The remote working security conundrum: what is reasonably secure anyway?

Usenix LISA 2021
Alex.sharp@orionvm.com

Qubes logo is licensed under: Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)
https://www.qubes-os.org/doc/style-guide/

Slides: https://github.com/orionvm/LISA2021
$ whoami

- Alex Sharp, Andrew Reimers
- Looking for a stack for secure Dev/sysadmin work
- Working at OrionVM –
  - A wholesale cloud computing provider
Disclosure

- We haven’t been provided discounted products from the vendors mentioned here
- Work in progress – new hardware
- Using Qubes for years (see LCA talks)
What’s reasonable? Threat model

- Zero day exploit – 100K USD for Firefox RCE (Zerodium)
- Cost per affected user
- Profit per attack
- Political motivation
- Ransomware
- Social engineering attacks not considered here
Agenda/Security pyramid

- Business continuity
- Application security
- Network security
- OS security
- Firmware level
- Physical level
Physical level

- Screen lock/Autolock
- BIOS password
- Boot from internal disk only
- Kensington lock
- Screen privacy filter
- “Glitter screws”
- Anti-interdiction shipping

https://mullvad.net/en/help/how-tamper-protect-laptop/
Physical level – Hardware kill switches

https://puri.sm/posts/librem-14-rave/
“We conduct extensive experiments and the results show that more than 72.2% of keystrokes can be successfully recovered.”


See also 'Listen to your key': HotMobile '20: Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications March 2020 Pages 3–8 https://doi.org/10.1145/3376897.3377853
# Architecture comparison

<table>
<thead>
<tr>
<th></th>
<th>Intel</th>
<th>AMD</th>
<th>Power9</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cost</strong></td>
<td>Reasonable</td>
<td>Cheaper</td>
<td>Enterprise</td>
</tr>
<tr>
<td><strong>Ram encryption /ECC</strong></td>
<td>No/No</td>
<td>Yes/Yes</td>
<td>No/Yes</td>
</tr>
<tr>
<td><strong>Management engine</strong></td>
<td>Closed/removable</td>
<td>Closed</td>
<td>Open</td>
</tr>
<tr>
<td><strong>Qubes/Heads support</strong></td>
<td>Best/Best</td>
<td>Good/Old</td>
<td>No*/No</td>
</tr>
</tbody>
</table>

* Actively being worked on
Firmware security: Librem 14

- Coreboot
- Reduced intel ME
- Coreboot SMM code
- Heads (Pureboot)/Librem Key
- Has a TPM
- Open source Embedded Controller (EC)
- Hyperthreading disabled
Hardware security tokens

https://puri.sm/products/librem-key/

https://en.wikipedia.org/wiki/YubiKey#/media/File:YubiKey-4-keychain-and-YubiKey-4-Nano.png
TPMs

- Like a security token
- In your computer
- Unlocks from boot measurements

https://upload.wikimedia.org/wikipedia/commons/6/64/TPM_Asus.jpg
Physical firmware protection

https://puri.sm/posts/librem-14-rave/
Operating system Level: Qubes

- “A reasonably secure operating System” focusing on security through isolation - “You can’t hit what you can’t see”
- Consists of multiple Qubes and an isolated management VM
  - A Qube is a Xen VM running an OS (Linux/FreeBSD/etc)
  - Has it’s own xserver for graphics
- Tied together via vchan, virtual networking
- Optional USB devices (proxy), PCIe devices (IOMMU)
- Managed by an internal agent (qreexec) via vchan.
Firefox and a password manager
Firefox and a password manager
USB isolation

• USB is a lovecraftian nightmare
• A ‘USB key’ can be a
  • Keyboard
  • Mouse
  • Virtual ethernet device
  • Storage device
  • Pizza oven

https://github.com/whid-injector/WHID
Qubes video call
Hardware isolation
“Our analysis found that the problem of insecure drivers is widespread, affecting more than 40 drivers from at least 20 different vendors [..] - all the vulnerable drivers we discovered have been certified by Microsoft [..] A vulnerable driver installed on a machine could allow an application running with user privileges to escalate to kernel privileges”


Eg. CVE-2021-21551 since 2009, CVE-2021-1052
Disposable Qubes
Networking security

- Local router security
- DNS security/HTTP content injection
- Security via network isolation, eg. From CVE-2019-14899
Network isolation

- work
- work-vpn
- hobby
- hobby-vpn
- disp1234
- disp1337
- vault
- web-vpn
- sys-firewall
- sys-net
- NAT
- Firewall
- WIFI

Deployments:
- disp1337: web-vpn
- disp1234: disp1337
- hobby-vpn: hobby
- work-vpn: work
- work: vault
- sys-net: sys-firewall
- WIFI: sys-net
Upgrade path

Dom0 ➔ sys-update ➔ web-vpn ➔ sys-firewall ➔ sys-net

Vchan

WIFI
'BeyondCorp'/L7 model example

- Qubes
  - Creds
  - disp1234
  - disp1337
  - Split SSH
  - U2F proxy
  - Ephemeral creds

- Auth
- Hashicorp vault

- Database
- Business system
- Split SSH
- U2F proxy

- Business system
  - U2F proxy
  - Split SSH

- Hashicorp vault
  - Split SSH
  - U2F proxy

- Database
  - U2F proxy
  - Split SSH

- Ephemeral creds
  - Split SSH
  - U2F proxy

- Qubes
  - Creds
  - disp1234
  - disp1337
  - Split SSH
  - U2F proxy
Backups and business continuity

- Local backup
- Remote backup
- "Append only" or "Separation of powers" backup principle. *(Tarsnap model)*
Going forward

- Upstream work
- Remote attestation
- Mobile investigation: Librem 5
- Better solutions for file/secret sharing
Thanks!
Any questions?

Usenix LISA 2021

Qubes logo is licensed under:
Creative Commons
Attribution-ShareAlike 4.0
International (CC BY-SA 4.0)
https://www.qubes-os.org/doc/style-guide/

Slides: https://github.com/orionvm/LISA2021