The future of the desktop is on hypervisor powered containers

Containers Miniconf at linux.conf.au 2020

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 –
  - A white label cloud computing provider

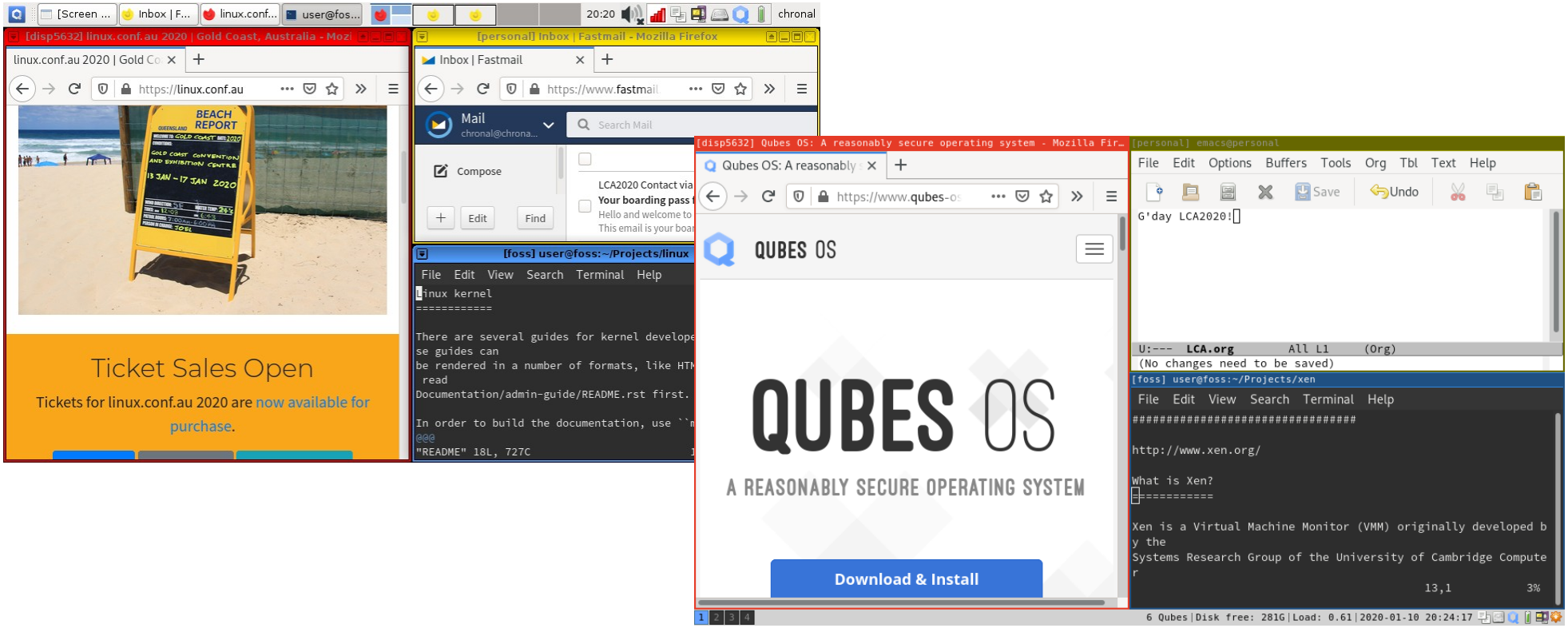
Agenda

- What is Qubes?
- What makes a usable/secure desktop?
- How does it compare to containers?
- Q&A

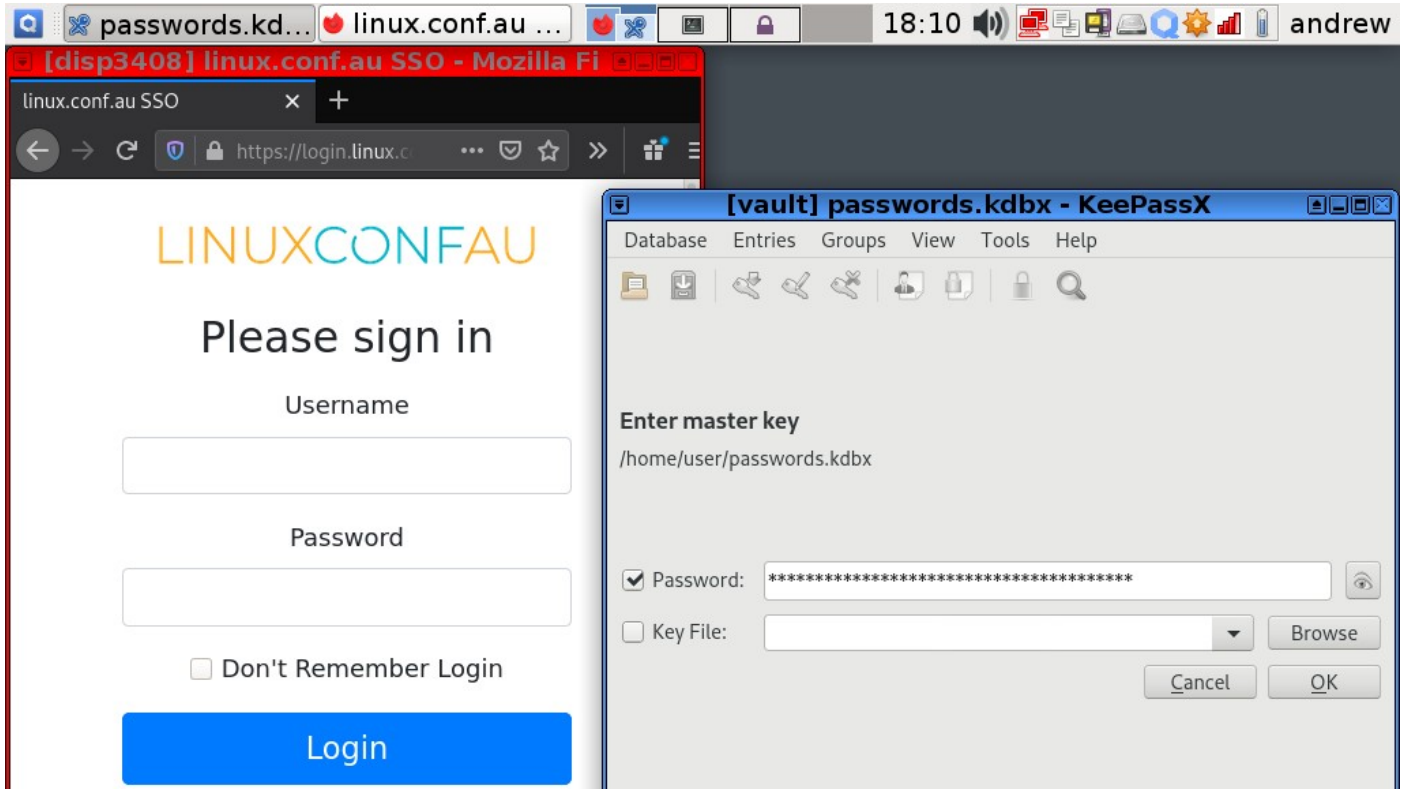
What is Qubes?

