

orionVMTM



Using a cloud to manage a cloud

Sysadmin Miniconf at [Linux.conf.au](https://linux.conf.au)



Slides: <https://github.com/orionvm/LCA2020>

\$ whoami

- Alex Sharp, Andrew Reimers, Anuj Dhavalikar
- Using Qubes for Dev/sysadmin work for ~ 3 years
- Working at OrionVM –
 - White-label cloud (IaaS)

Agenda

- Why protect sysadmins?
- What is Qubes?
- Isolations provided by Qubes:
 - Graphics
 - Networks
 - Ssh/GPG keys
 - USB/PCIe
- Recommended hardware
- Q&A

Threat model

- Zero day exploit – 100K USD for Firefox RCE
- Cost per exploited user
- Profit per attack
- Political motivation
- Ransomware
- Password stealing

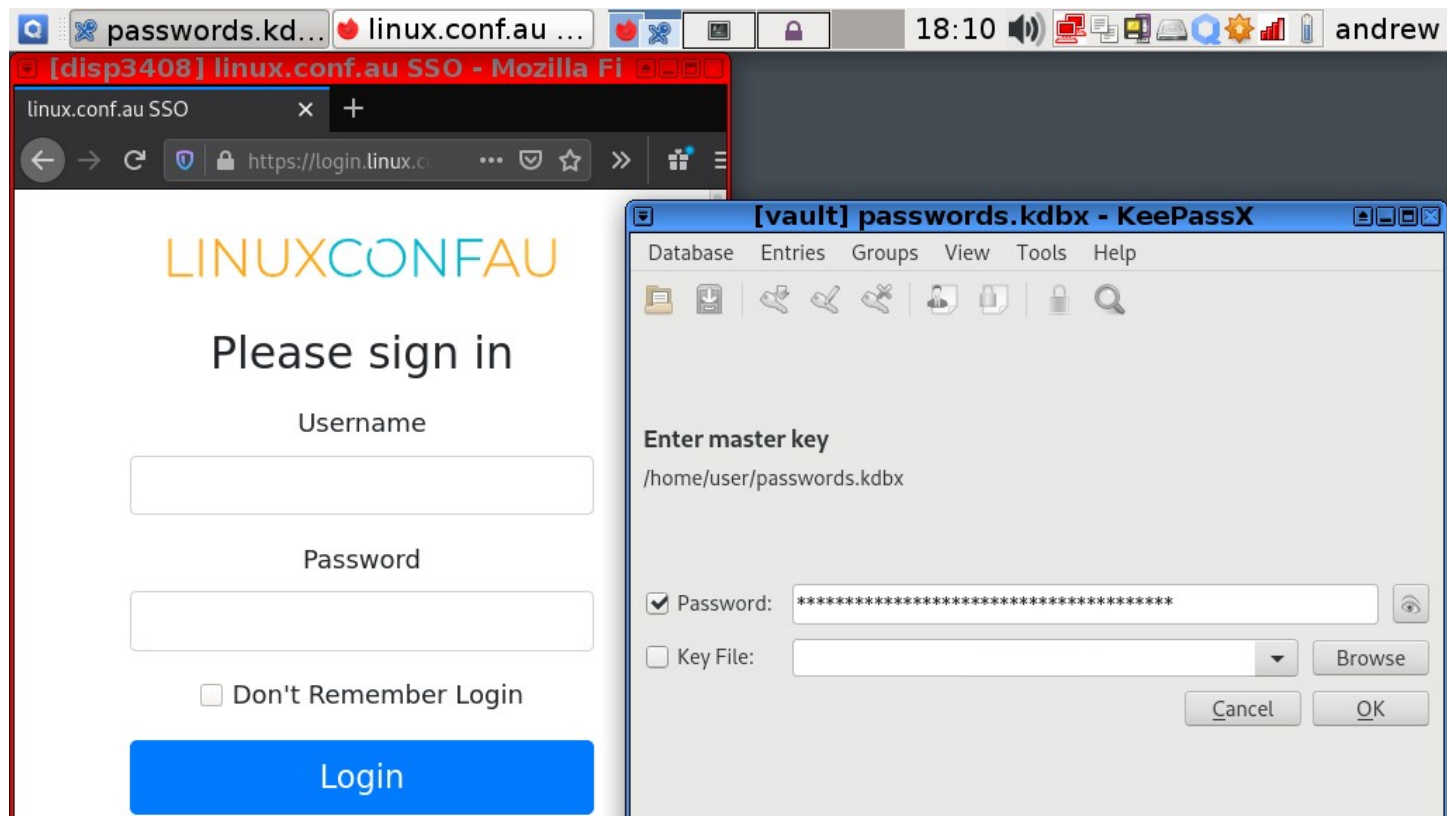
What is Qubes?

- “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
 - “Desktop Cloud”
- Tied together via vchan, virtual networking
- Optional USB devices (proxy), PCIe devices (IOMMU)
- Managed by an internal agent (qrexec) via vchan.

Is it usable?

- Generally yes.

