Qubes OS Architecture

Paper by Joanna Rutkowska & Rafal Wojtczuk

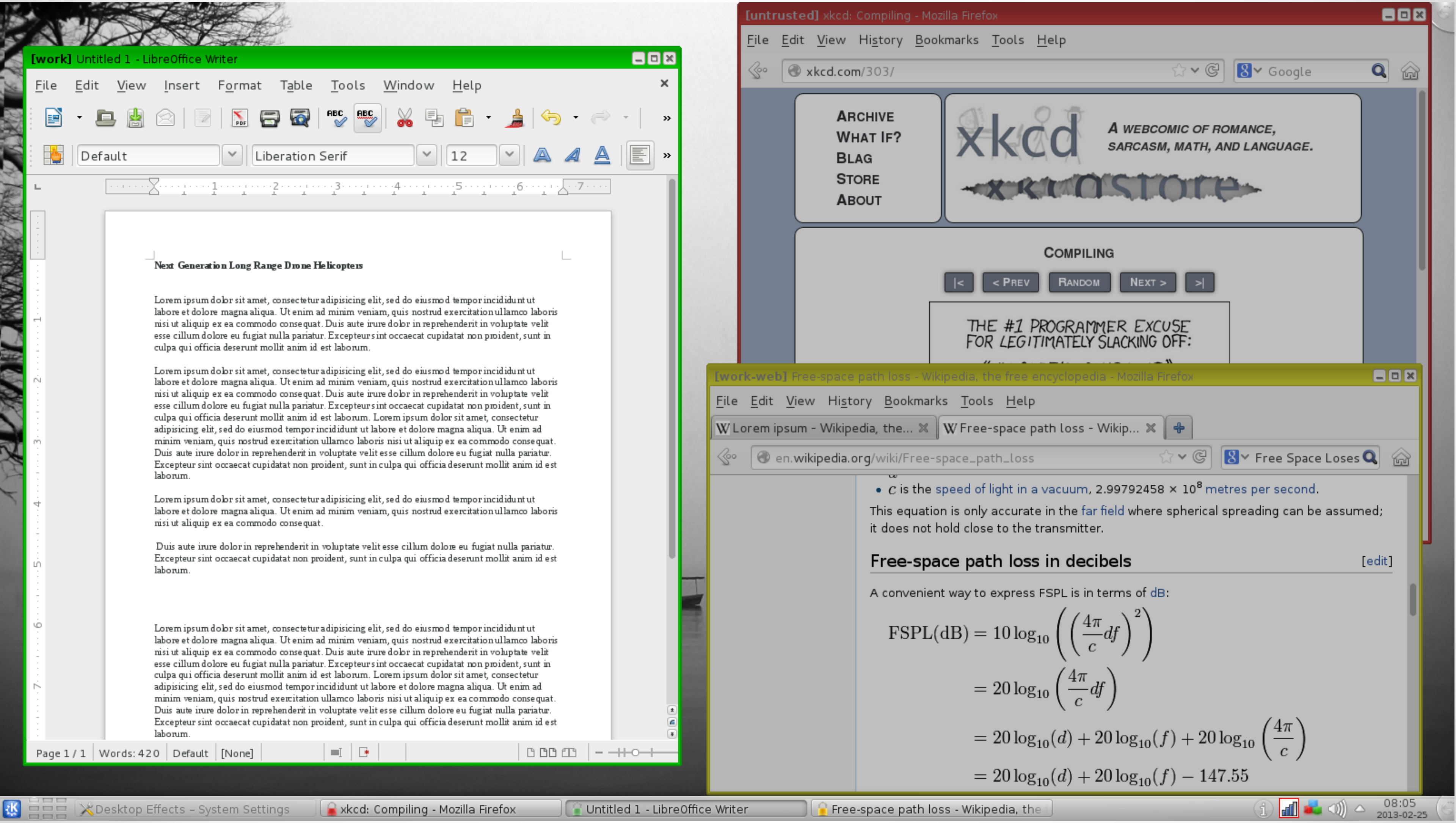
Presentation by Matt Burrough (burrogh2@illinois.edu)

