

SECURE APPLICATIONS ON MOBILE DEVICES

Will Dietz, Kevin Larson
Shivaram Venkataraman

SMARTPHONE SECURITY

Motivation

- Smartphones are the target of Malware attacks



Hacking the iPhone

BY: ADAM L. PENENBERG November 15, 2007

Just how vulnerable is your iPhone if someone wants to intercept your email or record your conversations? Pretty vulnerable.

Related Stories

- [Video: Hacking the iPhone](#)
Watch security expert Rik Farrow steal emails, bug conversations, and read web-browsing histories using his laptop.
- [Slideshow: Deconstructing the iPhone](#)

Some of the breakthrough features of Apple's iPhone are already offered by competing devices. But that won't stop us from lustng for one.

- [iPhone Backlash](#)

While researching FAST COMPANY's December/January cover story I ran across a startling claim: some computer security professionals were boasting that they could turn an iPhone into a piece of spyware that can intercept a target's voice mail and e-mail, hijack its Safari browser, and even surreptitiously record conversations, all without the owner's knowledge. H D Moore, Director of Security Research for BreakingPoint Systems, even posted a detailed [primer](#). Given Apple's own [marketing](#), which boasts that Macs are more secure -- and more virus-resistant -- than PCs, the fact the iPhone could be hacked seemed newsworthy.

Of course, the Web is rife with braggadocio, and just because a few computer engineers could gin up an obscure software exploit or two didn't mean anyone had actually unleashed any. Still, my editors and I wondered just how vulnerable is the "Jesus Phone" to an unscrupulous hacker? Could it really be turned into a tool of espionage?

SMARTPHONE SECURITY

Motivation

- Smartphones are the target of Malware attacks

The screenshot shows a news article from MacNN.com. The header features the Fast Company logo and the MacNN 'read me first' button. The main headline is 'Hackin...'. Below it, a sub-headline reads 'Just how vulnerable is your iPhone?'. A sidebar on the left lists 'Related Stories' including 'iPhone Watch series 3' and 'Farrow says...'. The main article discusses Apple's iPhone security claims, mentioning Nicolas Seriot and his comments at the Black Hat Conference. It highlights vulnerabilities in the iPhone's sandboxing system and the review process. A sidebar on the right shows a snippet of another article about SpyPhone.

Hackin...
BY: ADAM L. PEYSON
Just how vulnerable is your iPhone?
record your iPhone's location without your knowledge.
Related Stories
• Video:
[iPhone Watch series 3](#)
Farrow says...
conversat...
web-brow...
using his iPhone
• Slidesh...
[Deconstru...
iPhone](#)
Some of t...
features o...
are alrea...
competin...
that won...
lusting fo...
• iPhone

macnn news

Sec. expert: Apple's iPhone security claims 'exaggerated'
Decries iPhone sandboxing
The iPhone is not as secure as Apple would like people to believe, claims a software engineer and security specialist, Nicolas Seriot. Speaking at this week's Black Hat Conference in Arlington, Virginia, Seriot commented that while the iPhone OS theoretically sandboxes applications to restrict data access, the rules in place are "way too loose." Apple should not be claiming that apps cannot access data from another, he emphasized.
Proof of the vulnerability is said to lie with several apps, such as Aurora Feint and mogoRouge. Both were initially approved by Apple yet quietly stole phone and e-mail contacts before eventually being blocked from the App Store. Apple's review process can and does miss security problems, as pointed out, and vulnerabilities may only get worse given the increasing appeal of the iPhone for hackers and criminals. Devices can become still more exposed when jailbroken.

A demonstration app created by Seriot, SpyPhone, is said to reveal e-mail addresses, user names, Safari and YouTube searches and server information, although not the password. When an iPhone connects to Wi-Fi the app can also learn which networks a device connects to, a person's phone number, and the last call made. Most severe may be location info, which can be pulled from the device's GPS receiver.

SMARTPHONE SECURITY

Motivation

- Smartphones are the target of Malware attacks

The screenshot shows a news article from V3.co.uk. At the top, there's a navigation bar with links for 'mac news', 'reviews', 'blogs', 'forums', and 'services'. Below that is another navigation bar with 'Home' (which is highlighted), 'News', 'In-depth | Blogs | Audio/Video | Reviews | White papers | Downloads | Forums |', and '7 days | Business | Business hardware | Business software | Communications | Security | Empl...'. The main headline is 'Cyber-criminals target mobile banking'. A sub-headline reads 'TowerGroup research predicts an explosion of mobile malware during 2007'. The author is listed as 'Robert Jaques' from 'vnunet.com, 22 Jan 2007'. There's also a small image of a smartphone.

FAST COMPANY
macnn read me first

mac news reviews blogs forums services

V3.co.uk All the latest UK technology news, reviews and analysis

Home News In-depth | Blogs | Audio/Video | Reviews | White papers | Downloads | Forums |
7 days | Business | Business hardware | Business software | Communications | Security | Empl...

Where am I? > Home > News > Enterprise Security Technology

Cyber-criminals target mobile banking

TowerGroup research predicts an explosion of mobile malware during 2007

Robert Jaques
vnunet.com, 22 Jan 2007

IT managers must extend existing malware and virus security initiatives to include mobile phones

Cyber-criminals and identity thieves will turn their attention to mobile banking and payment initiatives during 2007, experts warned today.

