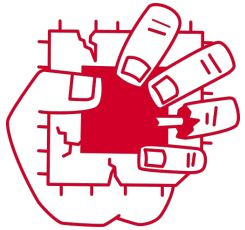
Když procesor netěsní

Michal Koutný, STG 2020-06-17



Zombieload (MDS)

I/2018

VII/2018

V/2019

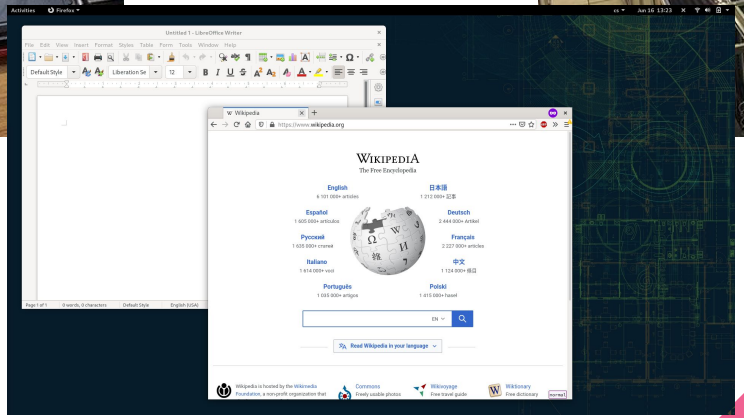
VI/2020

Crosstalk (SRBDS)