The Problem

- Today's OSes are inherently insecure
- Complex APIs
- Kernel Mode Exploits
- User Mode Exploits
- Fixing one flaw too reactionary
- Zero Days

Qubes Concept

- Segment portions of the OS into individual VMs (domains)
- Hypervisors more secure
- Hardware VT adds extra security
- Tie all domains together with a GUI


[work] Untitled 1 - LibreOffice Writer
File Edit View Insert Format Table Tools Window Help
Default
Liberation Serif
12
Page 1 / 1
Words: 420
Default
[None]
[untrusted] xkcd: Compiling - Mozilla Firefox
File Edit View History Bookmarks Tools Help
xkcd.com/303/
Google
ARCHIVE
WHAT IF?
BLAG
STORE
ABOUT
xkcd
A WEBCOMIC OF ROMANCE, SARCASM, MATH, AND LANGUAGE.
xkcd store
COMPILING
|<
< PREV
RANDOM
NEXT >
>|
THE #1 PROGRAMMER EXCUSE FOR LEGITIMATELY SLACKING OFF:
[work-web] Free-space path loss - Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Lorem ipsum - Wikipedia, the...
Free-space path loss - Wikip...
en.wikipedia.org/wiki/Free-space_path_loss
Free Space Loses
Desktop Effects – System Settings
xkcd: Compiling - Mozilla Firefox
Untitled 1 - LibreOffice Writer
Free-space path loss - Wikipedia, the
08:05
2013-02-25

Next Generation Long Range Drone Helicopters

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- c is the speed of light in a vacuum, 2.99792458 × 10^8 metres per second.

This equation is only accurate in the far field where spherical spreading can be assumed; it does not hold close to the transmitter.

Free-space path loss in decibels

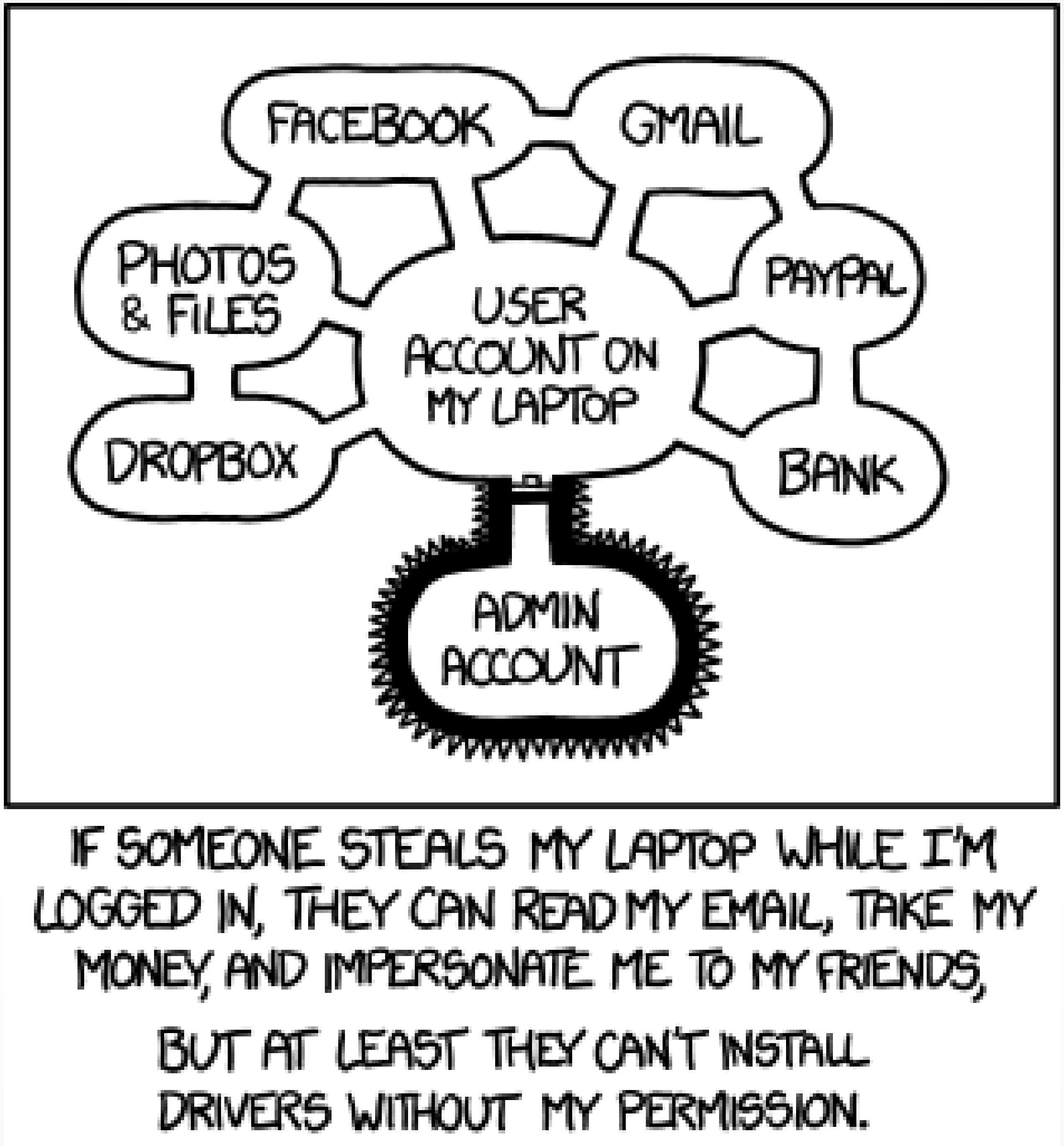
[edit]

