Taming the Robots: The L4Android Framework

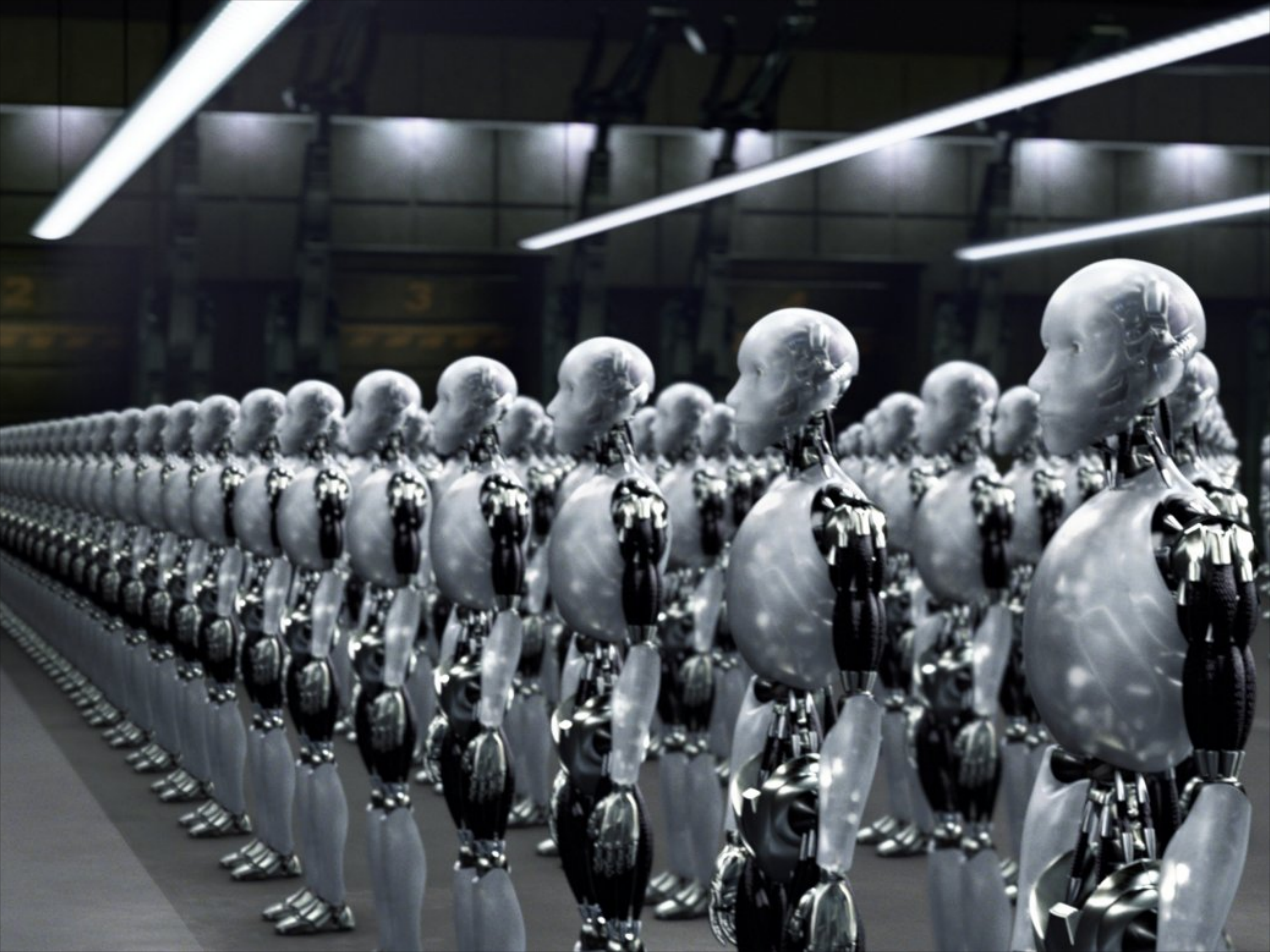
Matthias Lange, MOS, January 14th, 2014
matthias.lange@kernkonzept.com

Who am I?

Embedded Systems Developer at Bosch

Security Researcher at TU Berlin

Senior OS Engineer at Kernkonzept GmbH



2
3
4

PLEASE DO NOT
SCULPTURE STILL
UNDER
CONSTRUCTION
THANK YOU

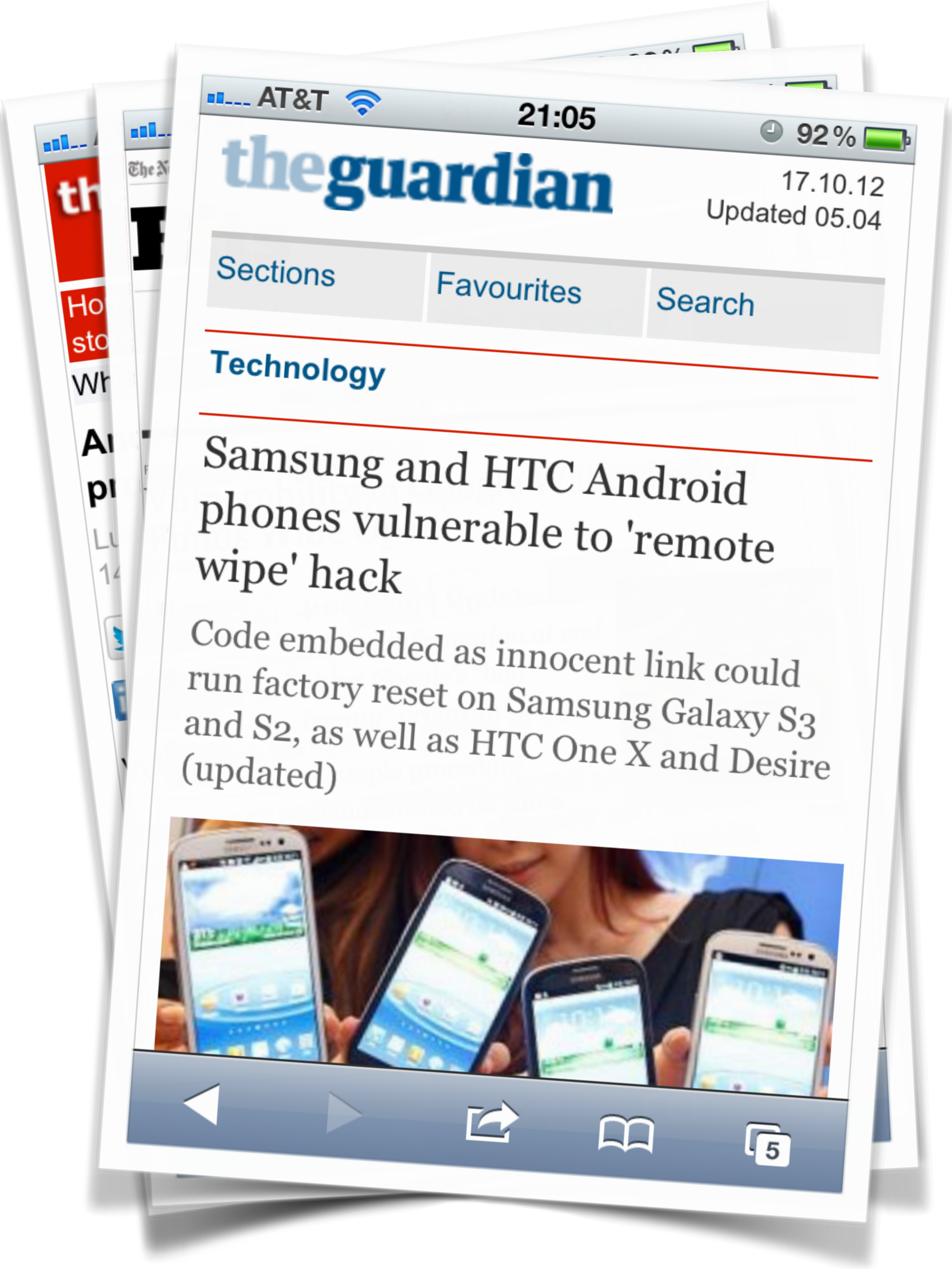
Motivation

Device Accumulation

- Private
- Business
- Development
- You name it

Security

- Emerging threats
- Existing OS not secure
- Future applications
    - eHealth
    - Mobile payment (NFC)
    - Encrypted voice and text



17.10.12
Updated 05.04

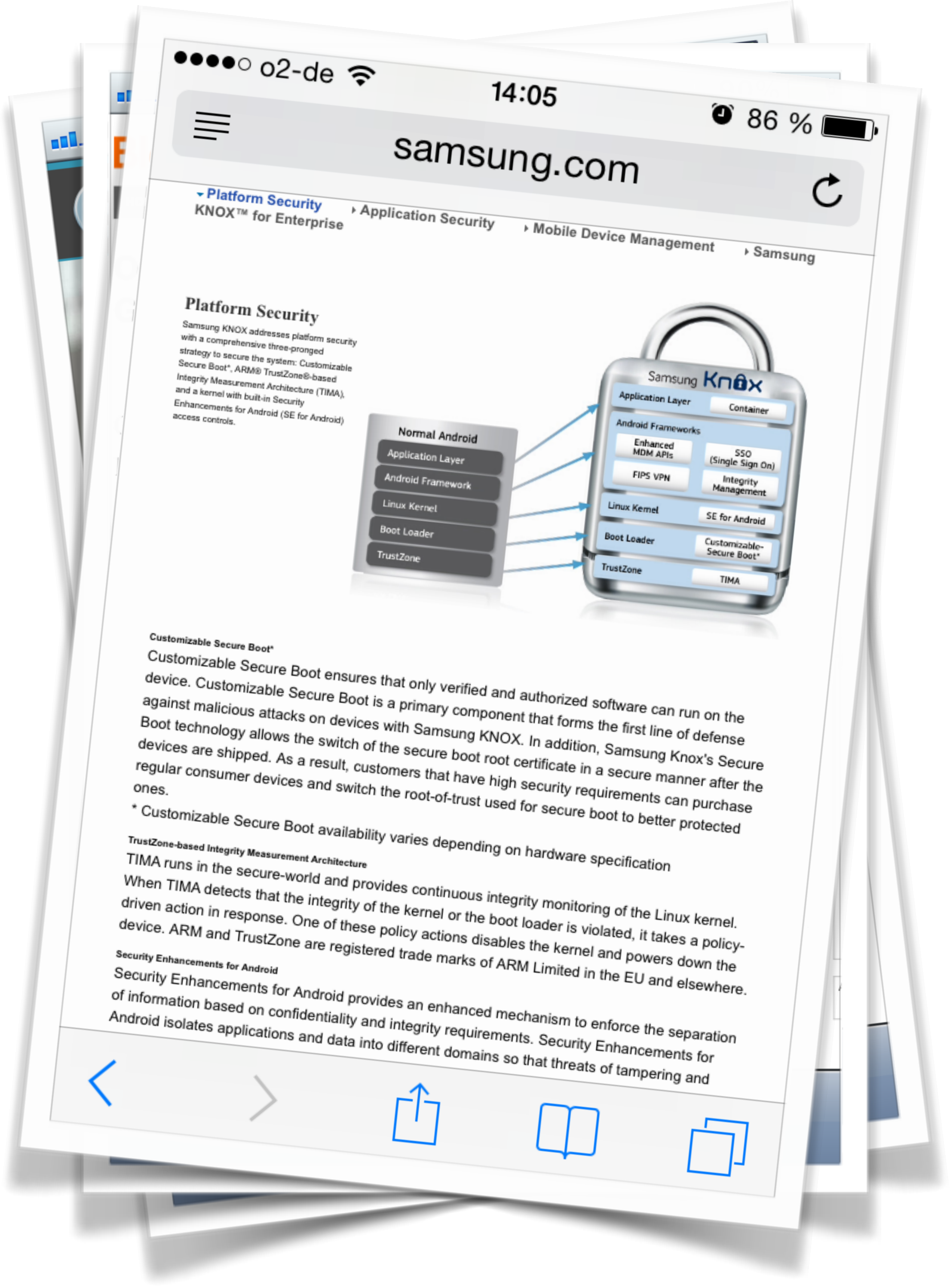
Technology

Samsung and HTC Android phones vulnerable to 'remote wipe' hack

Code embedded as innocent link could run factory reset on Samsung Galaxy S3 and S2, as well as HTC One X and Desire (updated)

Security cont.

- "Everybody" wants its own secure smartphone
- Governments
- Businesses



Platform Security

Samsung KNOX addresses platform security with a comprehensive three-pronged strategy to secure the system: Customizable Secure Boot*, ARM® TrustZone®-based Integrity Measurement Architecture (TIMA), and a kernel with built-in Security Enhancements for Android (SE for Android) access controls.

Customizable Secure Boot*

Customizable Secure Boot ensures that only verified and authorized software can run on the device. Customizable Secure Boot is a primary component that forms the first line of defense against malicious attacks on devices with Samsung KNOX. In addition, Samsung Knox's Secure Boot technology allows the switch of the secure boot root certificate in a secure manner after the devices are shipped. As a result, customers that have high security requirements can purchase regular consumer devices and switch the root-of-trust used for secure boot to better protected ones.