FORESHADOW

Bezpečnostní domény

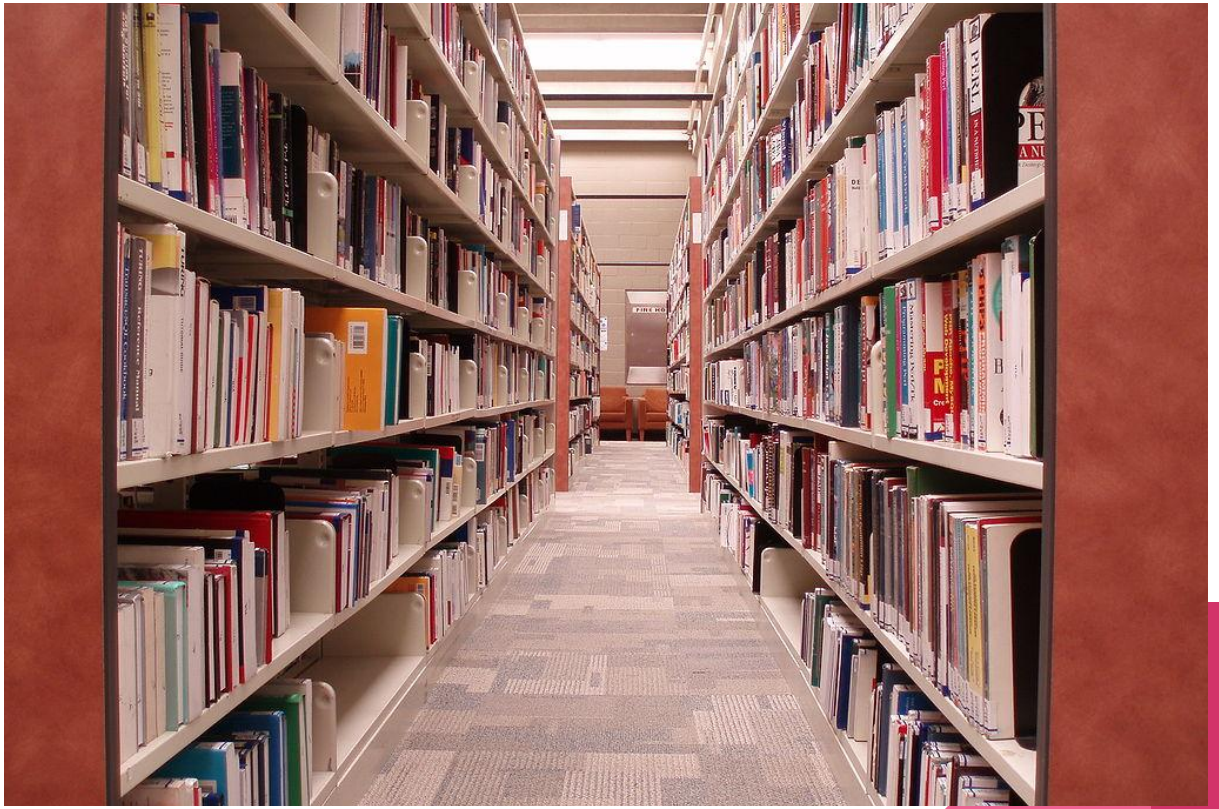
procesy



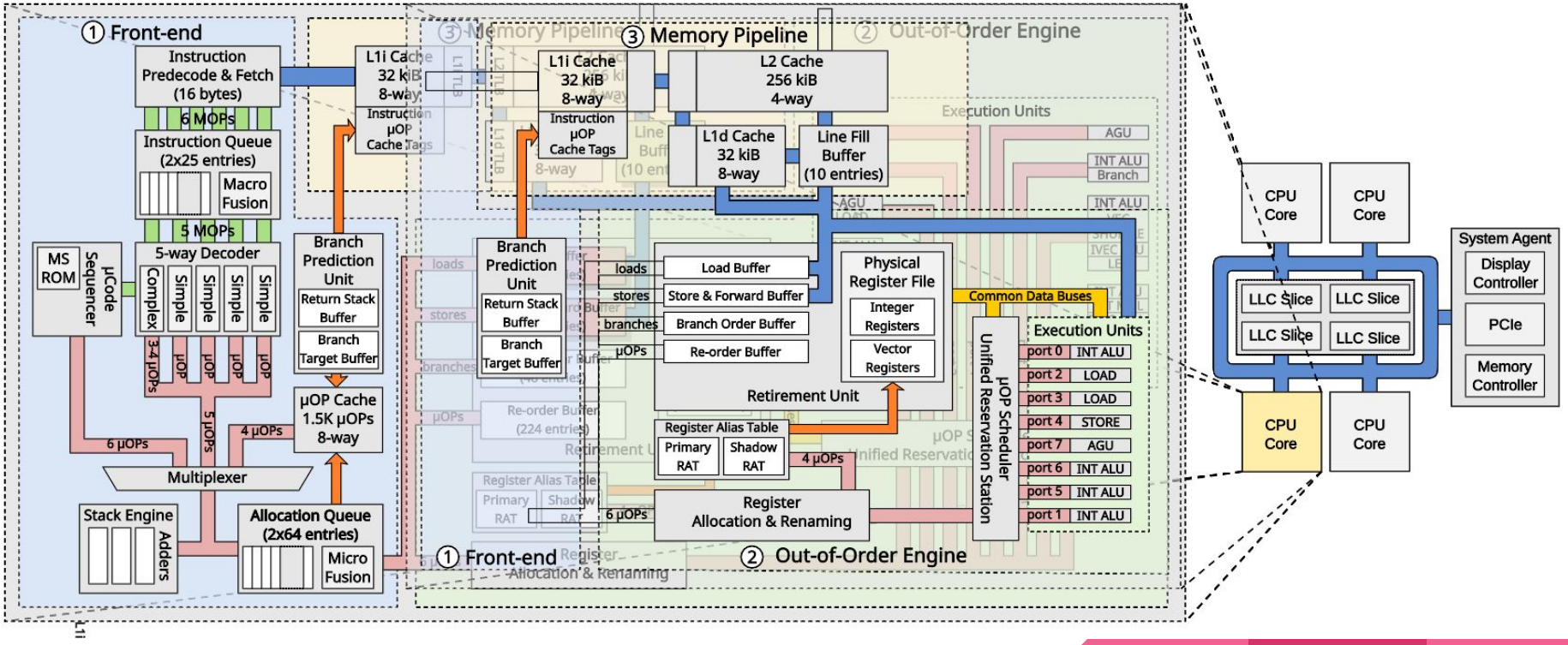
OS

cloud/VM

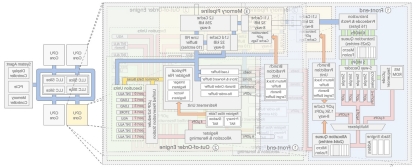
Které knihy jsou populární?