Firefox and a password manager

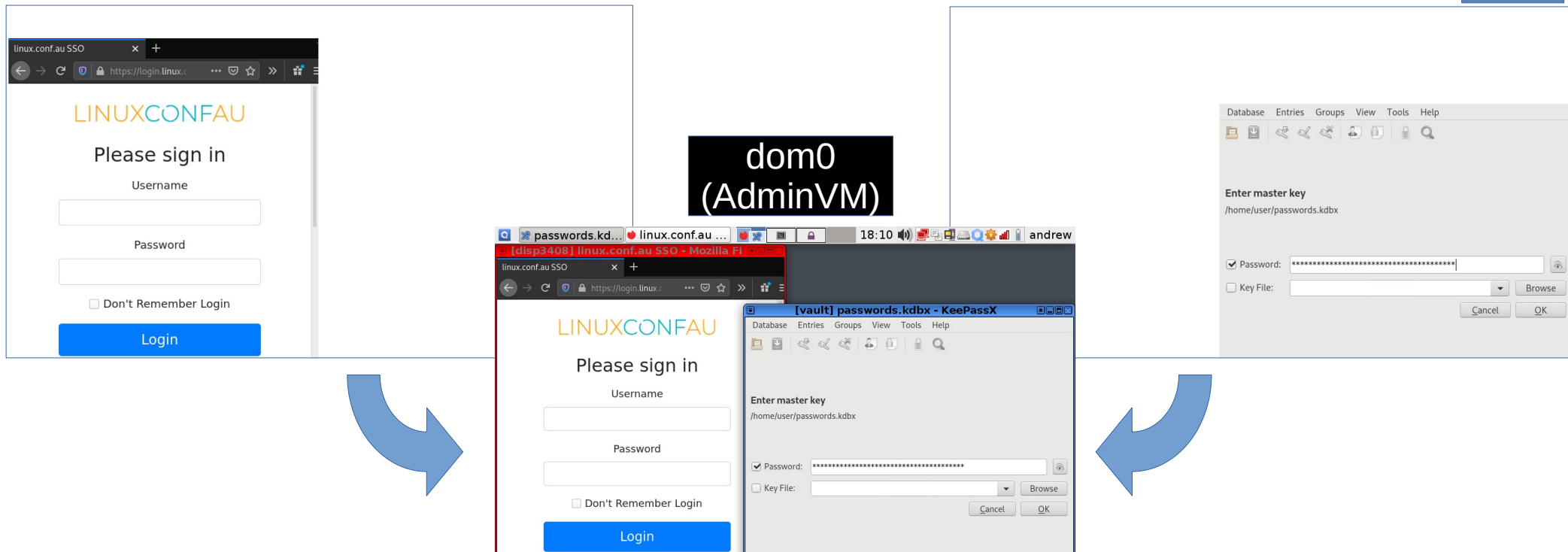


Firefox and a password manager