A convenient way to express FSPL is in terms of dB:

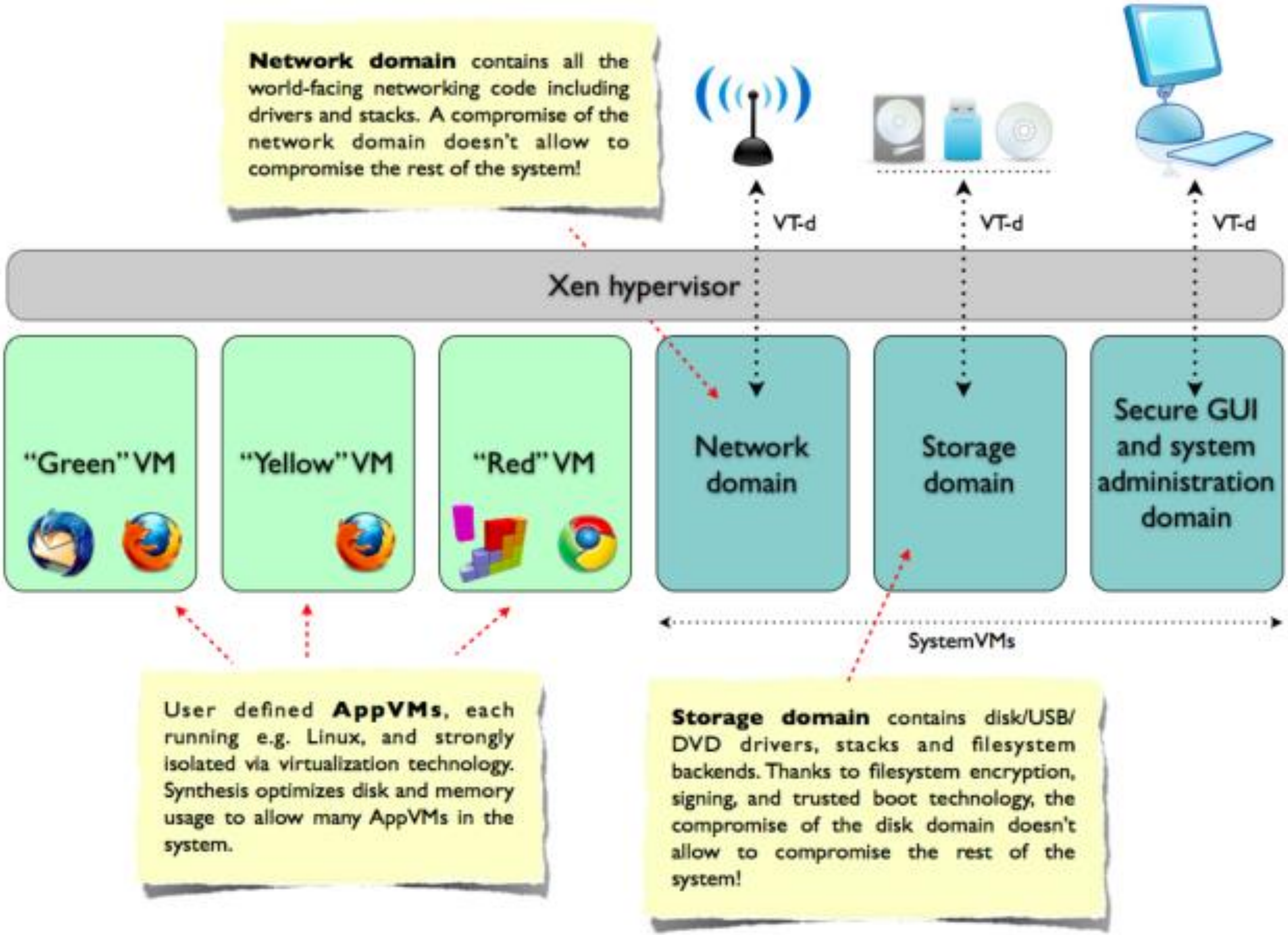
$$\begin{aligned}\mathrm{FSPL(dB)} &= 10\log_{10}\left(\left(\frac{4\pi}{c}df\right)^2\right)\\ &= 20\log_{10}\left(\frac{4\pi}{c}df\right)\\ &= 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right)\\ &= 20\log_{10}(d) + 20\log_{10}(f) - 147.55\end{aligned}$$

