CERT.LV

Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

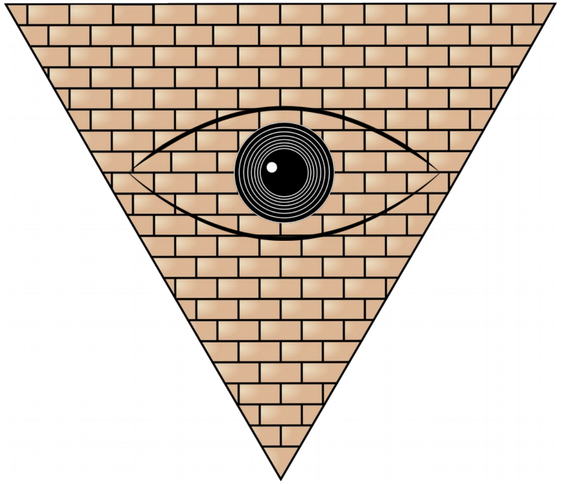
Vezums, cinītis un procesora optimizācijas

Kārlis Podiņš, Esi Drošs, 21.03.2018

Saturs

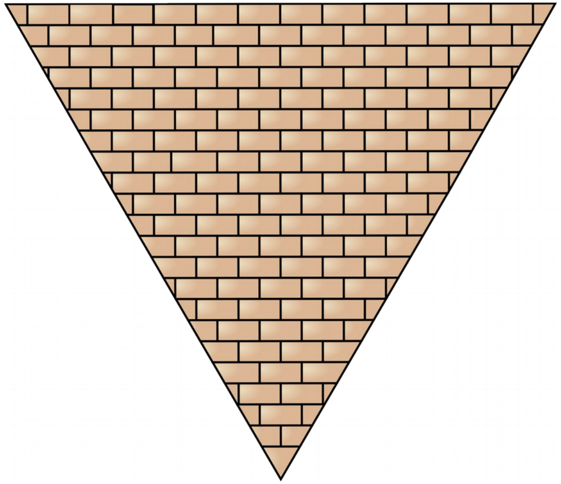
- **Procesora optimizācijas**
- **Meltdown**
- **Spectre**