* Customizable Secure Boot availability varies depending on hardware specification

TrustZone-based Integrity Measurement Architecture

TIMA runs in the secure-world and provides continuous integrity monitoring of the Linux kernel. When TIMA detects that the integrity of the kernel or the boot loader is violated, it takes a policy-driven action in response. One of these policy actions disables the kernel and powers down the device. ARM and TrustZone are registered trade marks of ARM Limited in the EU and elsewhere.

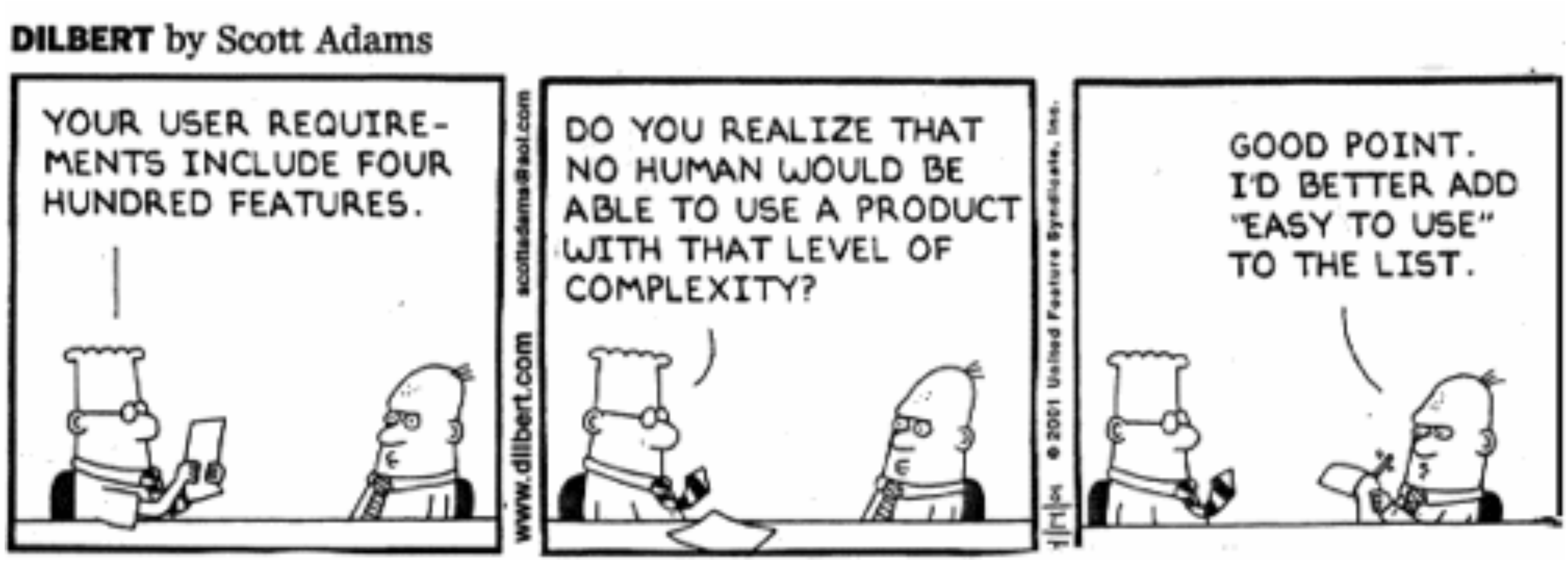
Security Enhancements for Android

Security Enhancements for Android provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements. Security Enhancements for Android isolates applications and data into different domains so that threats of tampering and

Usability vs. Security

- Bring your own device

- Security == bad usability


DILBERT by Scott Adams
YOUR USER REQUIREMENTS INCLUDE FOUR HUNDRED FEATURES.
DO YOU REALIZE THAT NO HUMAN WOULD BE ABLE TO USE A PRODUCT WITH THAT LEVEL OF COMPLEXITY?
GOOD POINT. I'D BETTER ADD "EASY TO USE" TO THE LIST.
scottadams@aol.com
www.dilbert.com
© 2001 United Feature Syndicate, Inc.

Easy to use!

What can we do?

picture © www.norebbo.com

Patch OS?

Bad update record
Fragmentation

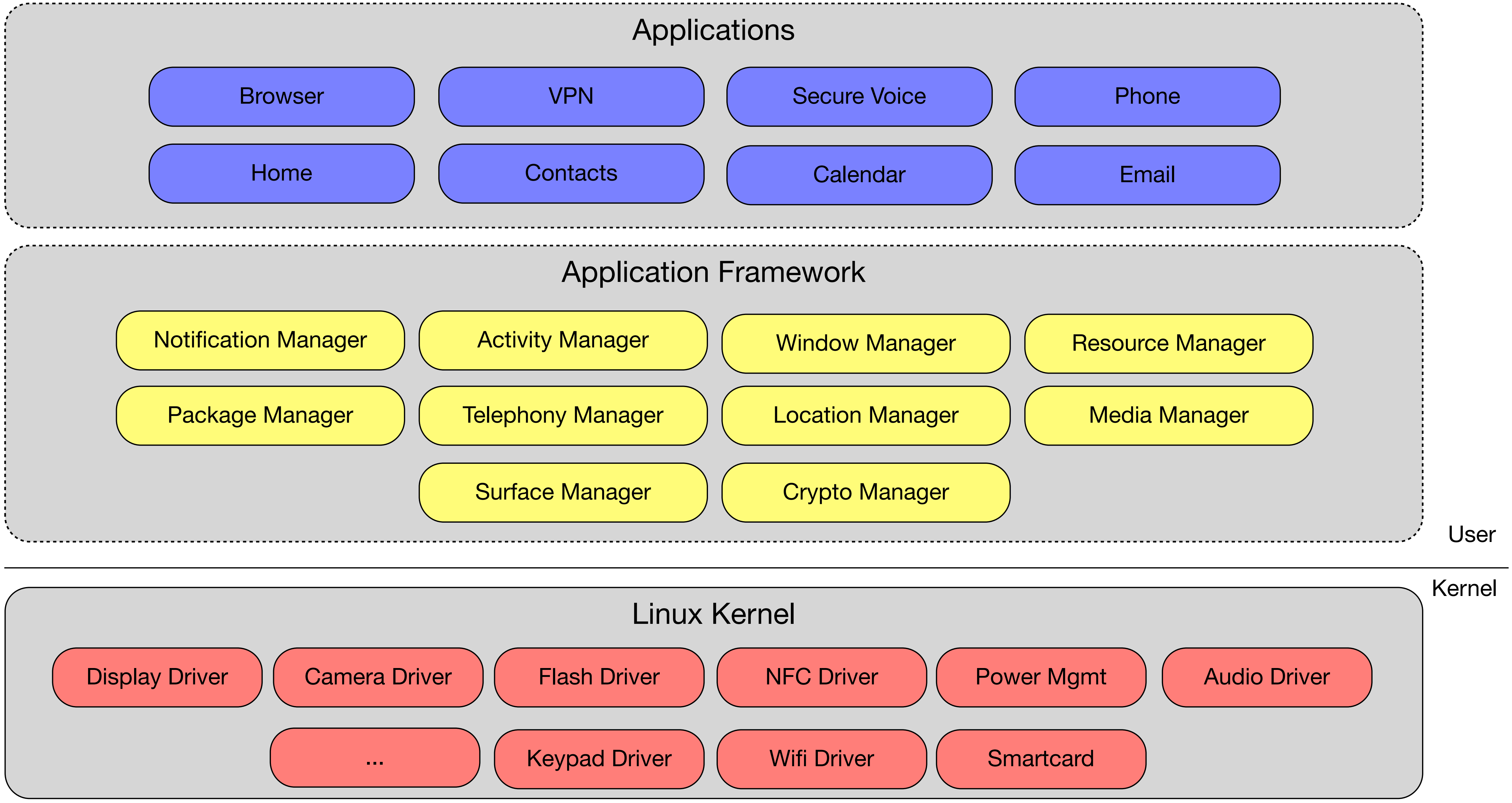
Add security layer?

Change middleware
Improve permission model

Virtualization

L4Android Framework

Make L4Linux run Android



Applications

Browser
VPN
Secure Voice
Phone
Home
Contacts
Calendar
Email

Application Framework

Notification Manager
Activity Manager
Window Manager
Resource Manager
Package Manager
Telephony Manager
Location Manager
Media Manager
Surface Manager
Crypto Manager

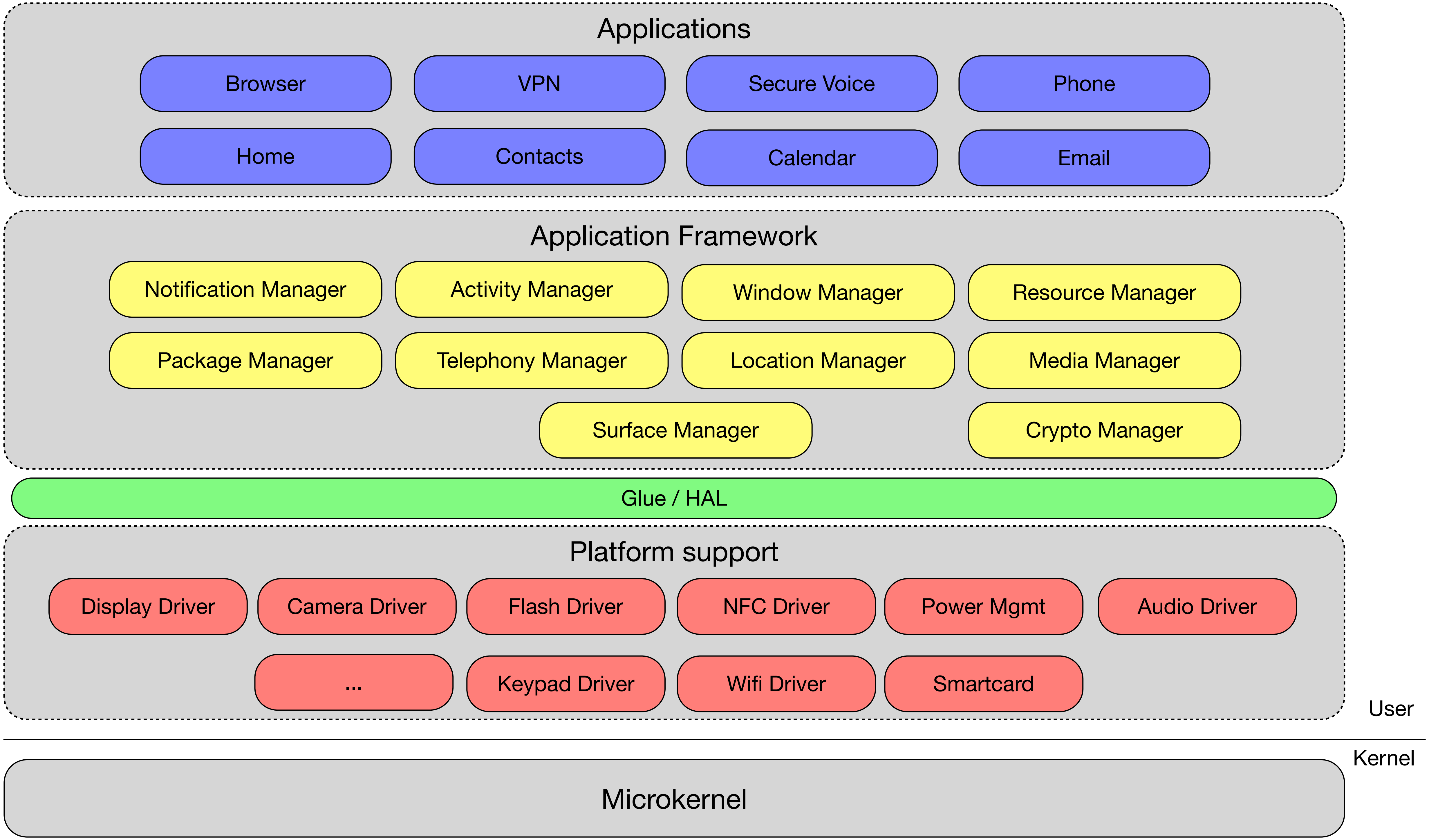
User

Kernel

Linux Kernel

Display Driver
Camera Driver
Flash Driver
NFC Driver
Power Mgmt
Audio Driver
...
Keypad Driver
Wifi Driver
Smartcard

