

SECURE APPLICATIONS ON MOBILE DEVICES

Will Dietz, Kevin Larson
Shivaram Venkataraman

SMARTPHONE SECURITY

Motivation

- Smartphones are the target of Malware attacks

FAST COMPANY

TECHNOLOGY DESIGN ETHONOMICS LEADERSHIP MAGAZINE | NEWSLETTERS |

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 lusting 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 portion of the MacNN website. At the top, there is a search bar with the MacNN logo and the tagline "read me first". Navigation buttons for "mac news", "reviews", "blogs", "forums", and "services" are visible. Below the navigation, there is a "Hot Stories" section with the headline "Adobe releases Flash for Mac beta with GPU acceleration". The main article is titled "Sec. expert: Apple's iPhone security claims 'exaggerated'" and is dated "updated 11:55 am EST, F". The article text discusses the iPhone's security, mentioning a software engineer and security specialist, Nicolas Seriot, who claims that the iPhone OS's sandboxing is "way too loose." The article also mentions that several apps, such as Aurora Feint and mogoRo, were initially approved by Apple but later found to have security vulnerabilities. A demonstration app called SpyPhone is mentioned as being able to reveal e-mail addresses, user names, Safari and YouTube searches, and server information, as well as Wi-Fi networks, phone numbers, and call logs.

macnn
read me first

mac news reviews blogs forums services

Hot Stories Adobe releases Flash for Mac beta with GPU acceleration

macnn news

Sec. expert: Apple's iPhone security claims 'exaggerated'
Decries iPhone sandboxing updated 11:55 am EST, F

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 apps 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.

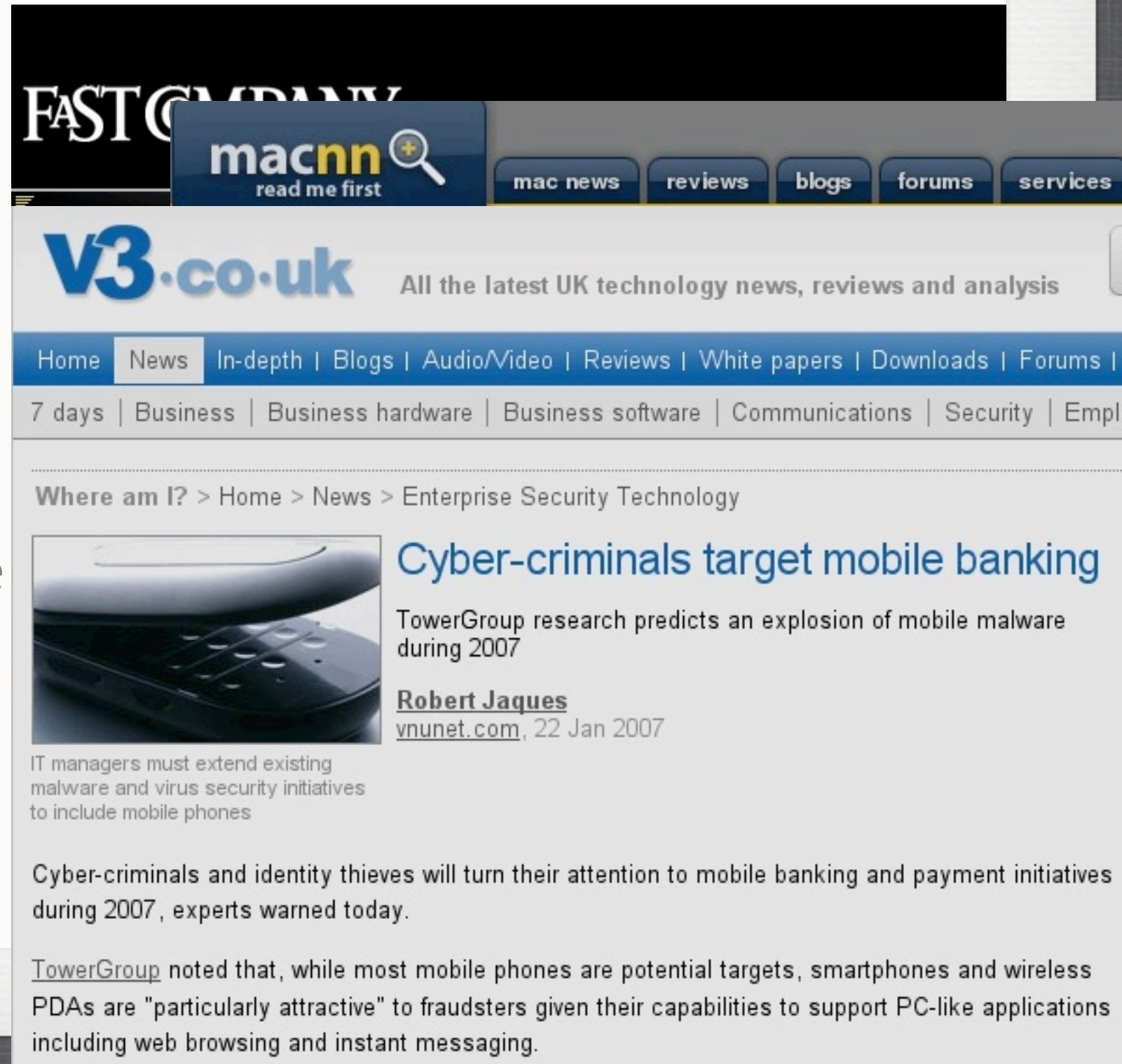
Proof of the vulnerability is said to lie with several apps, such as Aurora Feint and mogoRo. Both were initially approved by Apple yet quietly stole phone and e-mail contacts before eventually being blocked from the App Store. Apple's review process can and does miss security problems, Seriot pointed 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 app 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 location services.

