QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

The Operating System That Can Protect You Even If You Get Hacked

Hi, I’m Micah Lee, security engineer and journalist at The Intercept

🐦 @micahflee

🔑 927F419D7EC82C2F149C1BD1403C2657CD994F73

How is Qubes different than other OSes?

- Everything runs in **Virtual Machines** called “qubes”, powered by Xen
- VMs are **isolated** from each other in **security domains**
- The **admin domain** is called **dom0**, runs the window manager
- Some VMs are **disposable**
- Some VMs are **vaults**
- Qubes **networking** can do amazing things
- VMs **need permission to access hardware** (like your mic)
- Protects against hardware attacks like **malicious USB devices**
- Qubes is a **single user**, **desktop** operating system with about 30k users (it had about 5k users in 2015)

Types of VMs in Qubes

TemplateVMs

- fedora-28
- debian-9
- whonix-gw
- whonix-ws

AppVMs

- Shared root filesystem with the TemplateVM
- Separate private storage for /home
- Install or update software in the TemplateVM

Standalone VMs

- Like AppVMs, but with persistent root partition
- Can be based on TemplateVMs or installed from ISOs
- Great for VMs where you install lots of unrelated packages like software development, Capture the Flag
- Windows

Window decorations, working with files, and copying and pasting

DisposableVMs for web browsing, viewing documents, and making Trusted PDFs

Storing secrets in “vaults”, or network-less VMs

Open Thunderbird attachments in DispVMs, and store your secret keys in vaults

Porcupine

a web browser … sort of

https://github.com/micahflee/porcupine

As many Signal Desktops as you want

How to Use Signal Without Giving Out Your Phone Number
https://interc.pt/2xEcDY3

Windows®

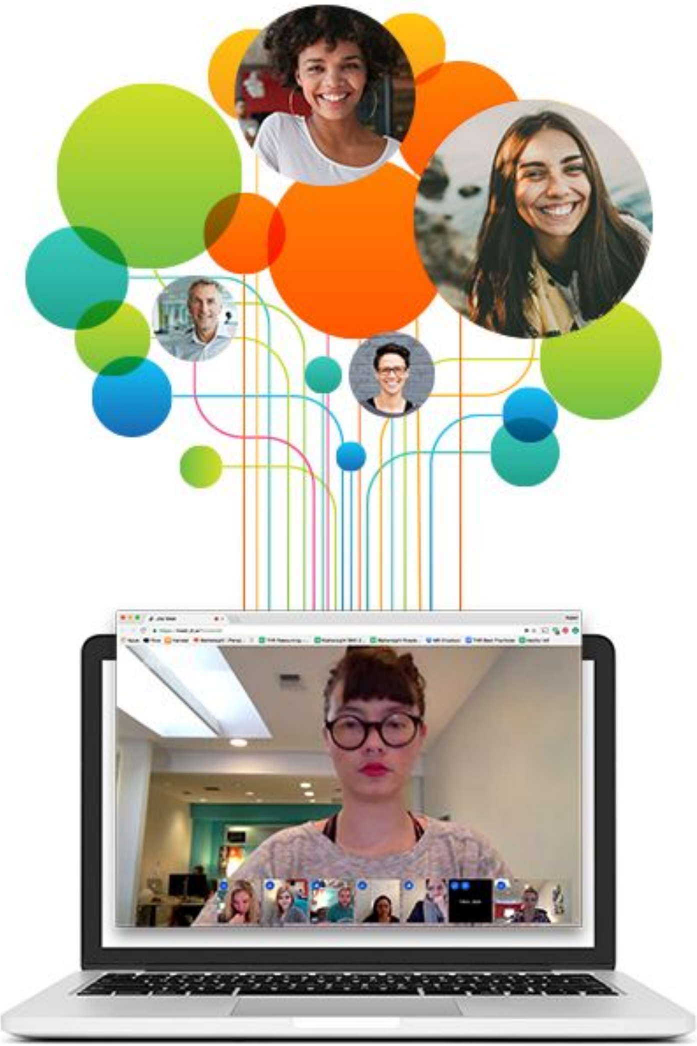
KALI

USB Passthrough

- sys-usb has access to USB controller PCI devices (**not dom0**)
- sys-usb is **untrusted**
- It can **passthrough** individual **USB devices** or **block devices** to VMs
- You **must manually attach** USB devices to VMs, or they can't access anything
- Microphone and SD card reader are attached to dom0
- See what USB devices are attached with `lsusb`