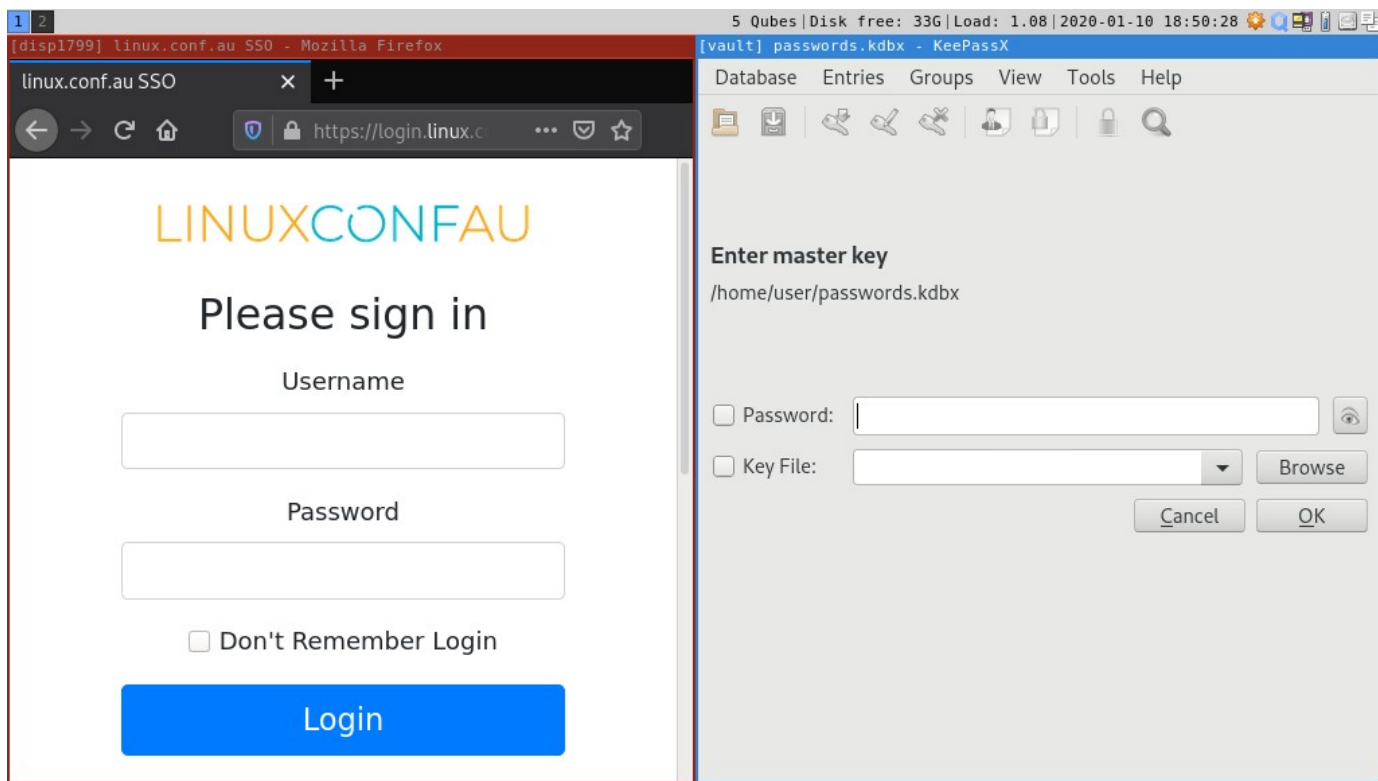
disp3408

vault

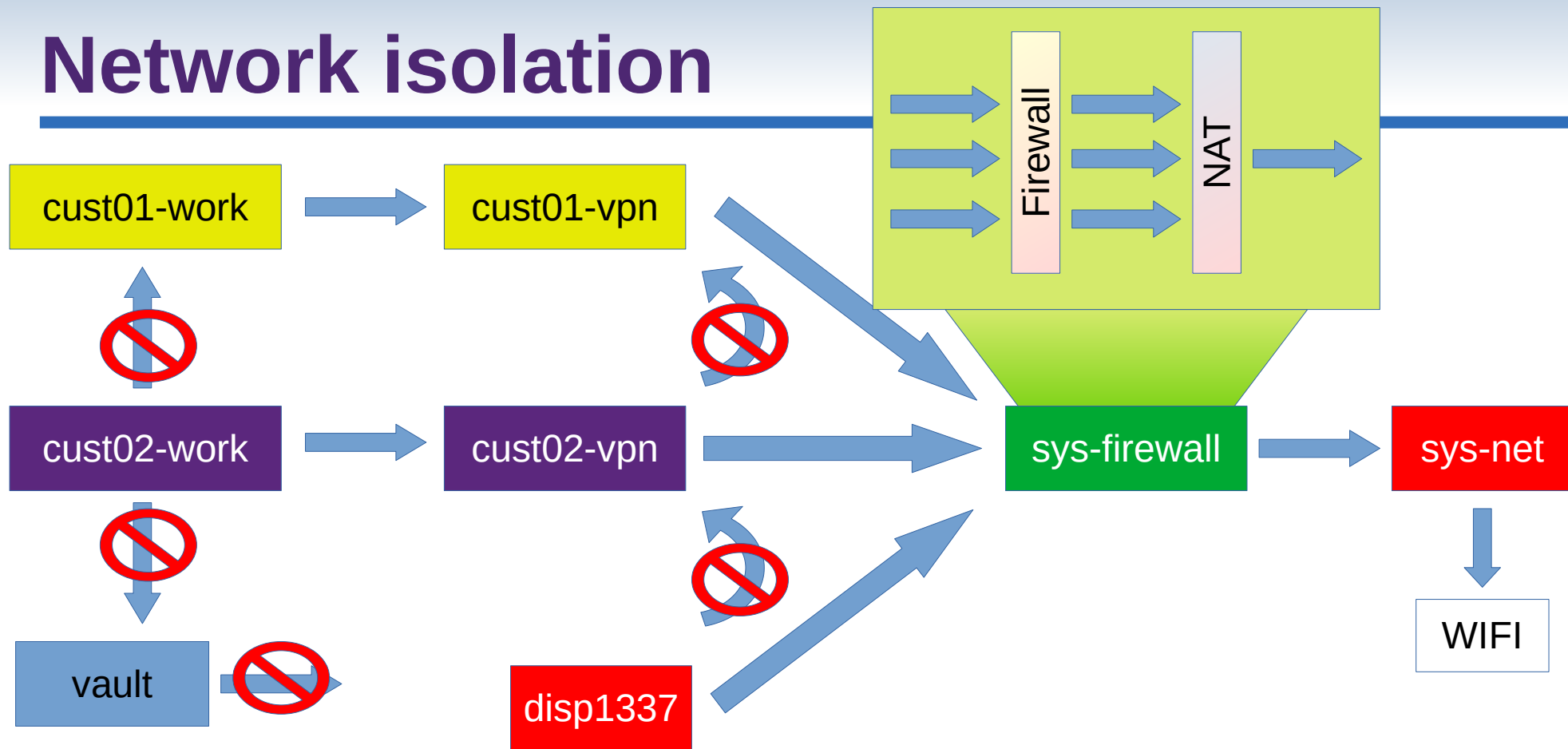
dom0
(AdminVM)



