QubesOS

Jan GOETTE

Waseda NSL english seminar Nov. 13, 2018

QubesOS Overview

- **Security-focused desktop operating system**
  - Let's consider a desktop system's attack surface!

- **Compartmentalization through hypervirtualization**
  - Isolates **devices** and their drivers
  - Isolates applications by **domain**

QubesOS History

- Project started in 2010 by Joanna Rutkowska and Rafal Wojtczuk, two experts in x86 hypervisor security
- Lead by Invisible Things Lab from Warsaw, Poland
- Initial release in 2012
- QubesOS 4.0 released March 2018

QubesOS concepts

Domain

Isolated **user data container** for information of the same security level.

→ work, personal, mail, vault, browsing, ...

Template

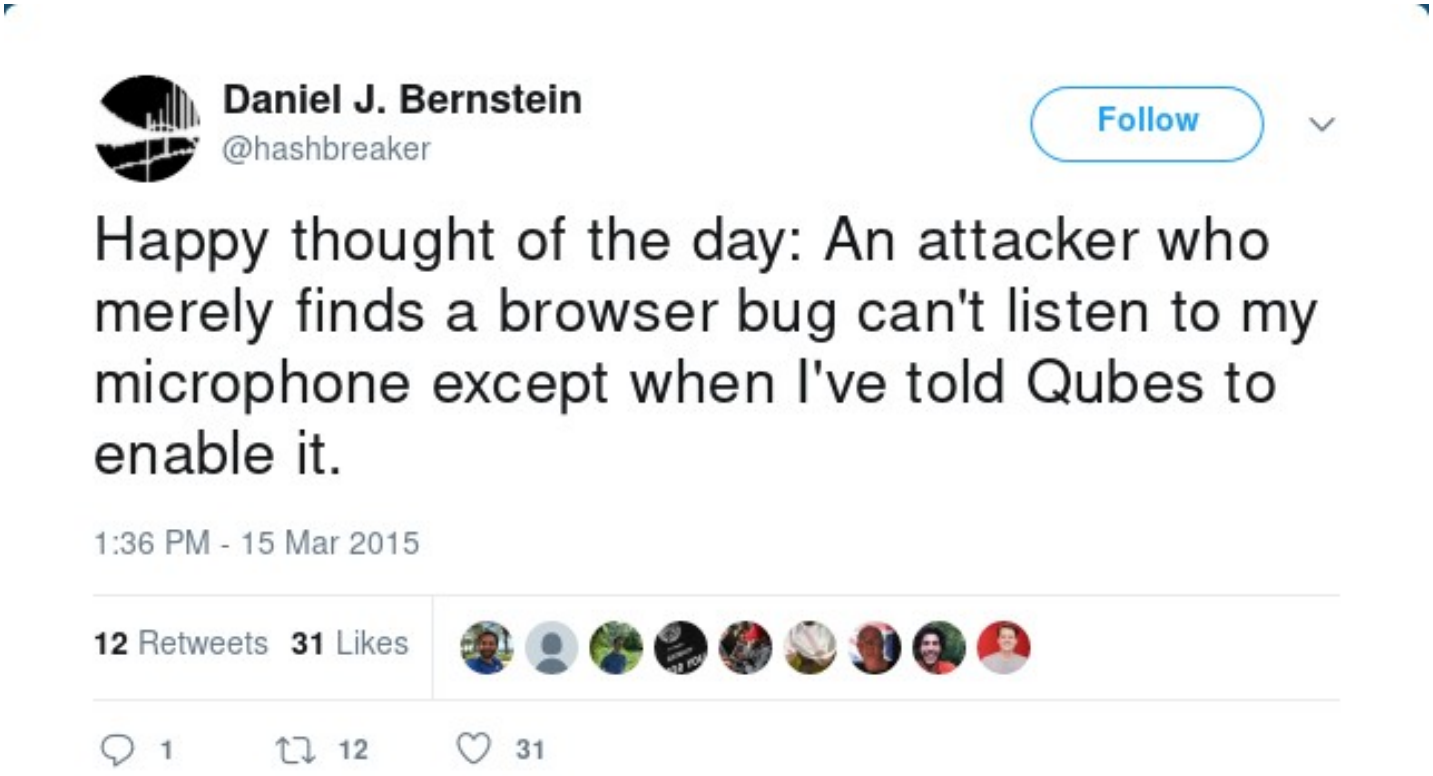
Base **system image** domains are booting into. Generally you have several templates.

→ fedora28, debian9, whonix, windows7, ...