Password managers and Yubikeys for U2F

(use them as PGP smart cards the same way)



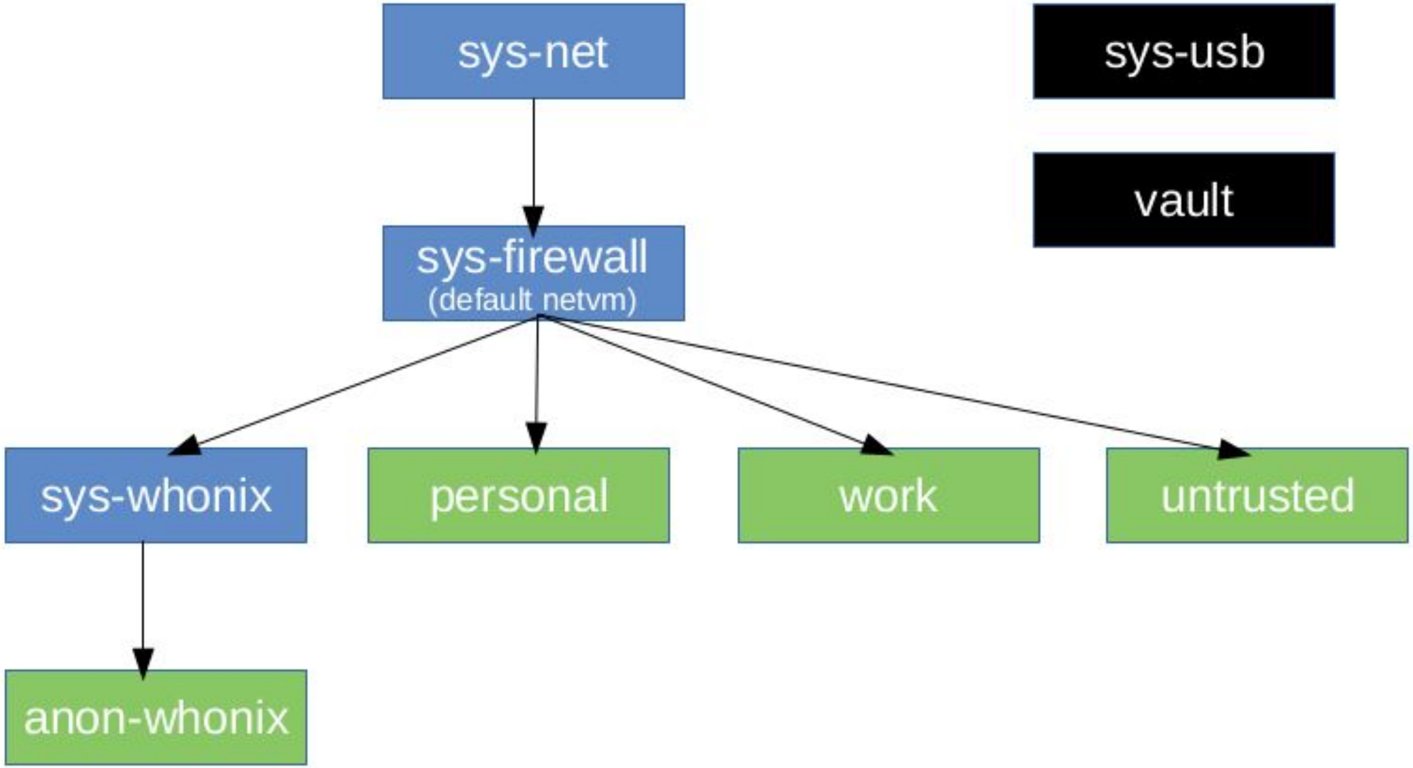
Video conferencing with Jitsi Meet

Other USB devices, wifi hacking using Kali

USB keyboards: It’s complicated

Malicious USB devices, like
USB Rubber Duckies