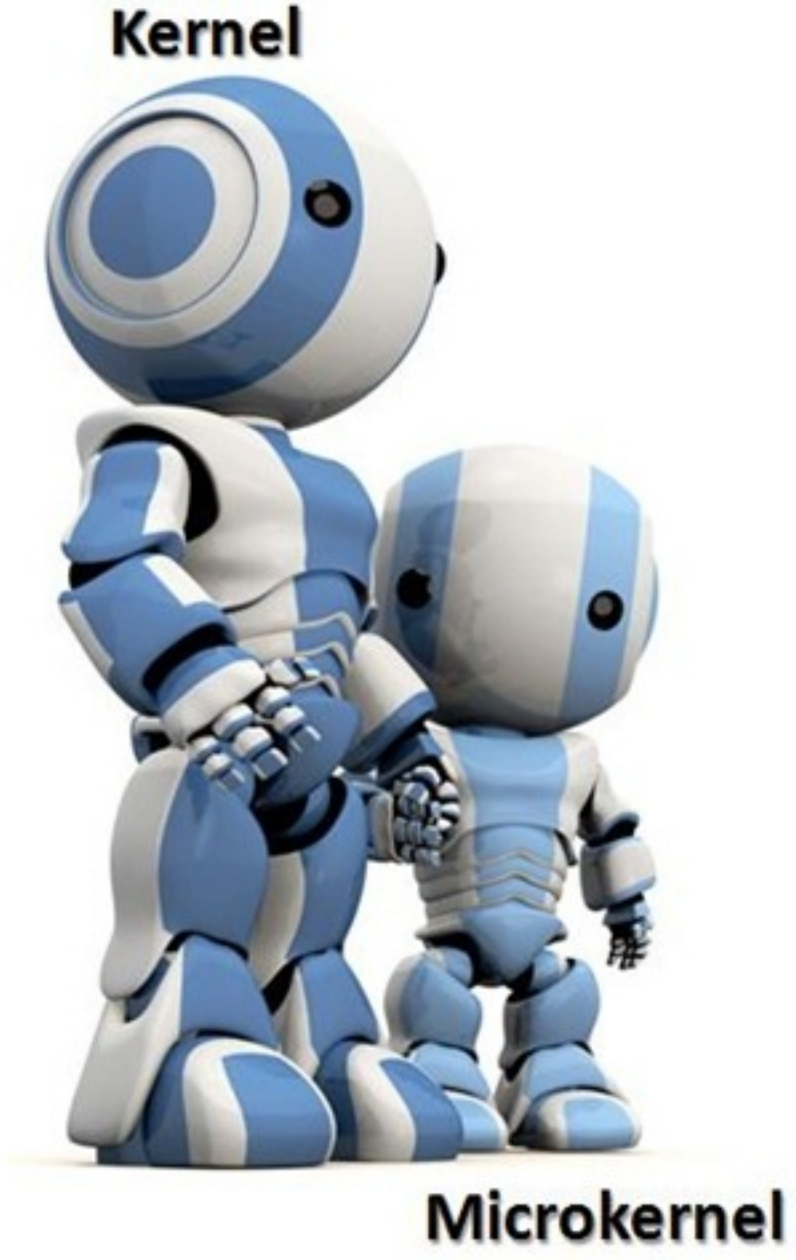
Instead of this ...


Applications
Browser
VPN
Secure Voice
Phone
Home
Contacts
Calendar
Email
Application Framework
Notification Manager
Activity Manager
Window Manager
Resource Manager
Package Manager
Telephony Manager
Location Manager
Media Manager
Surface Manager
Crypto Manager
Glue / HAL
Platform support
Display Driver
Camera Driver
Flash Driver
NFC Driver
Power Mgmt
Audio Driver
...
Keypad Driver
Wifi Driver
Smartcard
User
Kernel
Microkernel

... we want this

Microkernel as Hypervisor

- Less code, less errors
- Improvements over monolithic kernels
  - Fault isolation
  - Improved acces control
  - Flexibility
- Needs runtime environment

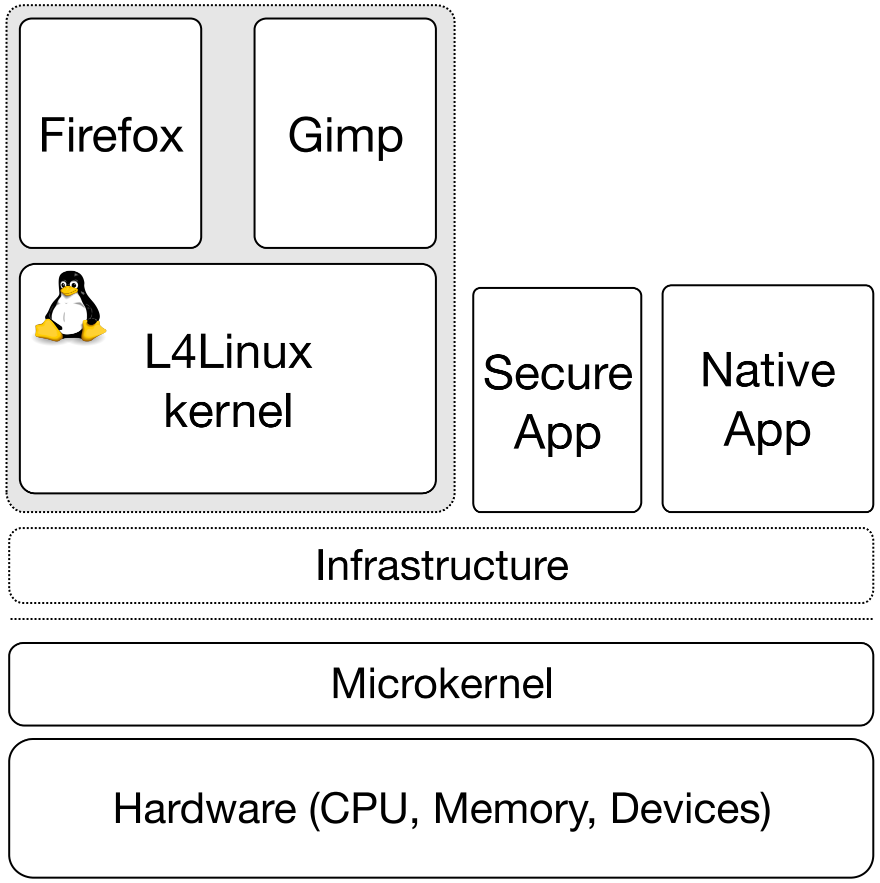


Fiasco.OC + L4Re

- 3rd gen. microkernel + runtime environment
    - x86 and ARM, SMP support
    - SVM, VT-x
    - L4Re provides basic services

Virtualization: L4Linux

- Applicable to non-virtualizable platforms
- Binary compatible to native
- Up-to-date Linux

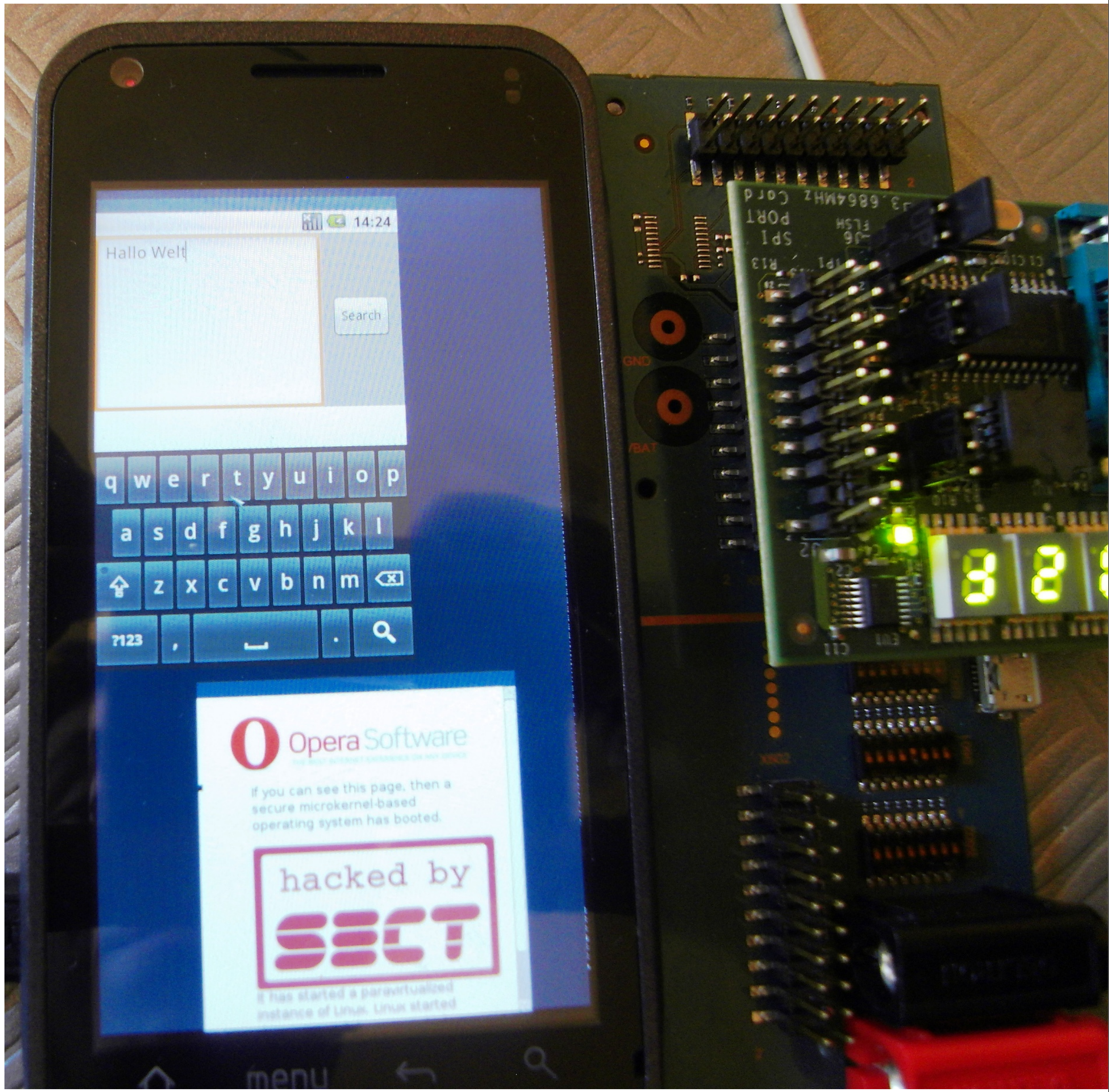


Steps and Building Blocks

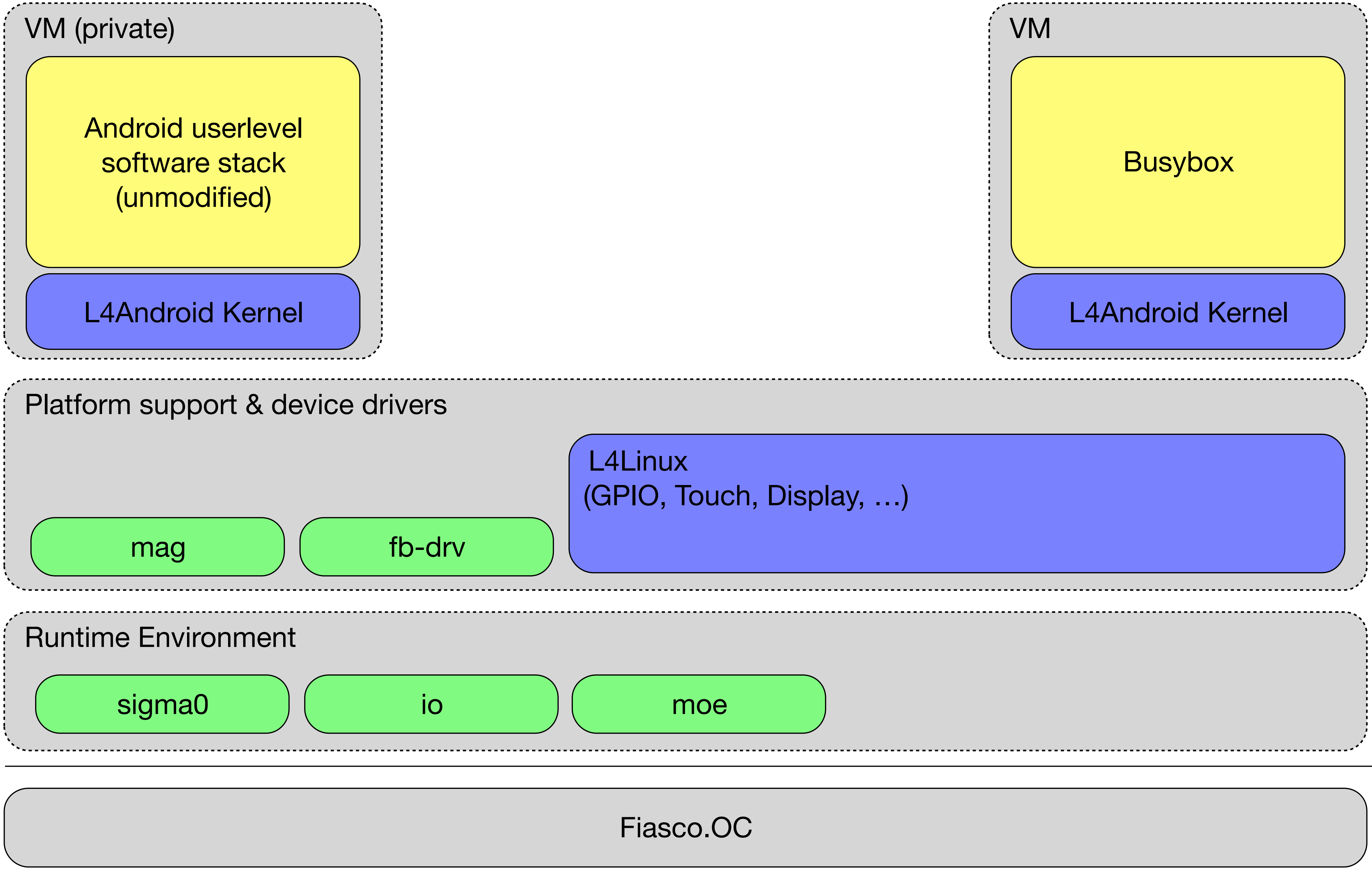
picture © www.norebbo.com

Cebit 2011

- Intel Moorestown prototype
- Virtualized Android + 2nd Linux + driver Linux
- No direct hardware access
- Only touchscreen and display
  - No sensors
  - No network