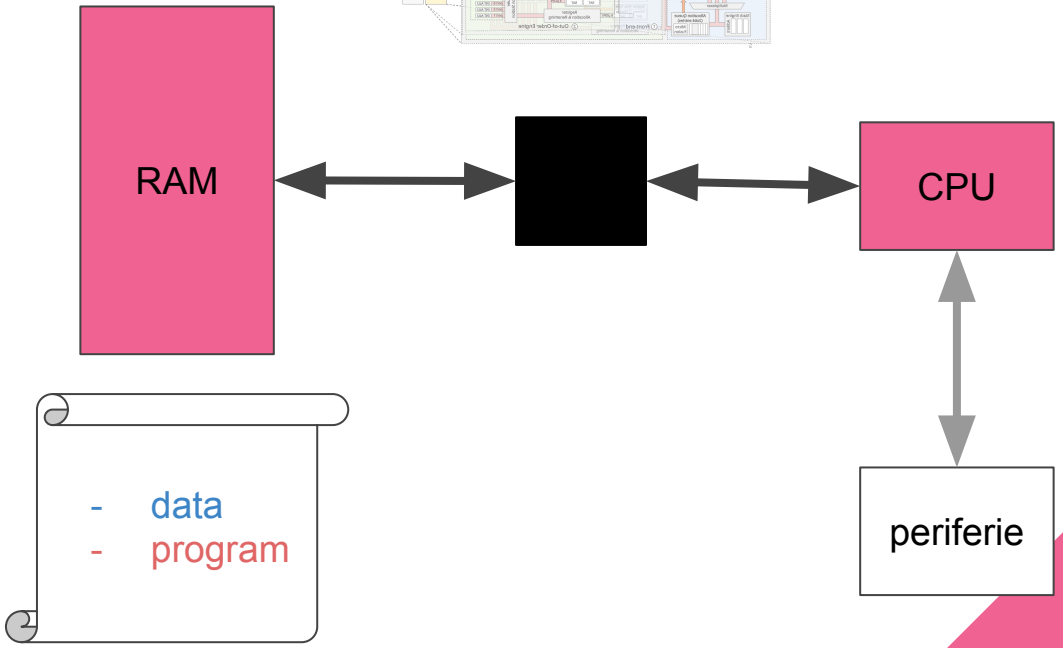


Architektura počítače*

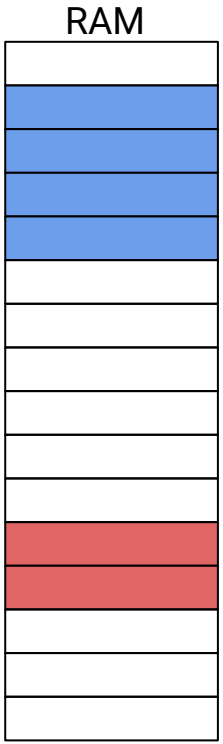


Architektura počítače*

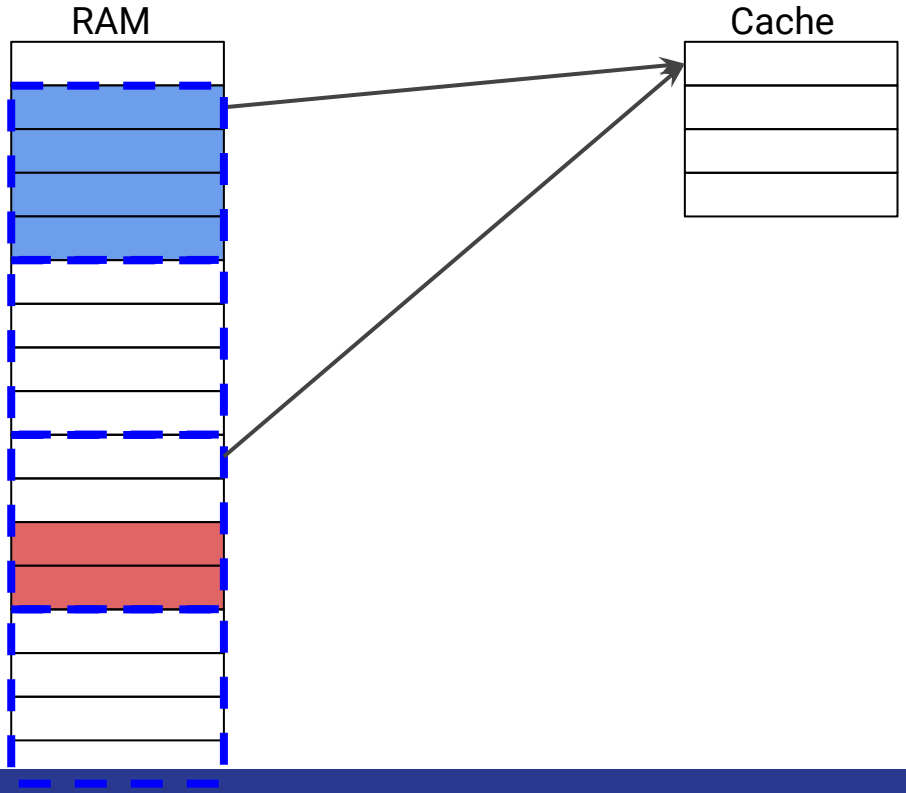




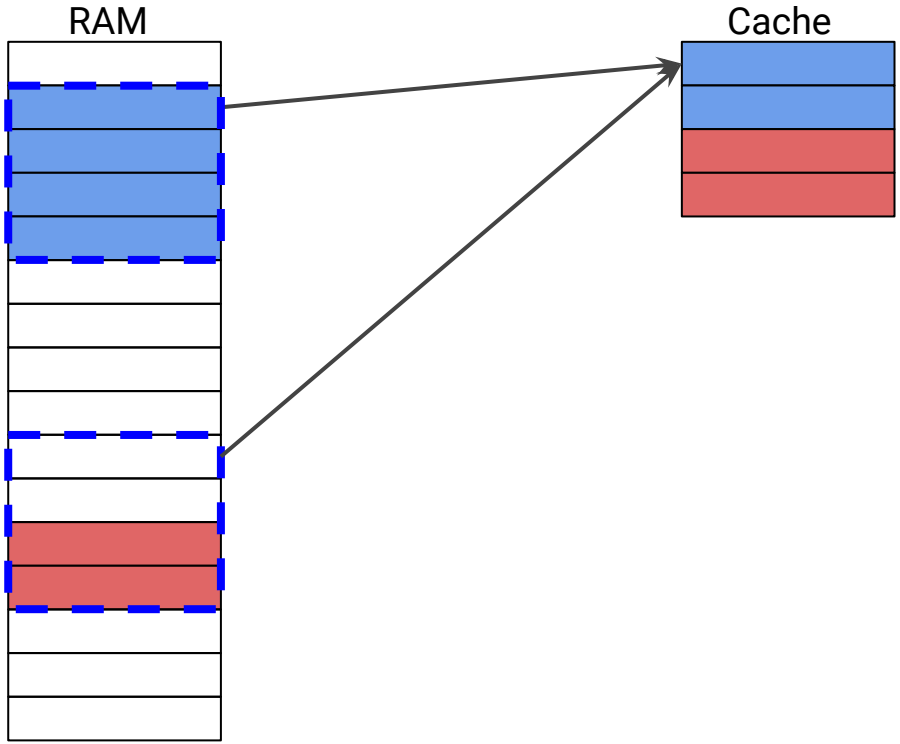
ASLR (address space layout randomization)



