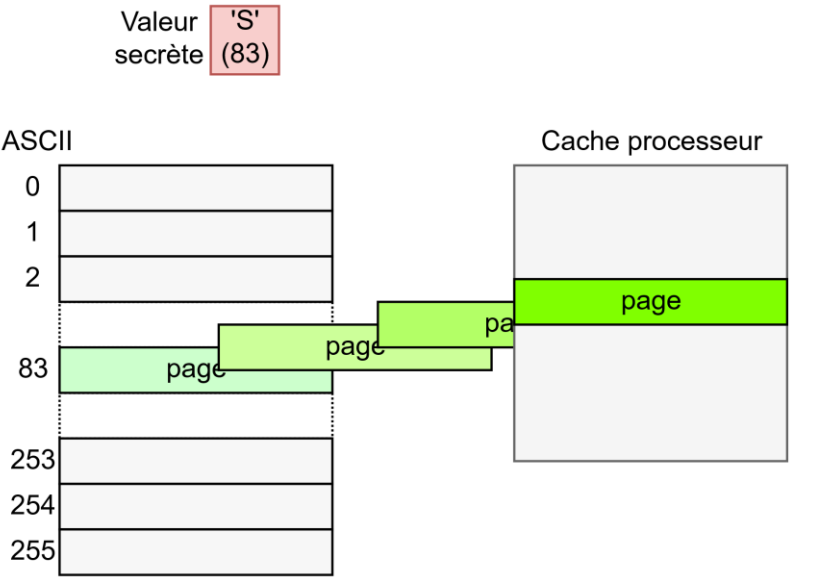
0b10

Mécanismes

0b11

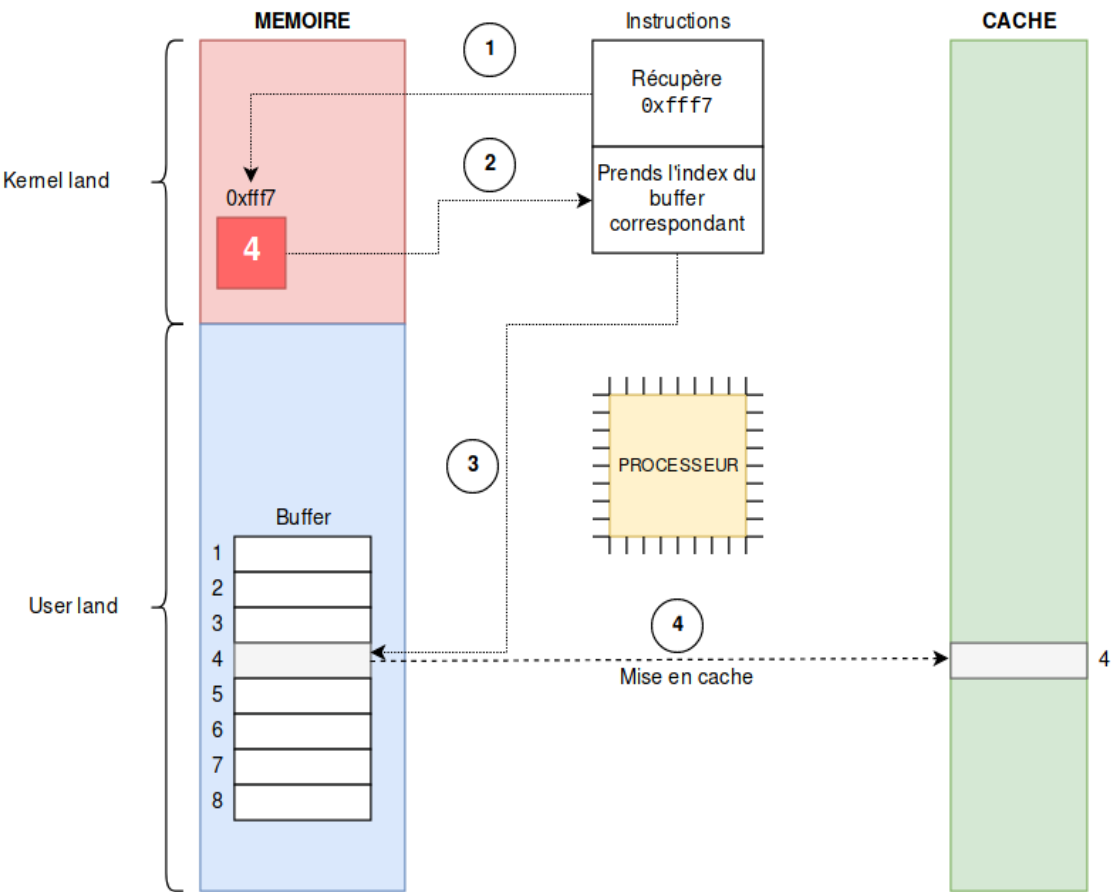
Meltdown & Spectre

# Cache side-channel attack



# Meltdown

```
/* ... instructions ... */
var_secrete = kernel_space[0xfff7];
junk = buffer[var_secrete];
```

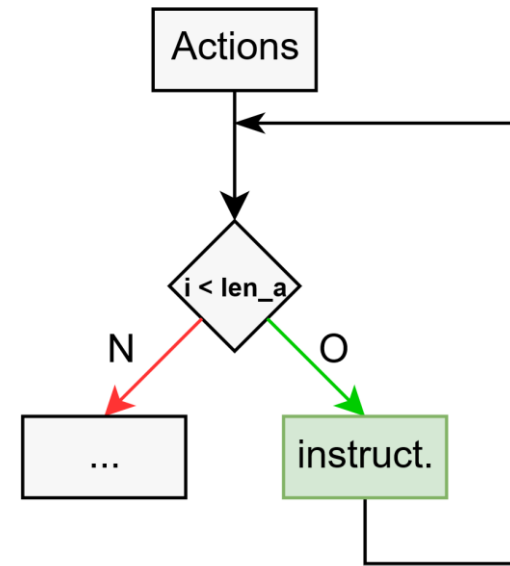
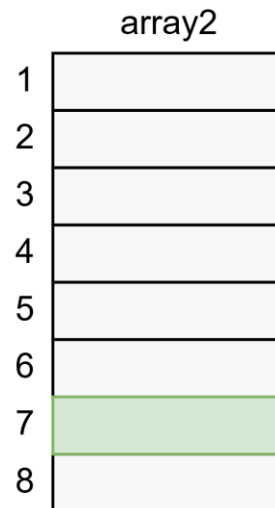
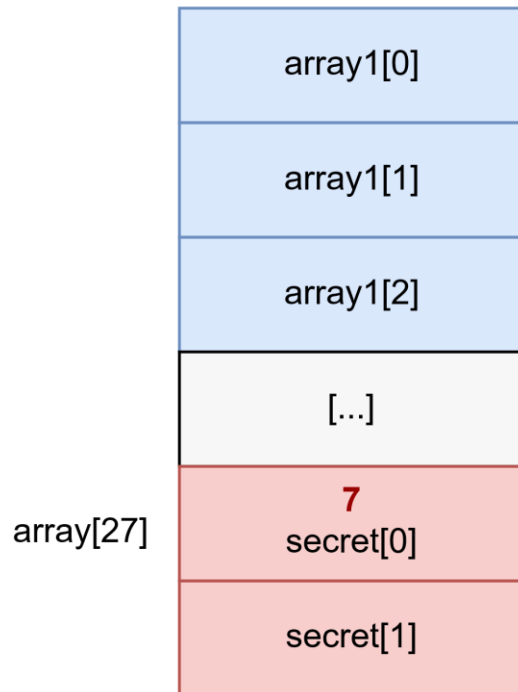


Temps d'accès  
aux « cases »

[1]	231
[2]	229
[3]	304
[4]	32
[5]	274
[6]	299
[7]	257
[8]	311

# Spectre

```
if (i < len_array1)
{
    var_secrete = array1[i];
    junk = array2[var_secrete];
}
```



# Proof of concept

<https://github.com/Hackndo/spectre-poc>

- poc\_no\_cache.c
- poc\_cache.c
- poc\_leak\_one\_byte.c
- poc\_final.c

<http://beta.hackndo.com/meltdown-spectre/>



@hackanddo

**MERCI !**



## About Capgemini

With more than 190,000 people, Capgemini is present in over 40 countries and celebrates its 50th Anniversary year in 2017. A global leader in consulting, technology and outsourcing services, the Group reported 2016 global revenues of EUR 12.5 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, [the Collaborative Business Experience™](#), and draws on [Rightshore®](#), its worldwide delivery model.

Learn more about us at

[www.capgemini.com](http://www.capgemini.com)



**People matter, results count.**

This message contains information that may be privileged or confidential and is the property of the Capgemini Group.

Copyright © 2017 Capgemini. All rights reserved.

Rightshore® is a trademark belonging to Capgemini.

This message is intended only for the person to whom it is addressed. If you are not the intended recipient, you are not authorized to read, print, retain, copy, disseminate, distribute, or use this message or any part thereof. If you receive this message in error, please notify the sender immediately and delete all copies of this message.