TowerGroup noted that, while most mobile phones are potential targets, smartphones and wireless PDAs are "particularly attractive" to fraudsters given their capabilities to support PC-like applications including web browsing and instant messaging.

DESKTOP - SMARTPHONE INTEGRATION

- Run Desktop Applications on Smartphones
- Enable Live Migration
- Additional Security Concerns



VISION

Common framework for applications to be

- Platform Independent
- Secure and Isolated

DESIGN PRINCIPLES

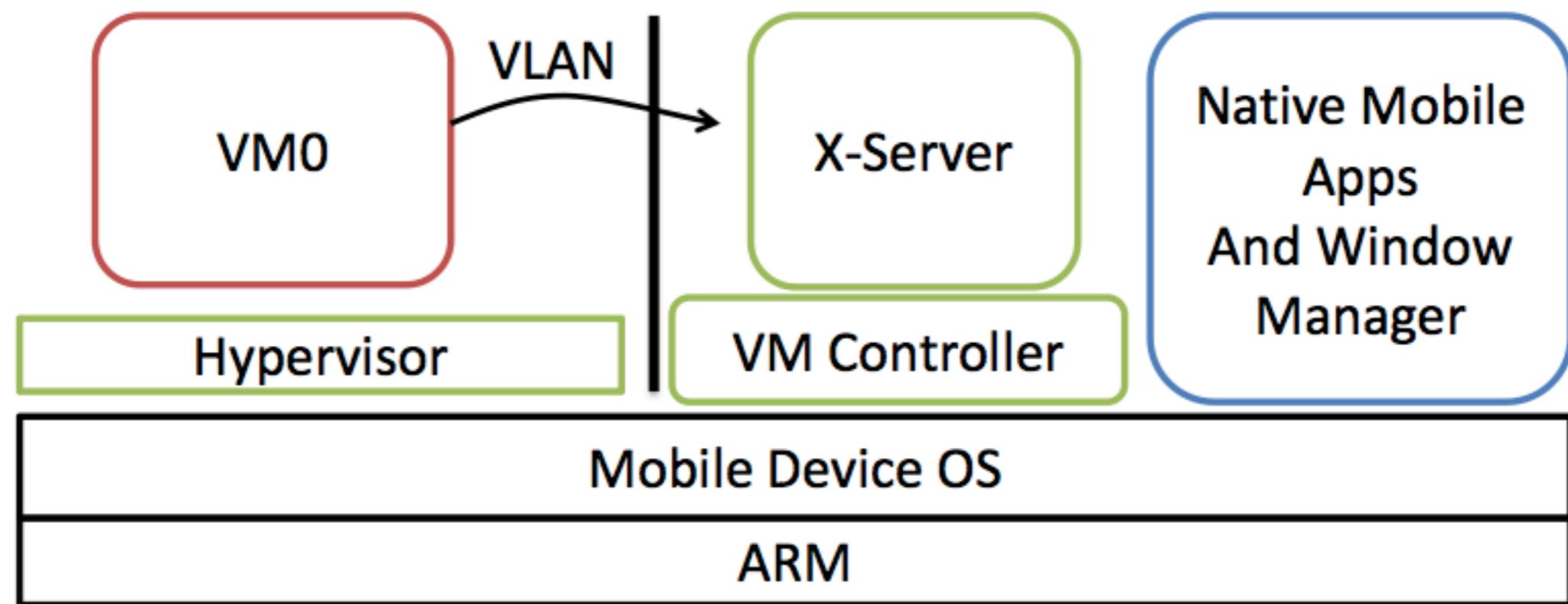
- Isolation

- Separate address space
- Virtualization abstractions protect resources

- Integration

- Usability is important
- Add to the existing device experience

DESIGN

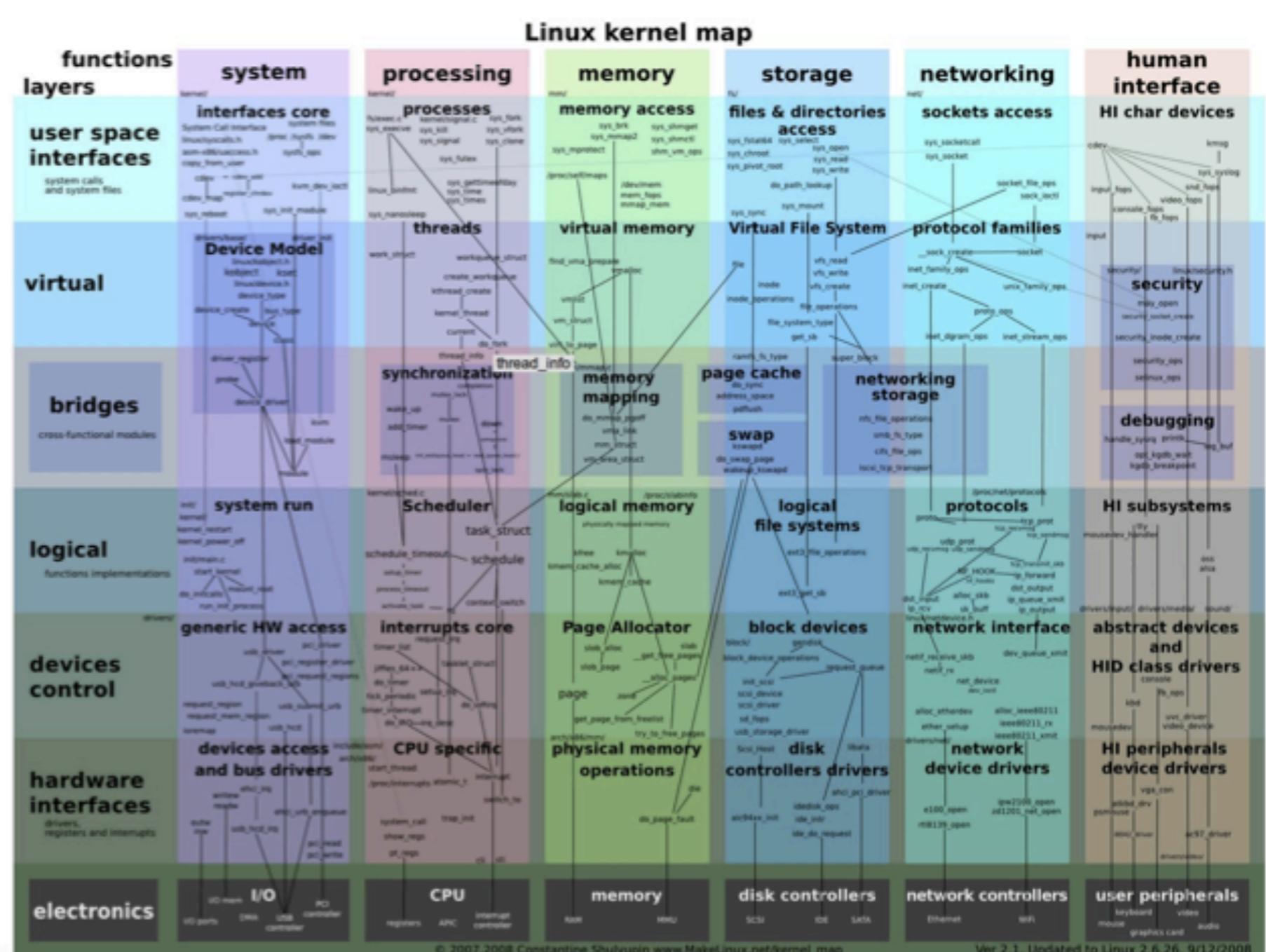


- Integrate apps with Native Window Manager

EXISTING SOLUTIONS

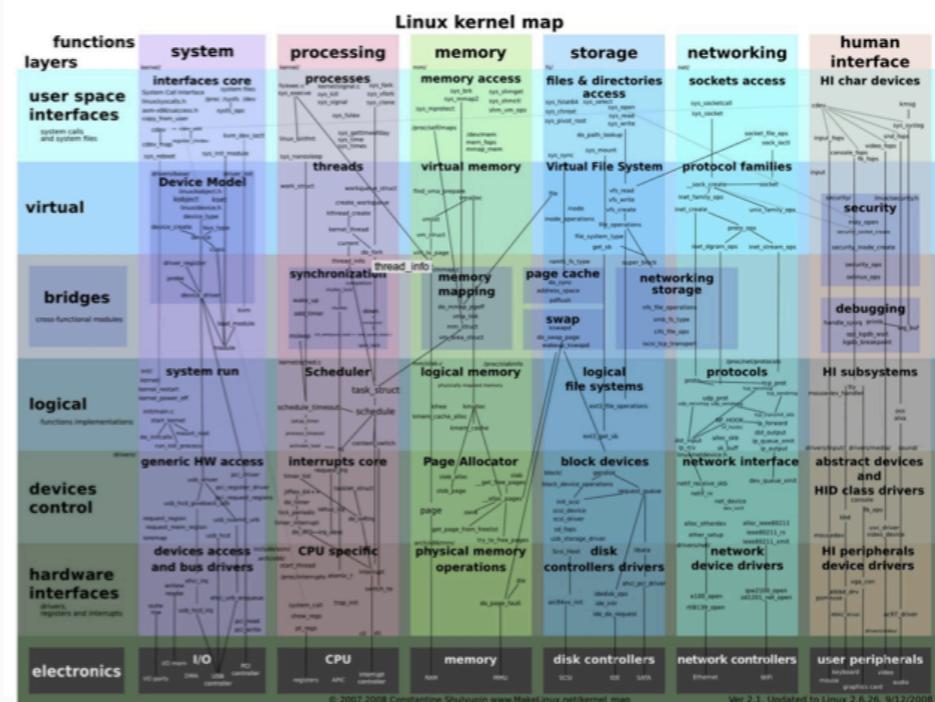
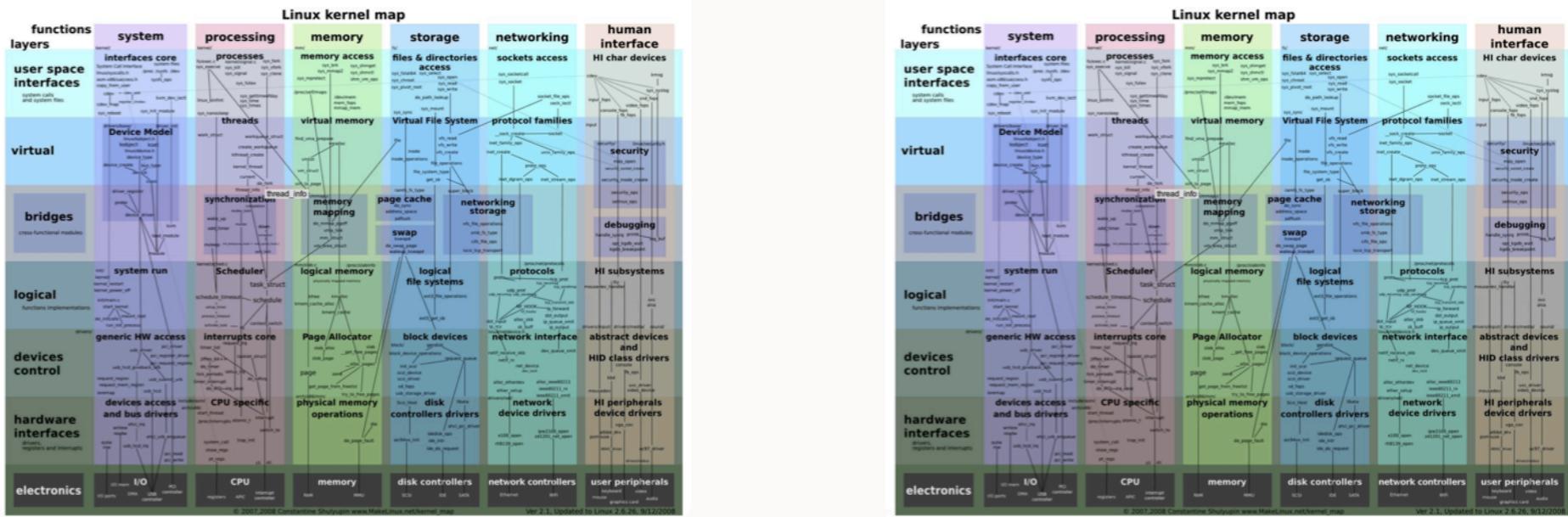