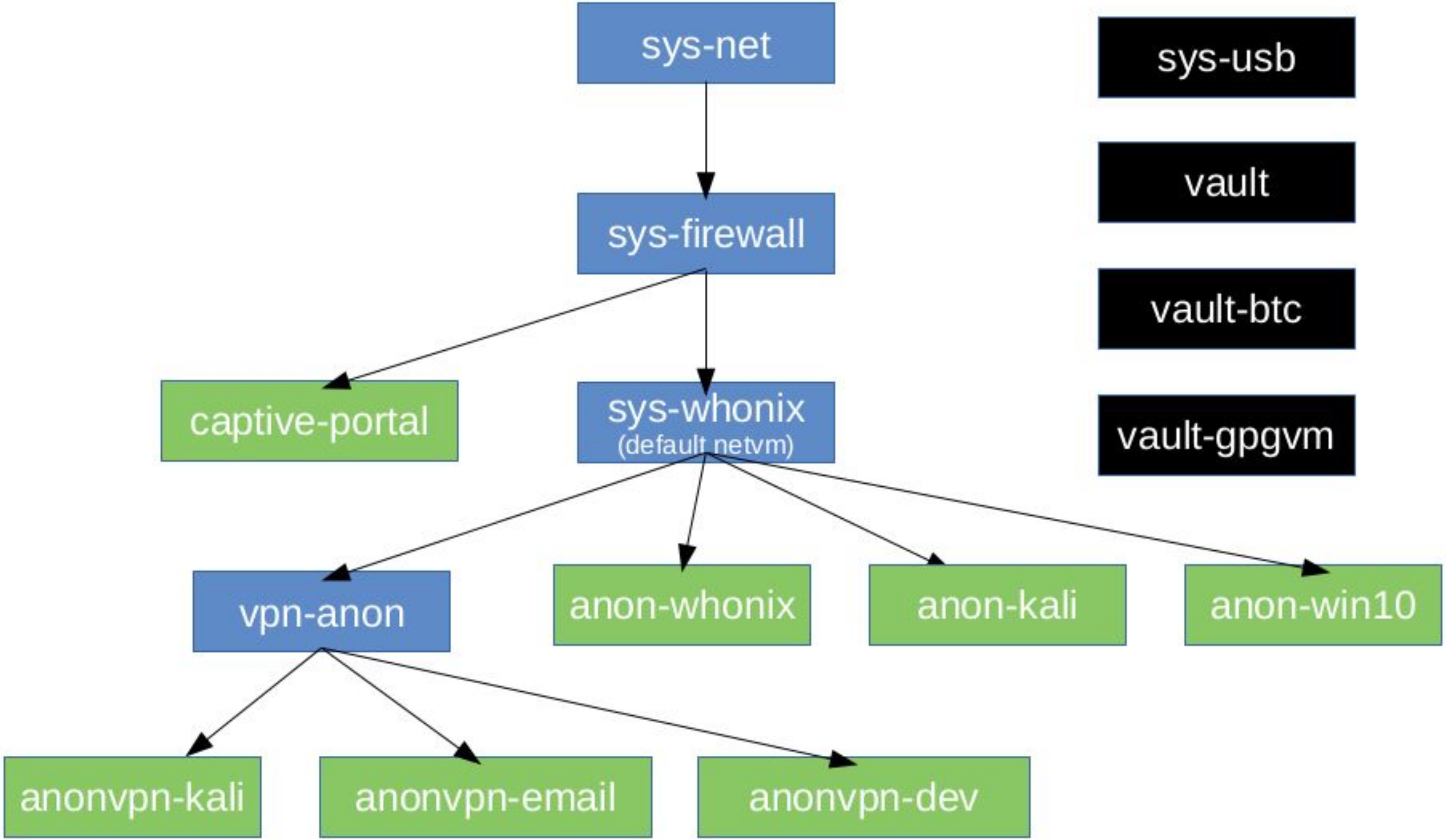
The Magical World of Qubes Networking

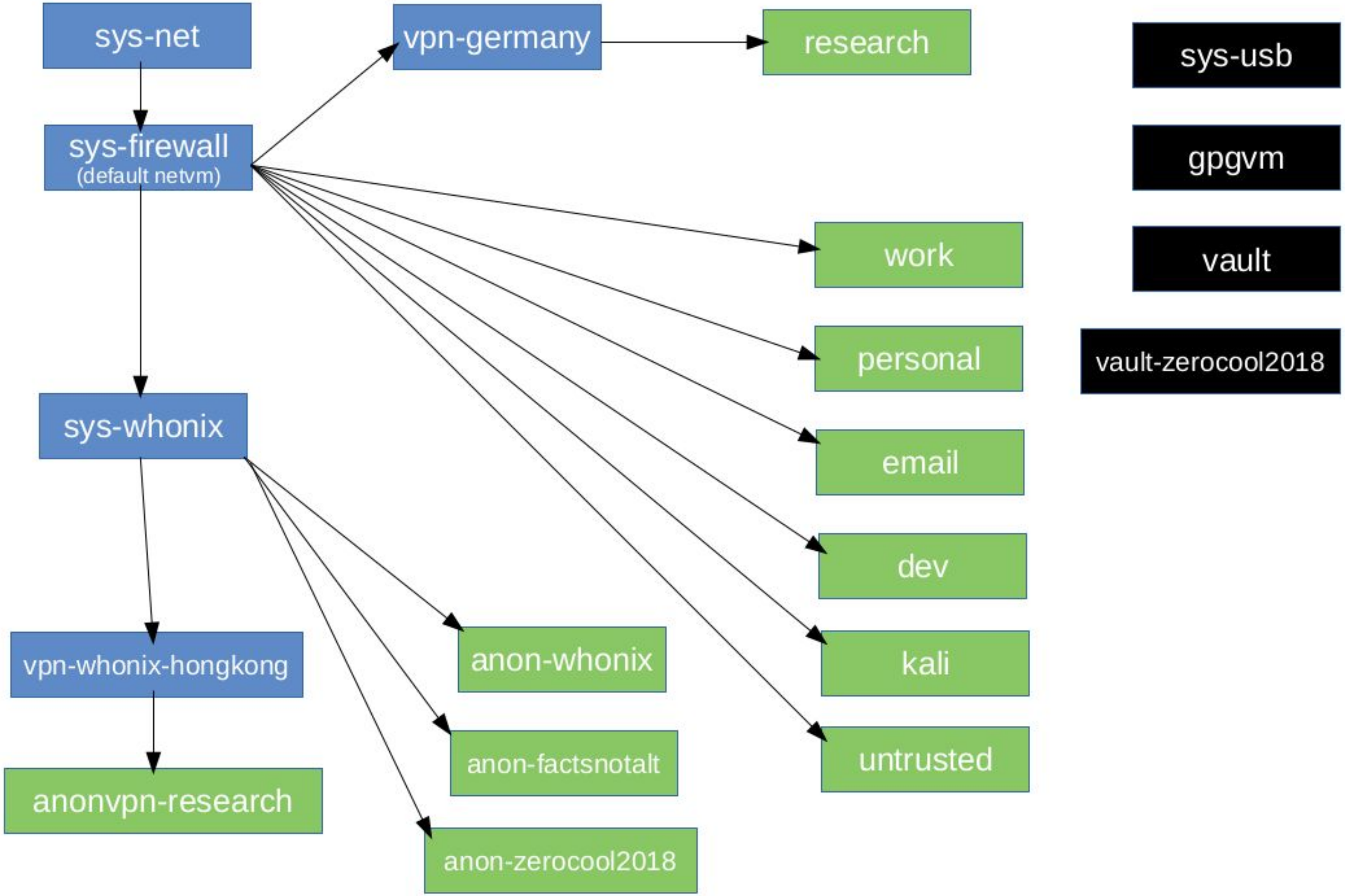


Managing secret identities with Whonix

Chatting in Secret While We’re All Being Watched
https://interc.pt/1Rx2a7A

How to Run a Rogue Government Twitter Account With an Anonymous Email Address and a Burner Phone
https://interc.pt/2kZB8YI


sys-net
sys-usb
sys-firewall
vault
vault-btc
captive-portal
sys-whonix
(default netvm)
vault-gpgvm
vpn-anon
anon-whonix
anon-kali
anon-win10
anonvpn-kali
anonvpn-email
anonvpn-dev



sys-net

sys-firewall
(default netvm)