Lielā patiesība



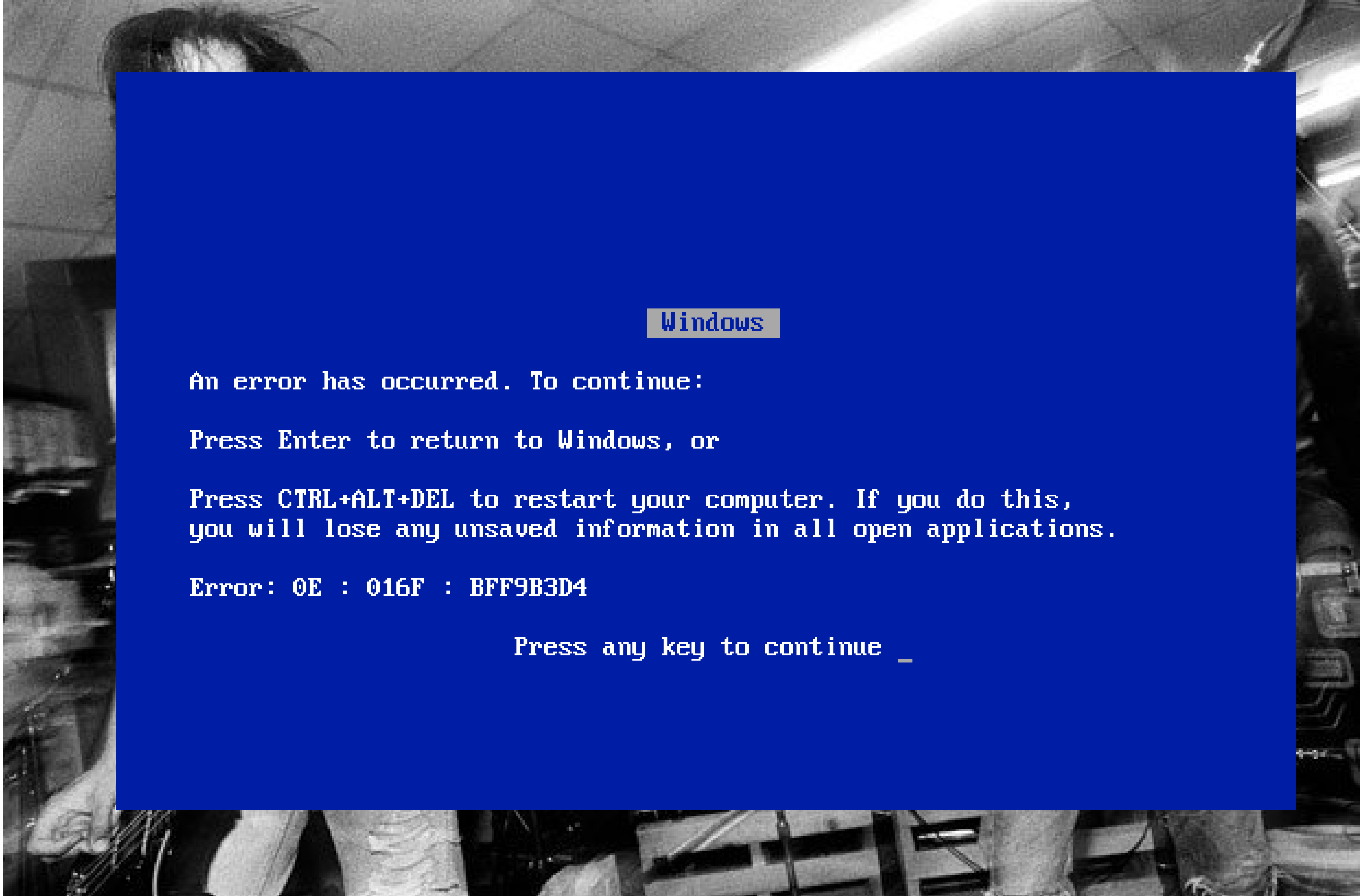
Drošības arhitektūra

- **Zema līmeņa drošības stūrakmeņi**
  - ***Kernel/user mode***
  - ***Process memory isolation***



Drošības arhitektūra

- **Zema drošības stūrakr**
  - ***Kerne r mode***
  - ***Proce mory isolation***
- **Viss ir slikti**
  - **sliktāk nevar būt**
  - **atpakaļ 90.gados**


Windows
An error has occurred. To continue:
Press Enter to return to Windows, or
Press CTRL+ALT+DEL to restart your computer. If you do this,
you will lose any unsaved information in all open applications.
Error: 0E : 016F : BFF9B3D4
Press any key to continue _

Vulnerability Note VU#584653

CPU hardware vulnerable to side-channel attacks

Original Release date: 03 Jan 2018 | Last revised: 03 Jan 2018

Overview

CPU hardware implementations are vulnerable to side-channel attacks. These vulnerabilities are referred to as Meltdown and Spectre.

Description

CPU hardware implementations are vulnerable to side-channel attacks referred to as Meltdown and Spectre (also KAISER and KPTI). These attacks are described in detail by Google Project Zero and the Institute of Applied Information Processing and Communications (IAIK) at Graz University of Technology (TU Graz).

Impact

An attacker able to execute code with user privileges can achieve various impacts, such as reading otherwise protected kernel memory and bypassing KASLR.