Implementation

- Xen Hypervisor
- Dom0 Administrative Domain
- Network (NIC) Domain
- Storage Domain
- 1+ AppVM domains


FACEBOOK
GMAIL
PHOTOS & FILES
PAYPAL
USER ACCOUNT ON MY LAPTOP
DROPBOX
BANK
ADMIN ACCOUNT
IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,
BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

- http://xkcd.com/1200/

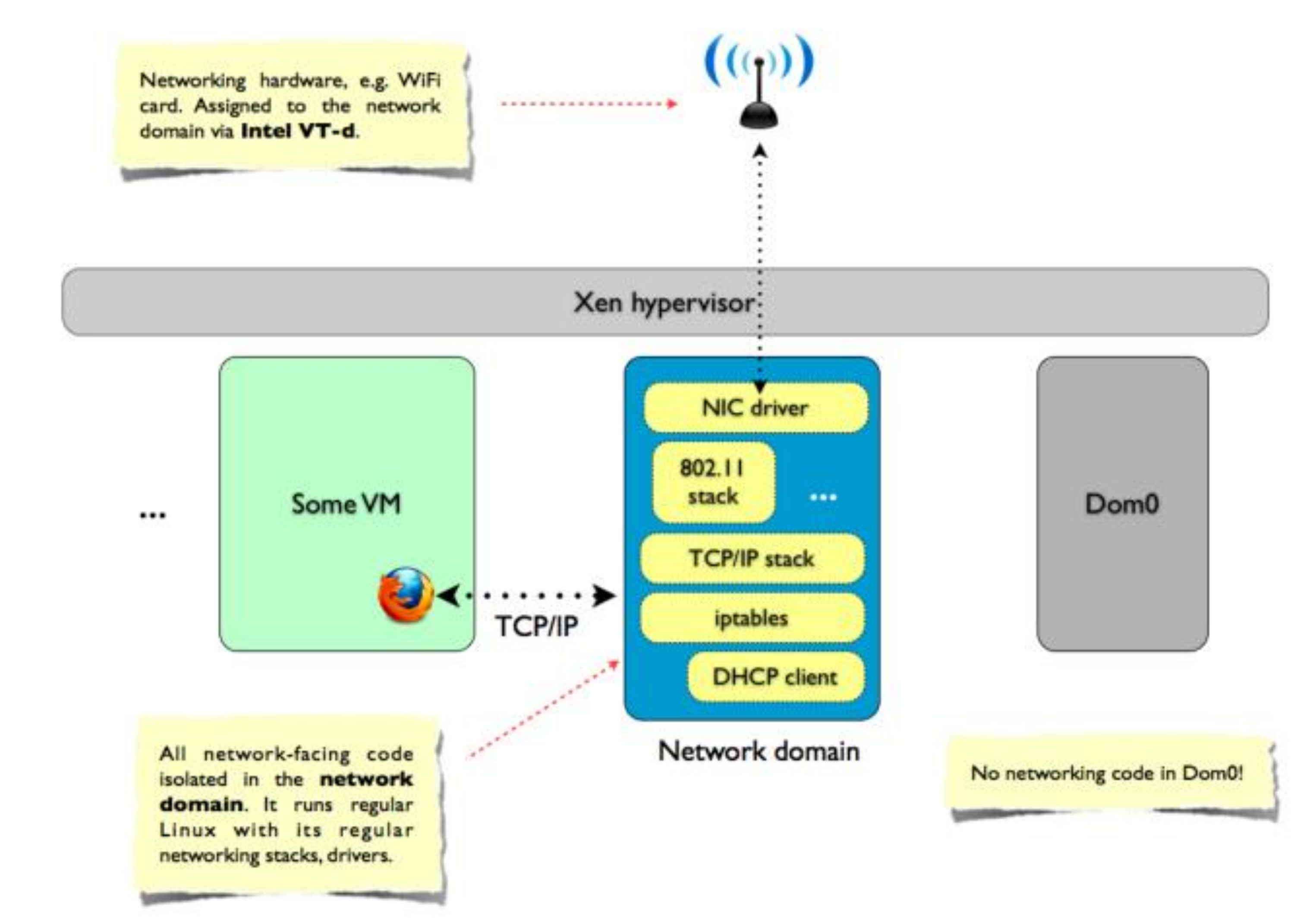


Network domain contains all the world-facing networking code including drivers and stacks. A compromise of the network domain doesn't allow to compromise the rest of the system!

User defined **AppVMs**, each running e.g. Linux, and strongly isolated via virtualization technology. Synthesis optimizes disk and memory usage to allow many AppVMs in the system.

Storage domain contains disk/USB/ DVD drivers, stacks and filesystem backends. Thanks to filesystem encryption, signing, and trusted boot technology, the compromise of the disk domain doesn't allow to compromise the rest of the system!

