

Who's afraid of Spectre & Meltdown?

OFSSFO
Latin America

Alexandre Oliva

lxoliva@fsfla.org

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

Twister, Pump.io: @lxoliva



Copyright 2018-2019 Alexandre Oliva (last changed in July 2019)

This work (minus images and video) is licensed under the [Creative Commons BY-SA 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/).

<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>

Grandma 2.033's Wisdom

- Prevention is better than cure
- Take a coat, for the cold!
... and a condom, for the heat :-)
- Don't let the **Big Bad Wolf** in
- Don't take candy **from** strangers
- Don't take strange programs
(it used to be easier)



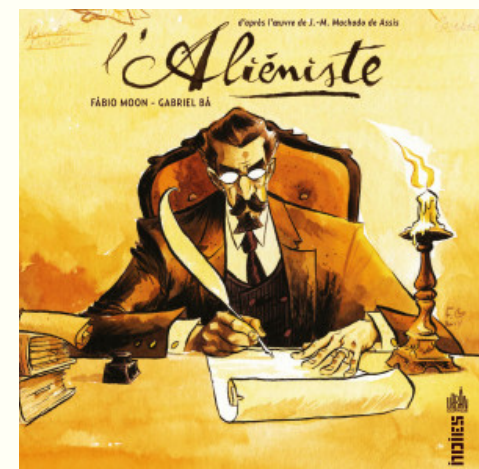
Data and Software

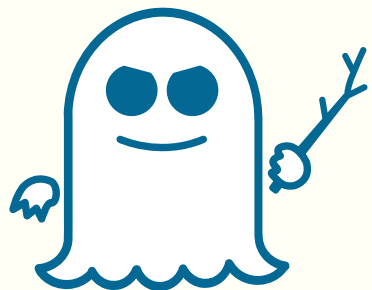
- Data: passive (text, tables)
- Software: active (instructions)
- Software embedded in data
 - Macros, Javascript
- Automatic execution: **strange sweetness**
 - Viruses, Worms and Trojan Horses
 - Trackers, miners, blockers



Madness and common sense

- Antivirus.ru banned in gov.us, .uk, .au
- Mobile.cn banned in gov.us
- Trojan horse in Iranian nuke research
- Sovereignty and jurisdiction over tech
- Our governments, armed forces, elections?
- How about us and our own computers?





Spectre & Meltdown



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

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

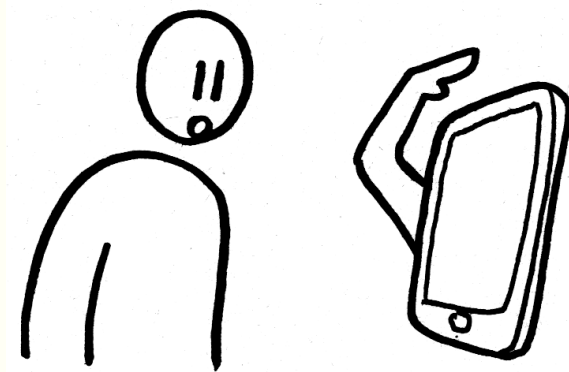
- Speculative execution: while obtaining n...
- Branch prediction: usually (x < n)
- Memory protection: m[x] inaccessible, but...
- Memory caches: holding *c[0] or *c[1]?
- Even with VM, in VMs and browsers!

Why Worry?

Got personal data on the computer?

Software you use either...

- is reliable? (not strangers' candy)
- serves you, under your control?
- is auditable **and** was audited?
- could be changed for direct access?



... or it does not serve you

Free Software

- Controlled by the user
- Essential freedoms
 - Run for any purpose
 - Study (audit) sources and adapt
 - ↑ Individual ↓ Community
 - Make and distribute copies
 - Improve and distribute improvements



Software Freedom

- Human right founded on ethics
- For your data security
- Operating system, apps
- Libraries, plugins, addons
- Software embedded in data!
- Drivers, firmware and microcode
- Service as a Software Substitute (SaaS)



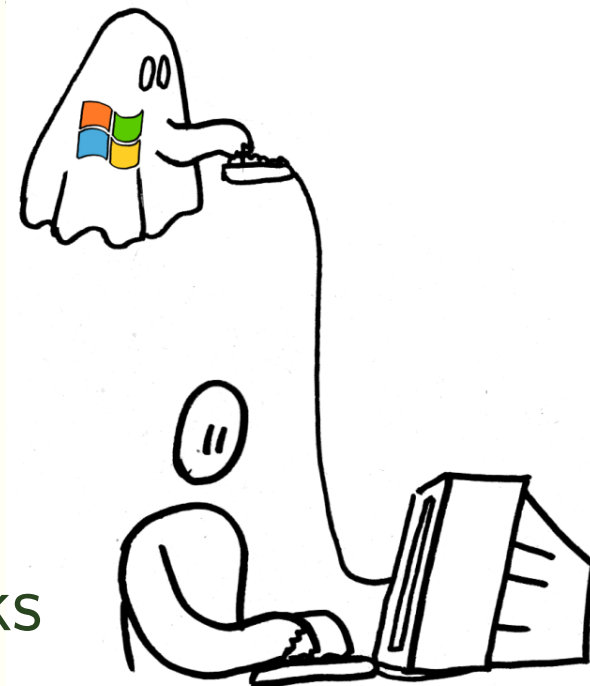
Virtual Machine, Real Risk

- Own local computer (IntelME? PSP?)
- Own remote computer
- Shared (virtual?) computer
- Isolation between customers by provider
- Ethics: independent computations
- Practice: panic among customers and providers



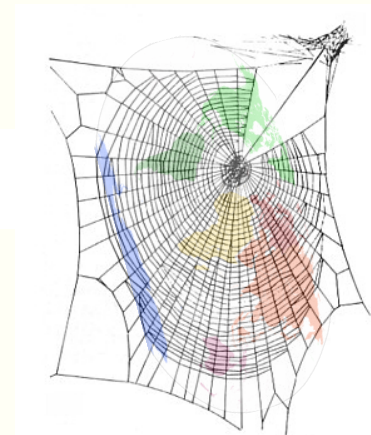
Freedom and Security

- Freedom is not enough for security
- But security requires freedom
- Controlling software and users
- Individual and collective defenses
 - Deliberate and elaborate attacks
 - Exploiting accidental errors
 - Exploitable (NetSpectre) gadgets



World Wide Execution Web

- Pages with Flash, Java, Javascript, ...
- Automatic execution under server's control
- GNU LibreJS, NoScript, Greasemonkey
- Auditing, adaptation, version selection
- Control by the user, or block
- Unwanted access, all lost: coincidence?



Holes and Patches

- Demand for non-Free microcode
- Updates with unwanted features?
- Slower and costlier computing
- Consider software freedom
- Who knows what other holes are there?
- The gravity of running blindfolded
- Don't let the Big Bad Wolf in!



Nothing to Fear...

Thank you!

OFFFO
Latin America

Be Free!



oliva@gnu.org, lxoliva@fsfla.org

Twister, Pump.io: @lxoliva

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