Solution

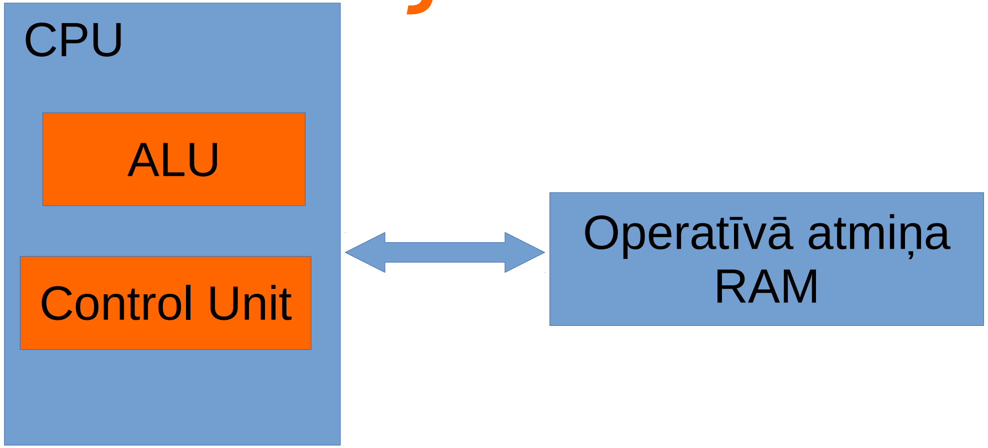
Replace CPU hardware

The underlying vulnerability is primarily caused by CPU architecture design choices. Fully removing the vulnerability requires replacing vulnerable CPU hardware.

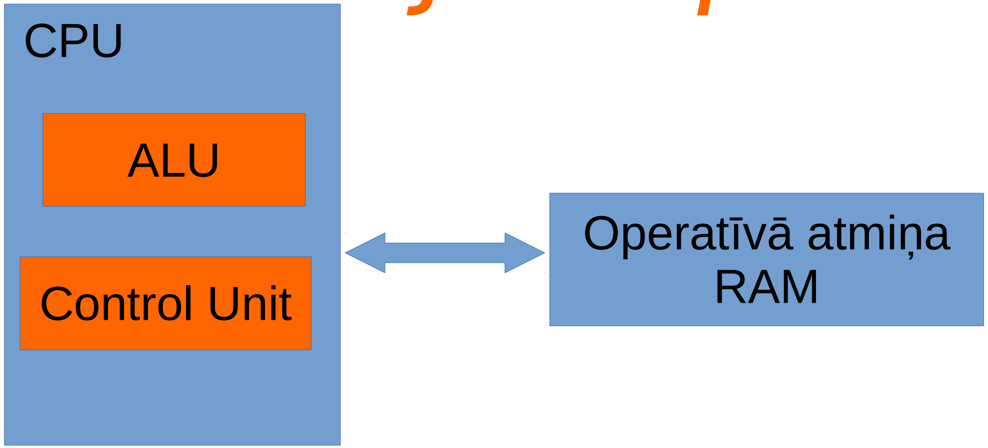
Apply updates

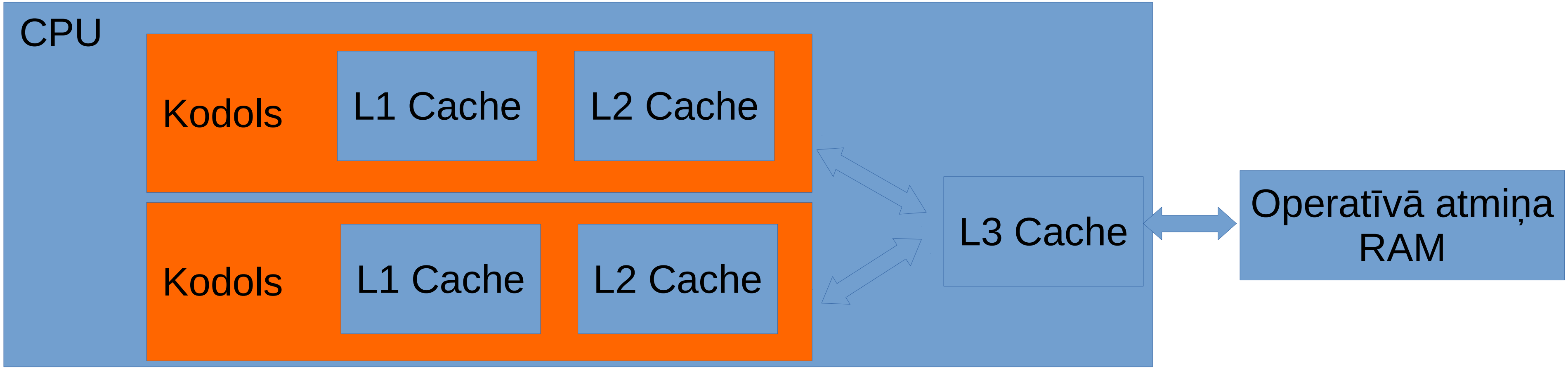
Operating system updates mitigate the underlying hardware vulnerability.