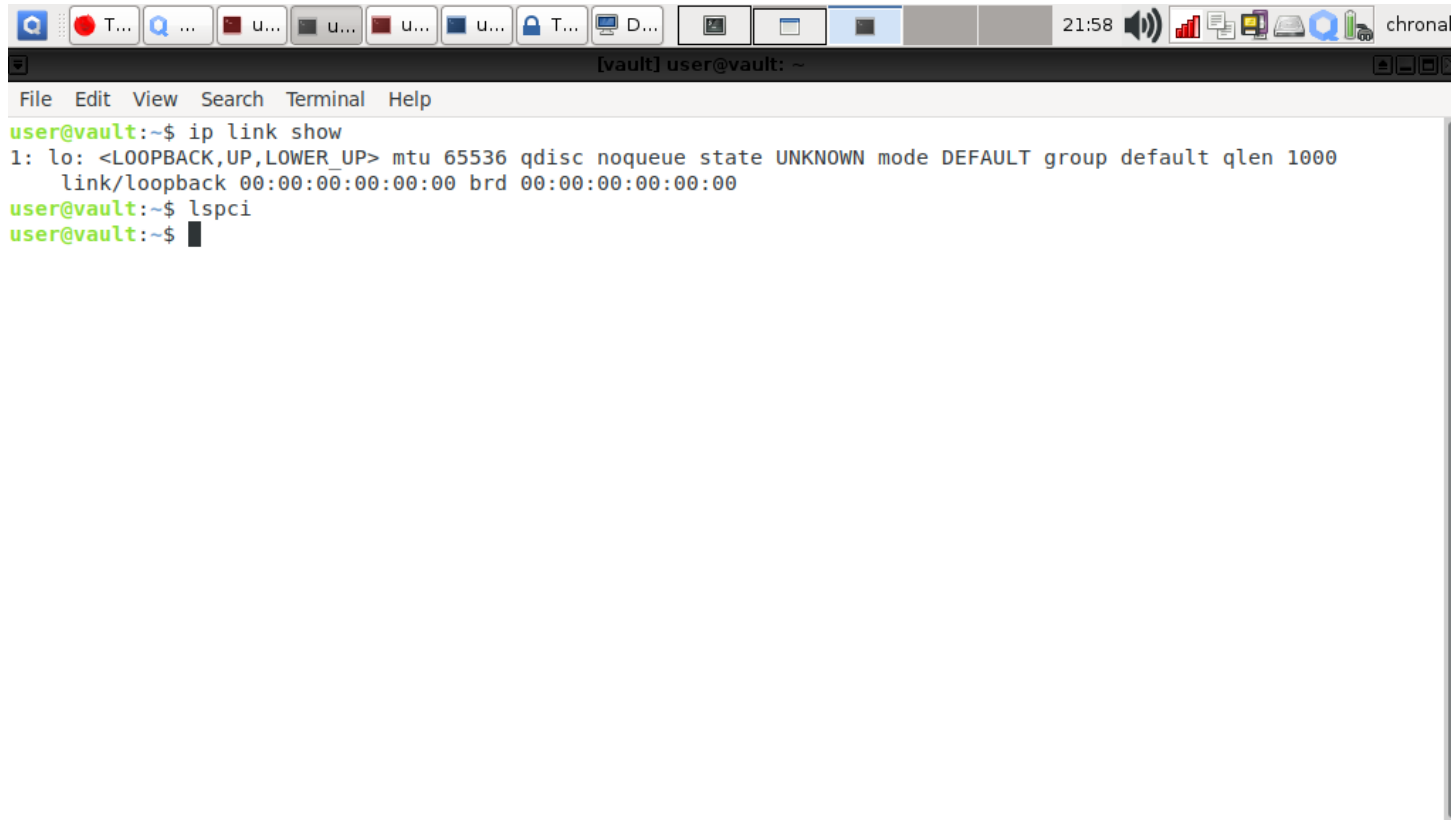
Firefox and a password manager



Network isolation



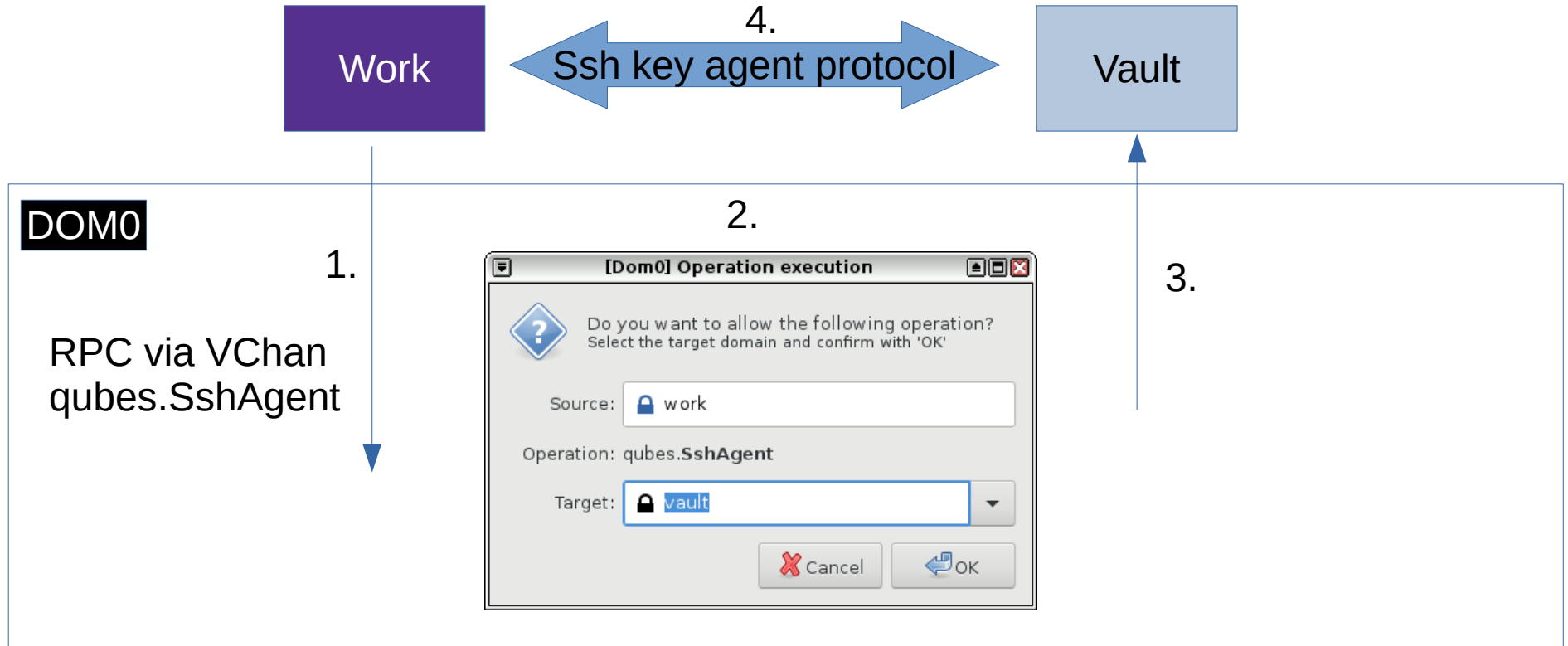
Vault isolation



The screenshot shows a terminal window within a virtual machine. The window title is "[vault] user@vault: ~". The terminal output is as follows:

```
File Edit View Search Terminal Help
user@vault:~$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
   link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
user@vault:~$ lspci
user@vault:~$
```