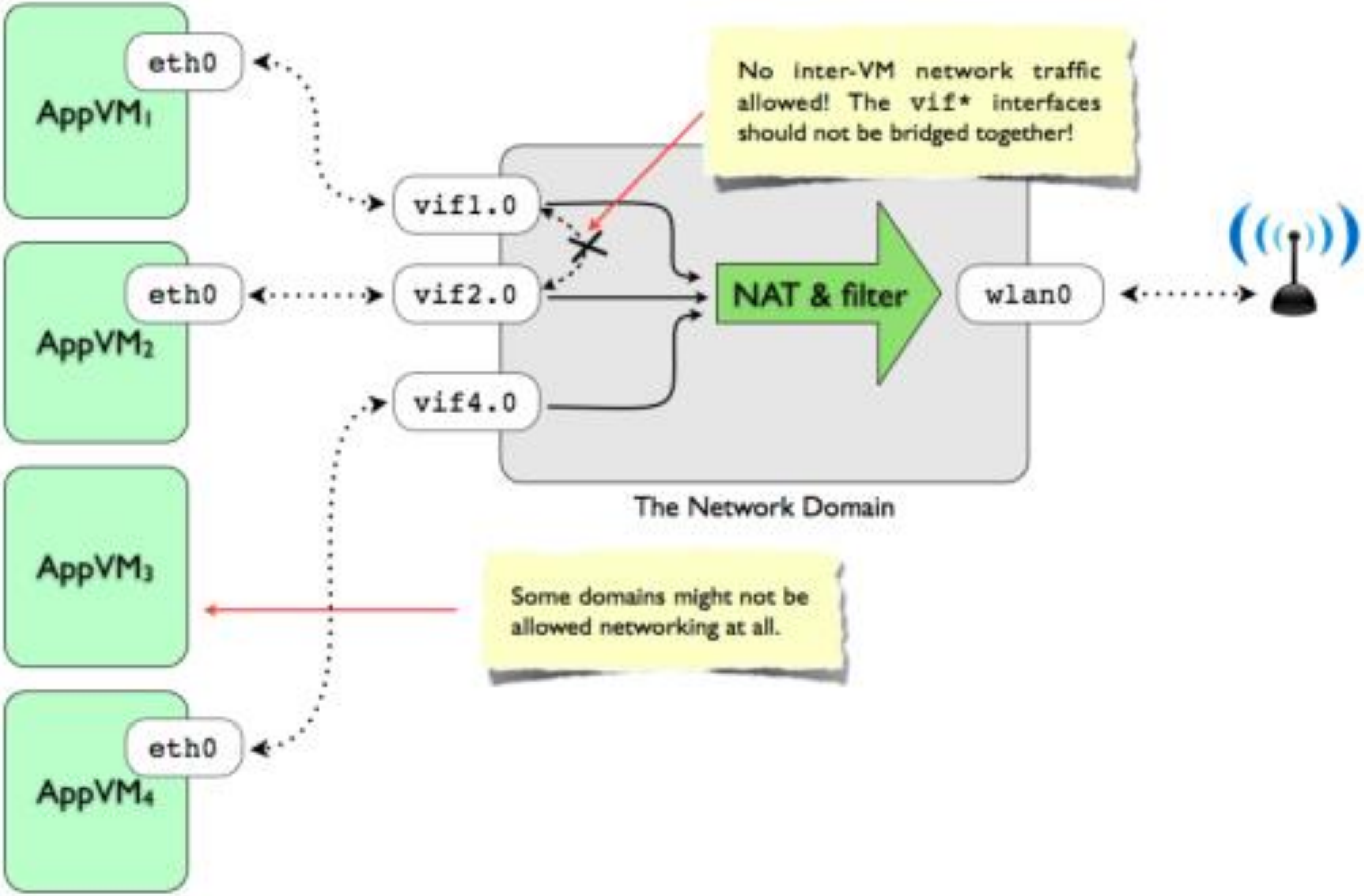
Networking



Networking hardware, e.g. WiFi card. Assigned to the network domain via **Intel VT-d**.

All network-facing code isolated in the **network domain**. It runs regular Linux with its regular networking stacks, drivers.