SMARTPHONE SECURITY

Motivation

- Smartphones are the target of Malware attacks



The screenshot shows a news article from V3.co.uk. The page header includes the V3.co.uk logo and the tagline "All the latest UK technology news, reviews and analysis". A navigation menu lists categories like Home, News, In-depth, Blogs, Audio/Video, Reviews, White papers, Downloads, and Forums. The article title is "Cyber-criminals target mobile banking" by Robert Jaques, dated 22 Jan 2007. The article text discusses TowerGroup research predicting an explosion of mobile malware during 2007 and notes that cyber-criminals and identity thieves will target mobile banking and payment initiatives. It also mentions that smartphones and wireless PDAs are particularly attractive to fraudsters.

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

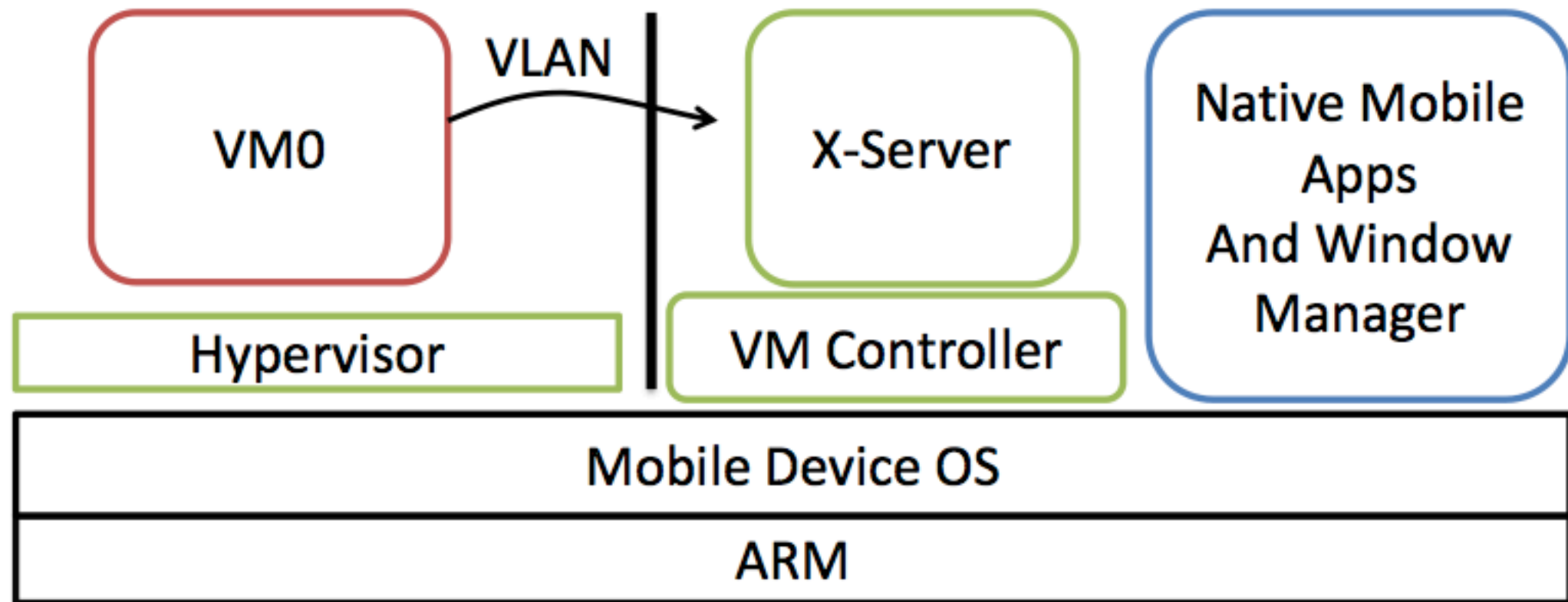
Common framework for applications to be

- 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

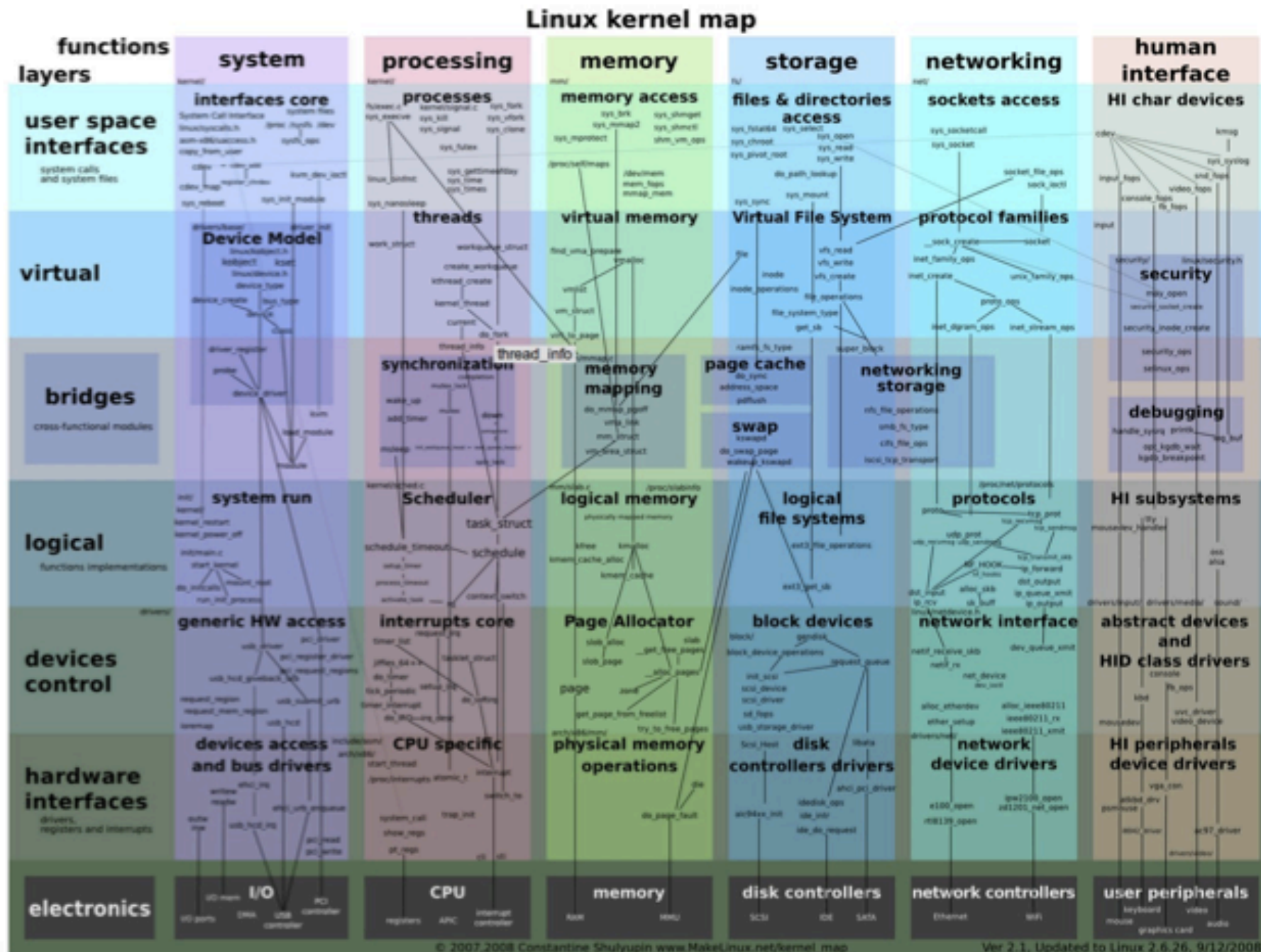


- Integrate apps with Native Window Manager

EXISTING SOLUTIONS

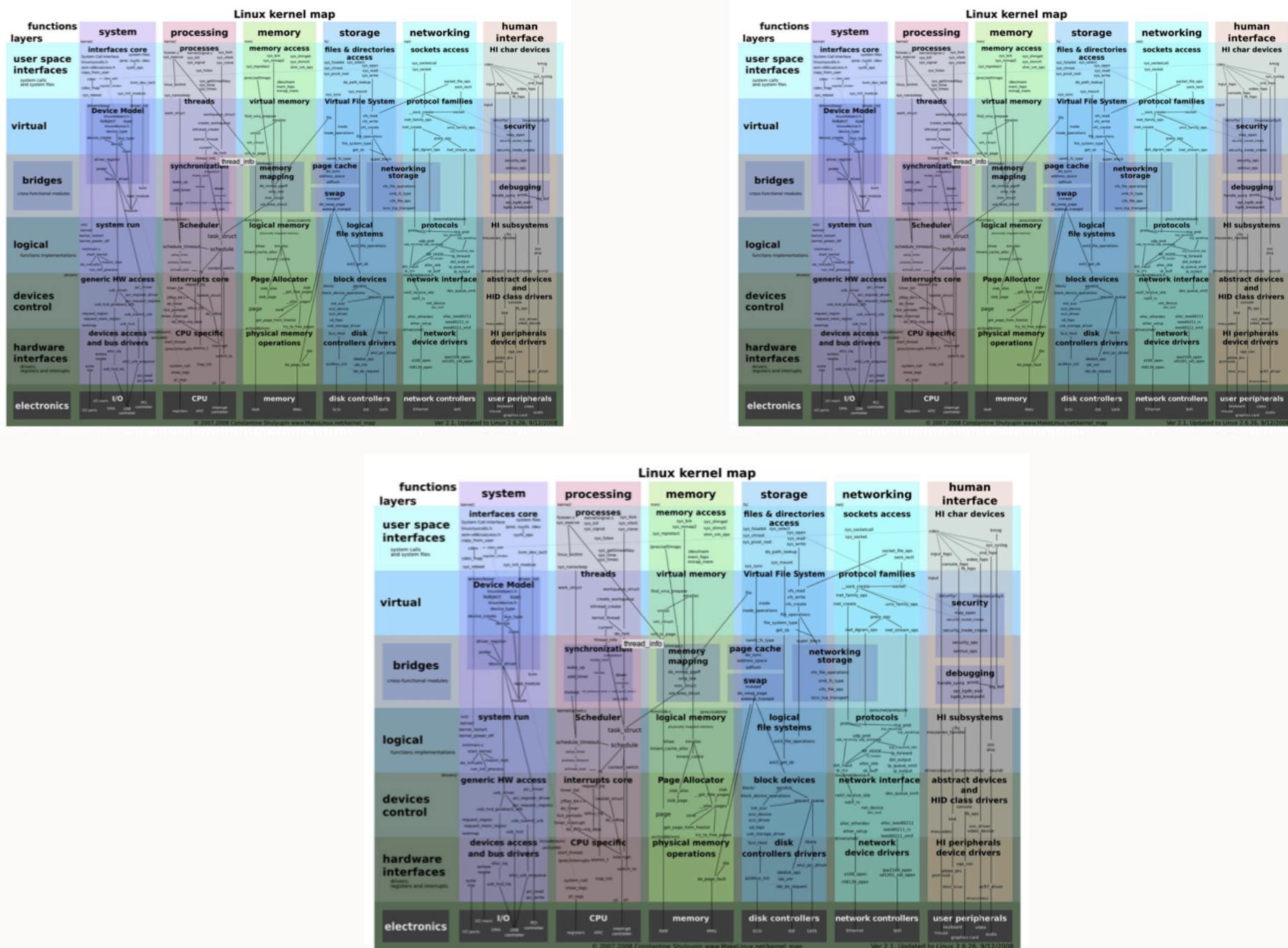
- VMWare MVP, OKL4 - Type 1 Hypervisors
 - Do not integrate with the host OS, but rather replace and contain it.
- KVM, Xen on ARM - Work in progress
 - Dual-boot the OS or require disabling the phone's existing runtime stack.