14:24
Hallo Welt
Search
Opera Software
If you can see this page, then a secure microkernel-based operating system has booted.
hacked by
SECT
menu

Prototype Architecture

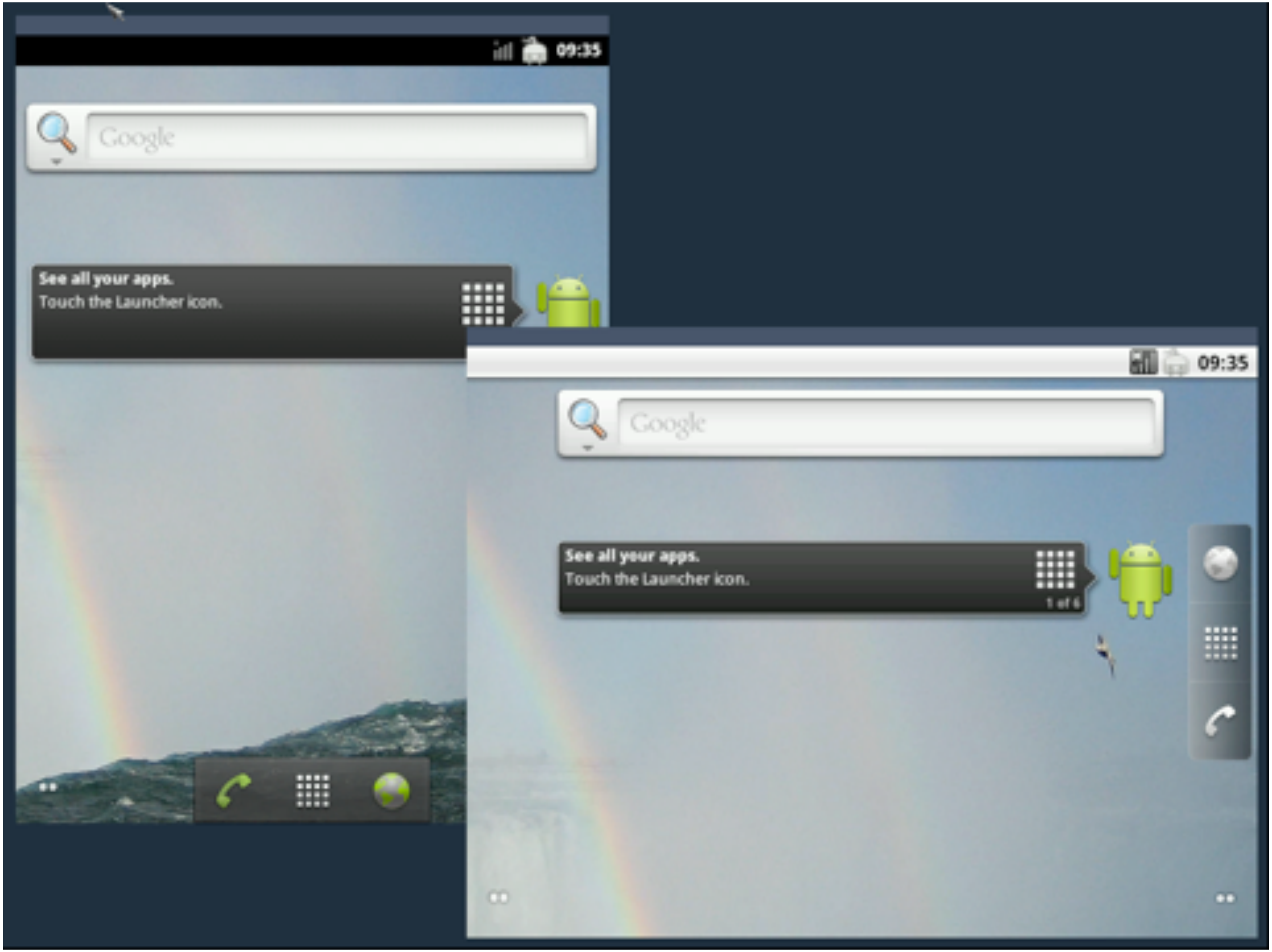


Implementation Steps

- Patch L4Linux with Android
  - binder, wakelocks, ashmem, …
- GPIO subsystem
  - Required for touchscreen and display
- fb-drv: MMIO replay from Linux driver

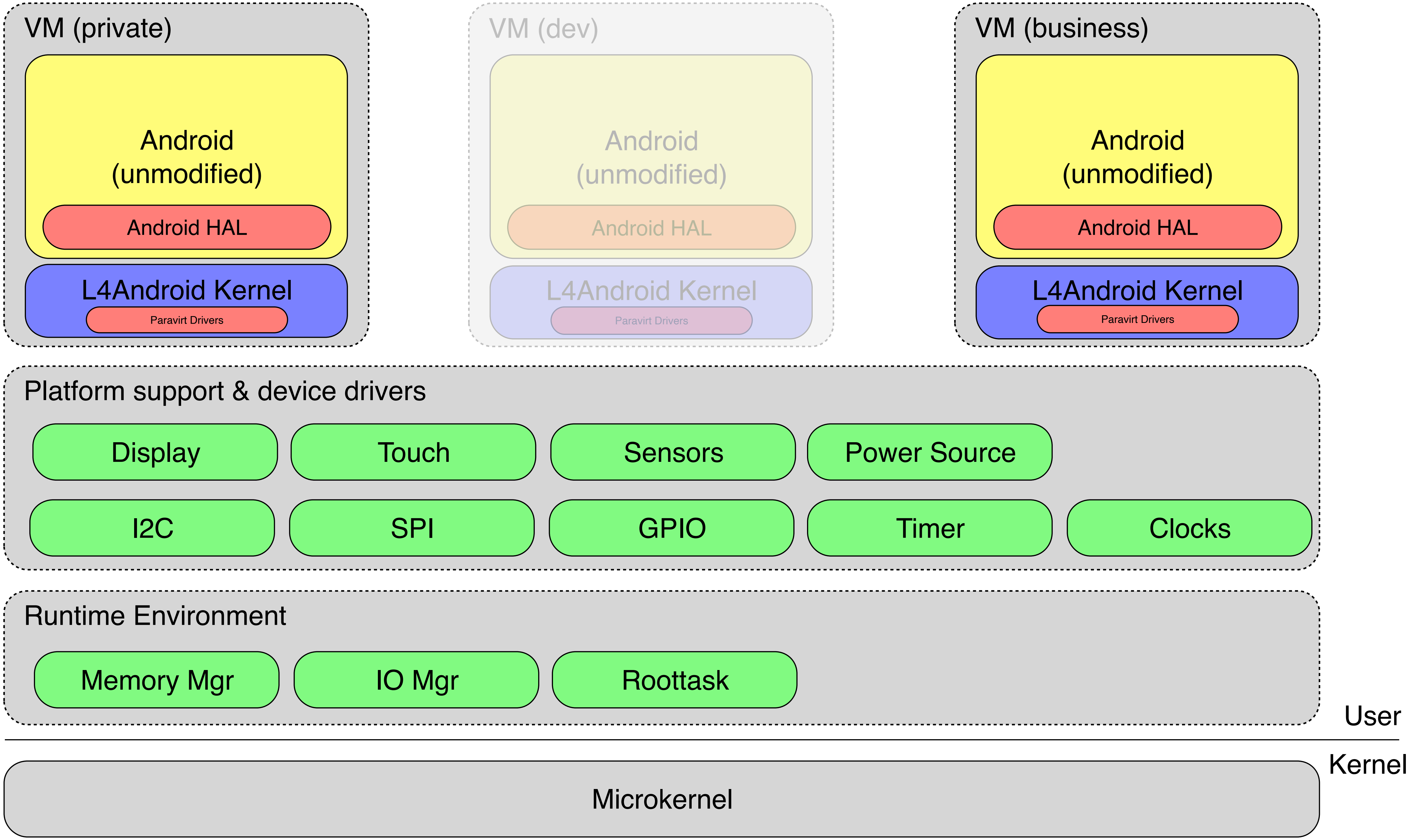
Towards the L4Android Framework

- Support for ARM and x86
- Android
    - Generic hardware interface for both architectures
    - Require no hardware modifications or extensions



09:35
Google
See all your apps.
Touch the Launcher icon.
09:35
Google
See all your apps.
Touch the Launcher icon.
1 of 6

Run in qemu



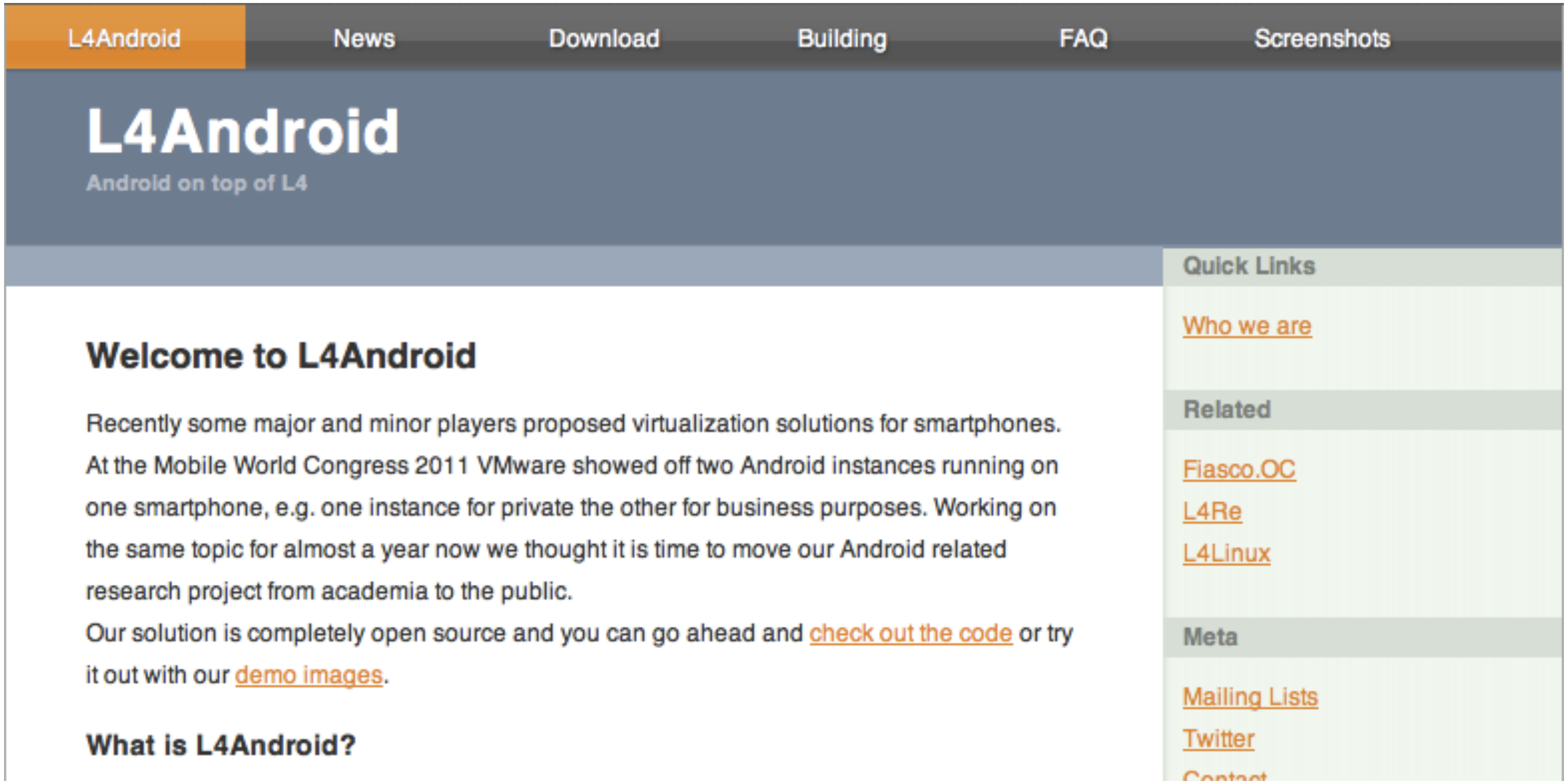
L4Android Architecture

“L4Android: A Generic Operating System Framework for Secure Smartphones”

–ACM SPSM ’11, Chicago, IL, USA

L4Android

- Open source project
- l4android.org



L4Android

Android on top of L4

Quick Links

Who we are

Related

Fiasco.OC

L4Re

L4Linux

Meta

Mailing Lists

Twitter

Contact

Welcome to L4Android

Recently some major and minor players proposed virtualization solutions for smartphones. At the Mobile World Congress 2011 VMware showed off two Android instances running on one smartphone, e.g. one instance for private the other for business purposes. Working on the same topic for almost a year now we thought it is time to move our Android related research project from academia to the public.
Our solution is completely open source and you can go ahead and check out the code or try it out with our demo images.

What is L4Android?