AppVM

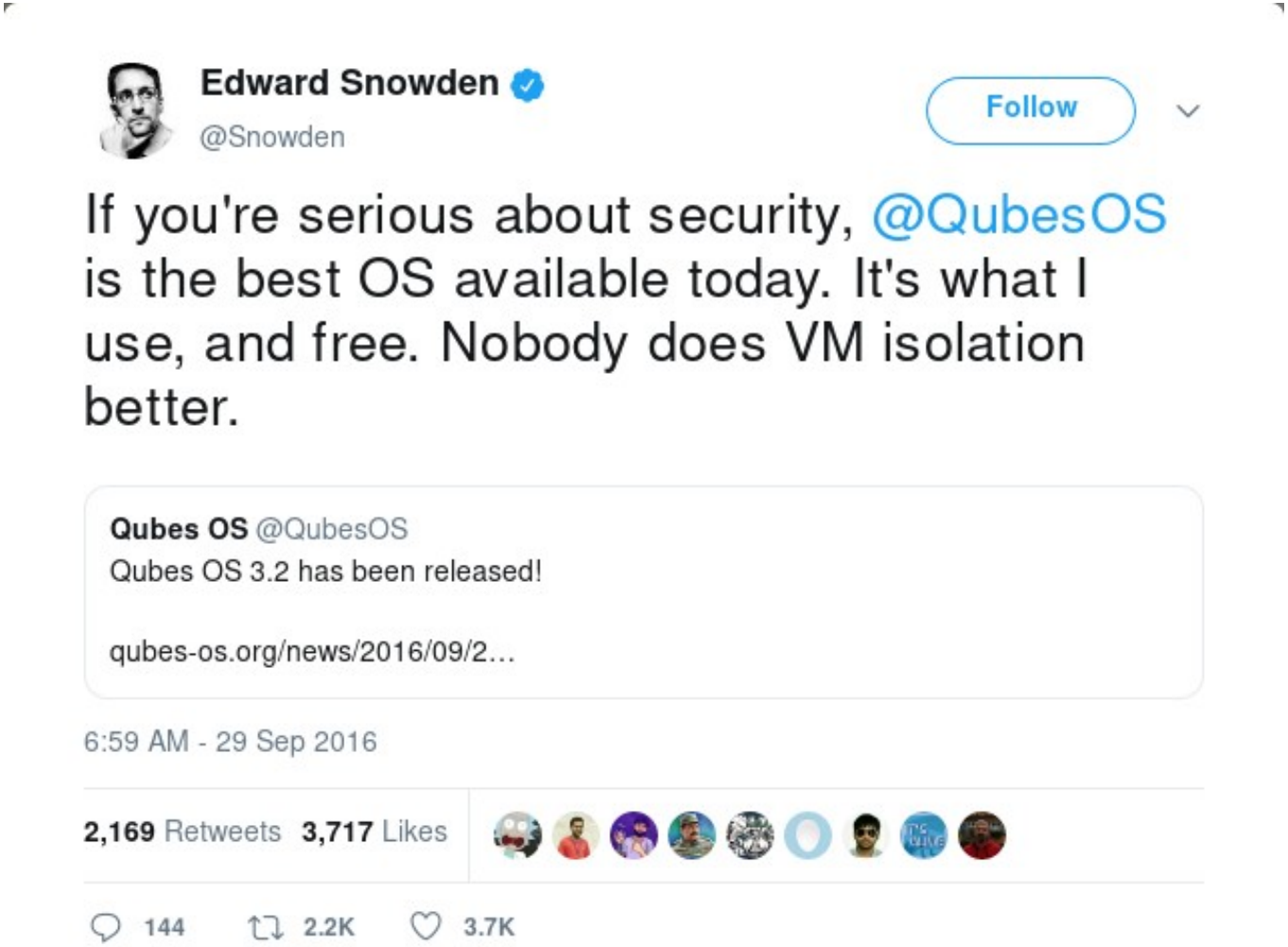
Virtual machine running with domain's data on Template image. Modifications on base system will be lost after reboot, but user data is persisted.

Testimonials



Testimonials

Testimonials



Edward Snowden ✓
@Snowden

Follow

If you're serious about security, @QubesOS is the best OS available today. It's what I use, and free. Nobody does VM isolation better.

> **Qubes OS** @QubesOS
> Qubes OS 3.2 has been released!
>
> qubes-os.org/news/2016/09/2…

6:59 AM - 29 Sep 2016

2,169 Retweets **3,717** Likes

144 2.2K 3.7K

Behind the scenes: QubesRPC

- **Inter-VM communication must be limited to reduce attack surface**
  - Source and target must be controlled
  - Protocols must be kept as simple as possible
- **QubesRPC is similar to named UNIX pipes**
  - Each VM exports RPC services
  - RPC services invoke handlers that get I/O per pipe
  - dom0 applies RPC policy rules to channel requests

Compartmentalization techniques

PCIe	Traditional IOMMU-based passthrough
USB	USB-over-IP over QubesRPC
Network	Xen built-in networking
GUI	Framebuffer over QubesRPC
Block devices	Xen built-in block device emulation
Speaker	PulseAudio buffers over QubesRPC
Microphone	PulseAudio buffers over QubesRPC

GUI isolation

- **dom0 drives monitor output**, AppVM runs stub X server
- Window manager in dom0 sees “ghosts” of AppVM windows, **framebuffers mapped through QubesRPC**
- dom0 stub window captures **input events, passed through** into AppVM
- Copy/Paste with **separate Qubes clipboard** and shortcuts

Application startup

What happens when the user clicks an entry in the application menu

1. Template image and domain data **snapshots** are created
2. **Xen VM is created** and booted
3. Mount template → / AppVM → /rw
4. **QubesRPC** server is launched via systemd
5. dom0 launches **application via QubesRPC**

Disposable VMs

”This never happened.”