Teorija



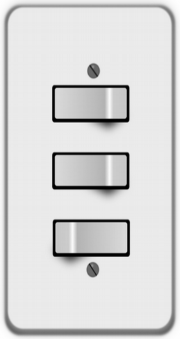
Teorija ≈ prakse

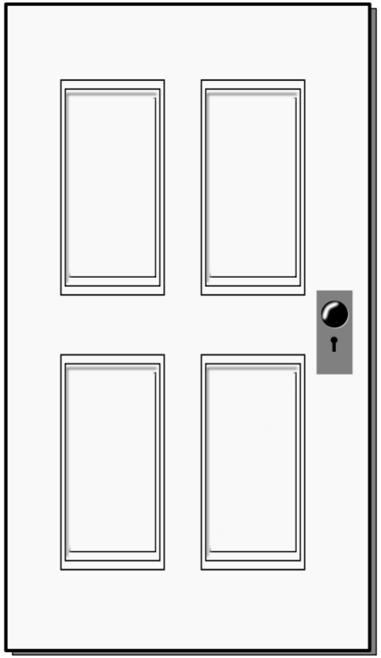


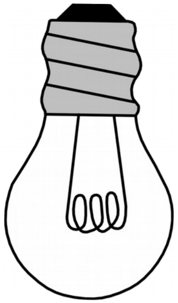


Duālā problēma

Netiešais mērījums



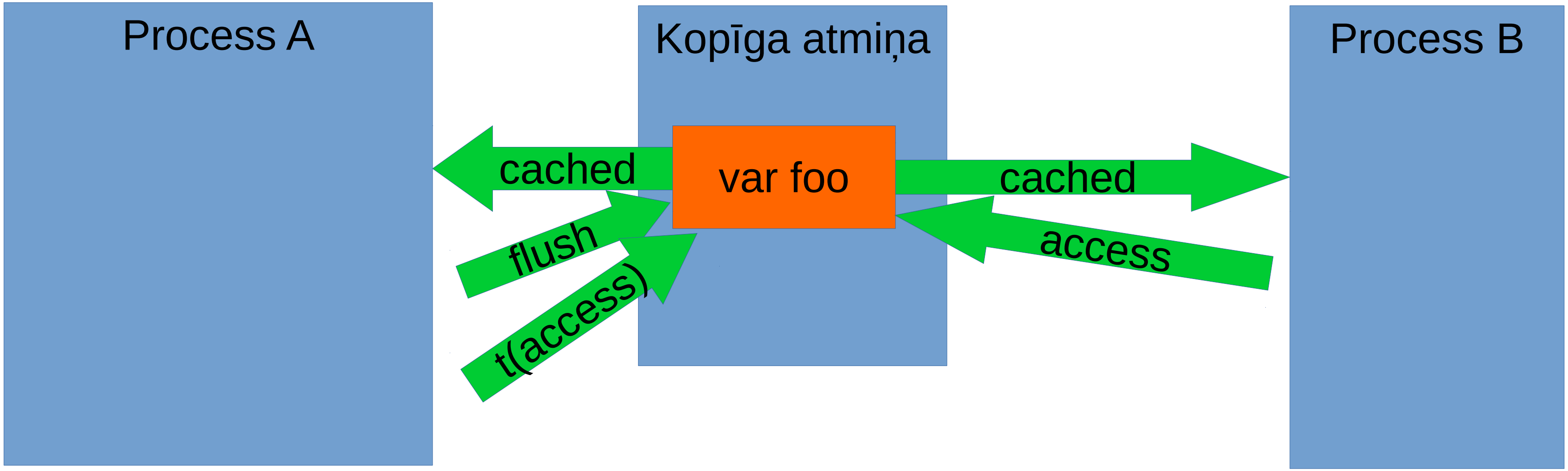