- VMWare MVP, OKL4 - Type 1 Hypervisors
 - Do not integrate with the host OS, but rather replace and contain it.
- KVM, Xen on ARM - Work in progress
 - Dual-boot the OS or require disabling the phone's existing runtime stack.

LINUX



Source: Linux Containers: virtualization without overhead or strange patches

QEMU



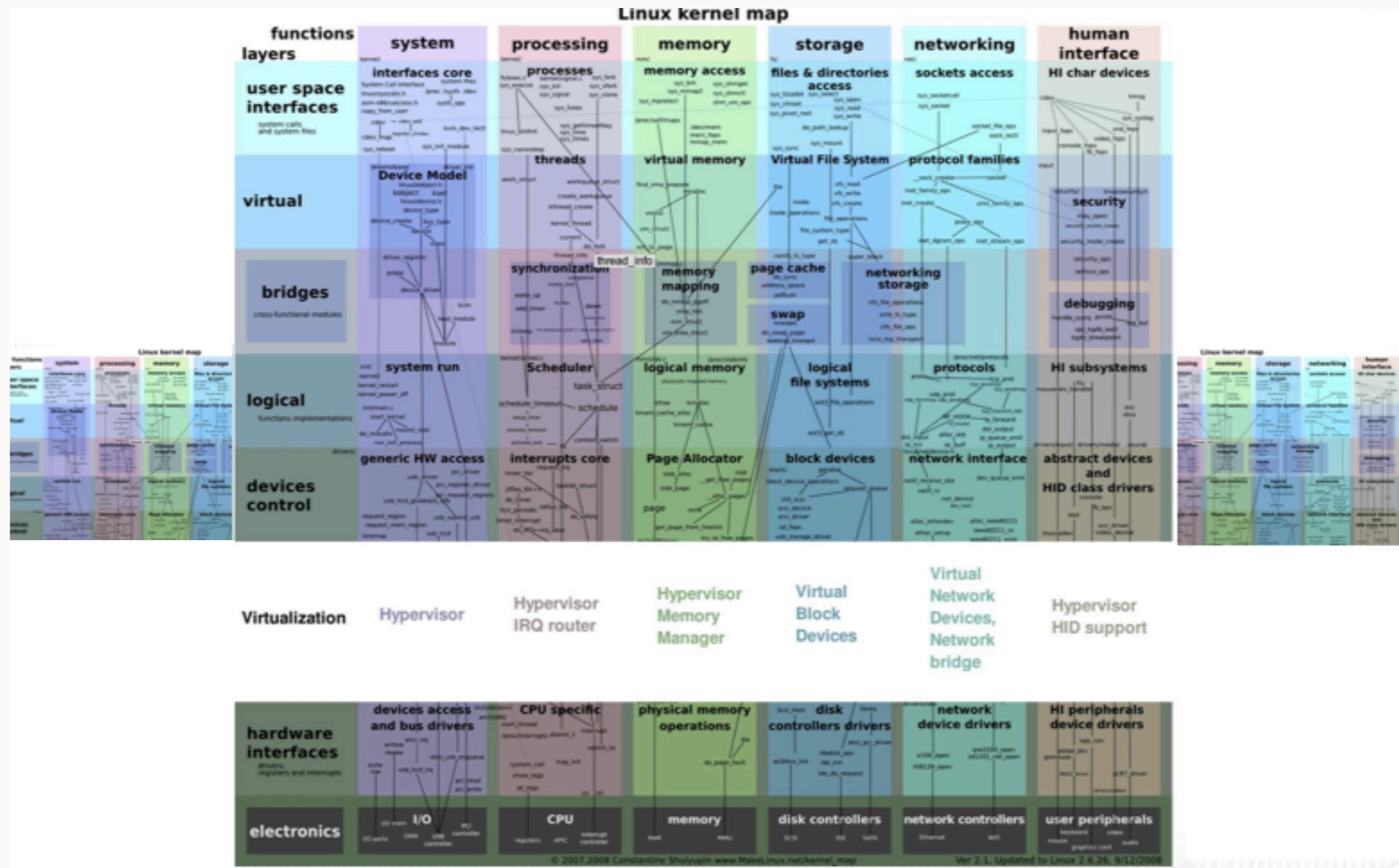
Source: Linux Containers: virtualization without overhead or strange patches