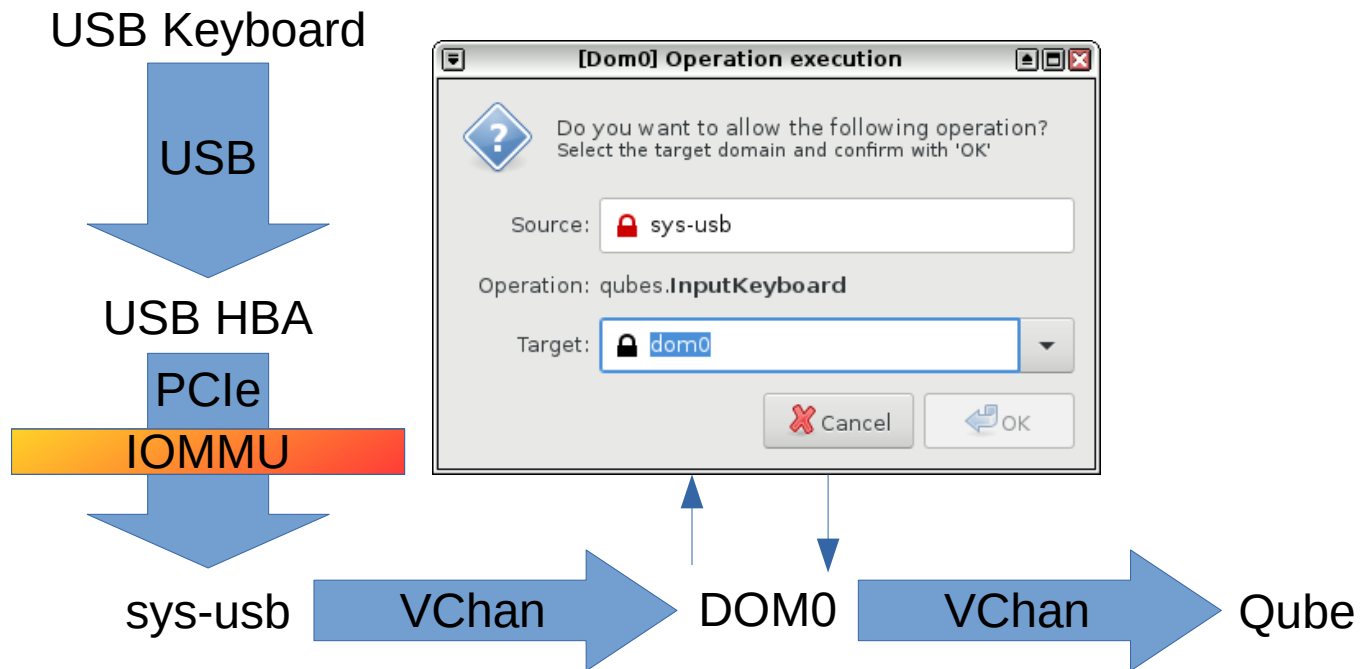
Vault isolation



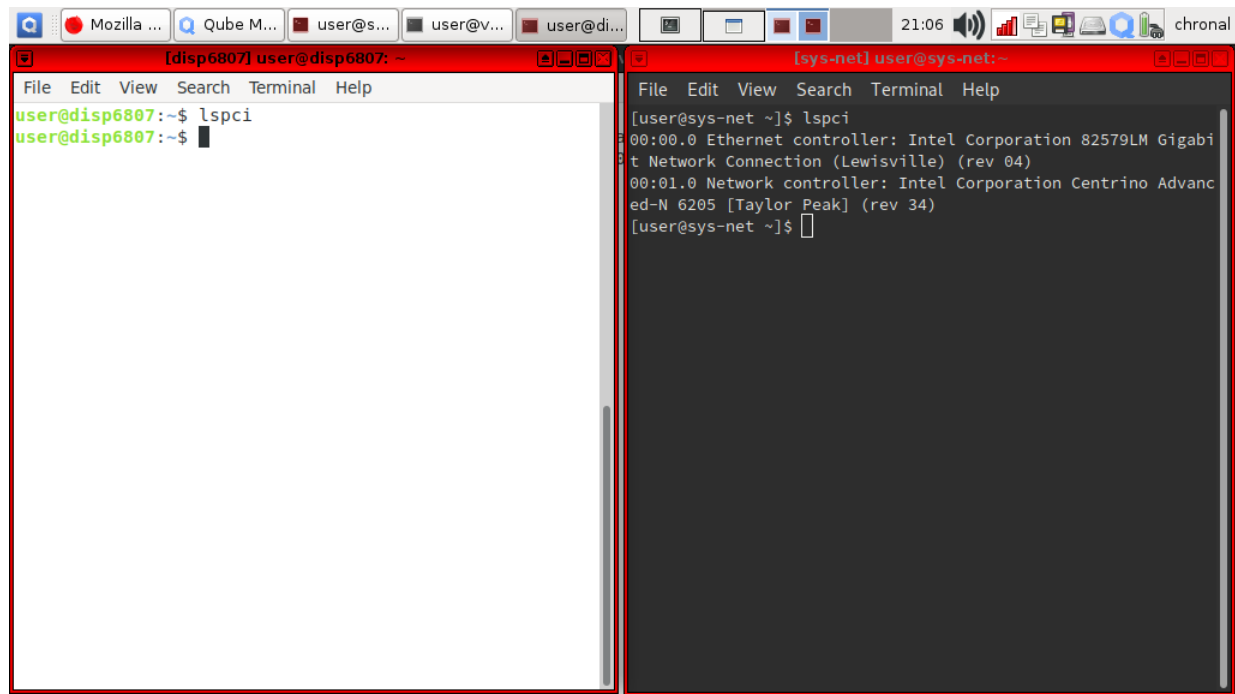
USB isolation

- USB is a lovecraftian nightmare
- A 'USB key' can be a
 - Keyboard
 - Mouse
 - Virtual ethernet device
 - Storage device
 - Pizza oven