- **Special VM on template that is launched to run a single application, then exit**
  - e.g. Firefox, terminal, PDF viewer
- **Files can be edited inside sub-dispVM with changes copied back on exit**

Picture: Vincent Huang on Wikimedia Commons

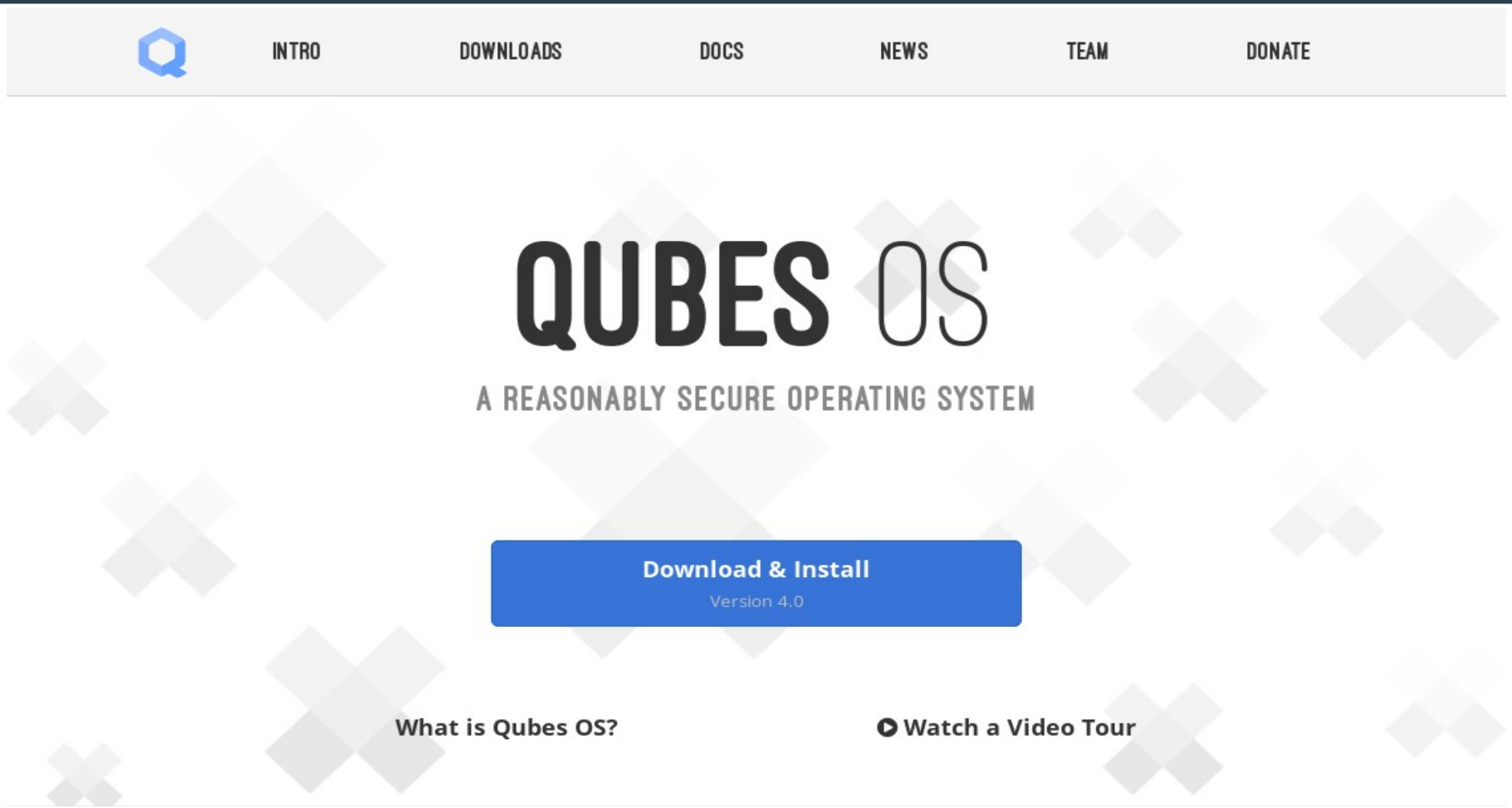
Demo Time!

Recap: Use cases

- Separating work and private life
- Isolating cryptographic keys
- Limiting damage during software development
- Not getting owned running untrusted code, opening untrusted files

Picture: Al Silonov on Wikimedia Commons

Further reading



https://qubes-os.org

Questions? qubes@jaseg.net

Questions?