LINUX



Source: Linux Containers: virtualization without overhead or strange patches

QEMU



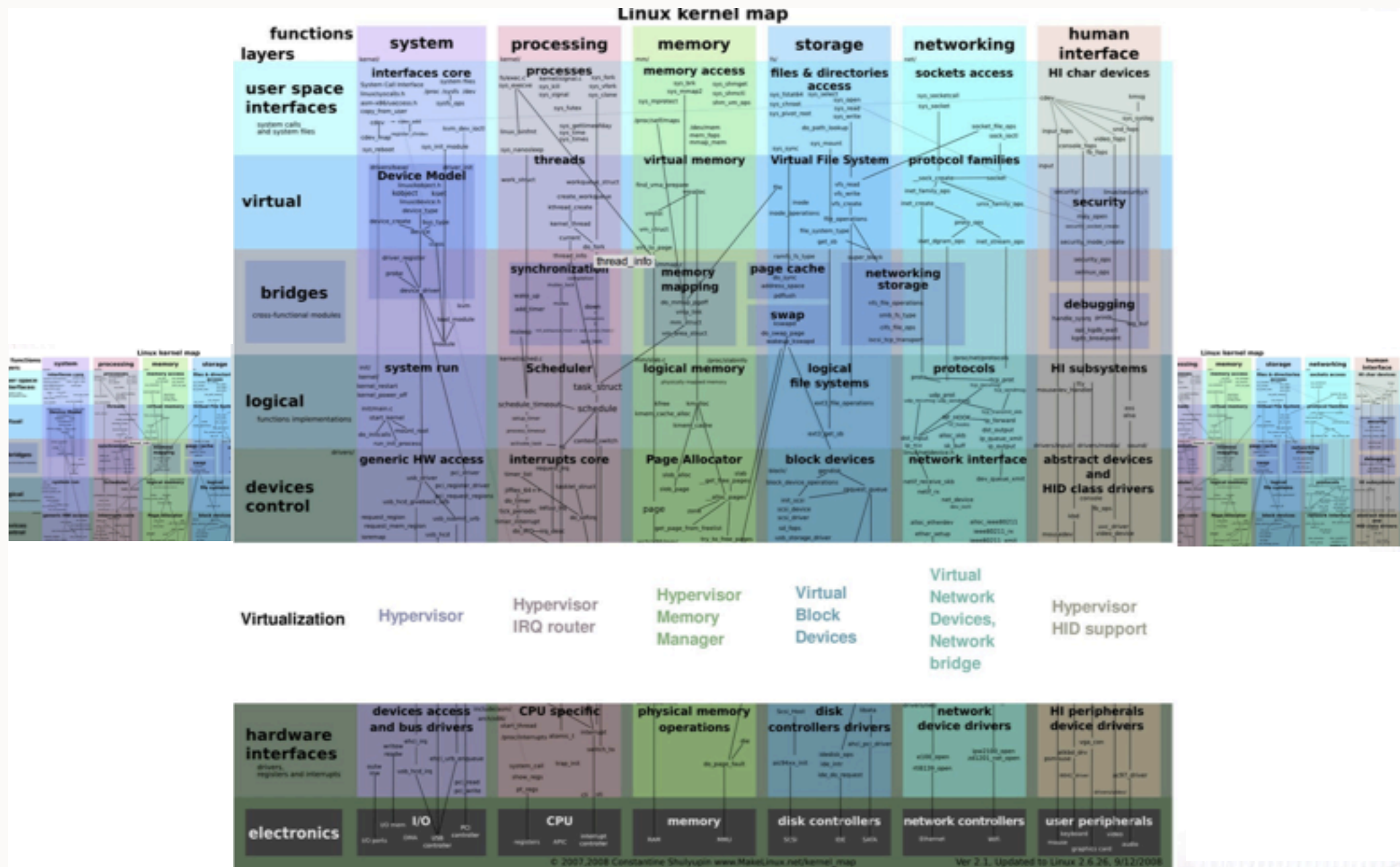
Source: Linux Containers: virtualization without overhead or strange patches