- “A reasonably secure operating System” focusing on security through isolation
- Consists of multiple Qubes and an isolated management VM
  - A Qube is a Xen domain running an OS (Linux/FreeBsd/etc)
- Tied together via vchan, virtual networking
- Optional USB devices (proxy), PCI-E devices (IOMMU)
- Managed by an internal agent (qrexec) via vchan.

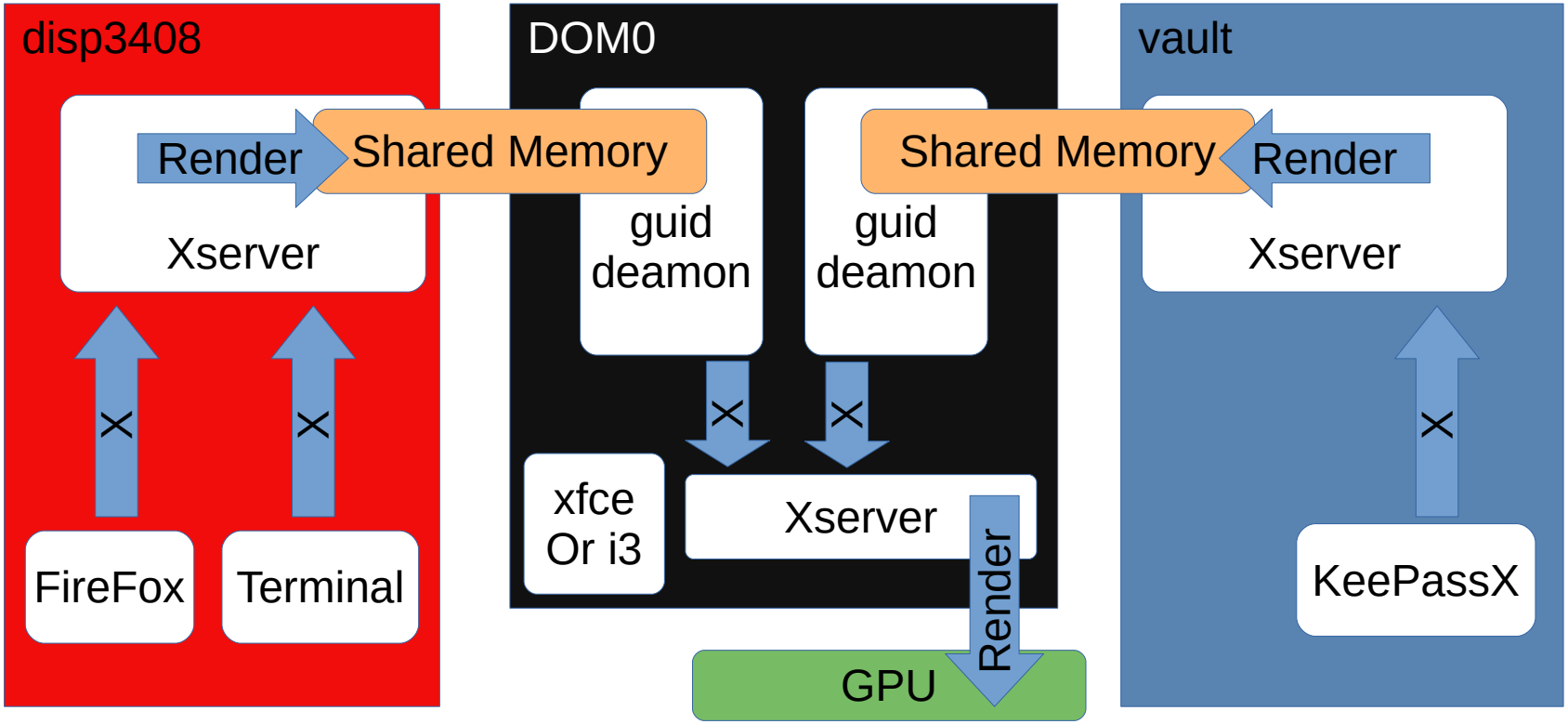
So what is Qubes?