Applications

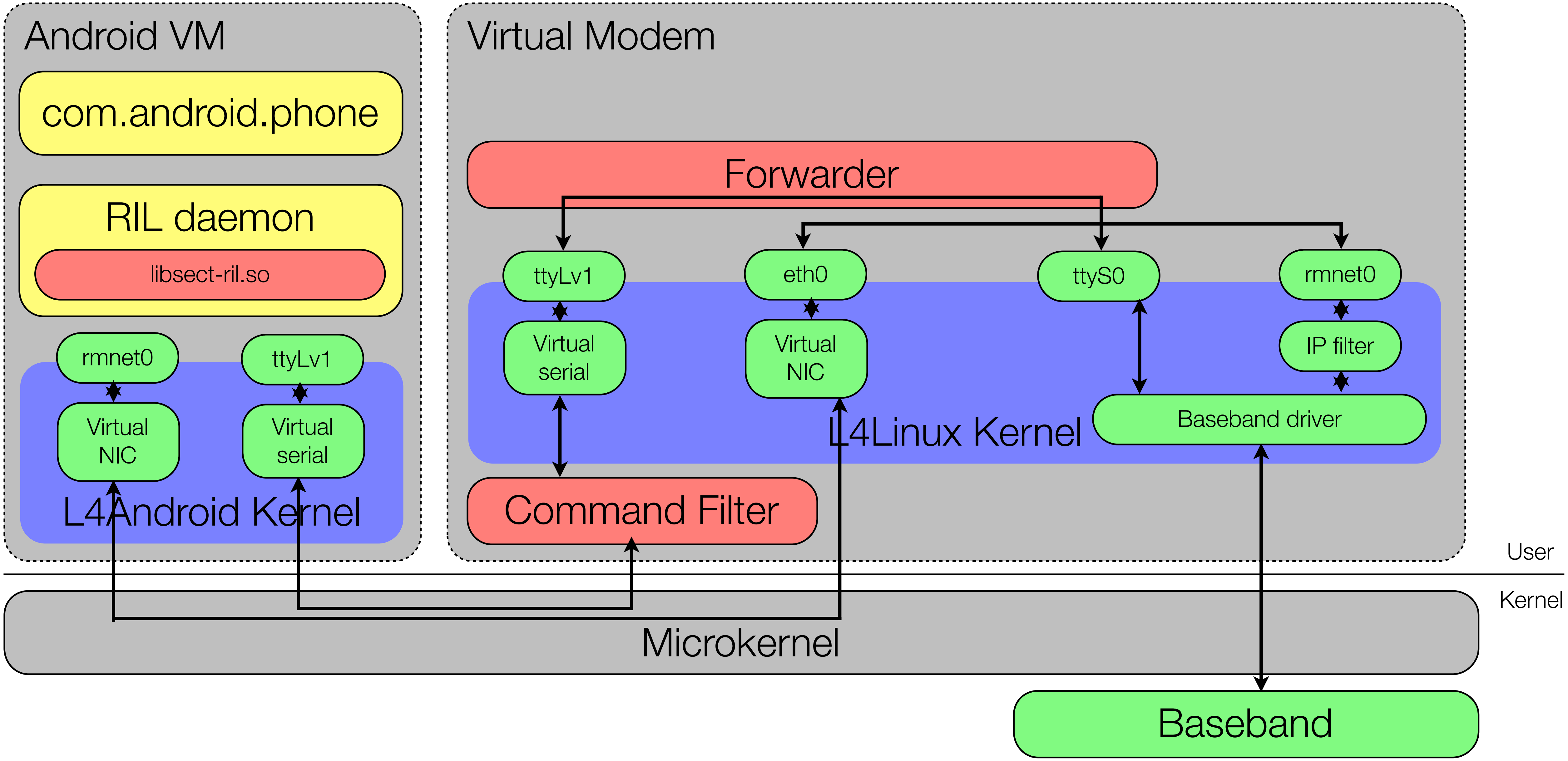
picture © www.norebbo.com

The Virtual Modem*

- Prevent signaling attacks on phone
- Protect user from cellular trojans

*Taming Mr. Hayes: Mitigating Signaling Based Attacks on Smartphones, IEEE DSN 2012

Virtual Modem Architecture



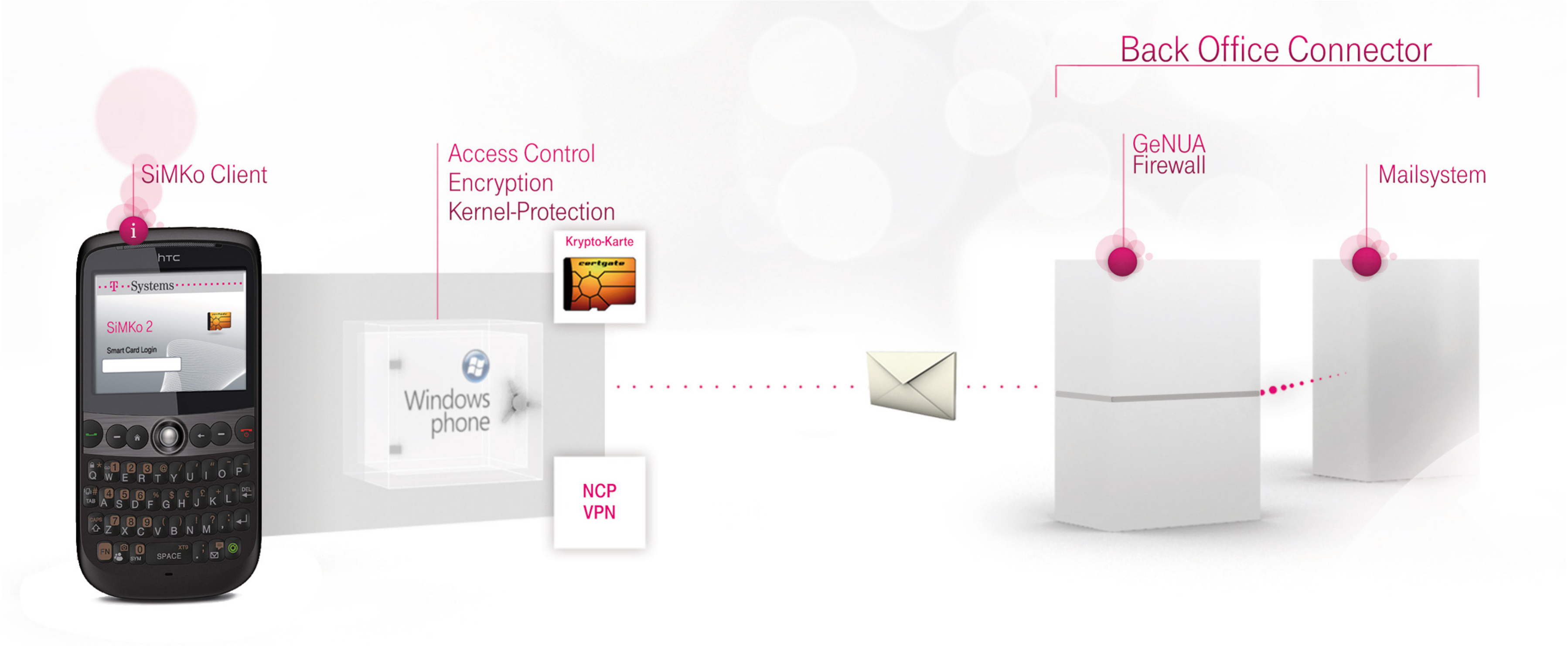
Virtual Modem Results

- Mitigate known signaling attacks
- Prevent premium number SMS
- Hinders SMS controlled botnets

SiMKo

SiMKo

- **Si**chere **M**obile **Ko**mmunikation
- Confidential government communication
  - Data never leaves infrastructure unencrypted
- Meet BSI requirements for VS-NfD (confidential)

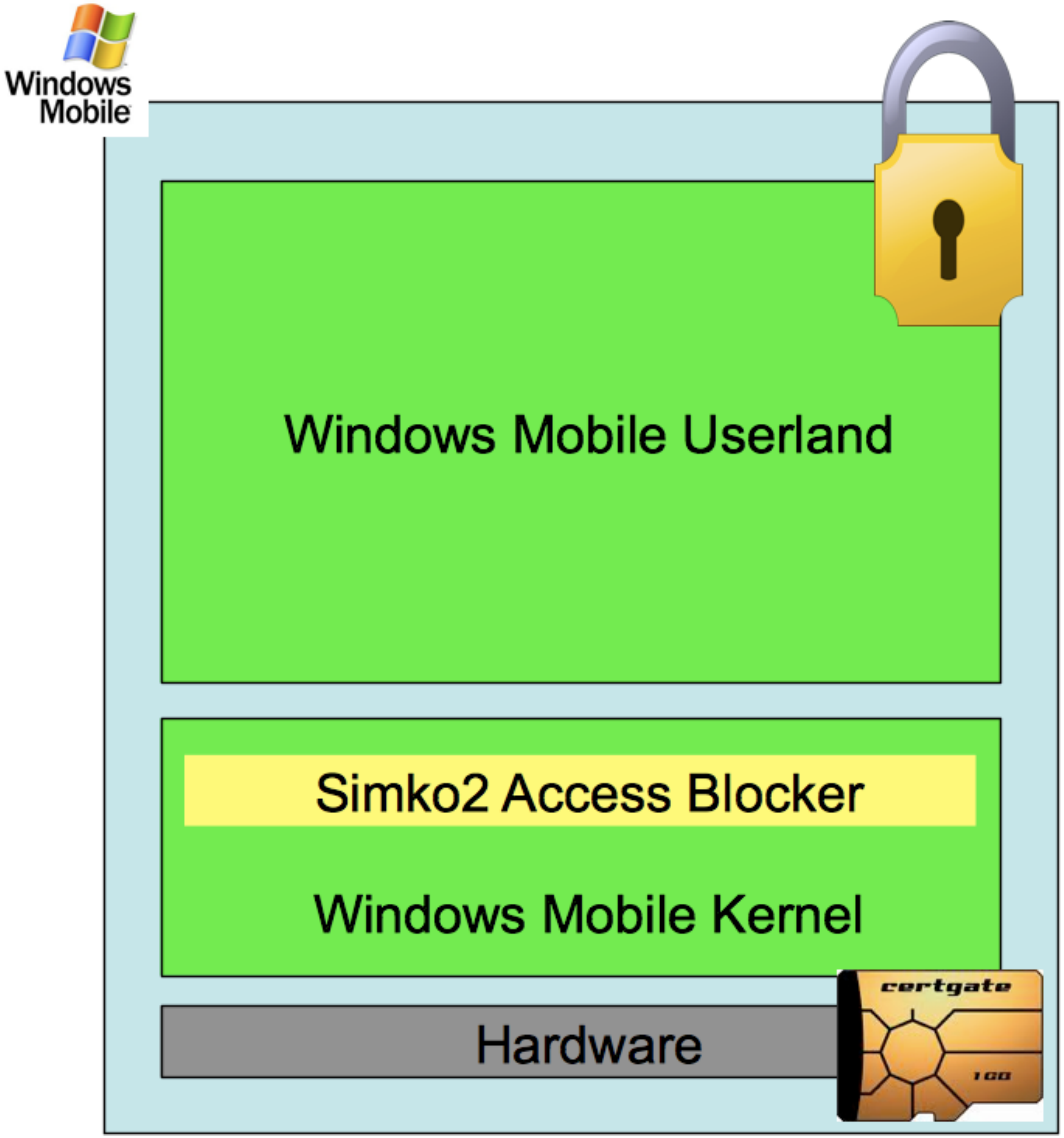


SiMKo2

picture © www.telekom.de

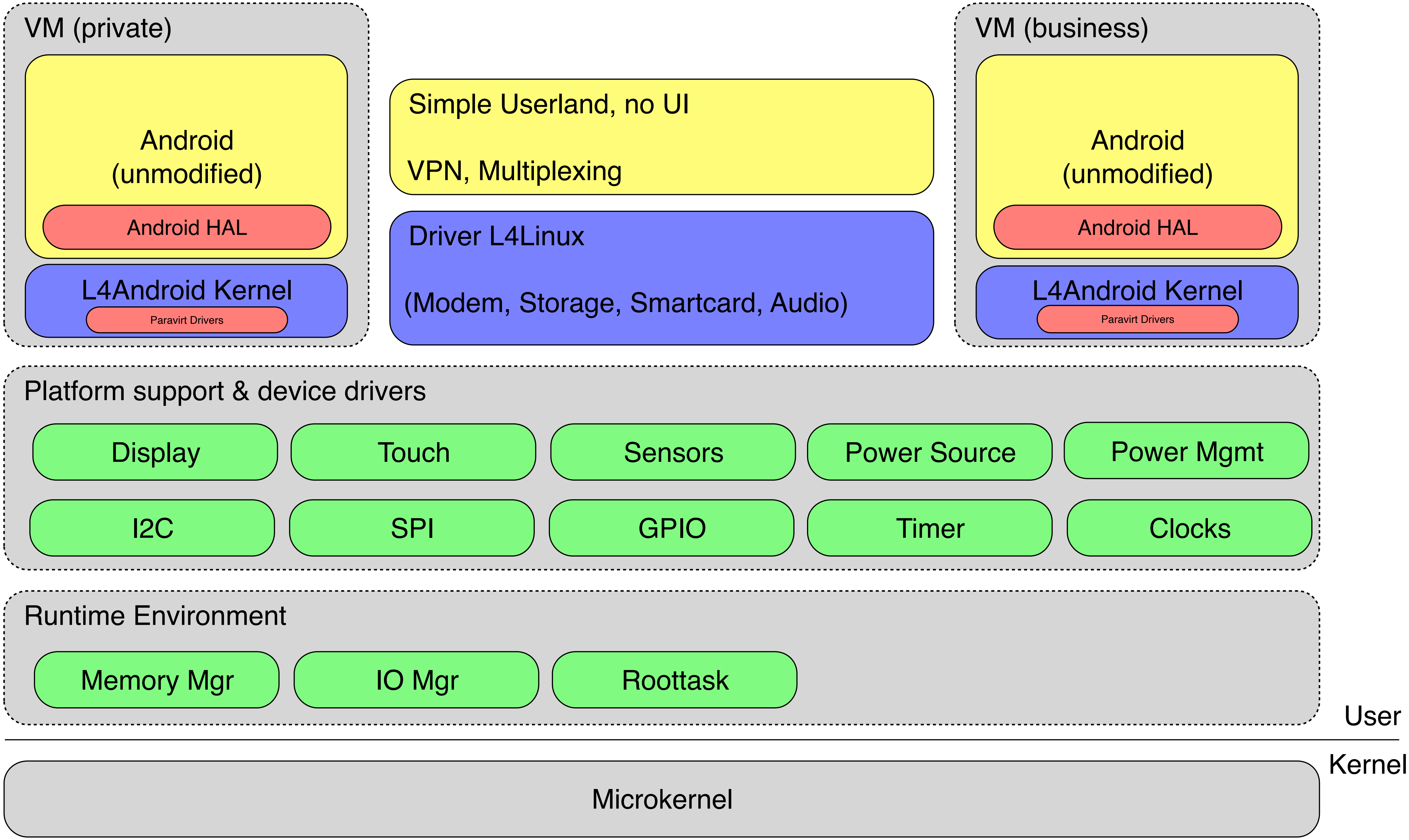
Why SiMKo3?