USB isolation



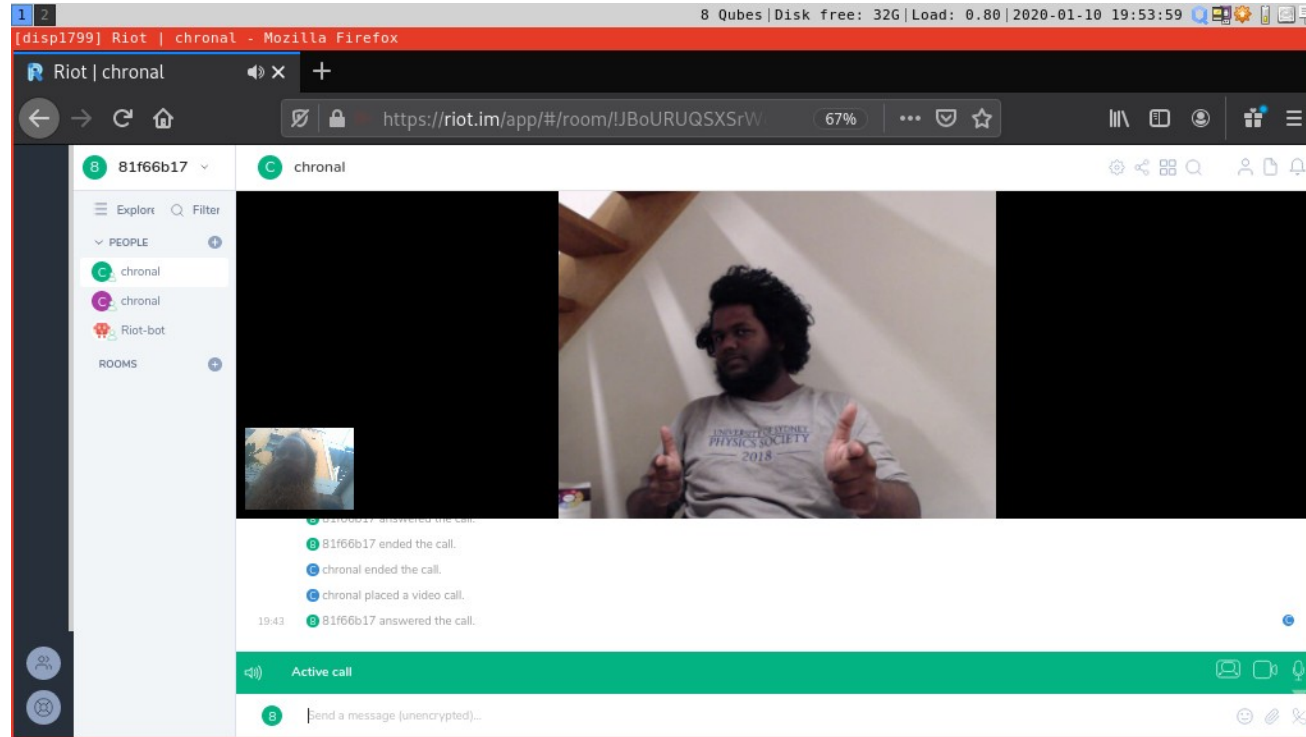
Hardware isolation



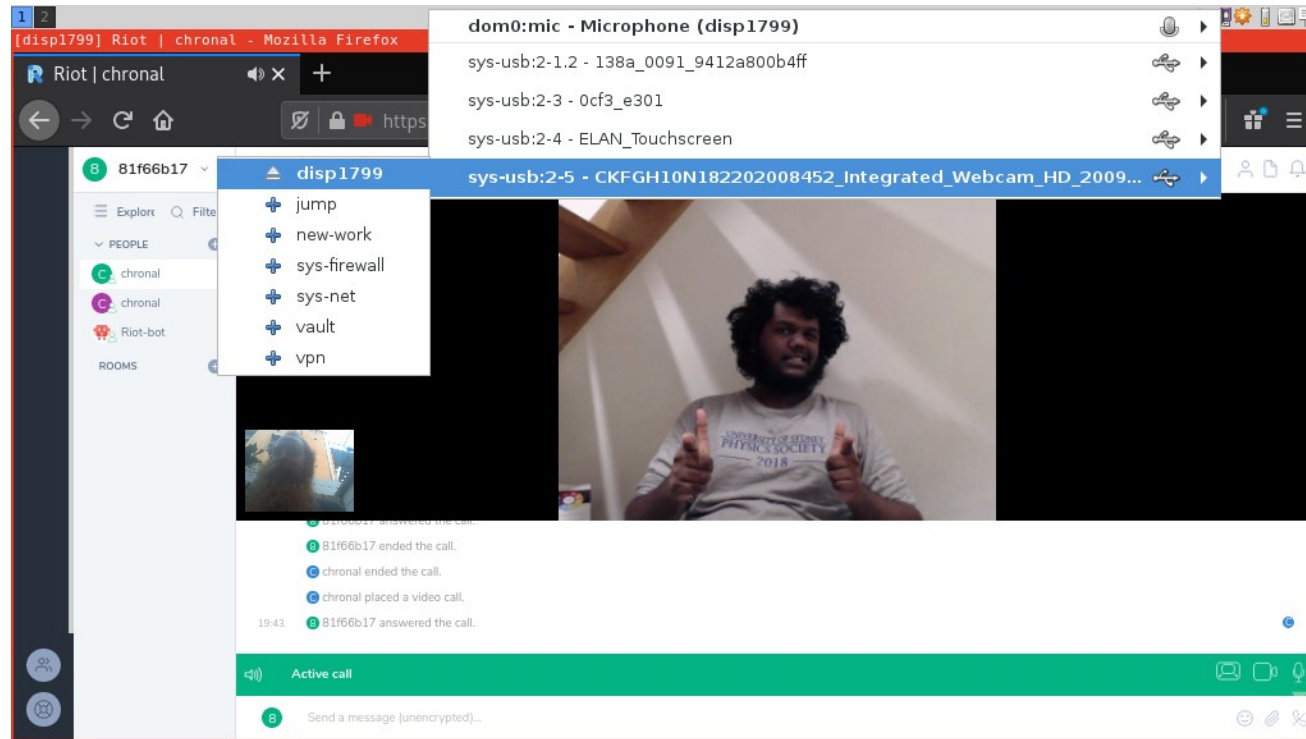
```
[disp6807] user@disp6807: ~  
File Edit View Search Terminal Help  
user@disp6807:~$ lspci  
user@disp6807:~$
```

```
[sys-net] user@sys-net: ~  
File Edit View Search Terminal Help  
[user@sys-net ~]$ lspci  
00:00.0 Ethernet controller: Intel Corporation 82579LM Gigabit Network Connection (Lewisville) (rev 04)  
00:01.0 Network controller: Intel Corporation Centrino Advanced-N 6205 [Taylor Peak] (rev 34)  
[user@sys-net ~]$
```