WHY NOT QEMU

Kernel Boot up time in QEMU

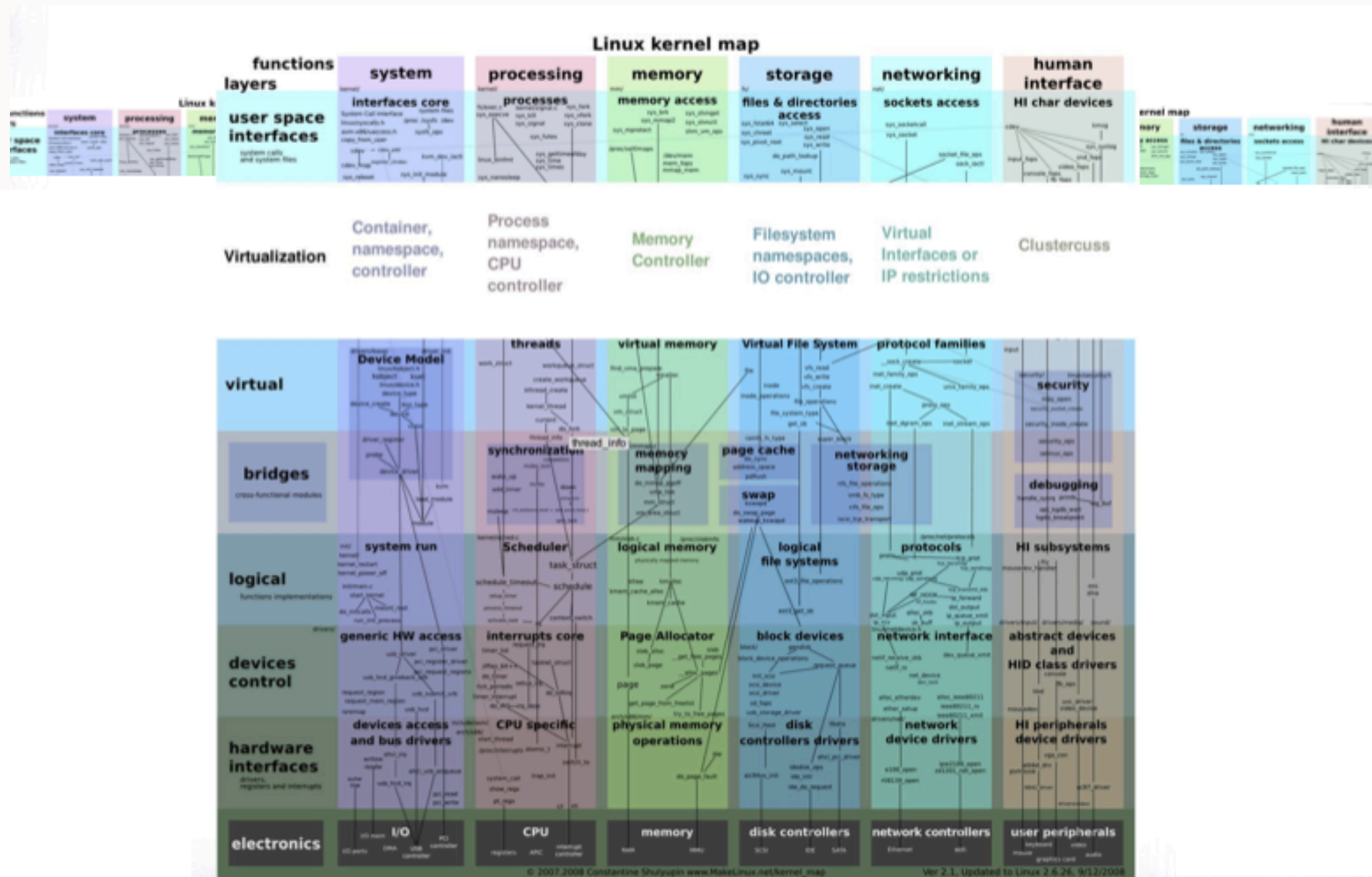
	Palm Pre Cortex - A8 256 MB RAM	Android ARM-1136JS 128 MB RAM
Basic ARM kernel	52 seconds	154 seconds
Debian ARM kernel	19 min 46s	Crashes during boot
TTY-Linux-i486	>30 min	Crashes during boot