- SiMKo2 problems
  - Hardware EOL
  - No real control
  - Locked system
  - No Apps



SiMKo3 Requirements

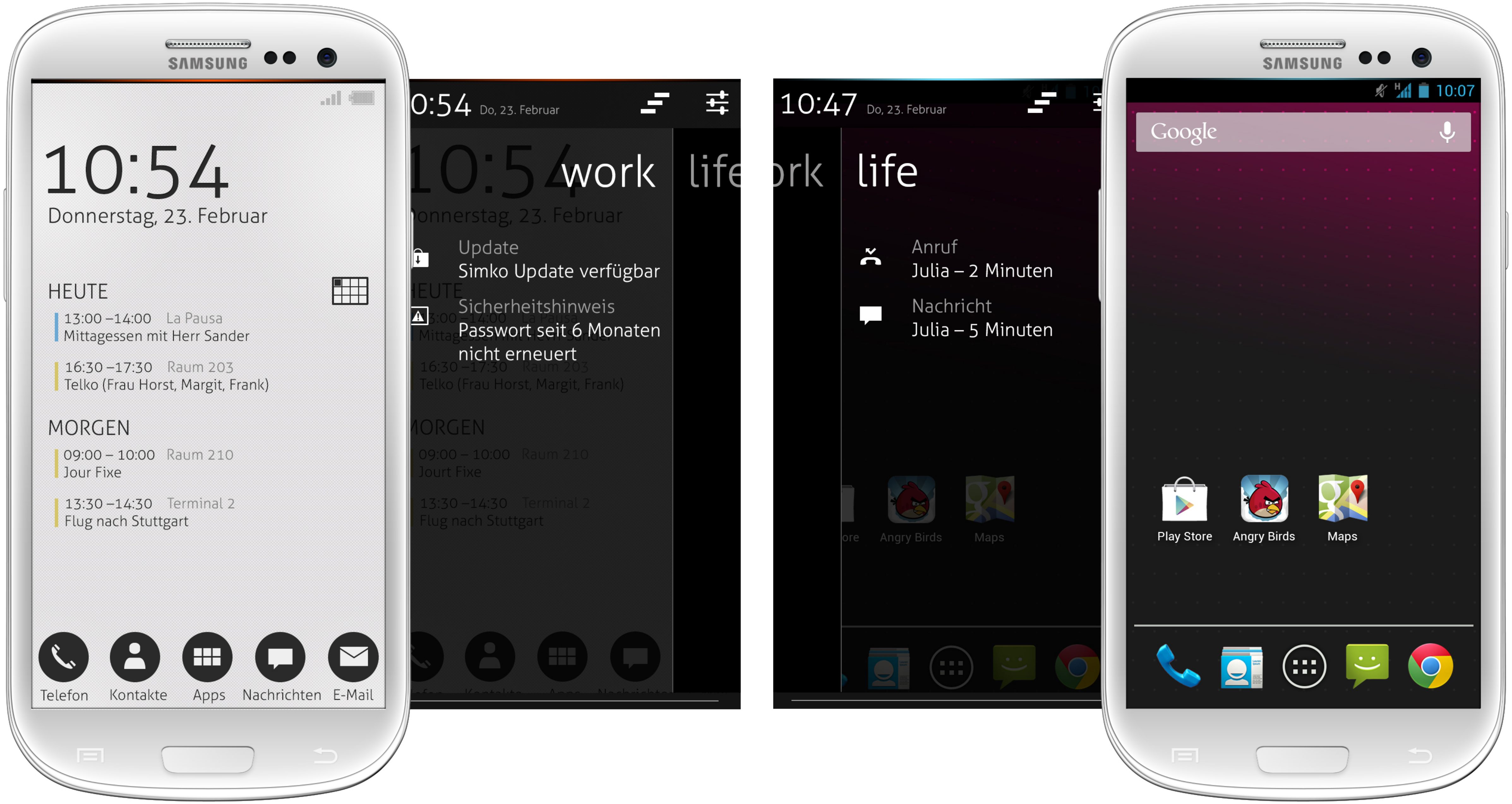
- Open Source Solution
  - Emphasis on security (MAC, small TCB)
- Reuse legacy software
  - with existing VS-NfD approval
  - Commodity OS



SiMKo3 Architecture

Multi-server OS

Life & Work



10:54
Donnerstag, 23. Februar

HEUTE

13:00 – 14:00 La Pausa
Mittagessen mit Herr Sander

16:30 – 17:30 Raum 203
Telko (Frau Horst, Margit, Frank)

MORGEN

09:00 – 10:00 Raum 210
Jour Fixe

13:30 – 14:30 Terminal 2
Flug nach Stuttgart

0:54 Do, 23. Februar

work

life

Update
Simko Update verfügbar

Sicherheitshinweis
Passwort seit 6 Monaten nicht erneuert

10:47 Do, 23. Februar

life

Anruf
Julia – 2 Minuten

Nachricht
Julia – 5 Minuten

picture © www.telekom.de

SiMKo3 Timeline

Team of 8 persons
Gave birth to 2 startups

Cebit 2011

Moorestown prototype

Summer 2011

Base system with 1 Android VM on ARM and x86

August 2011

Base system + 1 VM on Galaxy S2

Late 2011

Input + Sensor drivers, first HAL support

Cebit 2012

Galaxy S2 prototype, 2 VMs, Modem

Late 2012

Galaxy S3 port, first power management

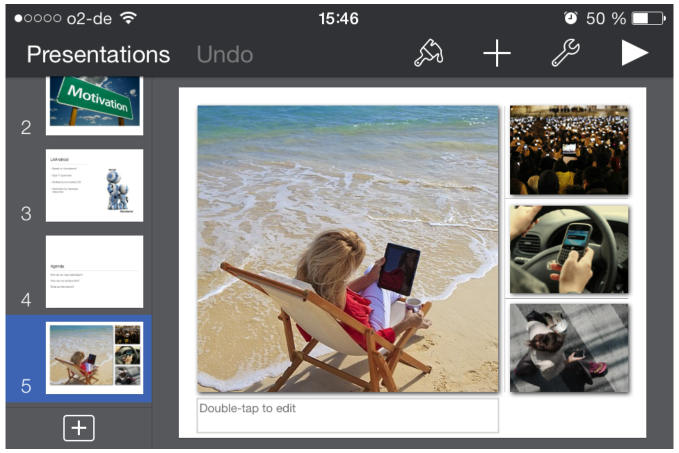
August 2013

BSI approval

Crossover: Secure UI

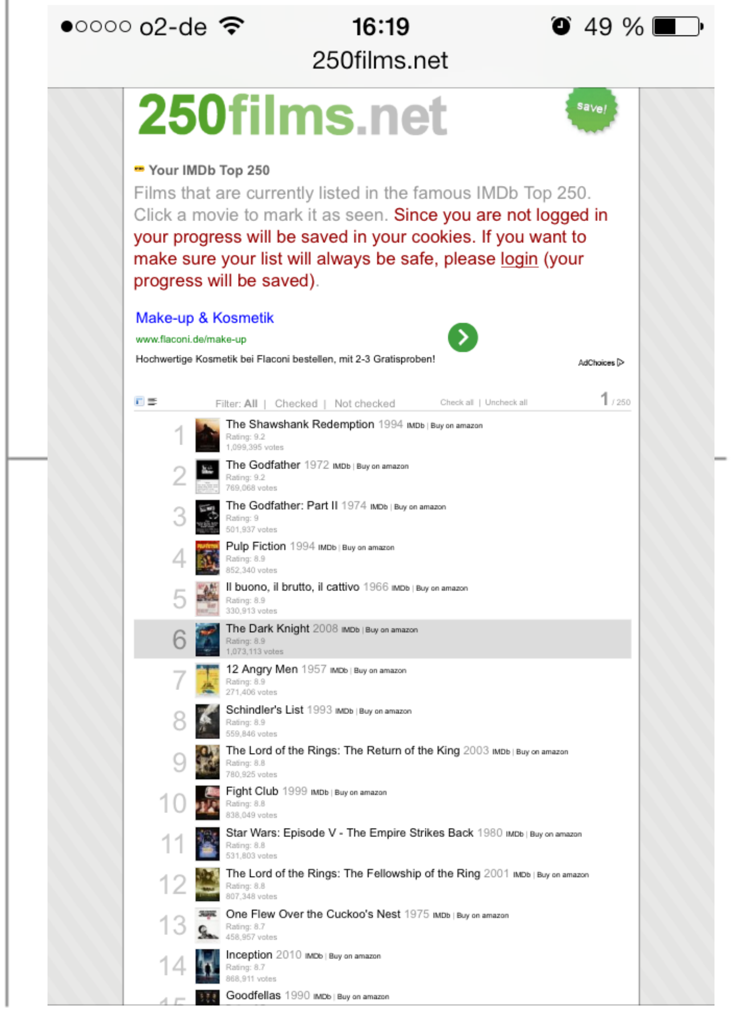
Observation 1: Rough conditions

Observation 2: Application-centric UI



- One application at a time

- Fullscreen + information panel



Your IMDb Top 250

Films that are currently listed in the famous IMDb Top 250. Click a movie to mark it as seen. Since you are not logged in your progress will be saved in your cookies. If you want to make sure your list will always be safe, please login (your progress will be saved).

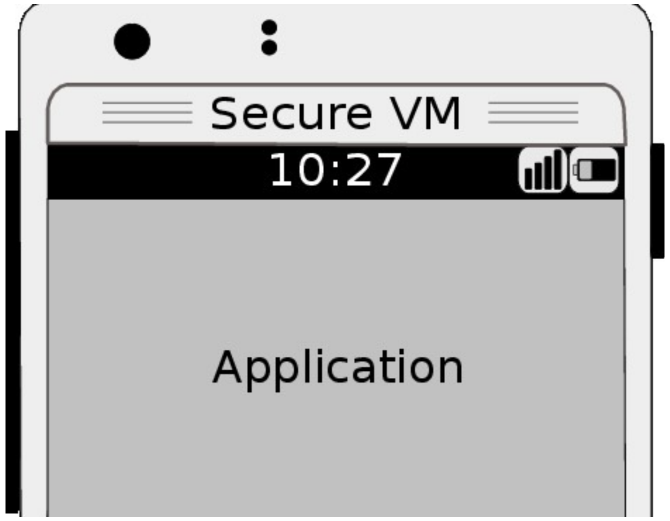
Filter: All | Checked | Not checked   Check all | Uncheck all   1 / 250

1	The Shawshank Redemption	1994	IMDb | Buy on amazon	Rating: 9.2	1,099,395 votes
2	The Godfather	1972	IMDb | Buy on amazon	Rating: 9.2	769,068 votes
3	The Godfather: Part II	1974	IMDb | Buy on amazon	Rating: 9	501,937 votes
4	Pulp Fiction	1994	IMDb | Buy on amazon	Rating: 8.9	852,340 votes
5	Il buono, il brutto, il cattivo	1966	IMDb | Buy on amazon	Rating: 8.9	330,913 votes
6	The Dark Knight	2008	IMDb | Buy on amazon	Rating: 8.9	1,073,113 votes
7	12 Angry Men	1957	IMDb | Buy on amazon	Rating: 8.9	271,406 votes
8	Schindler's List	1993	IMDb | Buy on amazon	Rating: 8.9	559,846 votes
9	The Lord of the Rings: The Return of the King	2003	IMDb | Buy on amazon	Rating: 8.8	780,925 votes
10	Fight Club	1999	IMDb | Buy on amazon	Rating: 8.8	838,049 votes
11	Star Wars: Episode V - The Empire Strikes Back	1980	IMDb | Buy on amazon	Rating: 8.8	531,803 votes
12	The Lord of the Rings: The Fellowship of the Ring	2001	IMDb | Buy on amazon	Rating: 8.8	807,348 votes
13	One Flew Over the Cuckoo's Nest	1975	IMDb | Buy on amazon	Rating: 8.7	458,957 votes
14	Inception	2010	IMDb | Buy on amazon	Rating: 8.7	868,911 votes
15	Goodfellas	1990	IMDb | Buy on amazon		