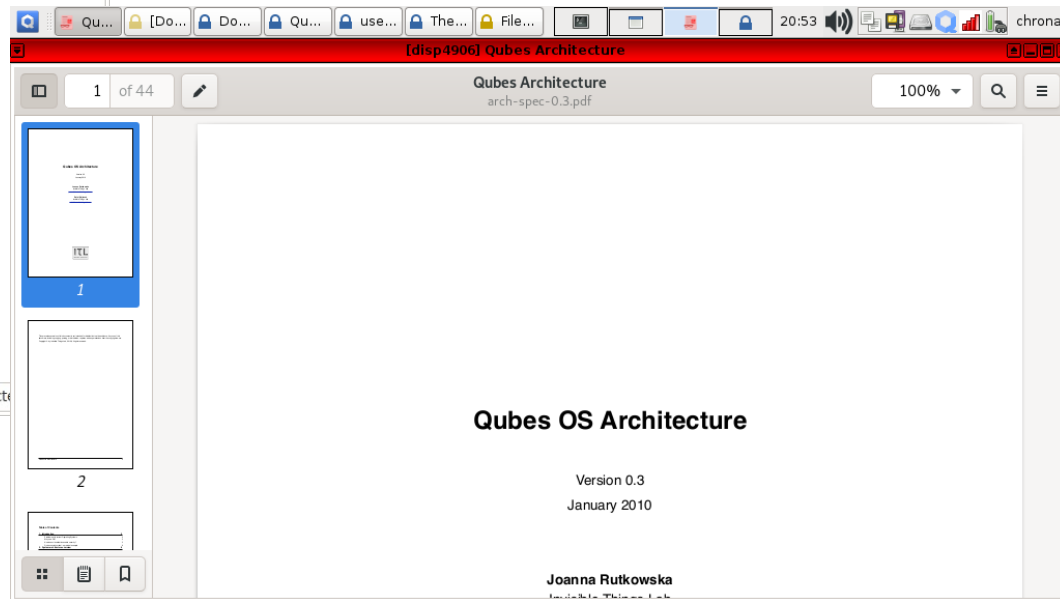
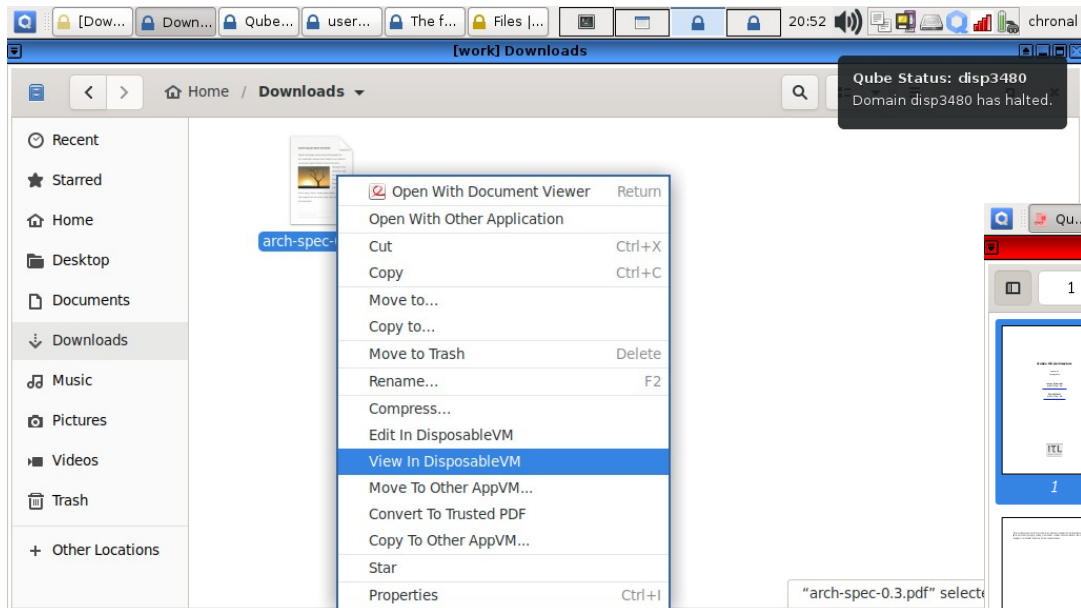
Qubes video call



Qubes video call



Disposable qube



Convert to trusted PDF

- Built on top of disposable qubes
- Did you know that printers update via printable documents?
Does your printer have an internet connection?

Qube Manager

[dom0] Qube Manager

System Qube View About

Search:

		Name	State	Template	NetVM	Disk usage	Internal	IP
		dom0	●	AdminVM	n/a	n/a		n/a
		personal-work	●	fedora-30	default (sys-firewall)	35773.44 MiB		10.137.0.17
		sys-firewall	●	fedora-30	sys-net	104.24 MiB		10.137.0.6
		sys-net	●	fedora-30	n/a	137.01 MiB		10.137.0.5
		sys-usb	●	fedora-30	n/a	172.85 MiB		10.137.0.15
		vault	●	fedora-30	n/a	105.68 MiB		
		anon-whonix		whonix-ws-15	sys-whonix	0.0 MiB		10.137.0.10
		deb-dvm		debian-10	default (sys-firewall)	145.82 MiB		10.137.0.20
		debian-10		TemplateVM	default (n/a)	8019.35 MiB		
		default-mgmt-dvm		fedora-30	n/a	0.0 MiB	Yes	

Recommended Hardware

- Intel integrated graphics best
- AMD/Nvidia with good OSS drivers will do
- Intel CPU with ME cleaner best
- Recent AMD cpus - Check kernel support.
- 8gb okay, 16gb good, 32gb overkill for most use cases.
- Coreboot/heads firmware not required but improves security
- Purism Librem 13/15 best, Insurgo PrivacyBeast X230/NitroPad good
- Intel NUC/Dell XPS/Lenovo Thinkpad etc. ok.
- <https://www.qubes-os.org/hcl/>

Help wanted

- Windows drivers!
- Python/Bash help needed!
- Open source project!
- <https://github.com/QubesOS/qubes-issues>
- <https://www.qubes-os.org/donate/>

More info

- BOF on Thursday at Lunch, room 7
- “The future of the desktop is on hypervisor powered containers” talk tomorrow
- <https://www.qubes-os.org/>
- <https://www.qubes-os.org/support/>
- <https://wiki.qubes.rocks>

orionVMTM



Qubes logo is licensed under CC BY-SA 4.0
<https://www.qubes-os.org/doc/style-guide/>

Both "OrionVM" and the OrionVM logo are trademarks, all rights reserved

All included Screenshots and diagrams are CC BY SA 4.0

Slide deck as a whole is CC BY ND 4.0

Thanks!
Any questions?

[Sysadmin Miniconf at Linux.conf.au](https://www.linux.conf.au/)



Slides: <https://github.com/orionvm/LCA2020>