Procesora optimizācijas

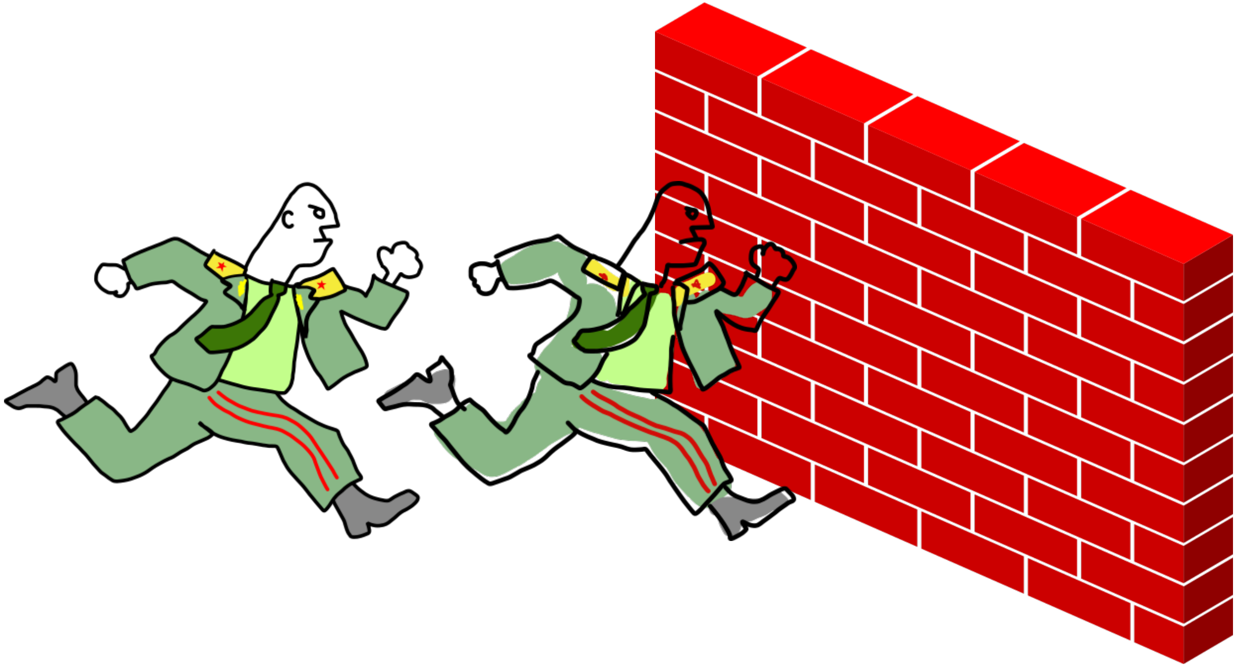
- **CPU gaidīšana = nauda vējā**
- ***Processor optimizations***
  - ***Out of order execution***
  - ***Speculative execution***
    - ***Branch prediction***