WHY NOT QEMU

Kernel Boot up time in QEMU

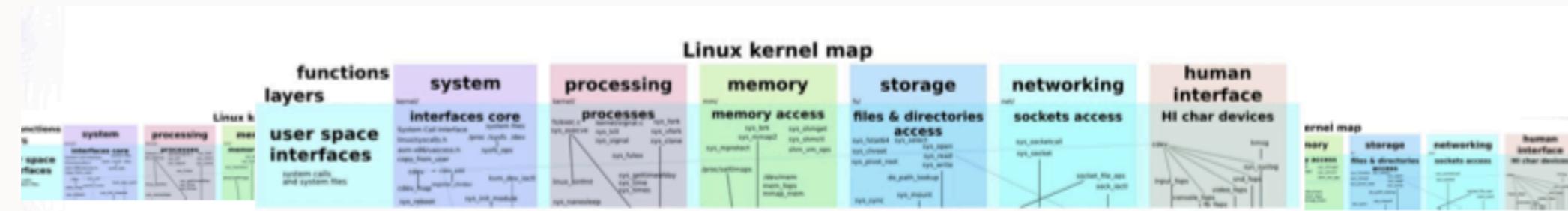
	Palm Pre Cortex - A8 256 MB RAM	Android ARM-1136JS 128 MB RAM
Basic ARM kernel	52 seconds	154 seconds
Debian ARM kernel	19 min 46s	Crashes during boot
TTY-Linux-i486	>30 min	Crashes during boot