GUI Isolation



Qubes GUI System

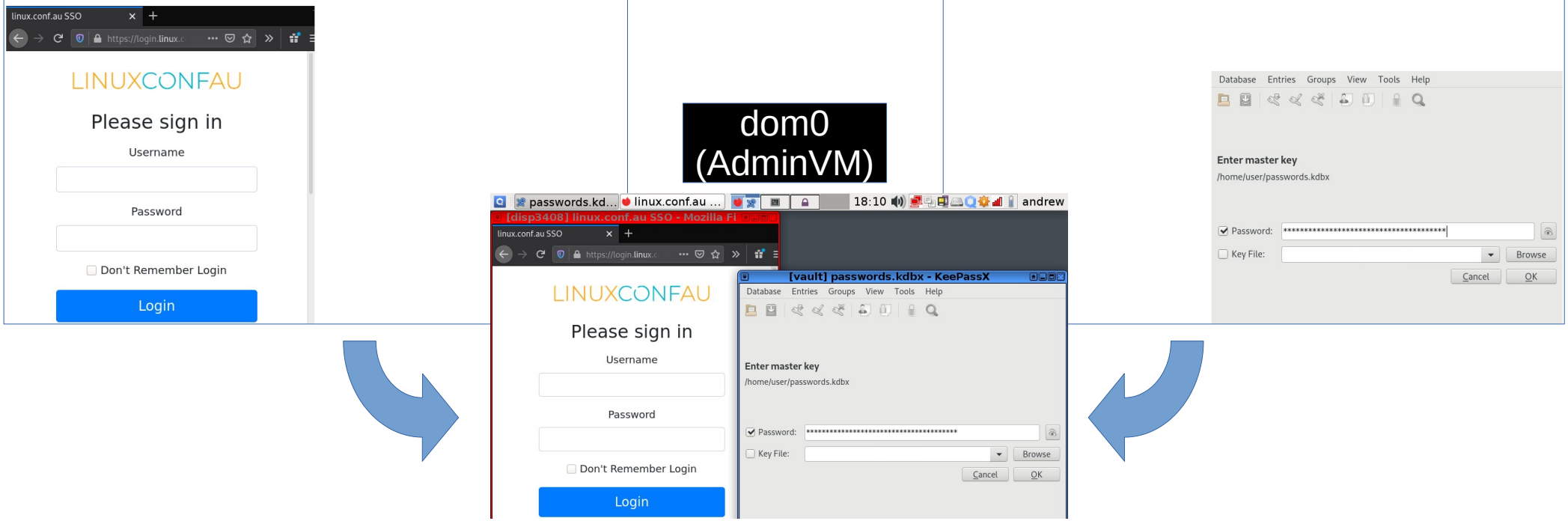


Firefox and a password manager

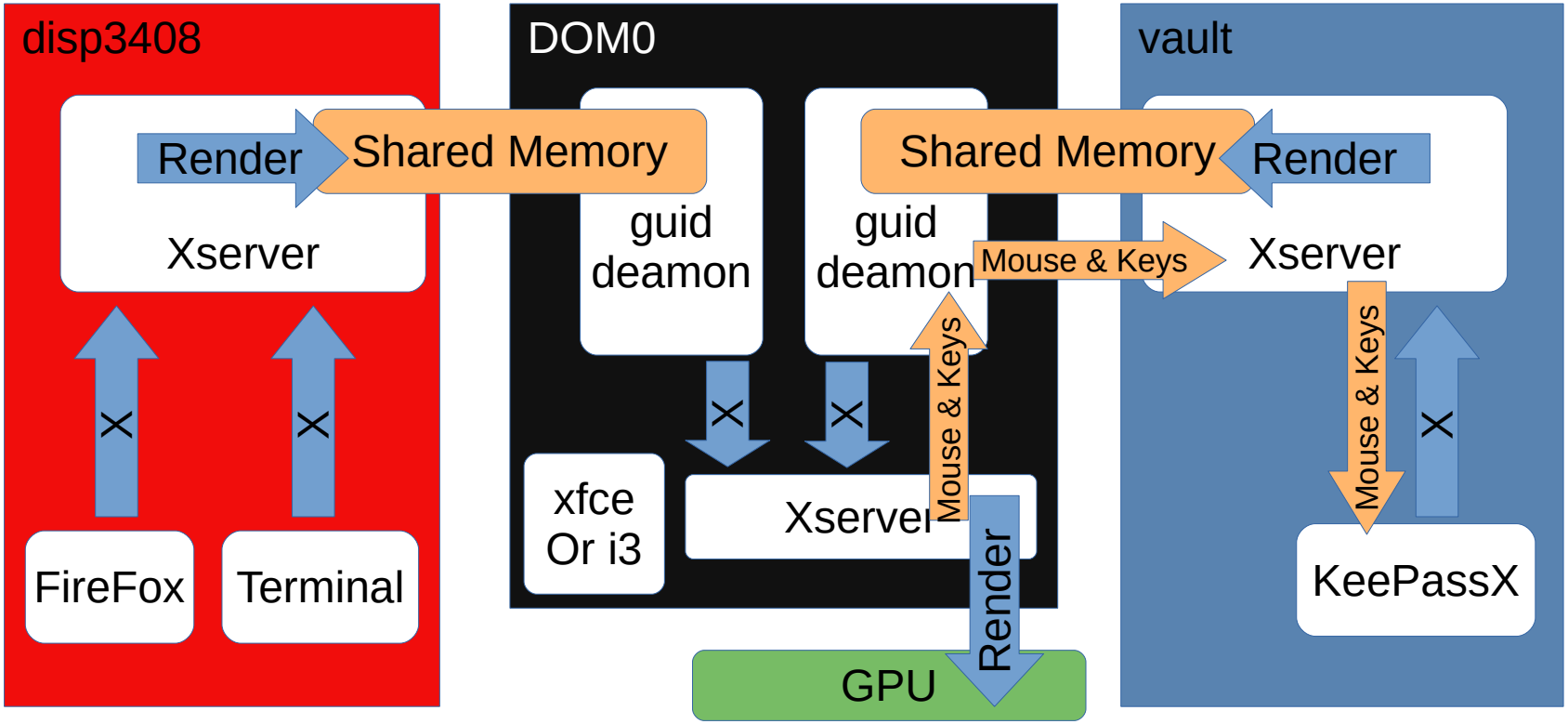
disp3408

vault

dom0 (AdminVM)