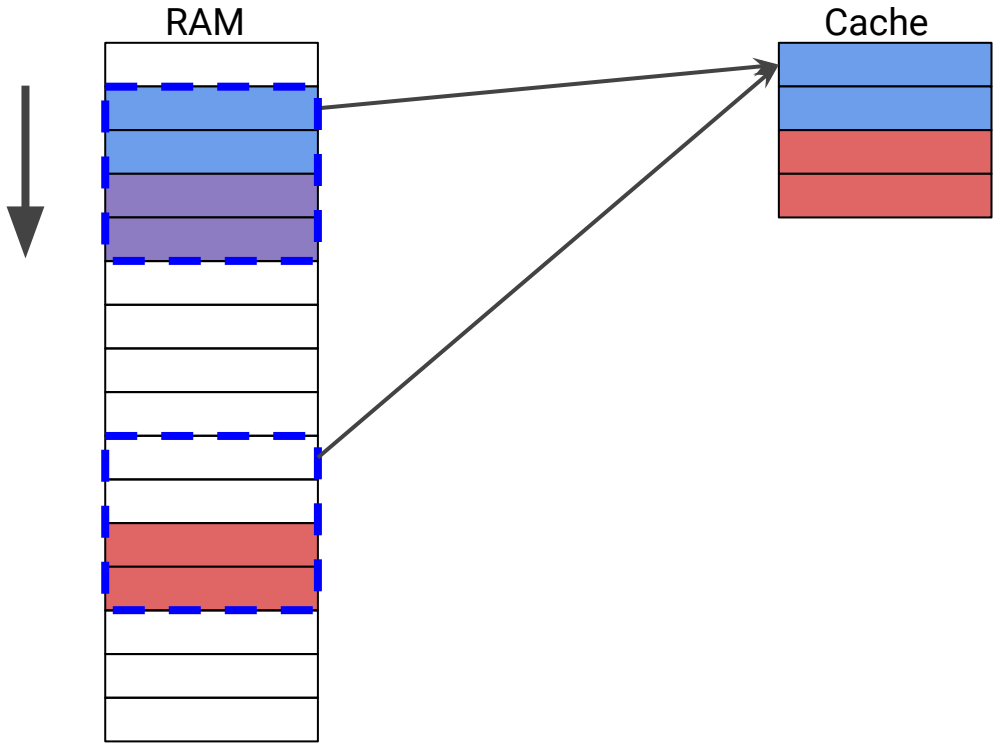
ASLR odhalení



ASLR odhalení

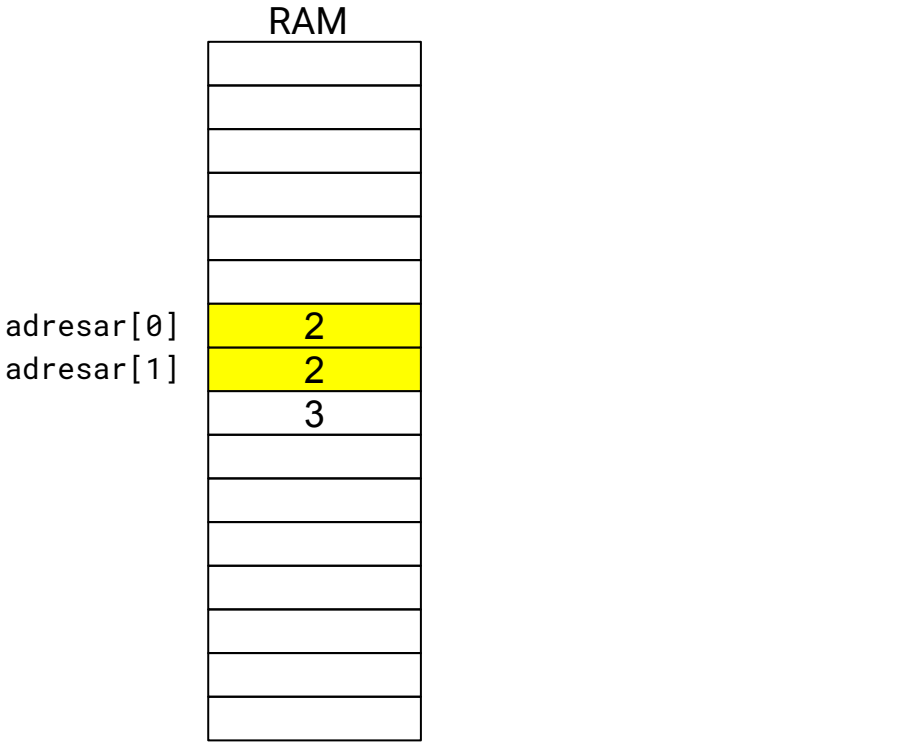


ASLR odhalení



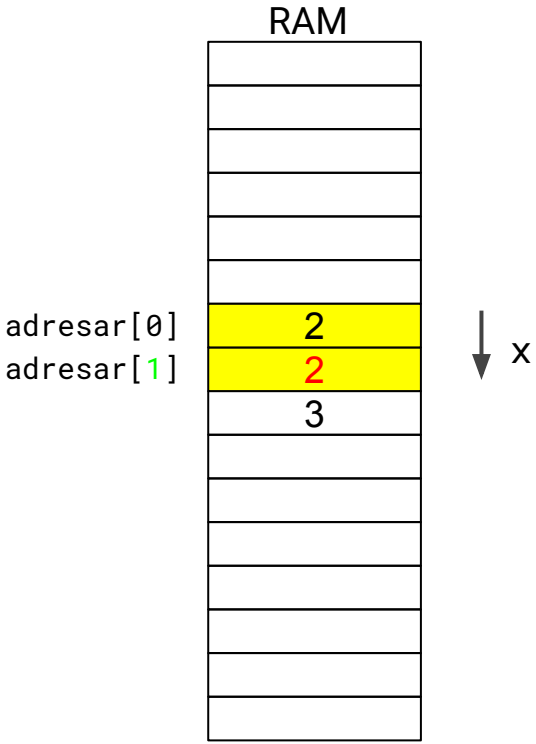
Víme kde

Spectre – úvod



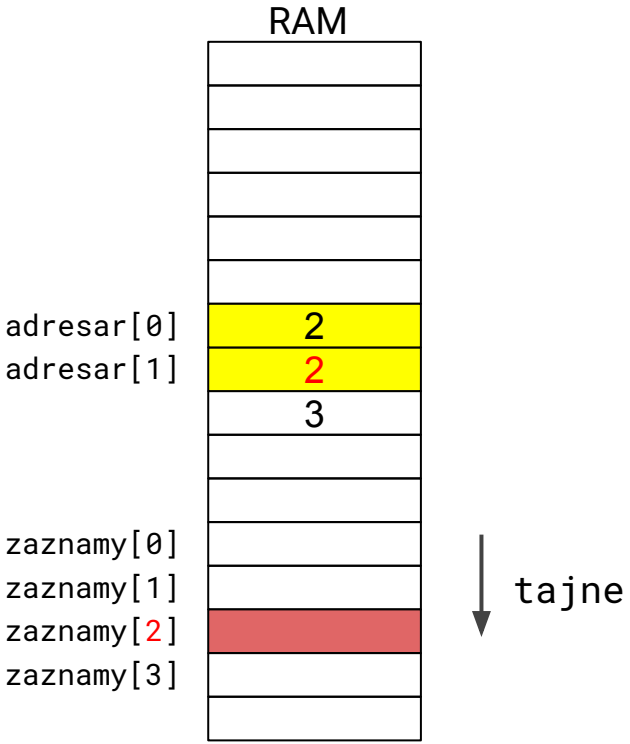