Flush+reload uzbrukums



Meltdown

Kā vējš skrien, kā miets atduras



Out of order execution

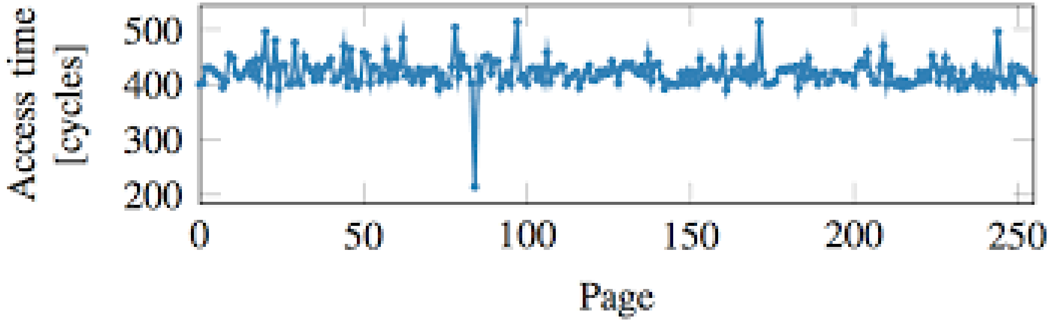
```
x=foo()
y = 42+13
z=x+y
```

Meltdown

- **Tiesību pārbaude pēc izpildes**
  - **Intel**
  - **Nepilnīga stāvokļa atjaunošana (izmaiņas *cache*)**
  - **Rezultātu iegūst no kešatmiņas (*flush+reload*)**

Meltdown - piemērs

```
char kernelData = * (char *) 0xFFFFB0DE
array[kernelData * 4096] = 0
```

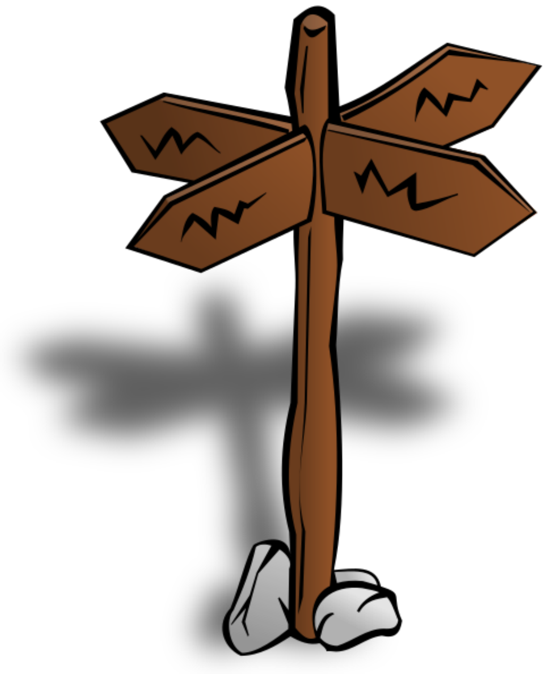


Meltdown - zāles

- ***Kernel memory not mapped in user space***
- **Palēnina pārslēgšanos starp *usermode* un *kernelmode***
- **Atkarīgs no uzdevuma**
  - **2%..400%**

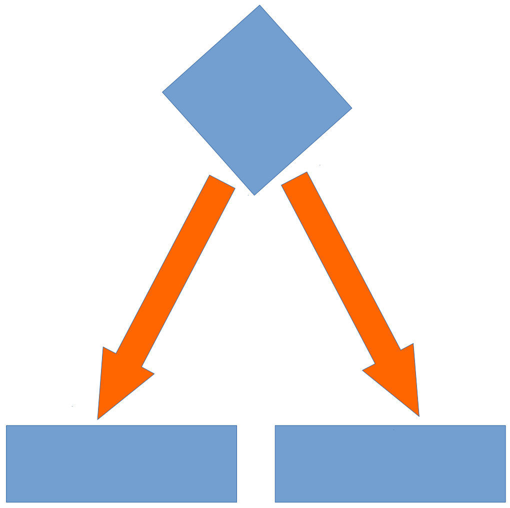
Spectre

Vai labo? Vai kreiso! Abas divas ne par ko!