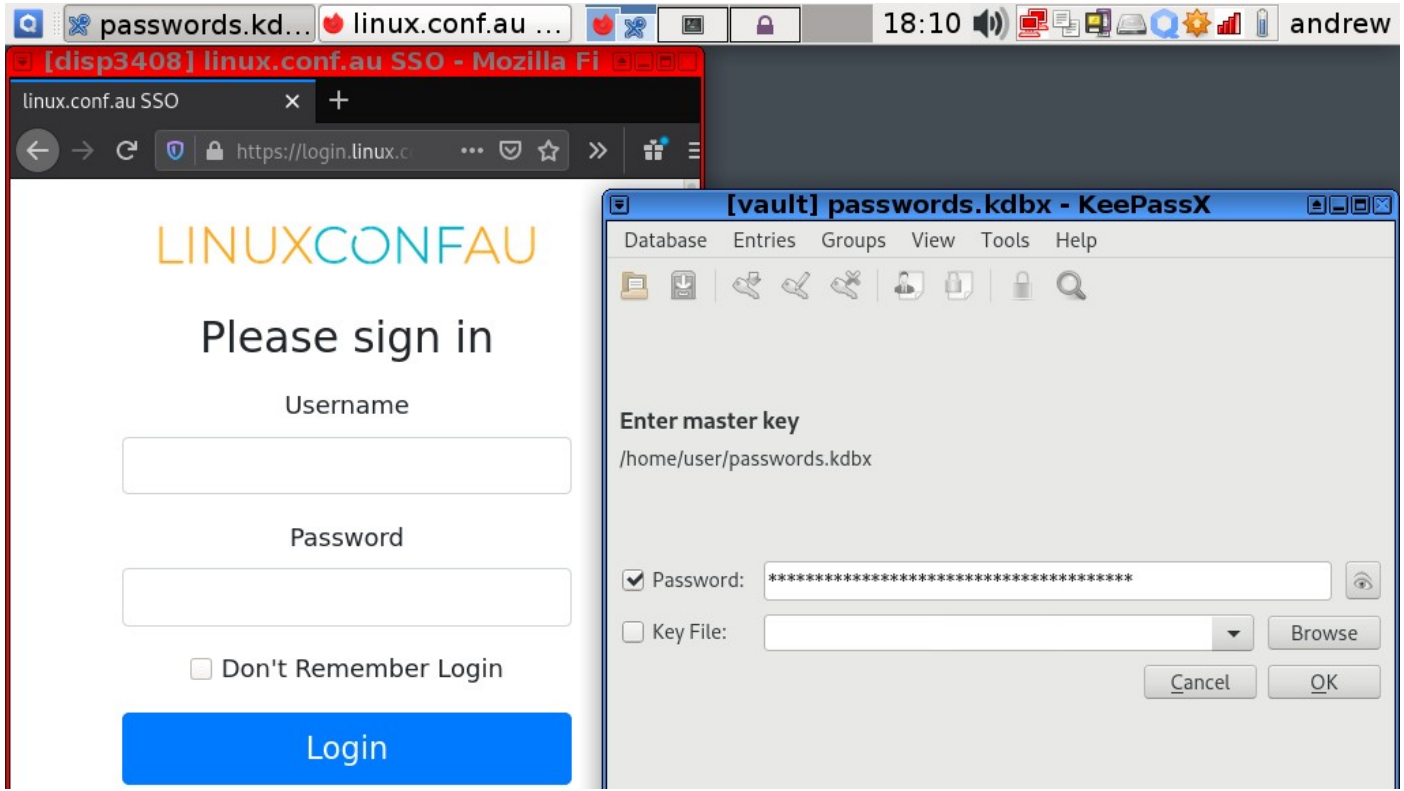
Qubes GUI System



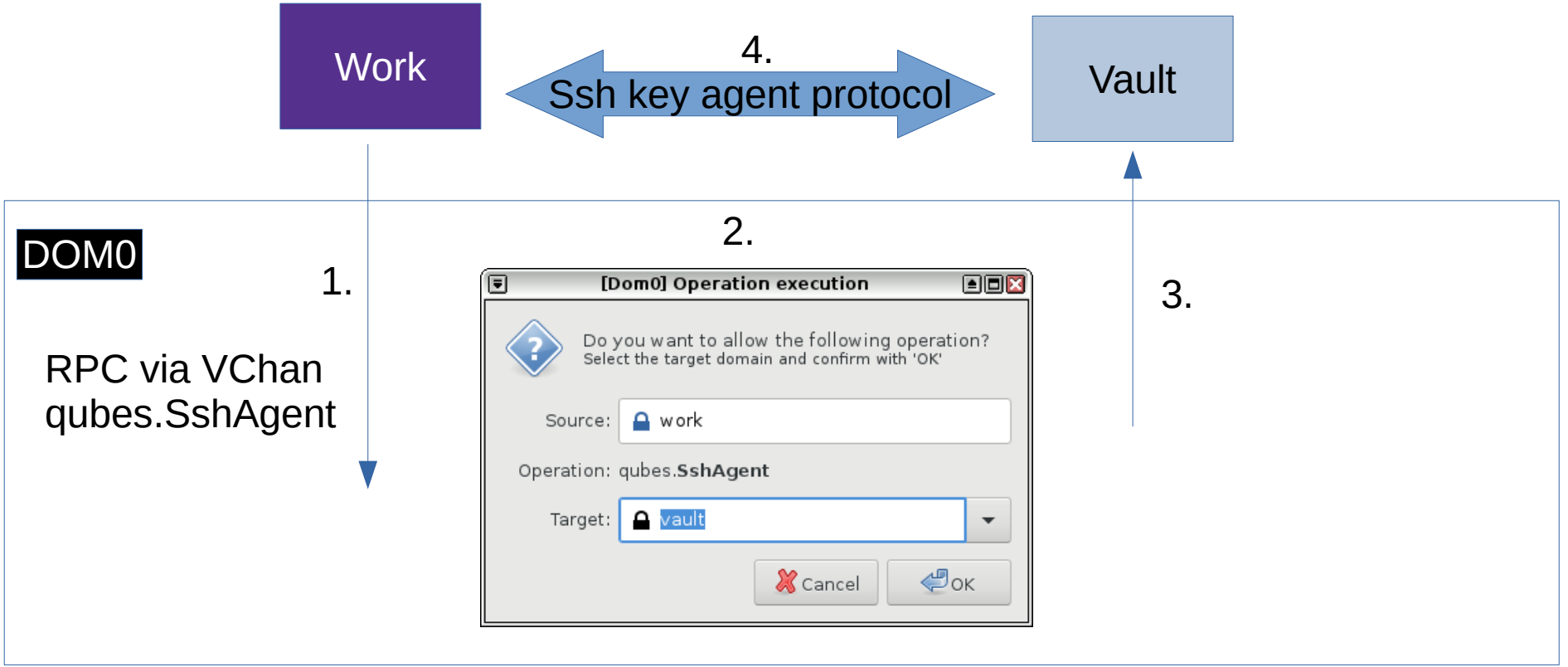
Vchan/Qubes RPC

- Vchan is a ‘peer to peer pipe between Qubes’
- RPC for Access control

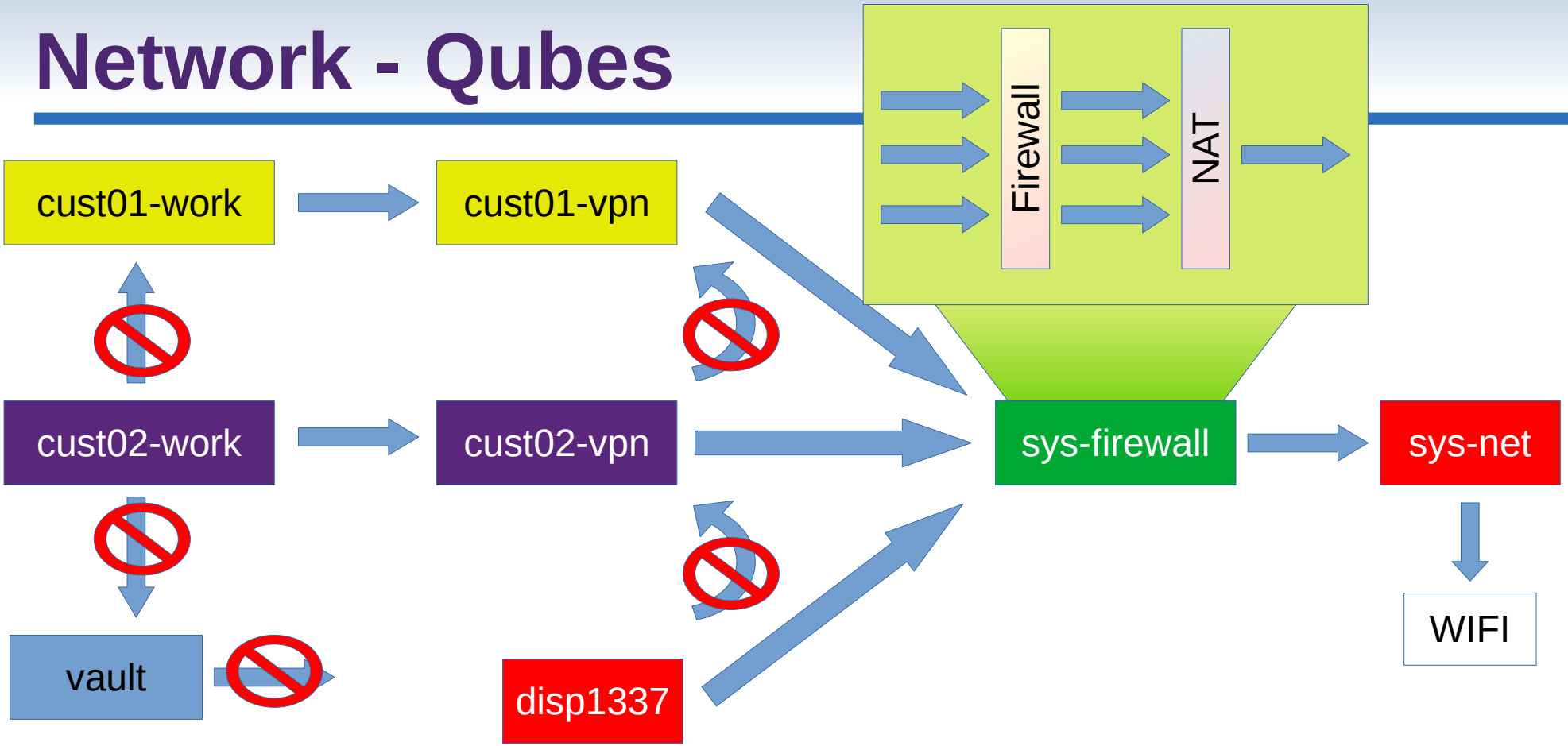
Split clipboards



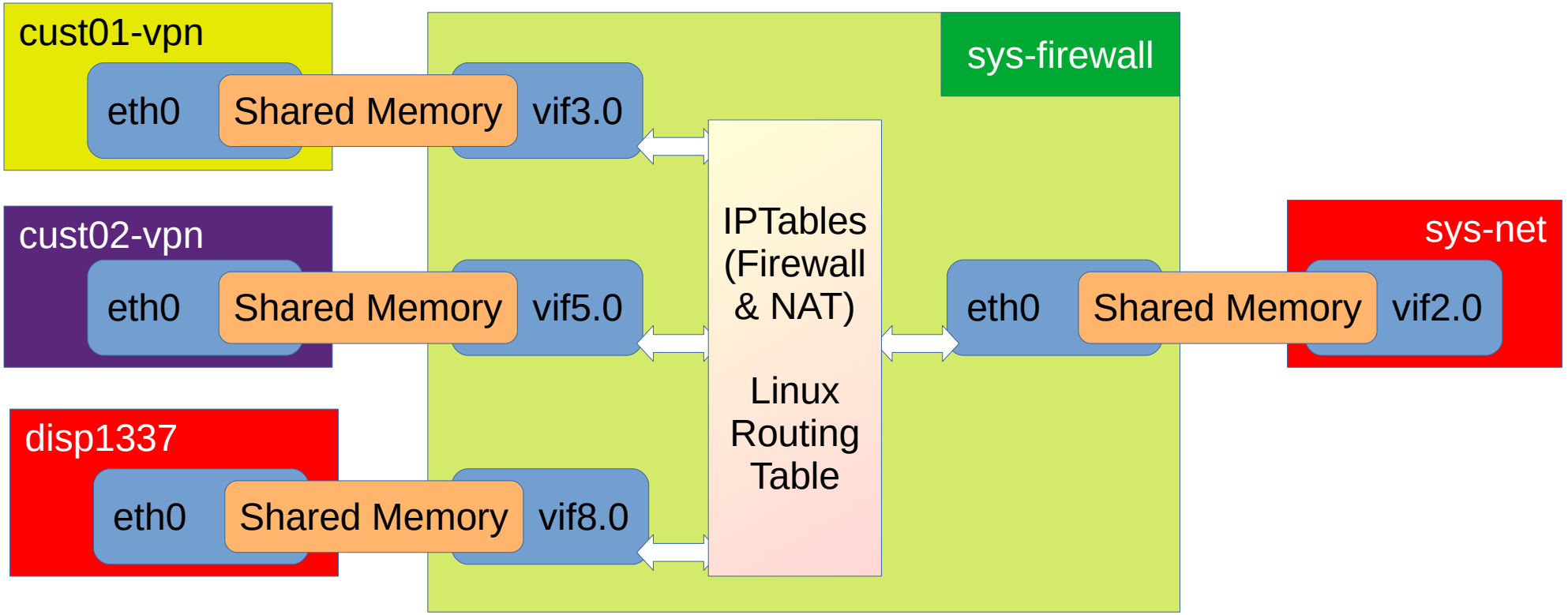
Vault isolation



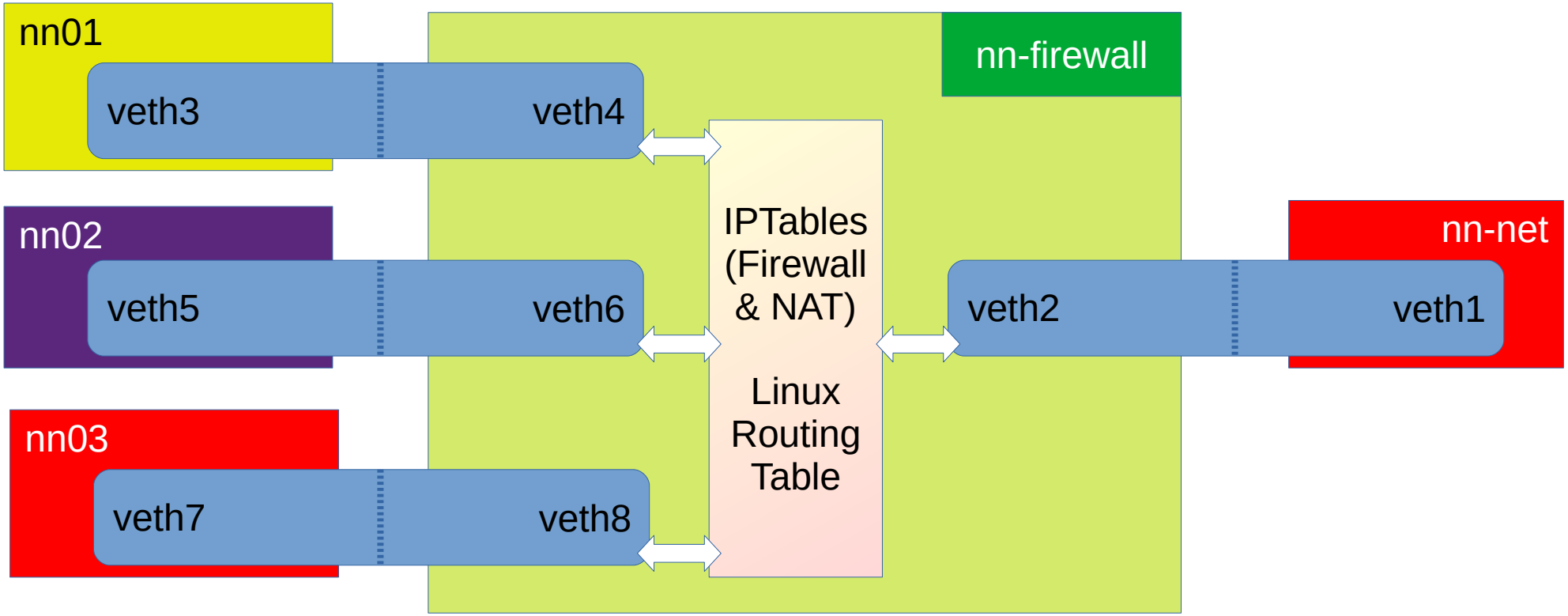
Network - Qubes



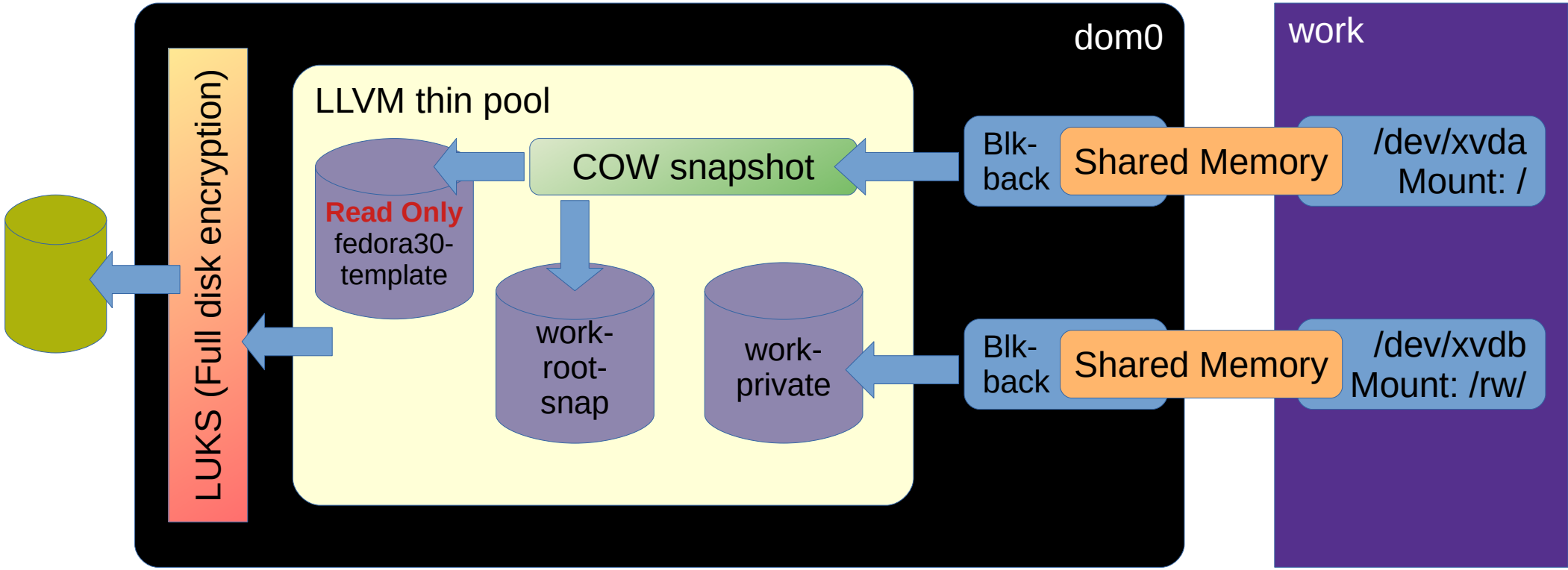
Network - Qubes



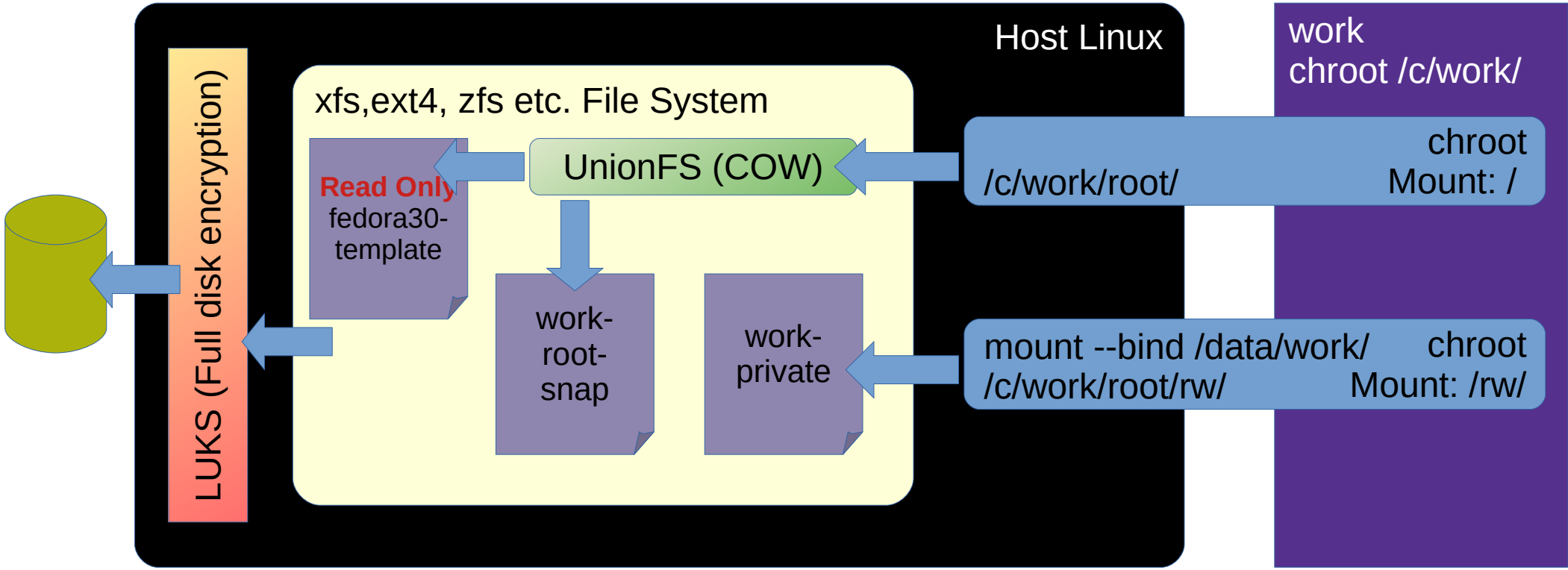
