

# Quem tem medo de Spectre & Meltdown?



Alexandre Oliva

lxoliva@fsfla.org

<https://www.fsfla.org/~lxoliva/>

Twister, Pump.io: @lxoliva



Copyright 2018 Alexandre Oliva (última modificação em julho de 2018)

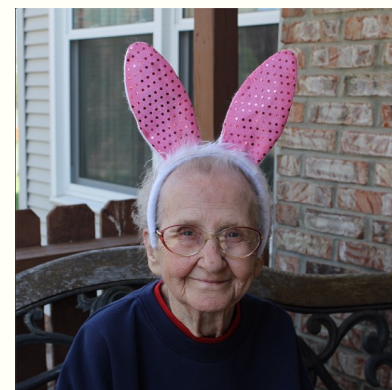
Esta obra está disponível sob a Licença Creative Commons BY-SA 4.0 International.

<https://www.fsfla.org/svn/fsfla/ikiwiki/blogs/lxo/pres/specmelt/>

<https://www.fsfla.org/blogs/lxo/pub/who-is-afraid-of-spectre-and-meltdown>

## Sabedoria da Vovó 2.030

- É melhor prevenir que remediar
- Leve uma blusa, pode esfriar!  
... e uma camisinha, pode esquentar :-)
- Não abra a porta para o **Lobo Mau**
- Não aceite doces **de** estranhos
- Não execute programas estranhos  
(já foi mais fácil)



## Dados e Programas

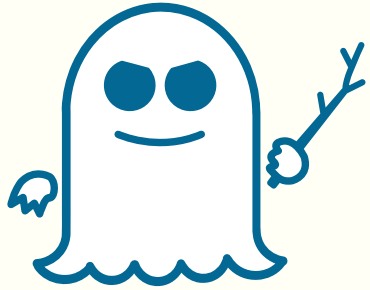
- Dados: passivos (textos, tabelas)
- Programas: ativos (instruções)
- Programas embutidos em dados
  - Macros, Javascript
- Execução automática: **estranha doçura**
  - Vírus, Vermes e Cavalos de Troia
  - Rastreadores, mineradores, bloqueadores



## Loucura e senso comum

- Antivírus .ru banido no gov.us, .uk, .au
- Celular .cn banido no gov.us
- Cav.Troia no programa nuclear iraniano
- Soberania e jurisdição sobre tecnologia
- E nossos governos, forças armadas, eleições?
- E nós e nossos próprios computadores?





## Spectre & Meltdown



```
if (x < n)
```

```
    a = m[x], b = a & 1, y = *c[b];
```

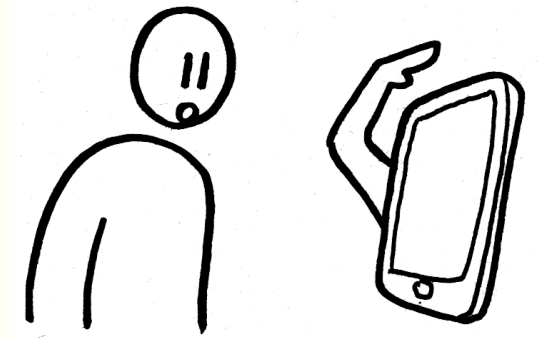
- Execução especulativa: enquanto recupera n...
- Predição de desvios: frequentemente (x < n)
- Proteção de memória: m[x] inacessível, mas...
- Caches de memória: contêm \*c[0] ou \*c[1]?
- Mesmo com MV, em MVs e navegadores!

## Por Que Pânico?

Quer proteger dados pessoais no computador?

### Programas que você usa ou...

- São confiáveis? (e não doces de estranhos)
- Servem a você, sob seu controle?
- São auditáveis **e** foram auditados?
- Poderiam ser modificados para acesso direto?