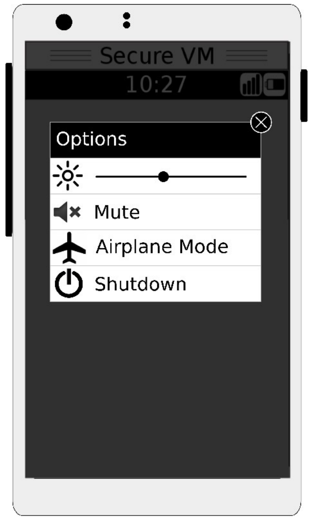
- Security Level Indicator as trusted path
- Identify active environment
- Switch between VMs

Secure VM
10:27
Application

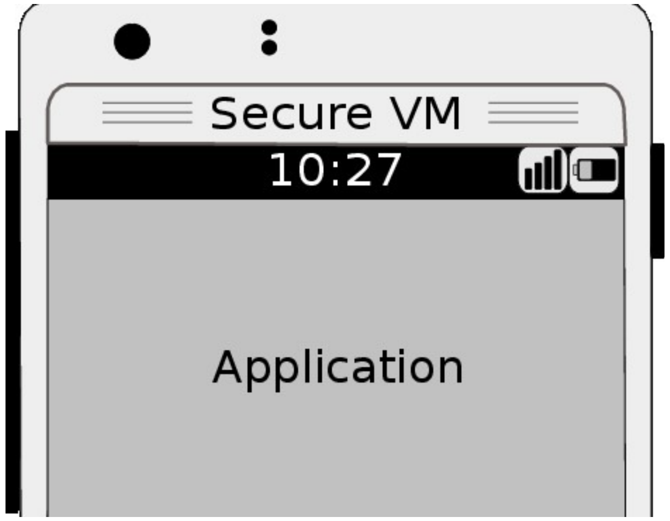
- Security Level Indicator as trusted path
- Identify active environment
- Switch between VMs



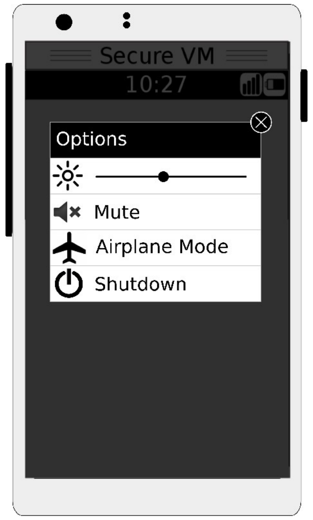
- Secure global menu
- Central policy for device-global functions



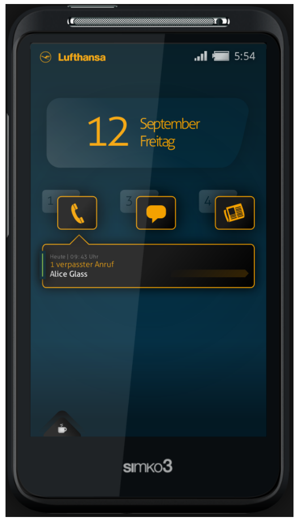
- Security Level Indicator as trusted path
- Identify active environment
- Switch between VMs



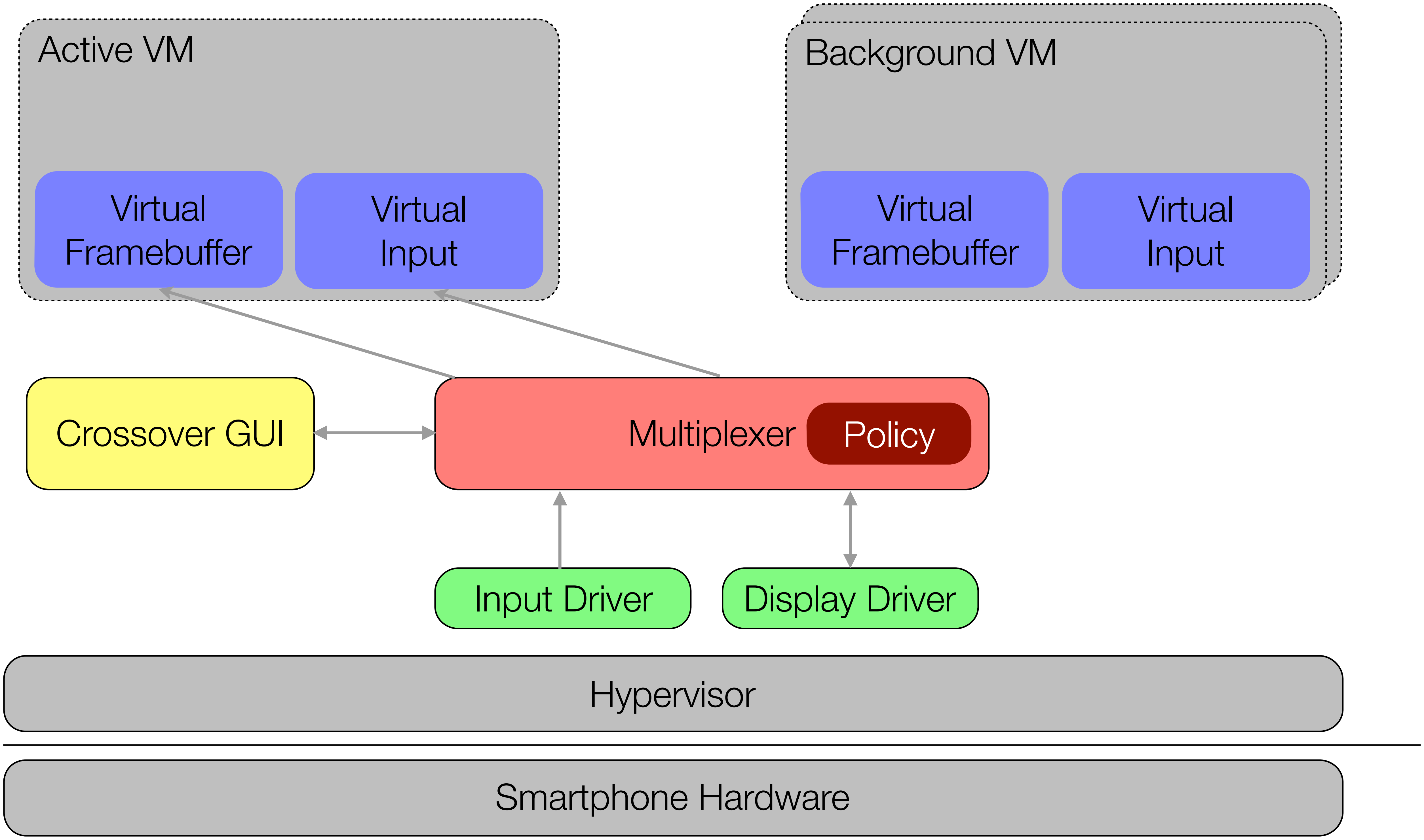
- Secure global menu
- Central policy for device-global functions



- Secure Lockscreen, lock device while idle
- Central notification center



Crossover Architecture



“Crossover: Secure and Usable User Interface for Mobile. Devices With Multiple Personalities”

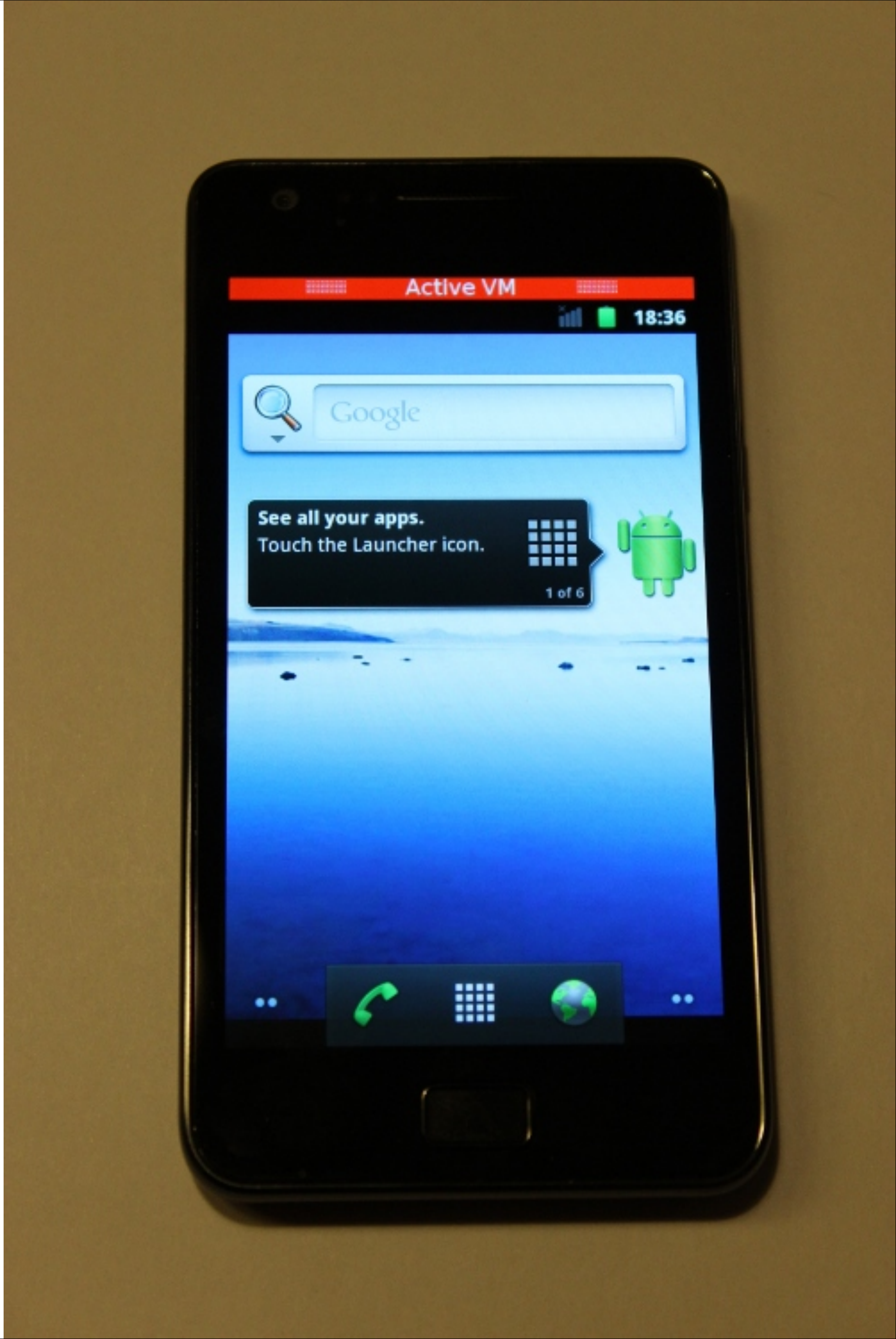
–ACSAC 2013, New Orleans, LA, USA

“Challenges”

picture © www.norebbo.com

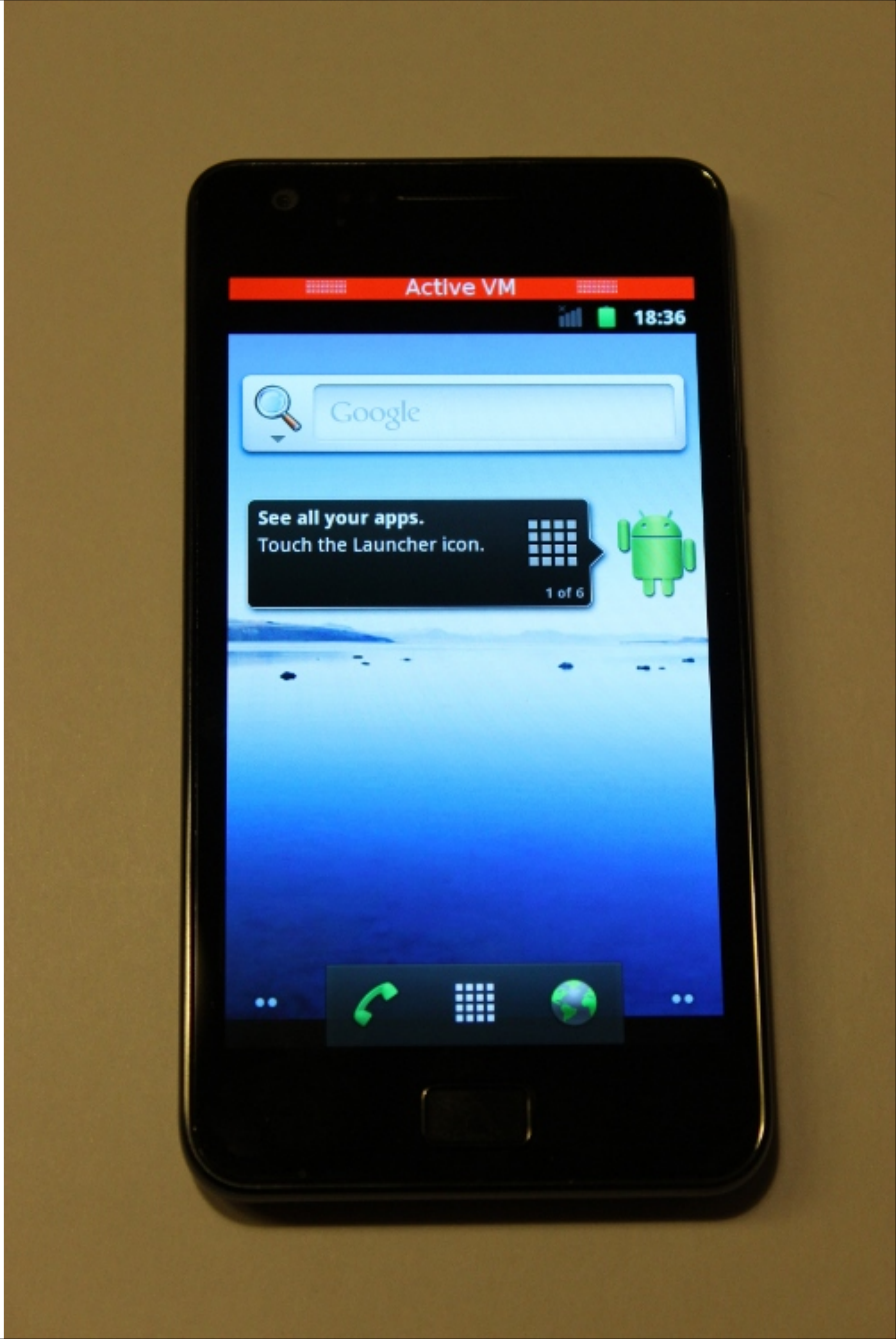
How to boot for fast development cycles?