Network - Containers



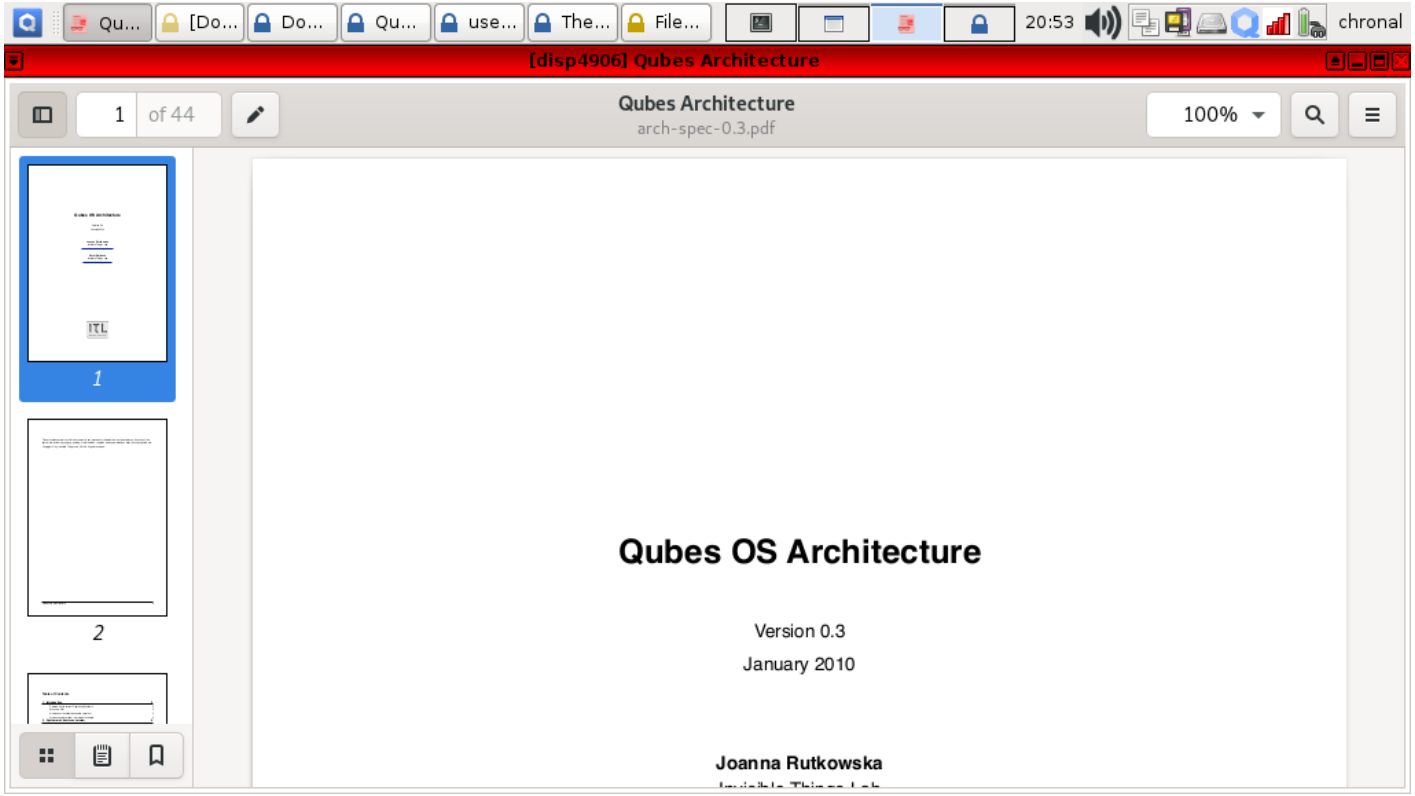
Qube storage



Container storage



Disposable Qube



Qubes Memory

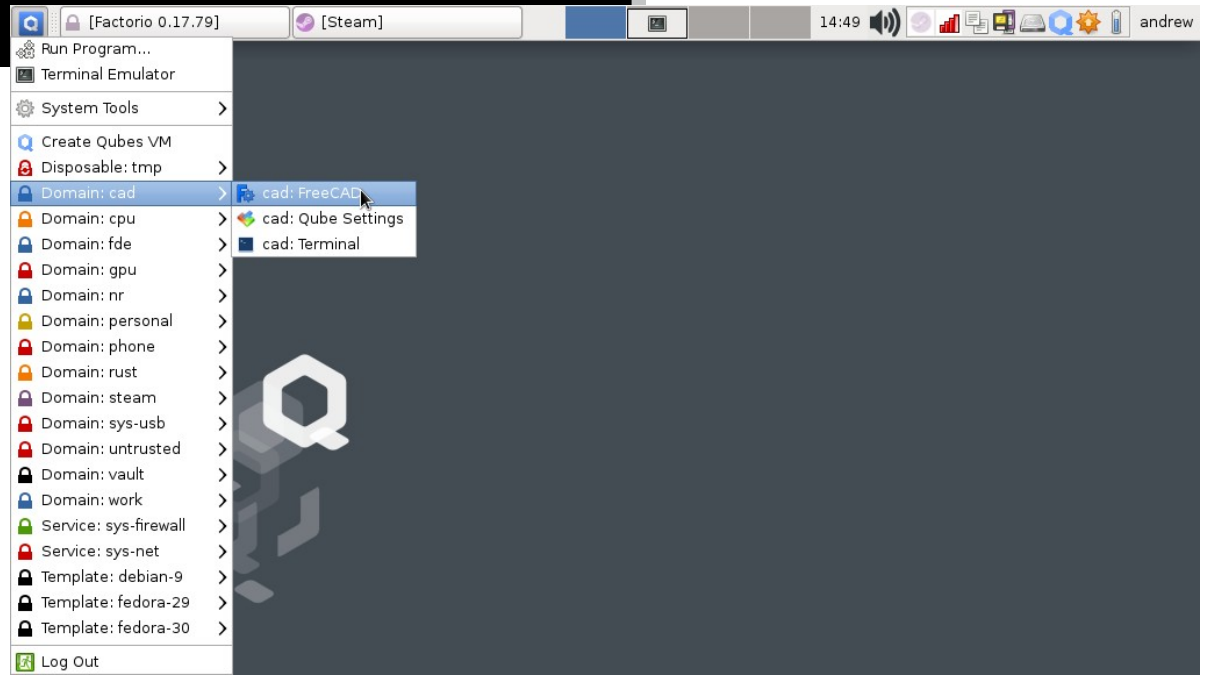
- Each qube has dedicated resizeble memory
- Memory rarely moves between qubes
  - Memory loadbalancing deamon
- Currently has memory balancing inefficiencies
- Communication via (small amounts of) shared memory

Containers Memory

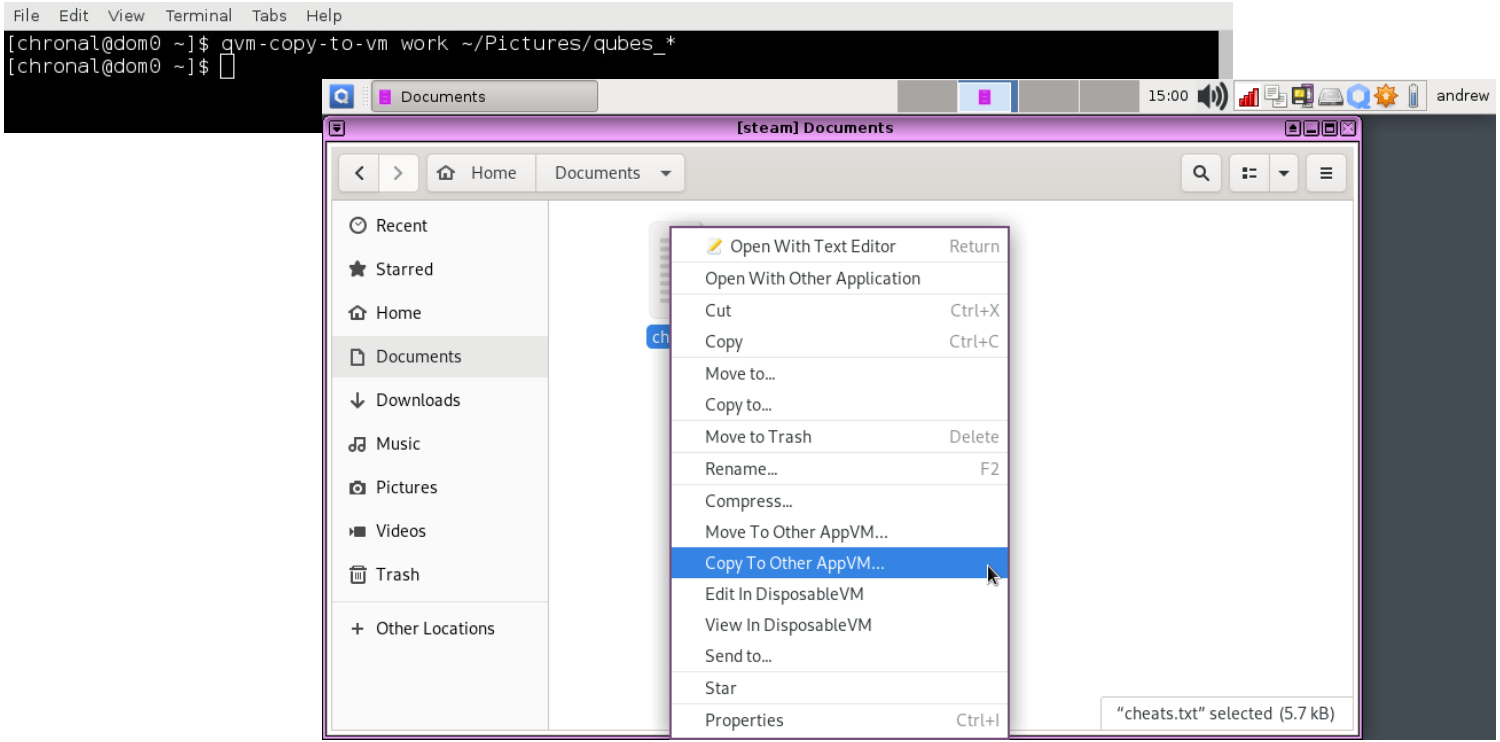
