Replicant: software freedom on mobile devices

Replicant

Paul Kocialkowski
paulk@replicant.us

Tuesday 8th July 2014

RMLL
MONTPELLIER 2014

Le libre et vous !
15èmes Rencontres Mondiales
du Logiciel Libre
Du 5 au 11 juillet 2014

Mobile devices

Mobile devices are **everywhere** : phones, tablets and more

Mobile devices are computers:

- Powerful hardware
- Operating systems, updates
- Applications

Telephony and freedom:

- Old-fashioned phones
- Current phones
- Feature phones
- Smartphones

Free software becomes relevant on these devices!

Mobile devices: introduction

Why care about **freedom**? Because we can!

Ethical reasons:

- Being in **control** rather than being **controlled**: fundamental four **freedoms** of free software
- Help your community
- A matter of **trust** and **security** for **data** and **communications**
- Control the **information** it gathers about you

Mobile devices: introduction

Why care about **freedom**? Because we can!

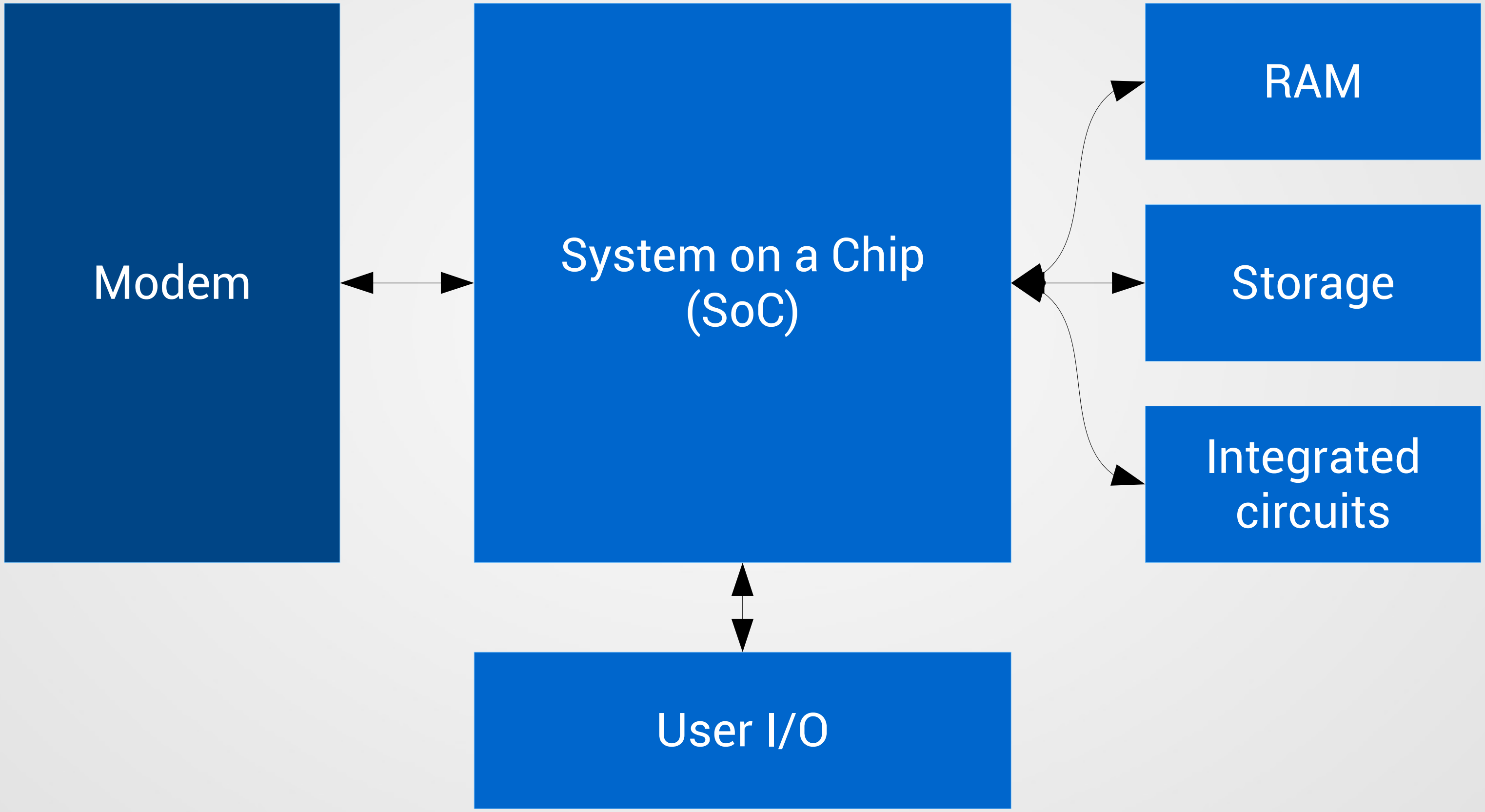
Ethical reasons:

- Being in **control** rather than being **controlled**: fundamental four **freedoms** of free software
- Help your community
- A matter of **trust** and **security** for **data** and **communications**
- Control the **information** it gathers about you

Technical reasons:

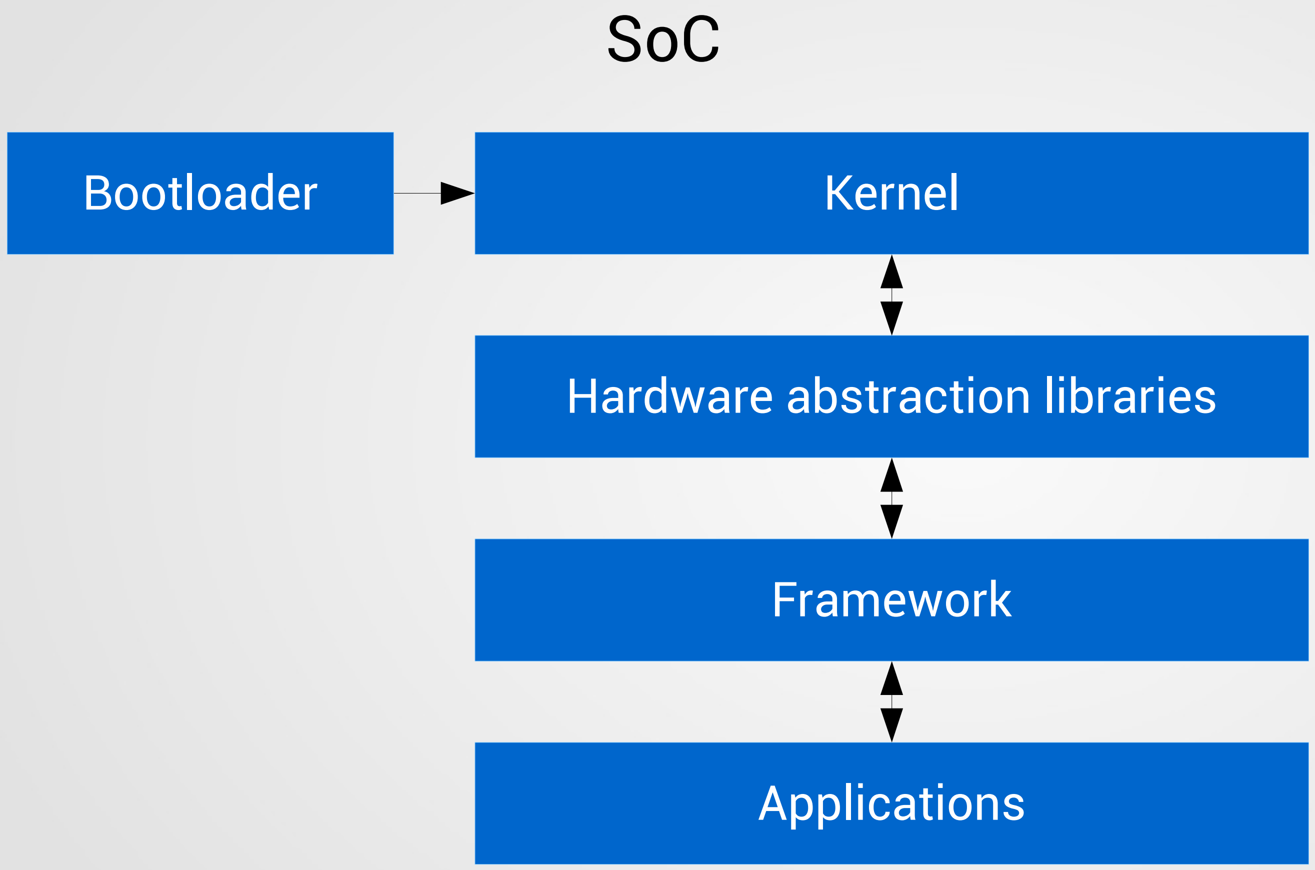
- **Adapt** software for your needs
- Make the software follow API changes and **new versions**