KVM/XEN



Source: Linux Containers: virtualization without overhead or strange patches

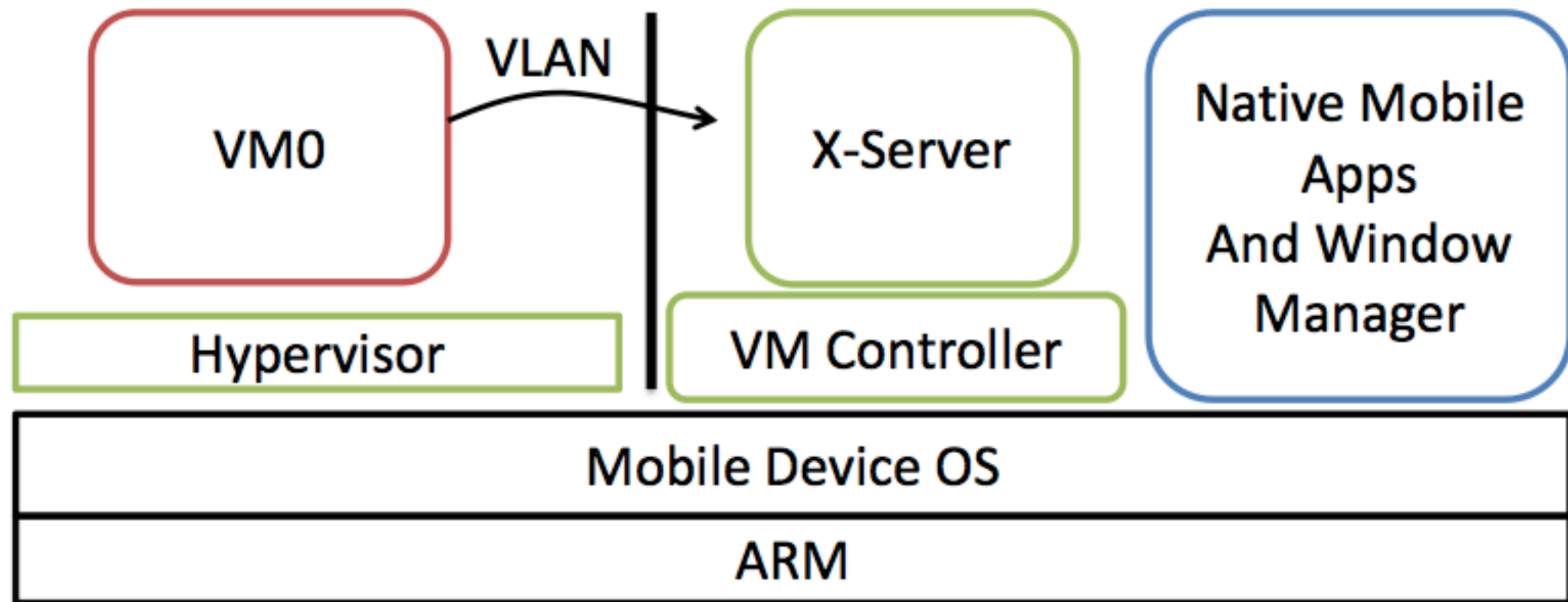
LINUX CONTAINERS



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

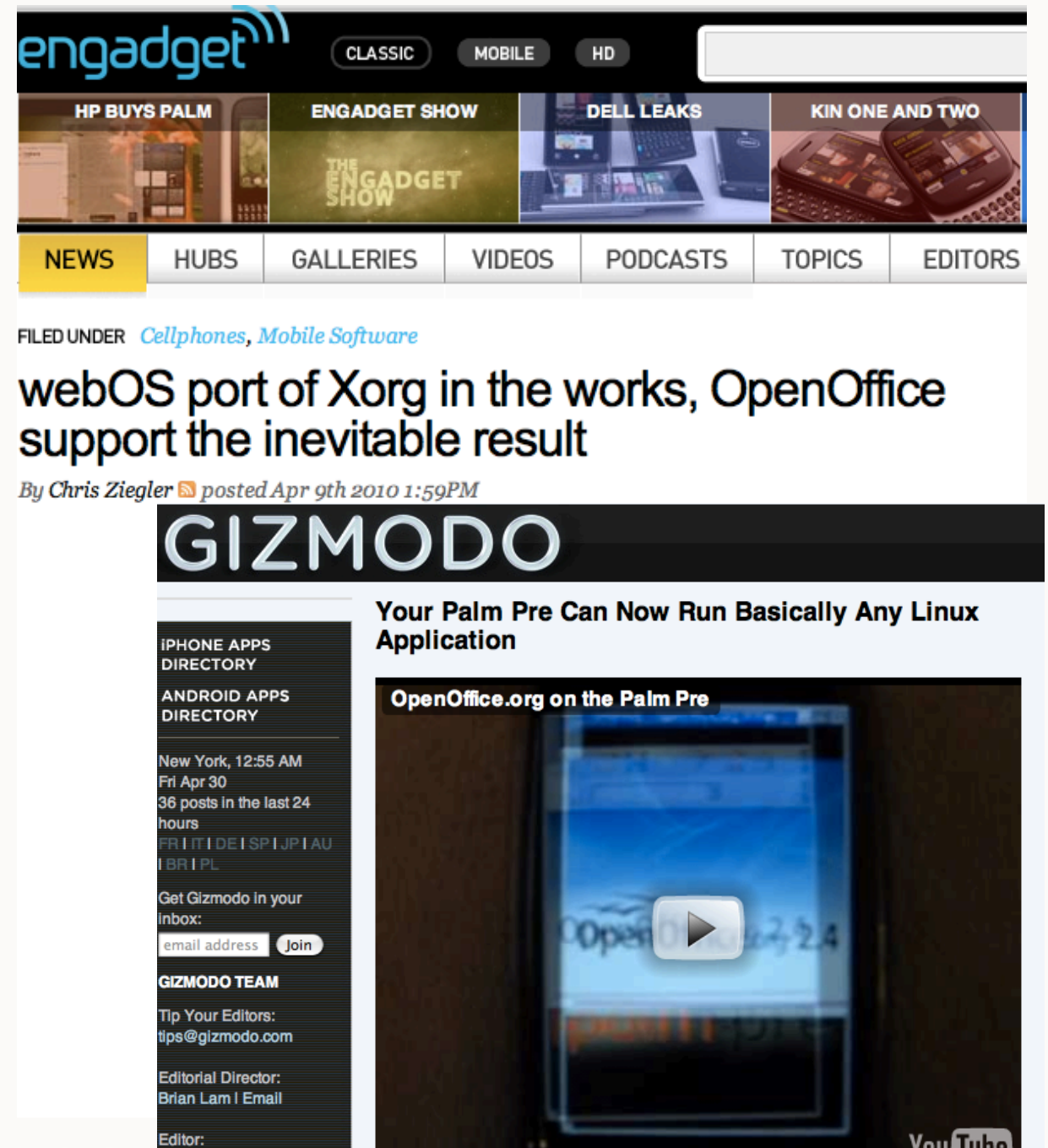


X-SERVER

- Traditional GUI protocol for Linux
- Platform independent
- Integration

XORG ON PALM-PRE

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

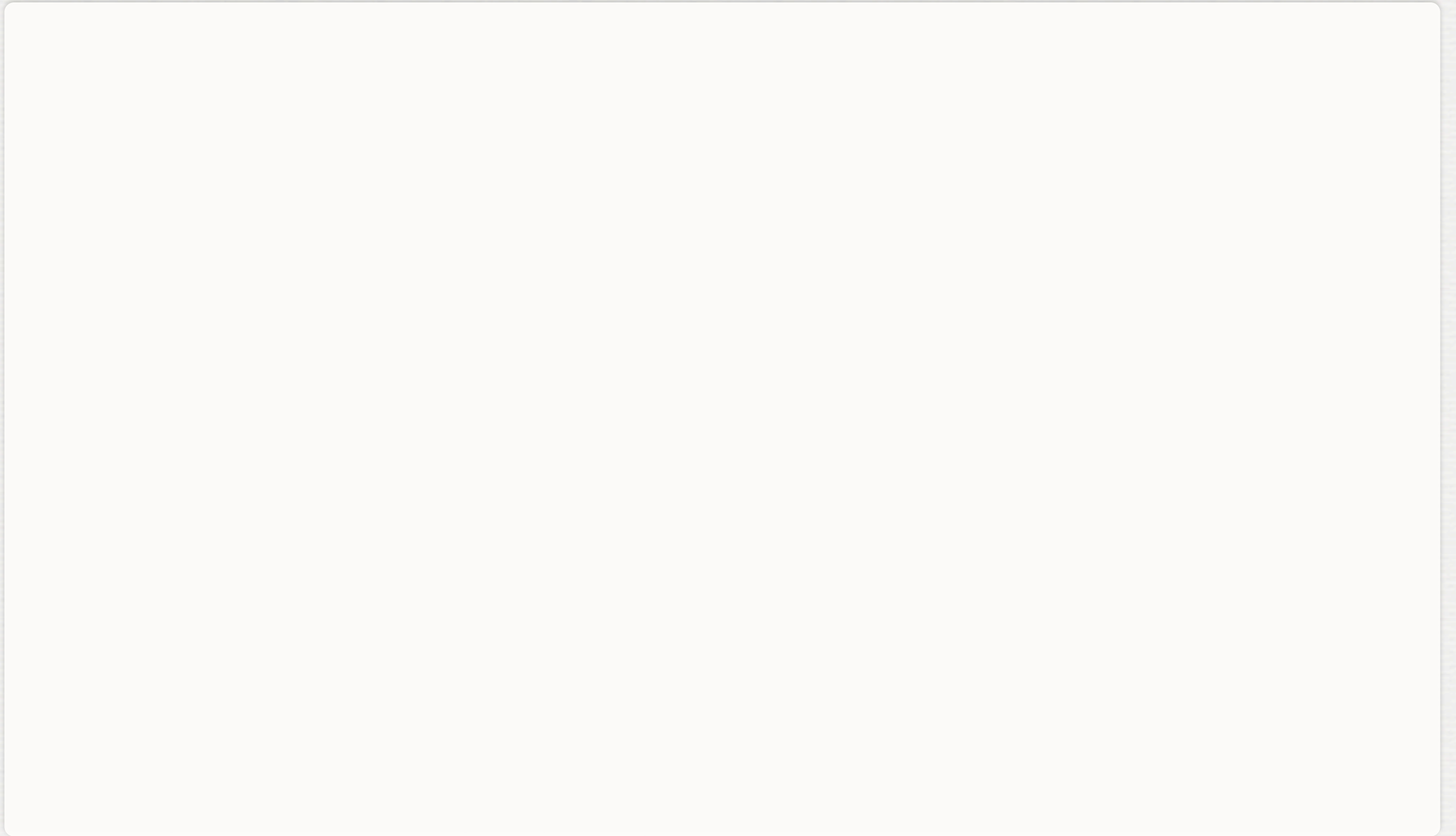


The screenshot shows the Engadget website interface. At the top, the Engadget logo is on the left, and navigation buttons for 'CLASSIC', 'MOBILE', and 'HD' are on the right. Below the logo are four featured article thumbnails: 'HP BUYS PALM', 'ENGADGET SHOW', 'DELL LEAKS', and 'KIN ONE AND TWO'. A horizontal menu below the thumbnails includes 'NEWS', 'HUBS', 'GALLERIES', 'VIDEOS', 'PODCASTS', 'TOPICS', and 'EDITORS'. The main content area features a news article titled 'webOS port of Xorg in the works, OpenOffice support the inevitable result' by Chris Ziegler, posted on April 9th, 2010. Below the article is a Gizmodo advertisement with the headline 'Your Palm Pre Can Now Run Basically Any Linux Application' and a video player showing 'OpenOffice.org on the Palm Pre'. The Gizmodo sidebar on the left contains a directory for iPhone and Android apps, a social media feed snippet, and contact information for the Gizmodo team.