Custom bootloader with USB and fastboot support.



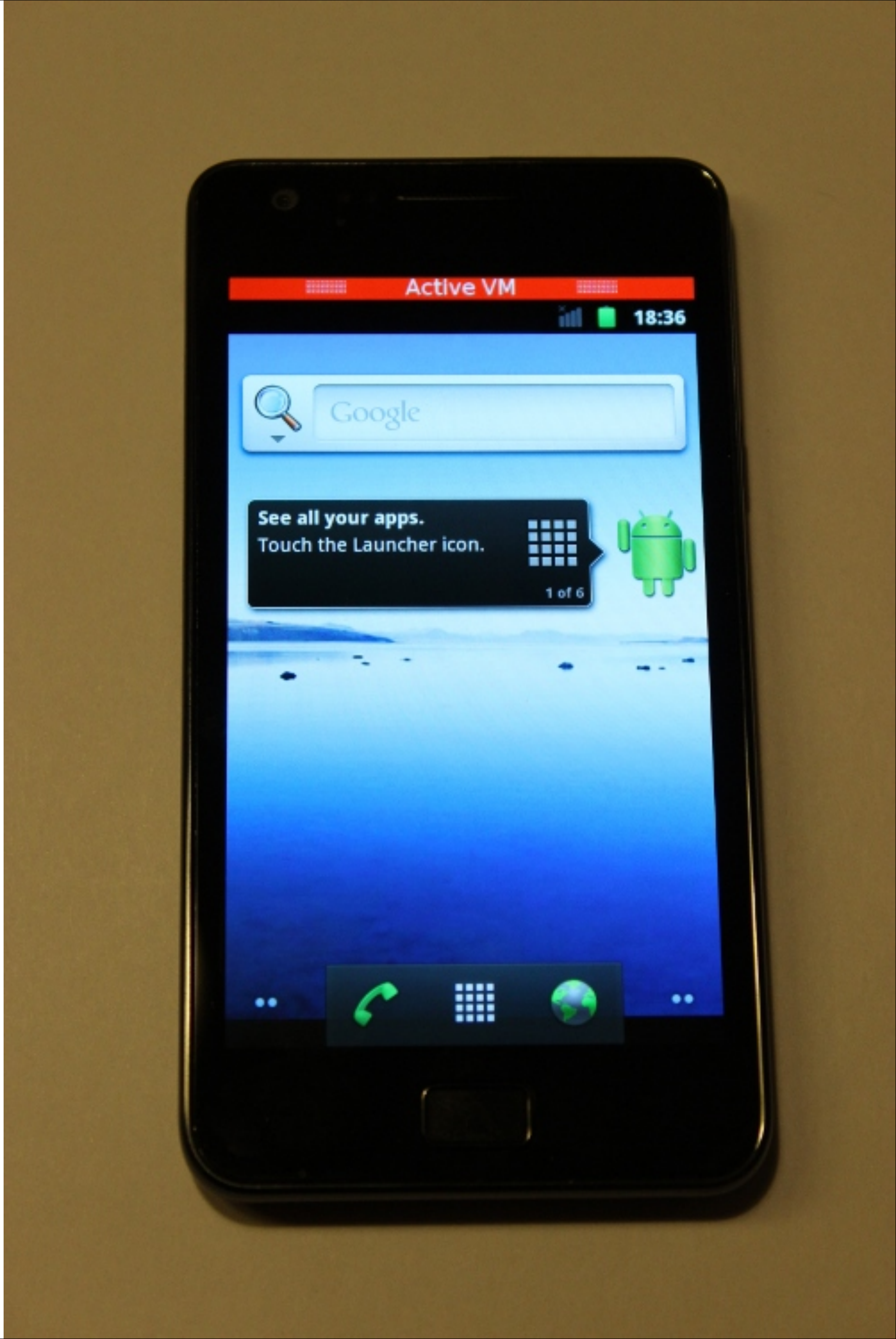
Is there a serial interface?

Multiplexed via micro USB port or audio jack.



How to develop native drivers?

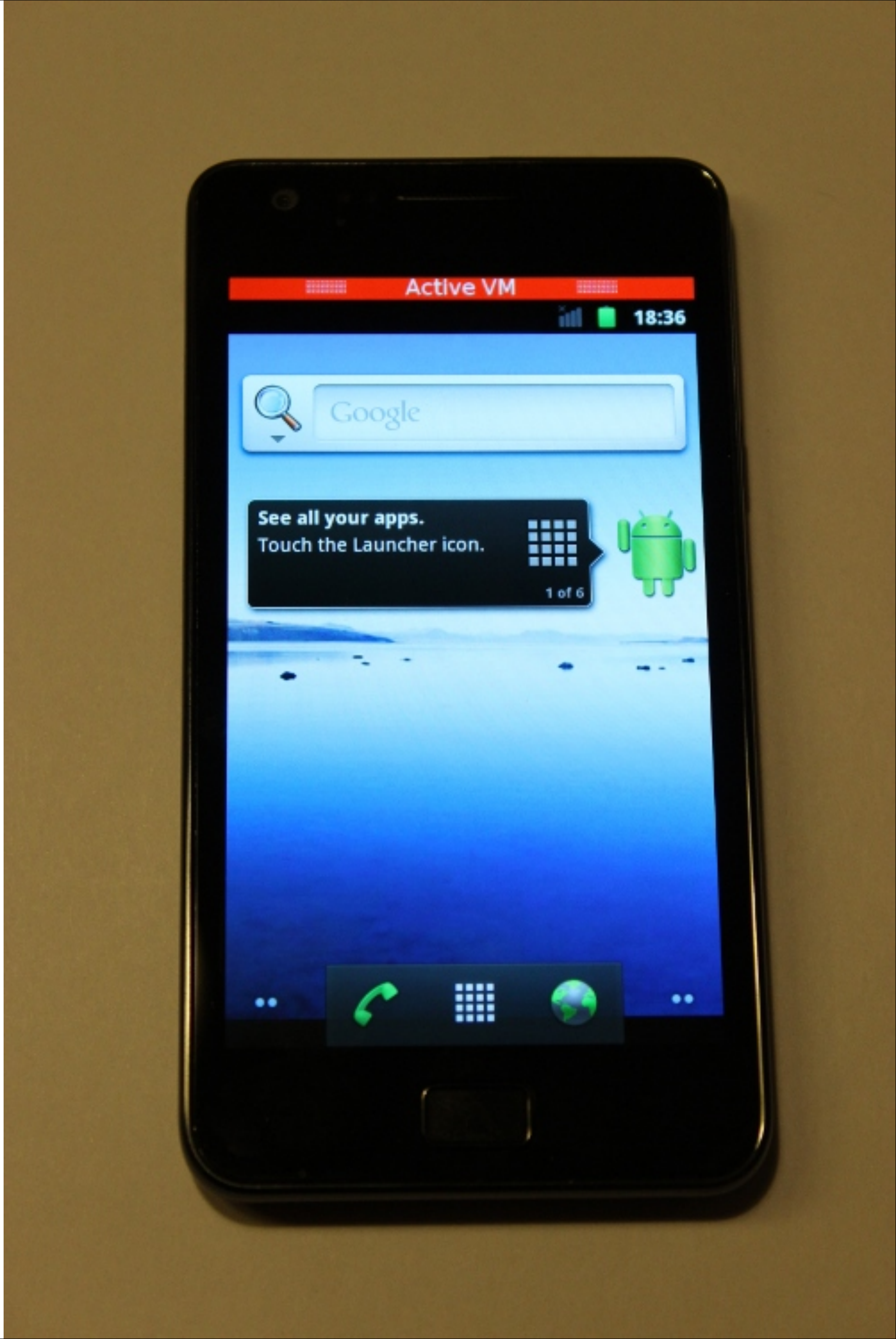
Read TRMs with 1000+ pages.
Read Linux drivers.



Reuse proprietary binary blobs?

3G baseband
Audio

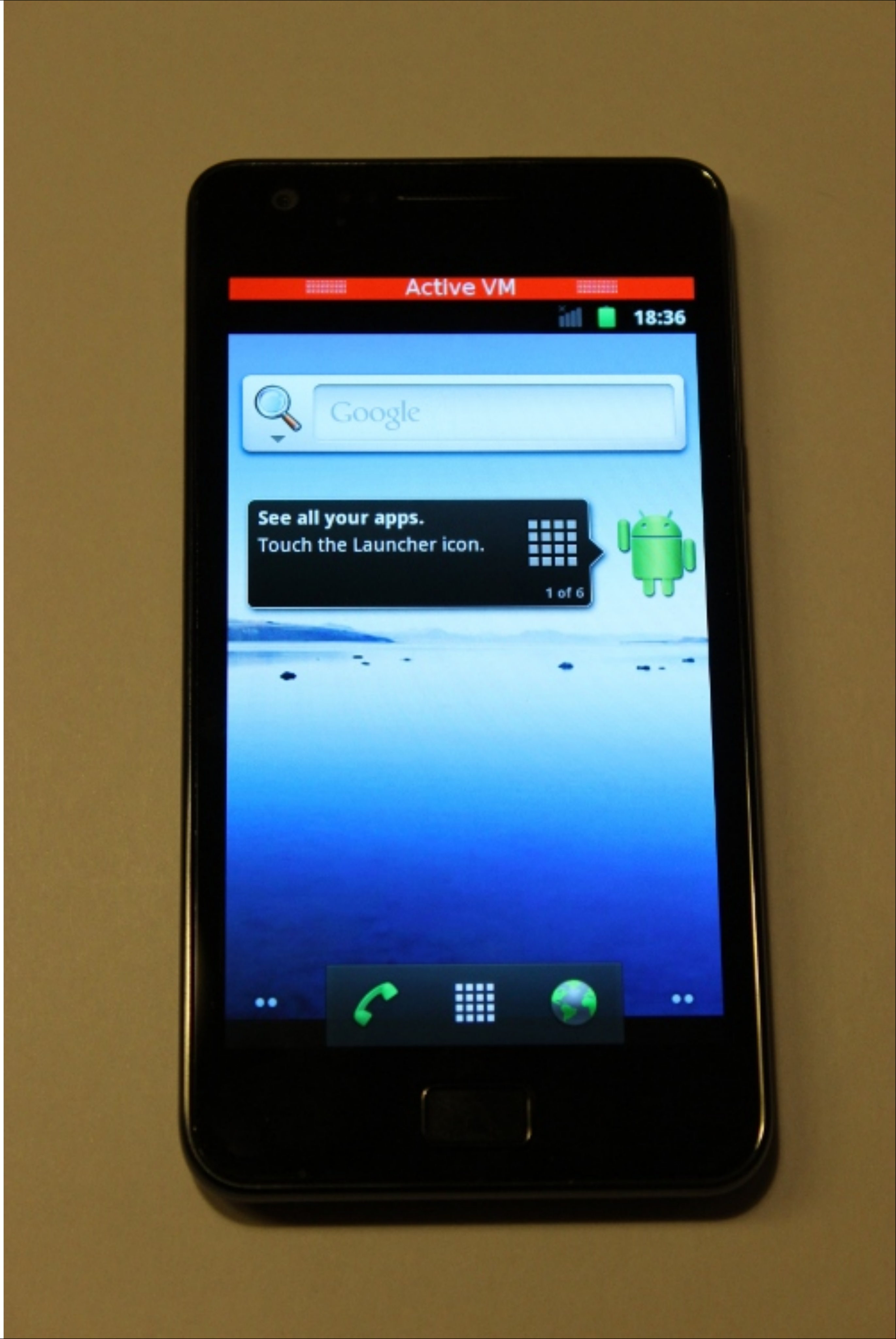
Use L4Linux as driver



Power management?

Frequency scaling
Shutdown idle cores

Now almost equal to native



(More) Questions?