KVM/XEN

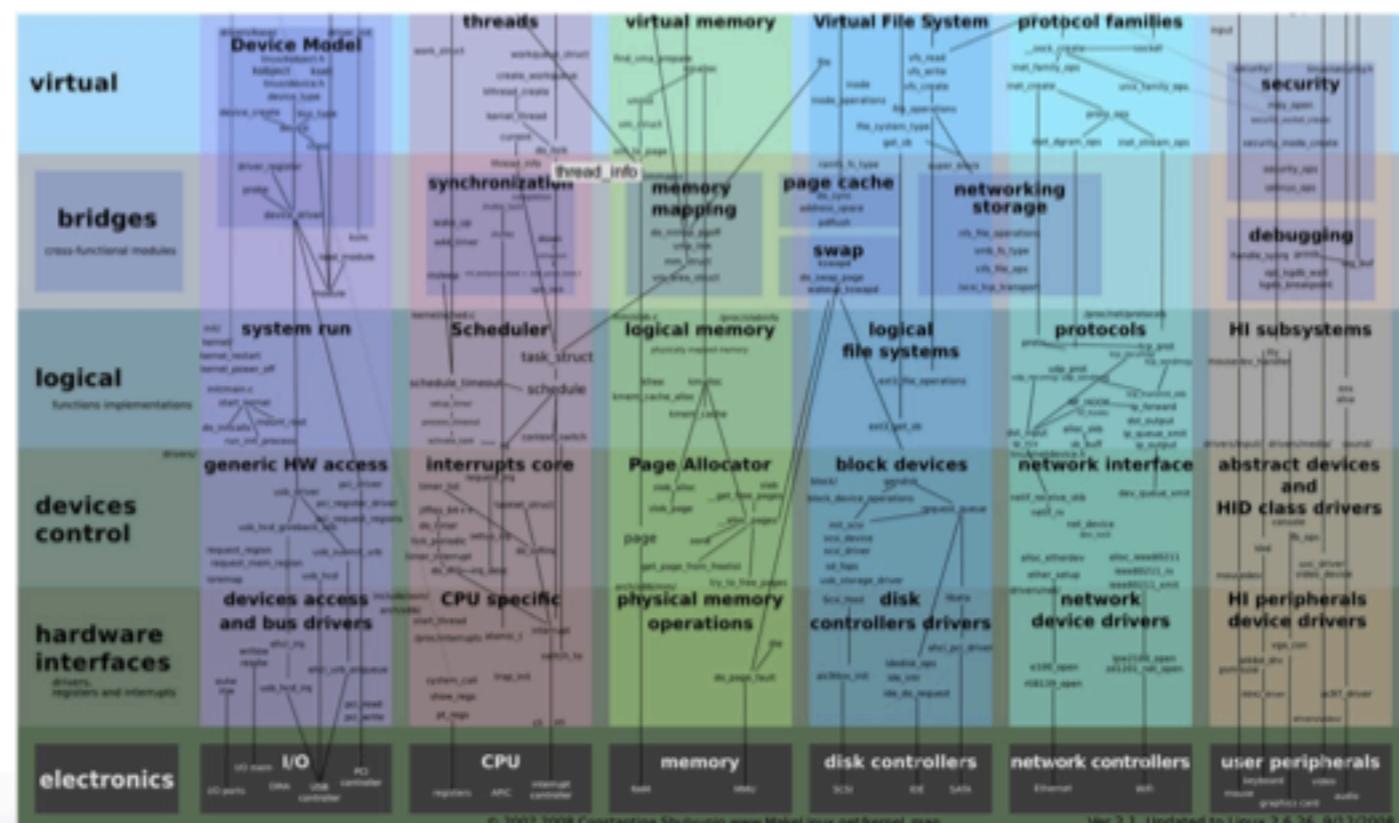


Source: Linux Containers: virtualization without overhead or strange patches

LINUX CONTAINERS



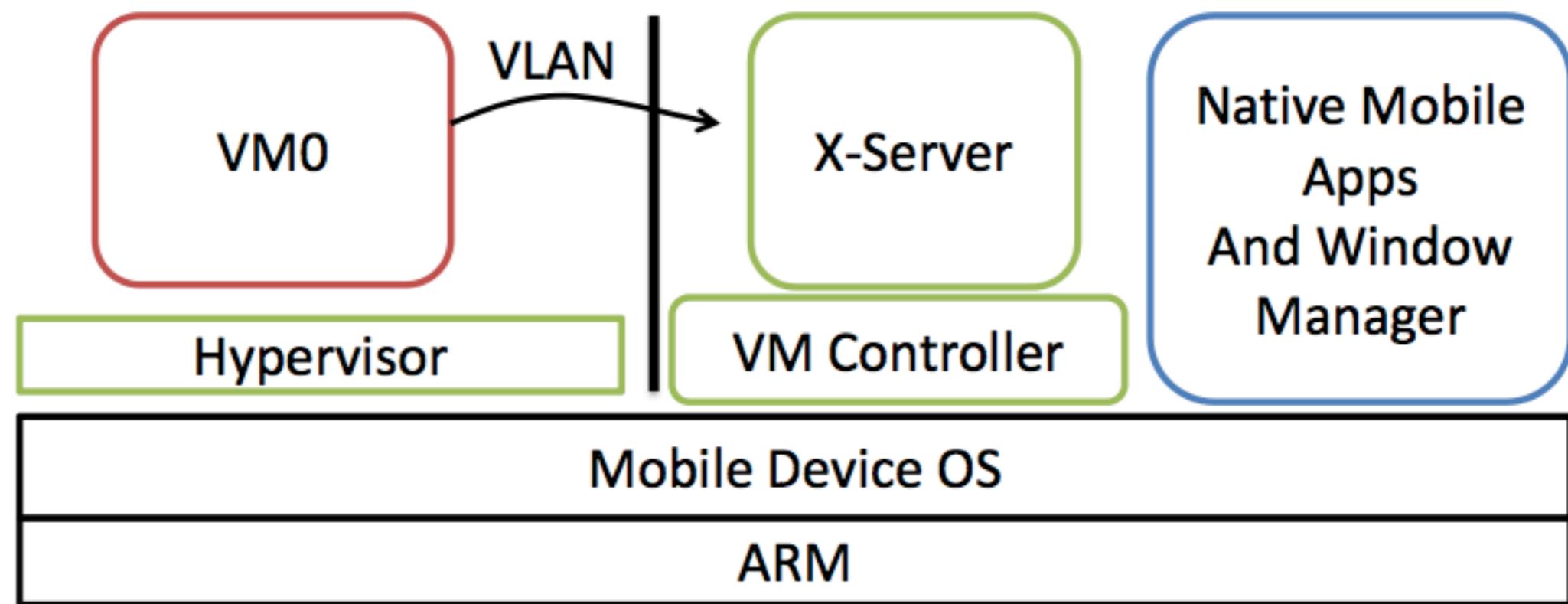
	Virtualization	Process namespace, CPU controller	Memory Controller	Filesystem namespaces, IO controller	Virtual Interfaces or IP restrictions	Clustercuss
Container, namespace, controller						