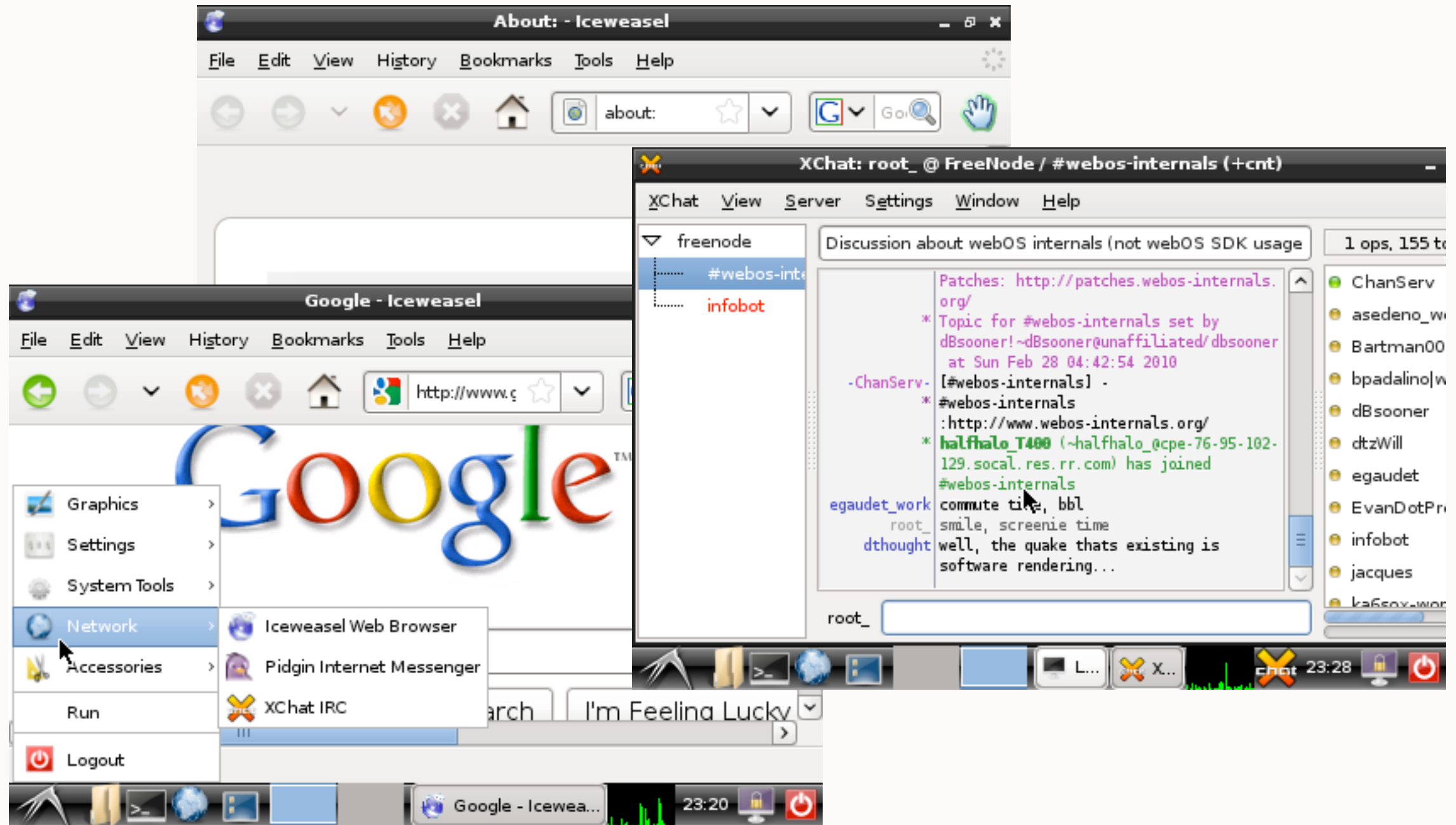
CONCLUSION

- 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<+   0:00 sh
 20 pts/0    R<+   0:00 ps ax
root@container1:/#
```

In a container

ps ax

```
Terminal 10:29
1043 ?      Ss     0:00 /usr/bin/PmNetConfigManag
1053 ?      Ss     0:00 /usr/bin/rxdx -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/PmWanDaemon
1190 ?      Ss1    0:59 /usr/lib/jvm/java-1.5-palm
1201 ?      Ss     0:01 /usr/bin/LunaSystemService
1207 ?      Ss     0:00 /usr/bin/LunaDownloadMgr
1220 ?      Ss     0:00 /usr/bin/luna-prefs-servic
1223 ?      Ss     0:00 /usr/bin/extractfs -f /var
1225 ?      Ss1    0:11 /usr/bin/fileindexer
1227 ?      Ss     0:00 /opt/sbin/sshd -D -p 22 -o
1229 ?      Ss1    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 --enab
1250 ?      Ss     0:02 /usr/bin/pubsubservice
1254 ?      Ss     0:01 /usr/bin/BrowserServer
1262 ?      Ss1    0:01 /usr/bin/TelephonyInterfac
1329 ?      S1     0:00 /usr/bin/PmBtStack -C /dev
1365 ?      Ss     0:00 /var/usr/sbin/org.webosint
1493 ?      S<     0:01 [wlan_main_servi]
1520 ?      Ss     0:00 /usr/sbin/wpa_supplicant -
1615 ttyACM0 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<     0:00 /bin/sh -l /media/cryptofs
2951 ?      S1     0:01 Xsdl -noreset -nolisten tc
2960 ?      S<     0:00 /media/internal/vmctl/newri
2961 ?      S<     0:00 /bin/sh /media/internal/vm
2978 ?      S<     0:00 /usr/local/bin/xterm -geom
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