```
if (x < A)
    tajne = adresar[x]
    cti(zaznamy[tajne])
else
    mimo_adresar()
```

Spectre – úvod



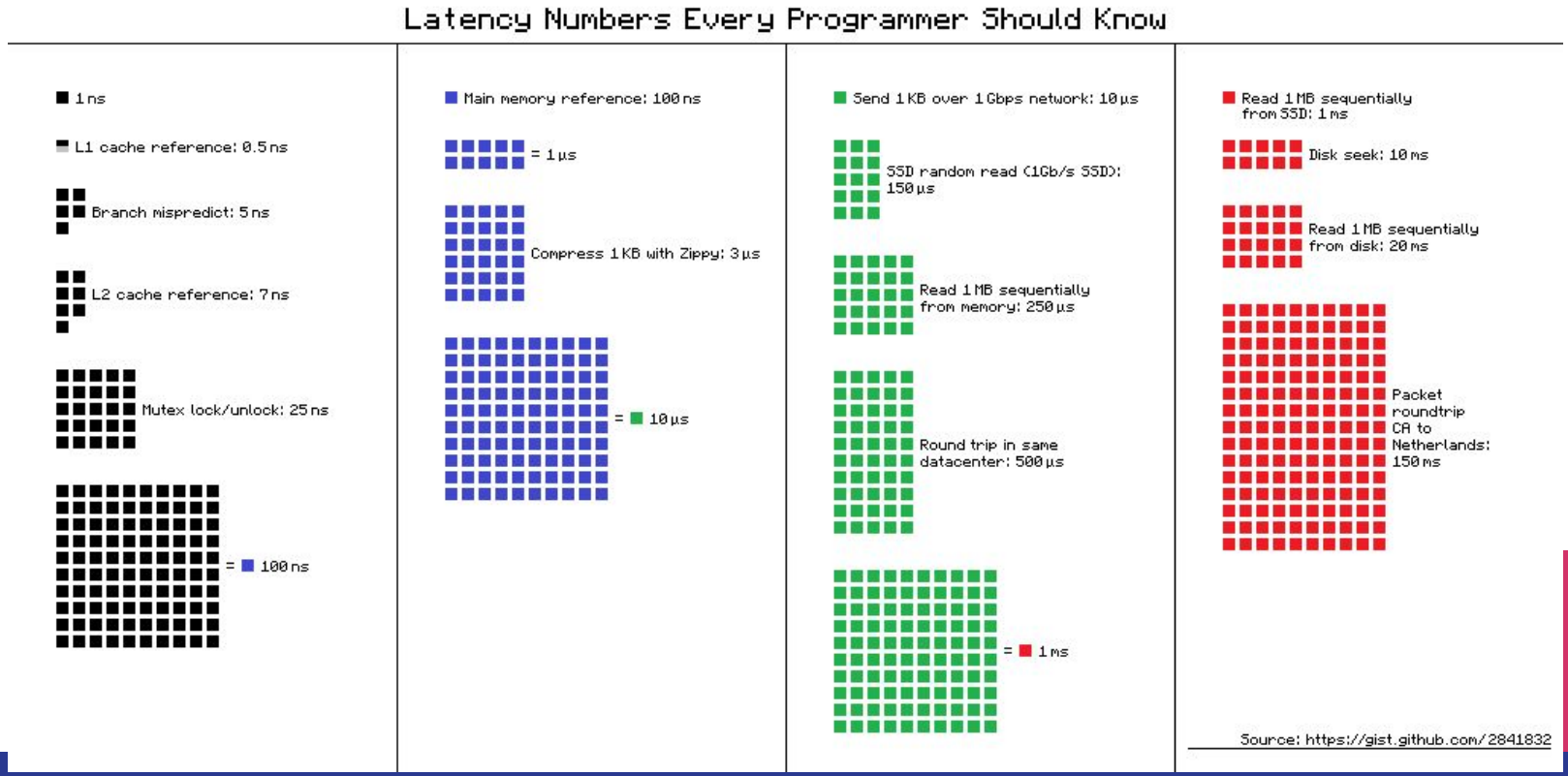

```
if (x < A)
    tajne = adresar[x]
    cti(zaznamy[tajne])
else
    mimo_adresar()
```