RESULTS

	Stock Kernel	Modified Kernel	Inside a container
gcc - apache	1229s	1239s	1232s
Prime Number Test	522s	590s	581s
unzip	76s	73.44s	76.29s

DESIGN

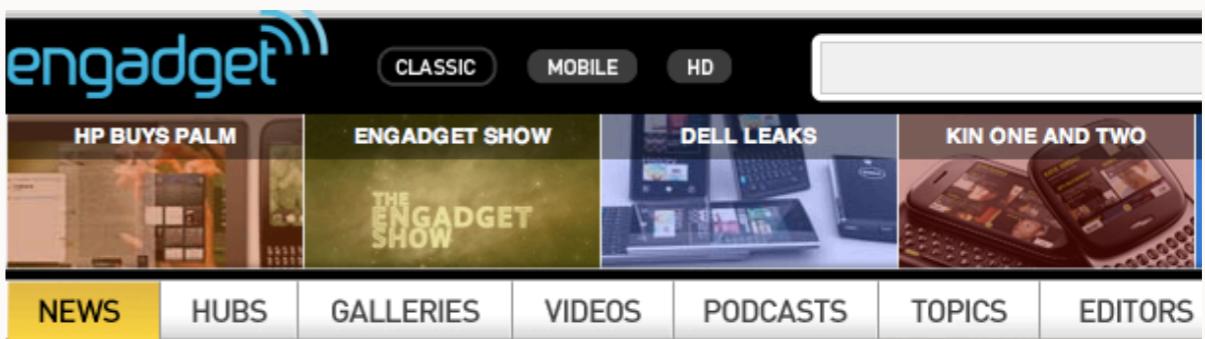


X-SERVER

- Traditional GUI protocol for Linux
- Platform independent
- Integration

XORG ON PALM-PRE

- Contributed Xorg port to Palm Pre Community
www.webos-internals.org



FILED UNDER [Cellphones](#), [Mobile Software](#)

webOS port of Xorg in the works, OpenOffice support the inevitable result

By Chris Ziegler posted Apr 9th 2010 1:59PM

GIZMODO

IPHONE APPS DIRECTORY
ANDROID APPS DIRECTORY

New York, 12:55 AM
Fri Apr 30
36 posts in the last 24 hours
FR IT DE ES PT JP AU
IBR I PL

Get Gizmodo in your inbox:
email address [Join](#)

GIZMODO TEAM
Tip Your Editors:
tips@gizmodo.com

Editorial Director:
Brian Lam | Email

Editor:

