Reasonably Secure Computing in the Decentralized World
(An Operating System Architect’s Perspective)

Joanna Rutkowska
Invisible Things Lab & Qubes OS Project

Berlin, September 7, 2017
“The network is the computer.”
No, how to make this computer (reasonably) secure?
Trust?

- Trusted(?)
- Secure
- Trustworthy

more desired
Challenge #1
Attacks from the host

- Confidentiality
- Integrity (is it really my software?)
Not to be confused with...
Attacks on the host (complementary scenario)

- VM/container escapes
- Areas of active research for at least a decade!
Challenge #2
“But there are no apps on the (thin) terminal!”
Attacks on terminals

- WiFi/Bluetooth
- USB devices
- Networking services (NTP, DNS resolver, etc)
- Simple physical attacks (Evil Maid)
Challenge #3
Some apps are less trusted than others...

How to prevent they don’t attack the others?
Qubes OS
Qubes OS

1. Compartmentalize

2. Carefully add integration on top of compartments
Example of Qubes integration on top isolation
work-email VM (container)

- Email client
- PDF attachment
work-email VM (container)

Email client
PDF attachment

Disposable VM (container)

PDF viewer (perhaps buggy)
PDF attachment

qubes.OpenInVM
Looks simple, but...
- How to transfer files w/o increasing attack surface?
- How to virtualize GUI for the VMs w/o increasing the attack surface?
- Etc, etc.
Xen, or: KVM? Cloud VMs? Golem?
Golem & Qubes
Golem & Qubes

- Both interested in solving similar challenges (#1-#3)
- Golem as a platform for Qubes?
Thanks!
https://qubes-os.org