Spectre – úvod

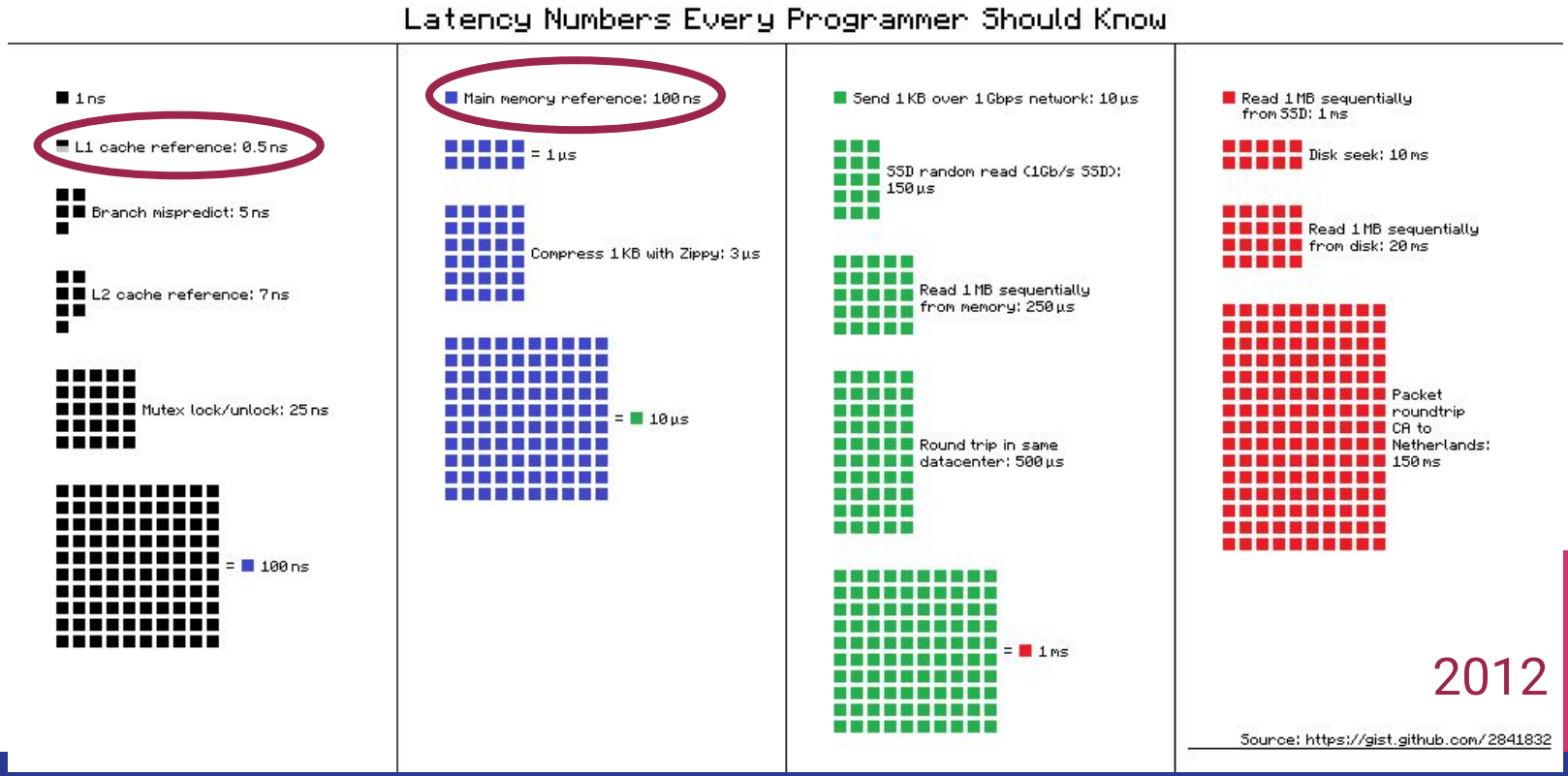



```
if (x < A)
    tajne = adresar[x]
    cti(zaznamy[tajne])
else
    mimo_adresar()
```

Čísla, co by měl znát každý (programátor)