- Shared memory pool between processes
- Cgroups for ‘limits’
- Memory rapidly circulated between of processes based on current demand and cgroup limits
- Far more memory efficient, however is more susceptible to side channel attacks

qvm-run

```
File  Edit  View  Terminal  Tabs  Help
[chronal@dom0 ~]$ qvm-run -u root --pass-io work 'whoami'
root
[chronal@dom0 ~]$ qvm-run -u root --pass-io work 'hostname'
work
[chronal@dom0 ~]$
```



qvm-copy-to-vm



Qubes made of containers?

- Containers isolate software
- Virtual Machines isolate both software & hardware
  - Protects software from malicious hardware
  - Enforces strict boundries
- SubgraphOS

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/

Our Wish list: Container integration

- Repository style functionality (push/pull/run)
- Git/dockerfiles generating templates
- Stackable templates with overlayfs

Our Wish list: SRIOV GPUs

- Intel GTV-G
- Nvidia/AMD equivalents
- ‘Can it run Crysis’

Our Wish list: Qubes cloud

- Secure zero knowledge backup/restore
- ‘Enterprise support’ - Paid version
- Qubes OEM

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
- “Using a cloud to manage a cloud” talk yesterday
- https://www.qubes-os.org/
- https://www.qubes-os.org/support/
- https://wiki.qubes.rocks

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?

Containers Miniconf at Linux.conf.au

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