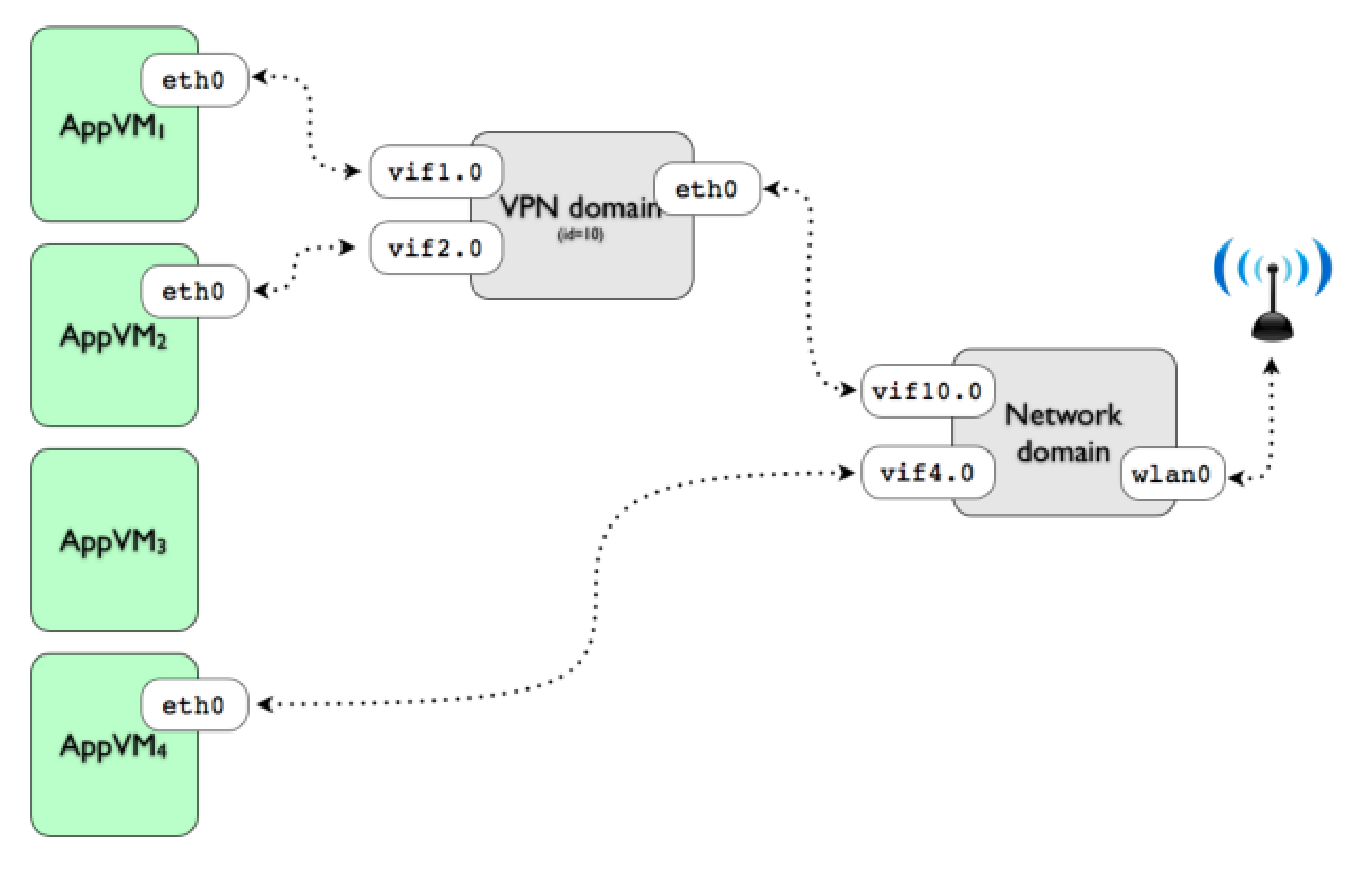
No networking code in Dom0!



No inter-VM network traffic allowed! The `vif*` interfaces should not be bridged together!

Some domains might not be allowed networking at all.

VPN Domain


eth0
AppVM₁
vif1.0
VPN domain
(id=10)
eth0
vif2.0
eth0
AppVM₂
vif10.0
Network domain
vif4.0
wlan0
AppVM₃
eth0
AppVM₄

Attack Vectors

- 1- vs. N-stage attacks
- Flaw in the Hypervisor
- Flaw in the GUI code
- Attack against Disk Drivers
- Attack against NIC driver

Related Works

- Windows SteadyState
  - http://www.microsoft.com/en-us/download/details.aspx?id=4310
- Breaking Up is Hard to Do: Security and Functionality in a Commodity Hypervisor
  - http://www.sigops.org/sosp/sosp11/current/2011-Cascais/printable/14-colp.pdf
- Citrix XenApp / TS RemoteApp
  - http://www.citrix.com/products/xenapp/overview.html
  - http://technet.microsoft.com/en-us/library/cc730673%28v=ws.10%29.aspx

Discussion Questions

- Does the shared clipboard and ease of moving files between domains compromise security?
- Do you agree with the decision to host the GUI system in the administrative domain?
- Do you think the Qubes concept would offer an improvement in security for a typical computer user? Consider that the user now potentially needs to patch multiple instances of an OS to keep all of the VMs up to date.
- In which types of environments do you foresee this OS model working well?