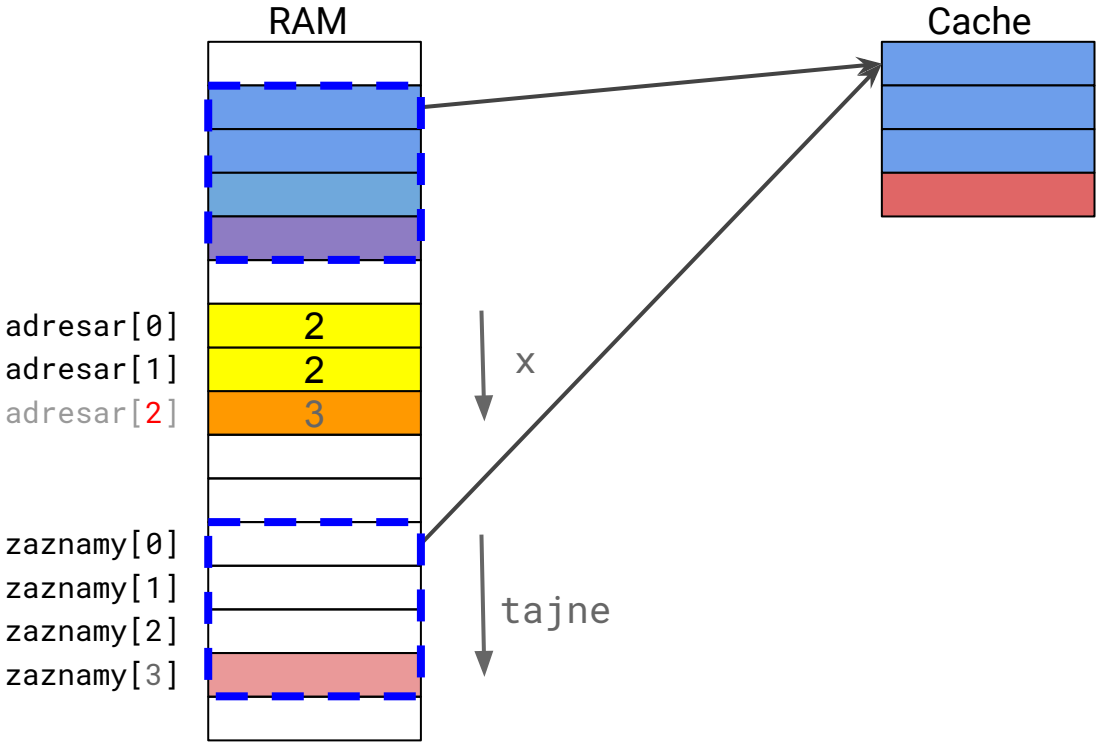


Čísla, co by měl znát každý (programátor)



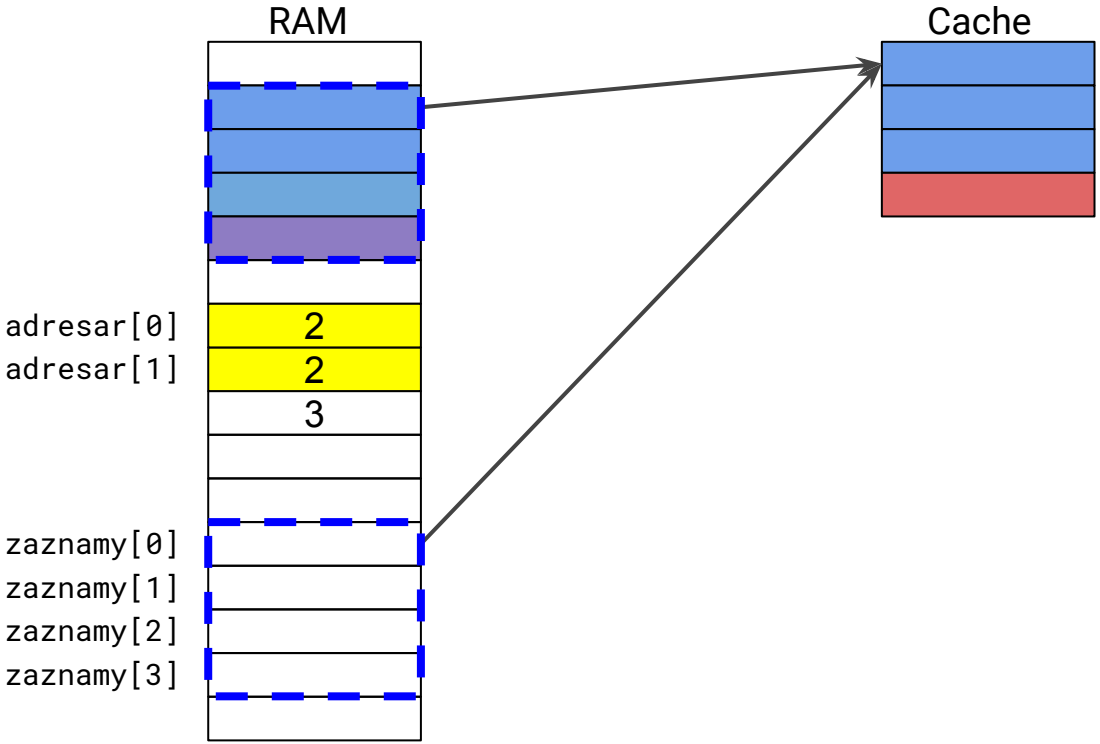
2012

Spectre




```
if (x < A)
    tajne = adresar[x]
    cti(zaznamy[tajne])
else
    mimo_adresar()
```