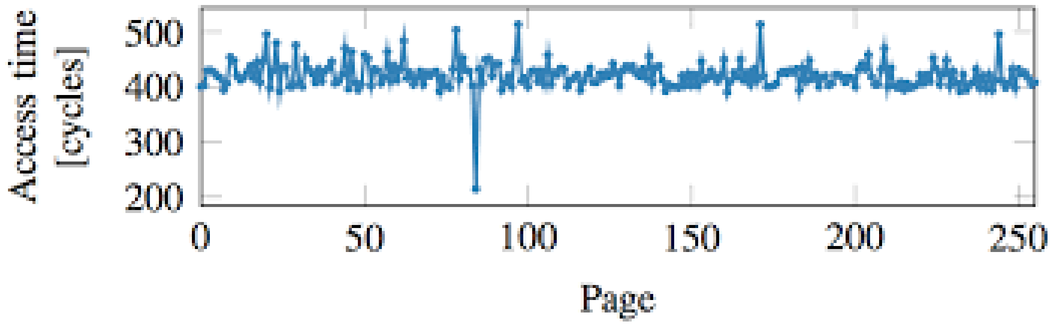
Spectre

- **Izmanto *branch prediction***
- **Spekulatīva izpilde nepareizajā zarā**
  - **Nepilnīga stāvokļa atjaunošana**
  - **Rezultātu iegūšana caur kešatmiņu (*flush+reload*)**
  - **Daudzi CPU ražotāji**



Spectre 1 - piemērs

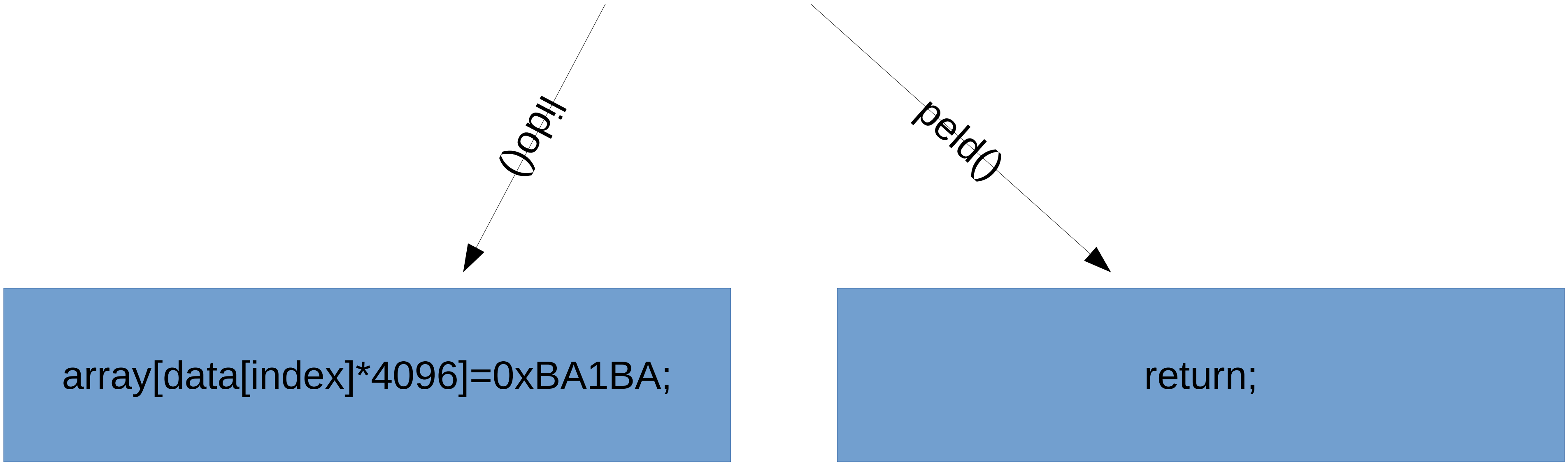
```
char* data = “esiDross”;
for(int i=0; i<8; i++)
{
    if(i<3)
        array[data[i] * 4
    else
        foo()
}
```



Spectre 2 - piemērs

lops* l = new putns;   //=new

l→kusties();



Spectre - zāles

- **NAV***
  - **Spectre 1**
    - **microcode updates**
    - **compiler extensions**
  - **Spectre 2**
    - **Indirect Branch Restricted Speculation**
    - **Indirect Branch Predictor Barrier**
    - **Single Thread Indirect Branch Predictors**
- **Sarežģītos veidos atspējot branch prediction**
  - **Branch prediction = CPU performance**

Secinājumi

- ***Public cloud***
- **Ātrdarbības samazinājums**
  - **Atkarīgs no uzdevuma**
- **CPU dokumentācijā aprakstītas iespējamā ietekme uz kešatmiņu**
  - **Ietekme uz drošību netika izvērtēta**


Paldies!