vpn-germany

research

work

personal

email

dev

kali

untrusted

sys-whonix

vpn-whonix-hongkong

anonvpn-research

anon-whonix

anon-factsnotalt

anon-zerocool2018

sys-usb

gpgvm

vault

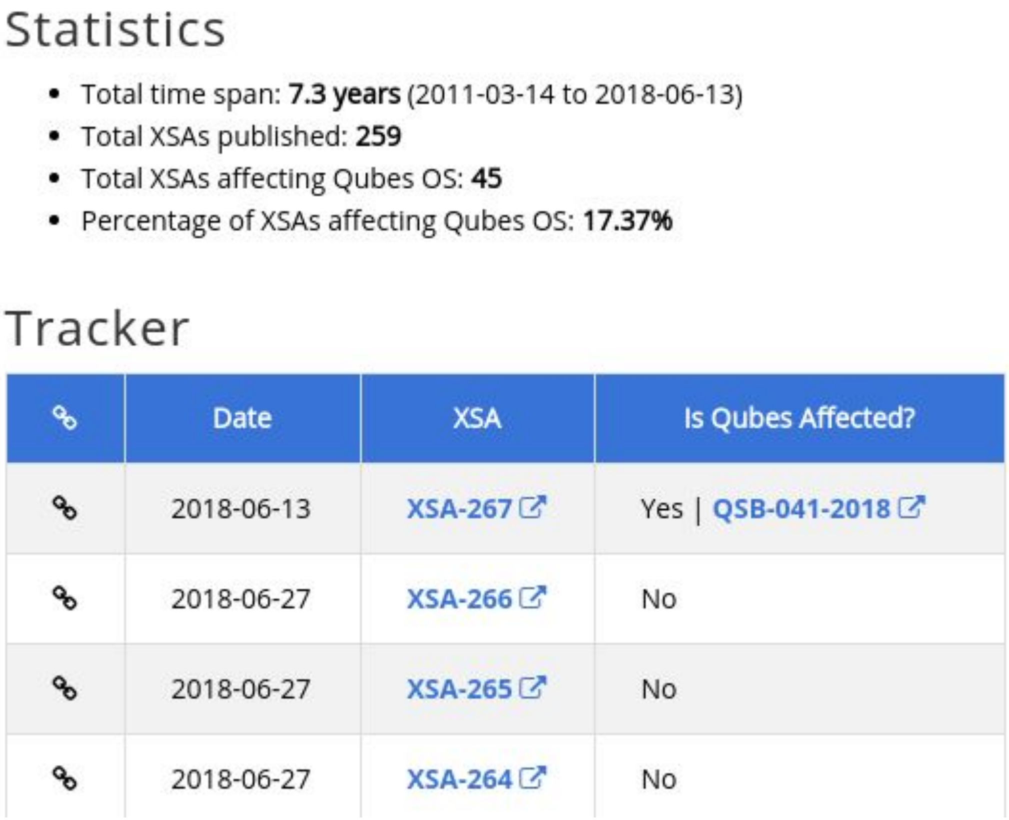
vault-zerocool2018

VPN over Tor

How to Hack Qubes

1. Hack one of the VMs using a client-side exploit (browser, PDF viewer, LibreOffice, VLC, etc.)

2. Use a Xen exploit to escape the VM and get arbitrary code execution in dom0



Statistics

- Total time span: **7.3 years** (2011-03-14 to 2018-06-13)
- Total XSAs published: **259**
- Total XSAs affecting Qubes OS: **45**
- Percentage of XSAs affecting Qubes OS: **17.37%**

Tracker

🔗	Date	XSA	Is Qubes Affected?
🔗	2018-06-13	**XSA-267**	Yes | **QSB-041-2018**
🔗	2018-06-27	**XSA-266**	No
🔗	2018-06-27	**XSA-265**	No
🔗	2018-06-27	**XSA-264**	No

https://www.qubes-os.org/security/xsa/

What You Can’t Do With Qubes

- No 3D acceleration, **not good for gaming :(**
- Windows VM support is limited
- macOS and Android VMs aren’t supported
- Bluetooth isn’t supported
- Command line is required for a lot of daily use
- Sometimes buggy, but fails closed
- Doesn’t work on low-end hardware: 8GB RAM minimum, 16GB recommended, 32GB if you can (this laptop has 12GB of RAM)

  Hardware Compatibility List: https://www.qubes-os.org/hcl/

QUBES OS

A REASONABLY SECURE OPERATING SYSTEM

About Qubes

Documentation: https://www.qubes-os.org/doc/
Source Code: https://github.com/qubesos
Support & Mailing Lists: https://www.qubes-os.org/support/
Code of Conduct: https://www.qubes-os.org/code-of-conduct/

About Me

Micah Lee
Email: micah@micahflee.com, micah.lee@theintercept.com
Twitter: @micahflee
PGP: 0x927F419D7EC82C2F149C1BD1403C2657CD994F73

Questions?

Coming up: *Qubes workshop*