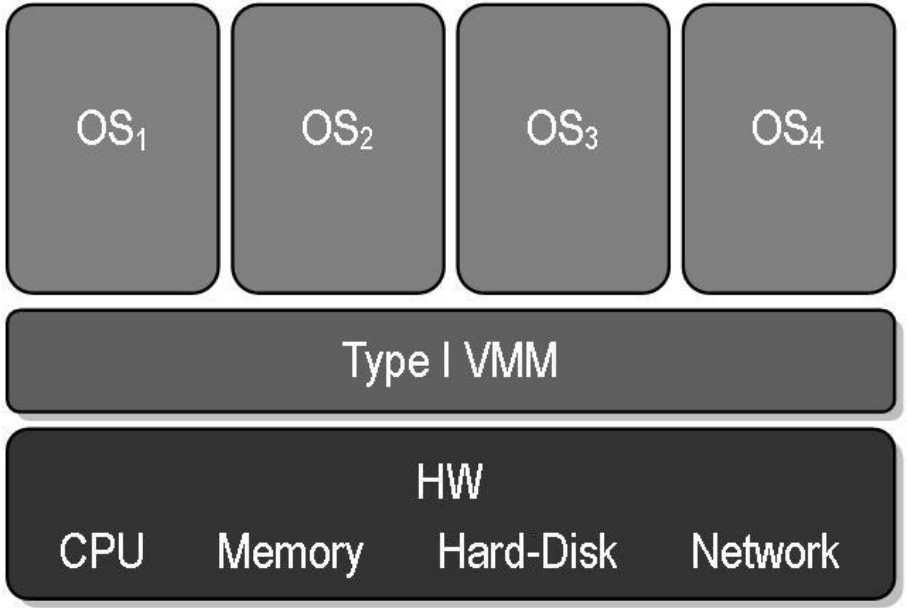
Spectre

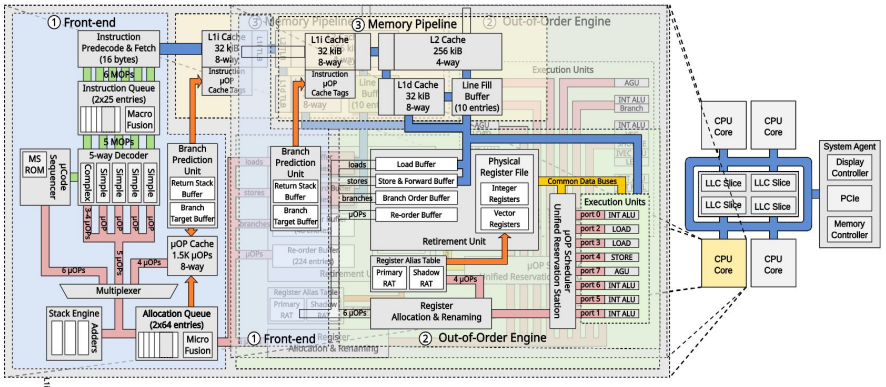



```
if (x < A)
    tajne = adresar[x]
    cti(zaznamy[tajne])
else
    mimo_adresar()
```

Víme co

Sdílení a virtualizace





Co to znamená v praxi

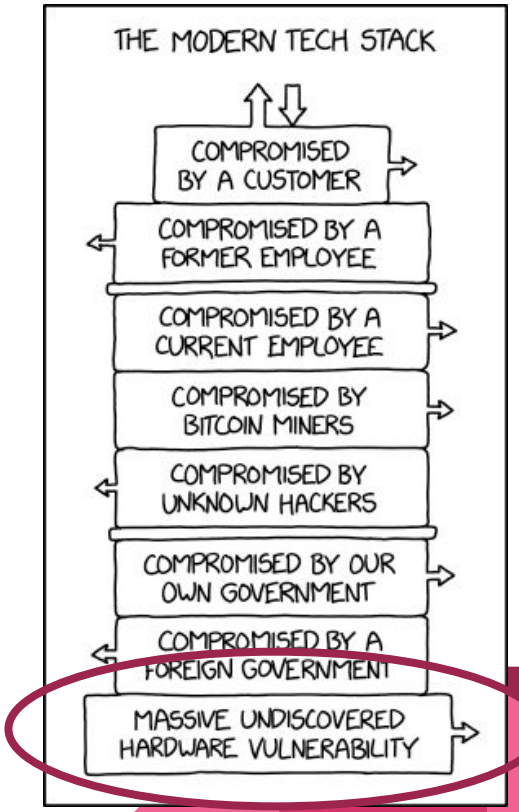
Zranitelnost	**Propustnost***
Meltdown	3,2–550 KB/s
Spectre	0,04–10 KB/s
Zombieload (MDS)	0,07–250 KB/s
Crosstalk	3 KB/s

Co to znamená v praxi 2

- Nový procesor
- Nový mikrokód
- Aktualizace SW
- Vypnutí SMT (symmetric multi-threading), core scheduling

Co to znamená v praxi 2

- Nový procesor
- Nový mikrokód
- **Aktualizace SW**
- Vypnutí SMT (symmetric multi-threading), core scheduling



Média

- https://commons.wikimedia.org/wiki/File:Cern_datacenter.jpg (Hugovanmeijeren, CC BY-SA 3.0)
- https://commons.wikimedia.org/wiki/File:Acer_Predator_Helios_300_back_panel_open.jpg (Vjdeep, CC BY 3.0)
- https://mdsattacks.com/images/skylake-color.svg
- https://xkcd.com/2166/
- https://gist.github.com/hellerbarde/2843375
- https://commons.wikimedia.org/wiki/File:20190316_135_roubaix.jpg (Jean Housen, CC BY-SA 4.0)
- https://commons.wikimedia.org/wiki/File:Lumaca_(Helix_pomat[illegible])_-_Romanengai_Gerenzano,_Italia,_09.2018_(5).jpg (Chindea Ciprian Emil, CC BY-SA 4.0)
- Public domain

Reference

- https://spectreattack.com/spectre.pdf
- https://meltdownattack.com/meltdown.pdf
- https://mdsattacks.com/files/fallout.pdf
- https://mdsattacks.com/files/ridl.pdf
- https://download.vusec.net/papers/crosstalk_sp21.pdf

Děkuji. Otázky?