The Whole Internet in a GreyBox

Gabriel Somlo
Fall 2015
A Simple STEP Exercise
A Simple STEP Exercise
A Simple STEP Exercise
Virtualization: It's Turtles All The Way Down!

- Classic Multitasking
- Application-level Virtualization
- Guest Virtual Machines
- Containers
Classic Multitasking

- Host OS
- File System & Networking
- App 1
- App 2
- App ...
- App ...
- App ...
- App ...
- App ...
- App ...
- App N
# Application-Level Virtualization

<table>
<thead>
<tr>
<th><a href="http://www.cmu.edu">www.cmu.edu</a></th>
<th>facebook.com</th>
<th>...</th>
<th>wikipedia.org</th>
<th>DNS Root servers</th>
<th>TLD servers</th>
<th>Public caching resolver</th>
<th>App ...</th>
<th>App N</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd (vhosts)</td>
<td>named (views)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## File System & Networking

## Host OS
TopGen: HTTP and DNS App Virtualization

<table>
<thead>
<tr>
<th><a href="http://www.cmu.edu">www.cmu.edu</a></th>
<th>facebook.com</th>
<th>...</th>
<th>wikipedia.org</th>
<th>DNS Root servers</th>
<th>TLD servers</th>
<th>Public caching resolver</th>
<th>App ...</th>
<th>App N</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td></td>
<td></td>
<td></td>
<td>named</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(30K vhosts)</td>
<td></td>
<td></td>
<td></td>
<td>(18 views)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

File System & Networking

Host OS
TopGen: HTTP and DNS App Virtualization
TopGen: HTTP and DNS App Virtualization
Guest Virtual Machines

Guest OS

File System & Networking

Host OS (w. hypervisor)
Exercise Assets are Guest VMs
Guest Virtual Machines

- App 1
  - Guest OS
  - File System & Networking

- App 2
  - Guest OS
  - File System & Networking

- App N
  - Guest OS
  - File System & Networking

Host OS (w. hypervisor)
Containers

<table>
<thead>
<tr>
<th>App A1</th>
<th>App A2</th>
<th>App A3</th>
<th>App B1</th>
<th>App B2</th>
<th>App B3</th>
<th>App B4</th>
<th>App B5</th>
<th>App B6</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System &amp; Networking A</td>
<td>File System &amp; Networking B</td>
<td>Host OS (w. container engine)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Containerizing Quagga / bgpd
Containerizing Quagga / bgpd
Containerizing Quagga / bgpd

Quagga bgpd (Verisign)  Quagga bgpd (Level3)  Quagga bgpd (AT&T)  Quagga bgpd (Sprint)  ...

FileSys & Netwk  FileSys & Netwk  FileSys & Netwk  FileSys & Netwk  ...

Host OS (w. container engine)
Containerizing Quagga / bgpd

GreySpace

Student Network / Enclave

DMZ
WWW  Auth.DNS

Users
usr1  usr2

Internal Svcs
SQL  FileSrv
Containerizing Quagga / bgpd
The GreyBox

GreySpace

Containers in single VM

Verisign

Level3

Sprint

AT&T

nginx-WWW

dnamed-DNS

Student Network / Enclave

DMZ

WWW

Auth.DNS

Users

usr1

usr2

Internal Svcs

SQL

FileSrv

Firewall

Int.Rtr.
The GreyBox
The GreyBox

GreyBox: Guest OS + container engine

Host OS (w. hypervisor)

<table>
<thead>
<tr>
<th>App 1</th>
<th>App 2</th>
<th>App ...</th>
<th>App N</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System &amp; Networking</td>
<td>File System &amp; Networking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>App 1</th>
<th>App 2</th>
<th>App ...</th>
<th>App N</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx</td>
<td>bind</td>
<td>Quagga BGPD</td>
<td>Quagga BGPD</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>App 1</th>
<th>App 2</th>
<th>App ...</th>
<th>App N</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS&amp;Net</td>
<td>FS&amp;Net</td>
<td>FS&amp;Net</td>
<td>FS&amp;Net</td>
</tr>
</tbody>
</table>

CERT | Software Engineering Institute | Carnegie Mellon University
Containers & Networking: **CORE**

- **Common Open Research Emulator**
  - Network simulator by Boeing, Naval Research Lab
  - [github.com/coreemu/core](https://github.com/coreemu/core)

- **Open Source**
  - BSD License
  - Python back-end for networking & LXC containers
  - TCL front-end for GUI / canvas
CORE Front-end (GUI)
node n1 {
    type router
    model router
    network-config {
        hostname Sprint
        !
        interface eth0
        ip address 10.0.1.1/24
        !
        interface eth1
        ip address 10.0.3.2/24
        !
        interface eth2
        ip address 10.0.10.1/24
        !
    }
    canvas c1
    iconcoords {340 500}
    labelcoords {340 400}
    interface-peer {eth0 n2}
    interface-peer {eth1 n3}
    interface-peer {eth2 n10}
    services {zebra BGP vtysh IPForward}
    custom-config {
        custom-config-id service:zebra:/usr/local/etc/quagga/Quagga.conf
        custom-command /usr/local/etc/quagga/Quagga.conf
        config {
            interface eth0
            ip address 10.0.1.1/24
            !
            interface eth1
            ip address 10.0.3.2/24
            !
            interface eth2
            ip address 10.0.10.1/24
            !
        }
    }
}
The Whole Internet in a GreyBox

Questions?
Please email glsomlo@cert.org

Next:
Demo of BGP failover with CORE