**... ou não lhe servem**

## Software Livre

- Controlado pelo usuário
- Liberdades essenciais
  - Executar para qualquer propósito
  - Estudar (auditar) fontes e adaptar
    - ↑ Indivíduo      ↓ Comunidade
  - Copiar e distribuir as cópias
  - Melhorar e distribuir as melhorias





## Liberdade de Software

- Direito humano fundado na ética
- Pela segurança dos seus dados
- Sistema operacional, aplicativos
- Bibliotecas, plugins, addons
- Programas embutidos em dados!
- Drivers, firmware e microcódigo
- Serviço como Substituto de Software (SaaS)





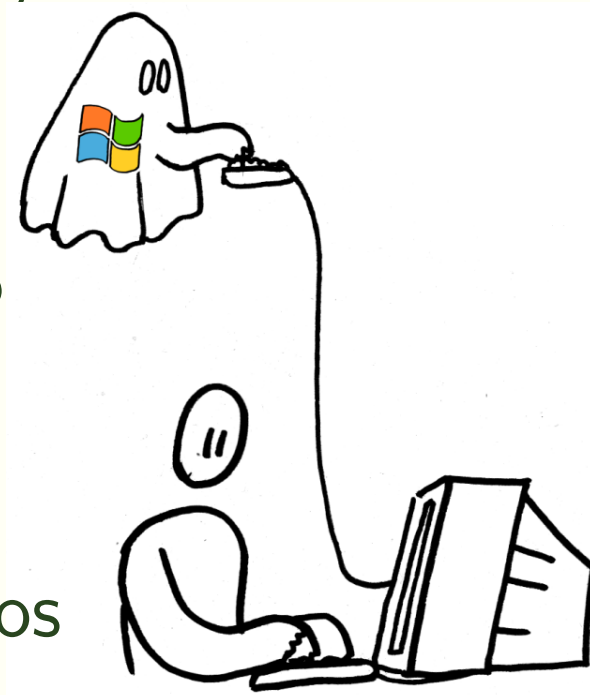
## Máquina Virtual, Risco Real

- Computador local, próprio (IntelME? PSP?)
- Computador remoto, próprio
- Computador (virtual?) compartilhado
- Isolamento entre clientes pelo provedor
- Ética: computações independentes
- Prática: pânico entre clientes e provedores

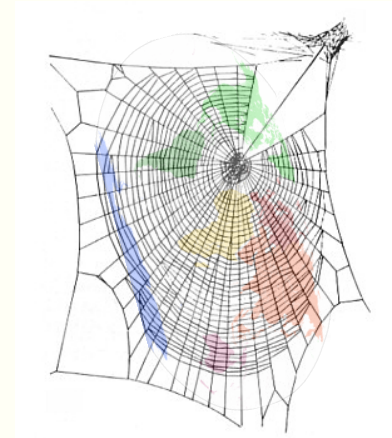


## Liberdade e Segurança

- Liberdade não basta para segurança
- Mas segurança requer liberdade
- Controle do software e do usuário
- Defesas individuais e coletivas
  - Ataques deliberados e elaborados
  - Exploração de erros acidentais



## Teia Global de Execução



- Páginas com Flash, Java, Javascript, ...
- Execução automática a mando do servidor
- GNU LibreJS, NoScript, Greasemonkey
- Auditoria, adaptação e seleção de versões
- Controle pelo usuário, ou bloqueio
- Acesso indevido, tudo perdido: coincidência?

## Furos e Remendos

- Exigência de microcódigo não-Livre
- Atualizações com novidades indesejadas?
- Computações mais lentas e caras
- Considere a liberdade de software
- Quem sabe que outros furos existem?
- Não deixe o Lobo Mau entrar!



**Nada a Temer...**

**Obrigado!**

**OFSSFO**  
América Latina

**Sê Livre!**



`oliva@gnu.org, lxoliva@fsfla.org`

Twister, Pump.io: `@lxoliva`

`https://www.fsfla.org/~lxoliva/`

