Introduction to Qubes OS

Improved Security and Privacy in Times of Global Surveillance

www.NoRulersNoSlaves.com

June 30, 2020

Qubes OS

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.
— Edward Snowden, *Twitter*[1]

[1] https://twitter.com/Snowden/status/781493632293605376
https://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013-present)

Outline

What is Qubes OS?

Qubes OS is a free and open-source security-oriented operating system meant for single-user desktop computing.[2]

[2] https://www.qubes-os.org/intro

What is a Hypervisor?

- A hypervisor is computer software, firmware or hardware that creates and runs virtual machines.[3]
  - Type 1: Xen[4], KVM[5], Hyper-V[6]
  - Type 2: VirtualBox[7], VMware Workstation[8], Parallels Desktop[9]
- Qubes OS uses Xen
  - \+ VM management infrastructure
  - \+ GUI virtualization infrastructure

[3] https://en.wikipedia.org/wiki/Hypervisor
[4] https://xenproject.org
[5] https://www.linux-kvm.org
[6] https://docs.microsoft.com/en-us/windows-server/virtualization
[7] https://www.virtualbox.org
[8] https://www.vmware.com/products/workstation-pro.html
[9] https://www.parallels.com/products/desktop

Key Features[13]

- Strong isolation
- Template system
- Multiple operating systems
- Disposable VMs
- Whonix[10] integration
- Controller isolation
- Split GPG[11]
- U2F proxy[12]

[10] https://www.whonix.org
[11] https://www.qubes-os.org/doc/split-gpg
[12] https://www.qubes-os.org/doc/u2f-proxy
[13] https://www.qubes-os.org/intro

Motivation – Security I

- Hackers attack every 39 seconds[14]
- Improved protection against zero-day vulnerabilities[15]
  - computer-software vulnerabilities that are unknown to, or unaddressed by, those who should be interested in mitigating the vulnerabilities[16]

If someone directly targets you, you gonna get pwnd.
— Matty McFatty, *YouTube*[17]

Trying out Qubes OS (qubes-os.org) recently; linux distro designed around increased security by virtualizing everything and making it really convenient to hop between VMs. Surprisingly good user-friendliness!
— Vitalik Buterin, Russian-Canadian programmer and writer, *Twitter*[18]

[14] https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
[15] https://www.economist.com/babbage/2014/03/28/a-digital-fortress
[16] https://en.wikipedia.org/wiki/Zero-day_(computing)
[17] https://www.youtube.com/watch?v=sbN5Bz3v-uA
[18] https://twitter.com/vitalikbuterin/status/1086465679904038912

Motivation – Security II

When I use Qubes I feel like a god. Software thinks that it's in control, that it can do what it wants? It can't. I'm in control.
— Micah Lee, Freedom of the Press Foundation, *Twitter*[19]

For those willing to put in the effort, Qubes is more secure than almost any other operating system available today.[20]

In Qubes OS, it's the user that is responsible for making all the security decisions [...].[21]

[19] https://twitter.com/micahflee/status/577998730340622337

[20] https://www.economist.com/babbage/2014/03/28/a-digital-fortress

[21] https://theinvisiblethings.blogspot.com/2012/09/introducing-qubes-10.html

Motivation – Privacy

> *We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government.*
> — William O. Douglas, *Associate Justice of the Supreme Court of the United States (1966)*[22]

- Comfortable Whonix integration
  - protect your identity
  - private communication
- Qubes with different VPNs

[22] `https://openjurist.org/385/us/323`

Target Group

- Individuals who
  - are vulnerable or actively targeted e.g. researchers or political activists
  - want to run multiple operating systems simultanously
  - prefer FOSS
  - want to lower effects of mistakes
  - want to separate their data in spaces for work, surfing, ...

Not Target Group

- Individuals who
  - play a lot of games
    - GPU acceleration is problematic[23]
  - need nested virtualization[24]
  - prefer convenience out of the box over security
  - are not technic affine
  - don't want to use the command line
  - want a multi-user[25] OS
  - are impatient

[23] https://github.com/tabit-pro/Qway-qubes-repo/wiki/Intel-GVT_g-on-Qubes

[24] https://github.com/QubesOS/qubes-issues/issues/4104

[25] https://groups.google.com/forum/#!msg/qubes-devel/XnTly2JNfPw/BppN_D5vn4kJ

Development

- Xen has been existing for more than 16 years now
- Qubes OS has been existing for more than 10 years now
  - active development on GitHub[26]
- is FOSS, GPLv2 License[27]
- Currently 668 open and 2,407 closed bugs[28]

[26] https://github.com/QubesOS

[27] https://opensource.org/licenses/gpl-2.0.php

[28] https://github.com/QubesOS/qubes-issues/issues

Funding[34]

- Main funding from “Invisible Things Lab”[29]
  - over 100,000$ per year
  - founded in 2007 in Warsaw, Poland
  - Joanna Rutkowska[30] is the founder and CEO
  - privately held company based in Berlin, Germany
  - primary source of revenue is security research and development
- Further funding from
  - Open Technology Fund[31]
  - Freedom of the Press Foundation[32]
  - Mullvad[33]
  - and more...

[29] https://invisiblethingslab.com
[30] https://blog.invisiblethings.org/about
[31] https://www.opentech.fund
[32] https://freedom.press
[33] https://mullvad.net
[34] https://www.qubes-os.org/partners

Hardware Requirements[36]

- CPU
  - 64-bit Intel or AMD
  - Intel VT-x with EPT or AMD-V with RVI
  - Intel VT-d or AMD-Vi (aka AMD IOMMU)
- GPU
  - Intel IGP or AMD
  - Nvidia GPUs require significant troubleshooting
- RAM
  - at least 4 GB
  - more than 8 GB recommended
- Disk space
  - at least 32 GB
  - SSD recommended
- Tip: Check hardware compatibility list[35]

[35] https://www.qubes-os.org/hcl

[36] https://www.qubes-os.org/doc/system-requirements

Alternatives

- Different computers
- Different boot drives
- Different VMs on Linux
- Different Browser Profiles, Tor
- VPN/VPS

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Summary

- Focus on security
- You are responsible for security decisions
- For individuals who value security and are willing to take the required effort for achieving it
- Actively developed for over 10 years
- High hardware requirements
- Famous users: Edward Snowden and Micah Lee
- Even Qubes OS is not 100% secure

Thank you for watching!

visit

www.NoRulersNoSlaves.com