Your Palm Pre Can Now Run Basically Any Linux Application

OpenOffice.org on the Palm Pre

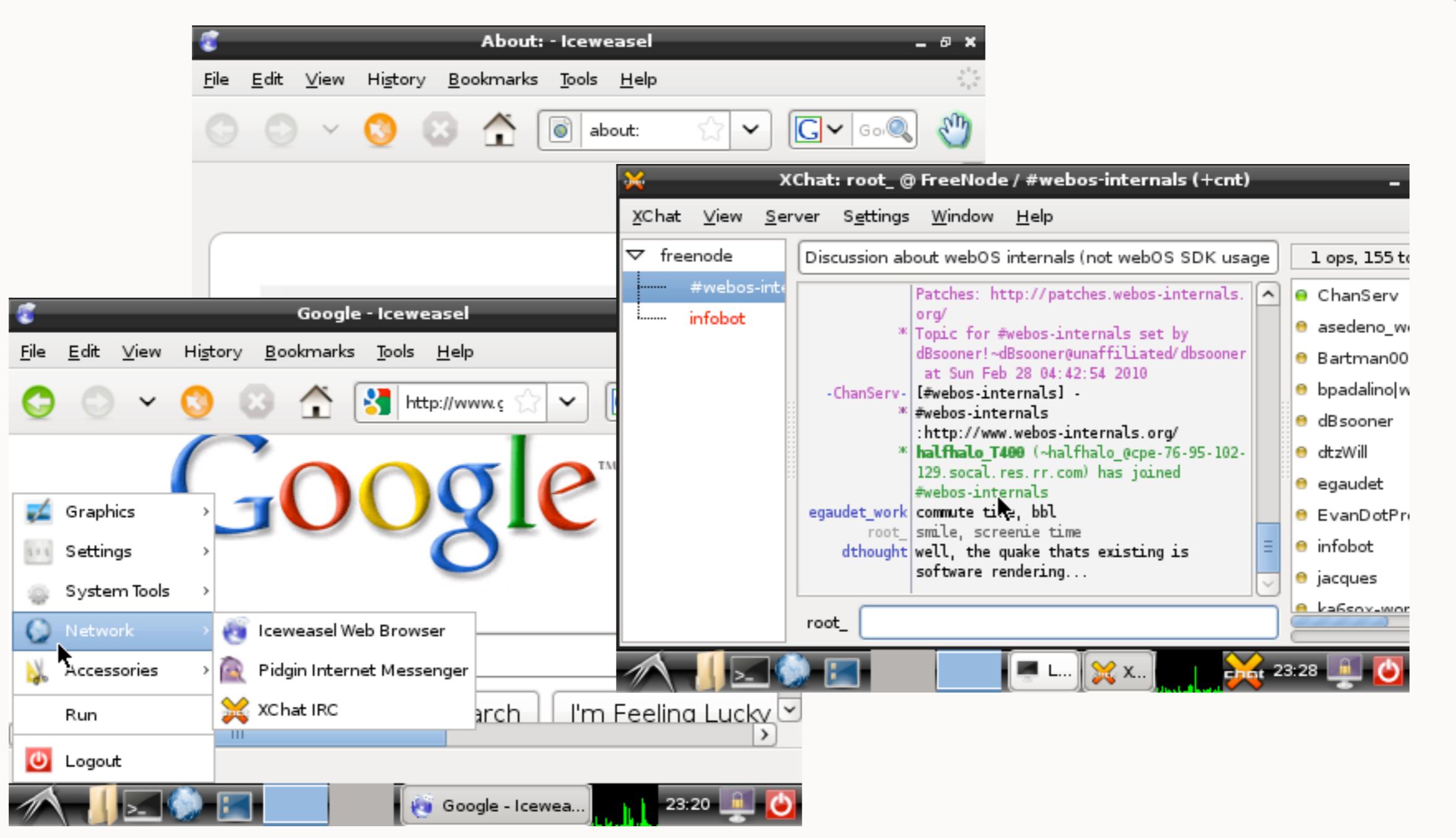


CONCLUSION

- Secure and Portable applications are the future
- Linux Containers and X11 provide the necessary framework
- Future Work:
 - Live Migration using xpra
 - Linux containers - 2.6.33
- Public Git Repo: <http://wdtz.org/cs523>

QUESTIONS

XORG SCREENSHOT



CONTAINERS SCREENSHOT

```
root@container1:/# ps ax
PID TTY      STAT   TIME COMMAND
 1 ?        S<     0:00 /bin/sh /media/internal/v
 18 ?       R<    0:00 /usr/local/bin/xterm -geo
 19 pts/0    R<s   0:00 sh
 20 pts/0    R<+   0:00 ps ax
root@container1:/# 
```

In a container

ps ax

```
Terminal ▾ 10:29
1043 ?      Ss1   0:00 /usr/bin/PmNetConfigManager
1053 ?      Ss    0:00 /usr/bin/rdxd -s
1061 ?      S<s1  0:10 /usr/bin/hidd -v -f /etc/h
1072 ?      Ss    0:00 /usr/sbin/storaged -s -d
1074 ?      Ss    0:00 /usr/bin/uploadd -v
1087 ?      Ss    0:00 /usr/bin/provisioner
1089 ?      Ss    0:00 /usr/bin/UpdateDaemon
1106 ?      Ss1   0:00 BluetoothMonitor
1116 ?      S<s   0:00 /usr/sbin/audiod -n -1
1142 ?      Ss    0:00 /var/usr/sbin/org.webosint
1150 ?      Ss    0:00 /usr/bin/nappmgr
1182 ?      Ss1   0:00 /usr/bin/PmLanDaemon
1190 ?      Ss1   0:59 /usr/lib/jvm/java-1.5-palm
1201 ?      Ss    0:01 /usr/bin/LunaSysService
1207 ?      Ss    0:00 /usr/bin/LunaDownloadMgr
1220 ?      Ss    0:00 /usr/bin/luna-prefs-service
1223 ?      Ss    0:00 /usr/bin/extractfs -f /var
1225 ?      SNs1  0:11 /usr/bin/fileindexer
1227 ?      SNs   0:00 /opt/sbin/sshd -D -p 22 -o
1229 ?      Ss    0:08 /usr/sbin/powerd
1232 ?      S<s1  0:05 /usr/bin/pulseaudio --log-
1234 ?      Ss    0:00 /usr/sbin/memchute
1236 ?      Ss    0:11 /usr/bin/PmWiFiService
1238 ?      S<ls1  3:00 /usr/bin/LunaSysMgr -s
1244 ?      Ss    0:00 /usr/bin/dnsmasq -d --enable
1250 ?      Ss    0:02 /usr/bin/pubsubservice
1254 ?      Ss    0:01 /usr/bin/BrowserServer
1262 ?      Ss1   0:01 /usr/bin/TelephonyInterface
1329 ?      S1    0:00 /usr/bin/PmBtStack -C /dev
1365 ?      Ss    0:00 /var/usr/sbin/org.webosint
1493 ?      S<
1520 ?      Ss    0:00 /usr/sbin/wpa_supplicant -
1615 ttymACM0 Ss+   0:00 pppd /dev/tts/modem0 file
1751 ?      S     0:00 /usr/bin/contextupload
2186 ?      S<s1  0:00 /usr/bin/mediaserver --gst
2255 ?      S     0:00 /sbin/dhclient -d -cf /etc
2946 ?      S<
2951 ?      SNI   0:01 Xsd1 -noreset -nolisten tc
2960 ?      S<
2961 ?      S<
2978 ?      S<
2979 pts/0    S<s+  0:00 sh
2983 pts/1    S<s   0:00 -sh
2988 pts/1    R<+   0:00 ps ax
root@palm-webos-device:/var/home/root# 
```

Outside container