Qubes OS: Flexible Virtualization For (Not Only) Power Users

Qubes OS is a virtualization-based, security-focused operating system that aims to provide users with a secure way to take control of their computer. Using Xen virtualization with multiple virtual machines, Qubes OS compartmentalizes your machine, separating and isolating both dangerous components (such as USB controller, camera and microphone or networking) and dangerous activities.

In this talk, I wish to provide a bird’s eye overview of Qubes OS, explaining its concepts to potentially interested users. I will also draw attention to particularly interesting security and usability decisions that can serve as inspiration to other projects interested in creating more secure computing.

* Introduction to the ideas behind Qubes OS: isolation and separation

* Explanation of how and why Qubes OS is (reasonably) secure, with a little technical background for interested listeners

* Device isolation: how virtualization enables isolating potentially dangerous parts of a computer and managing access to them

* Disposable virtual machine: how Qubes OS enables simple and easy to use disposable virtual machines for interacting with untrusted devices, data or content

* Usability in the service of security: how Qubes OS uses UX to encourage secure choices and make isolation work better

* Use cases for Qubes OS: how hackers, developers and activists use Qubes OS, based on user research and testimony

* Limitations and constraints: hardware requirements and GPU acceleration