Mobile devices: simplified overview



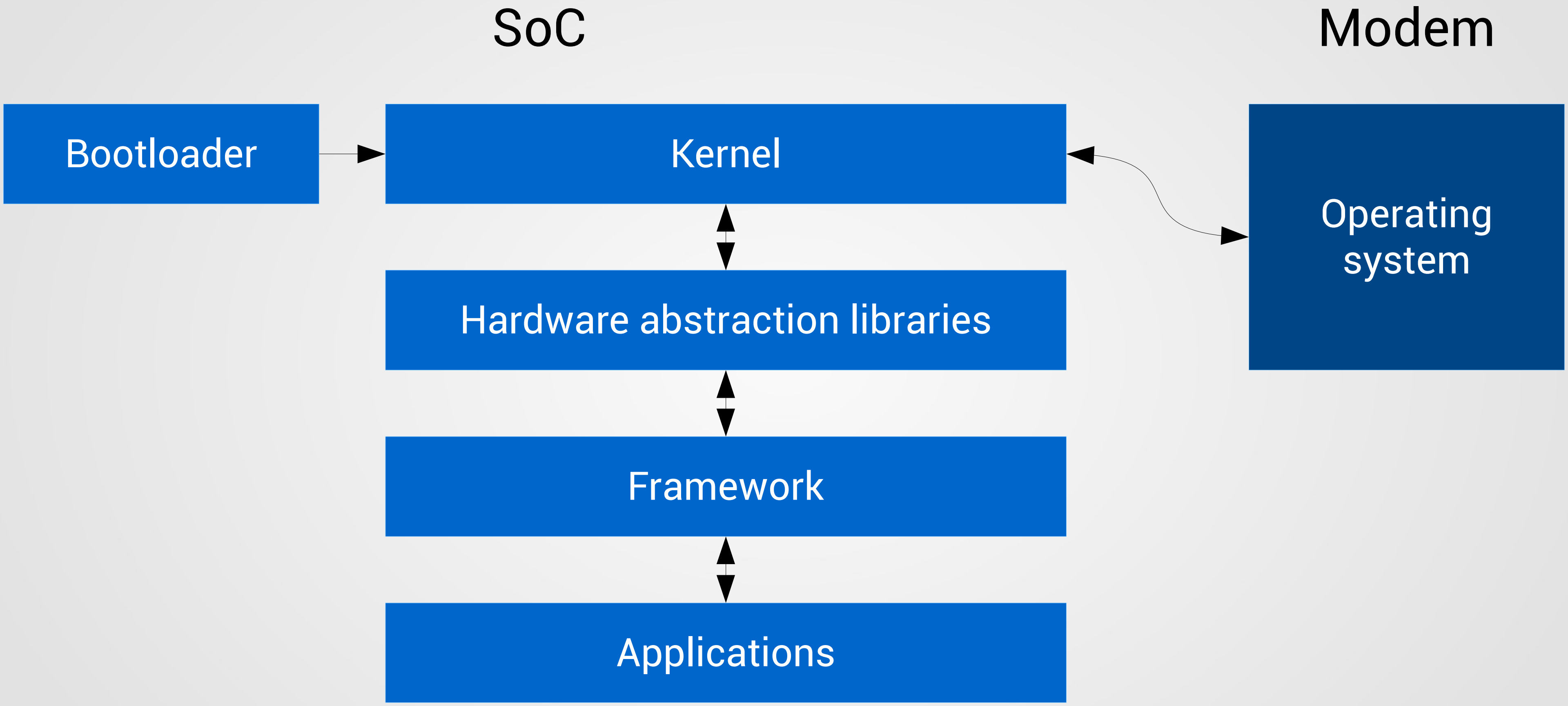
Hardware-side overview

Mobile devices: simplified overview



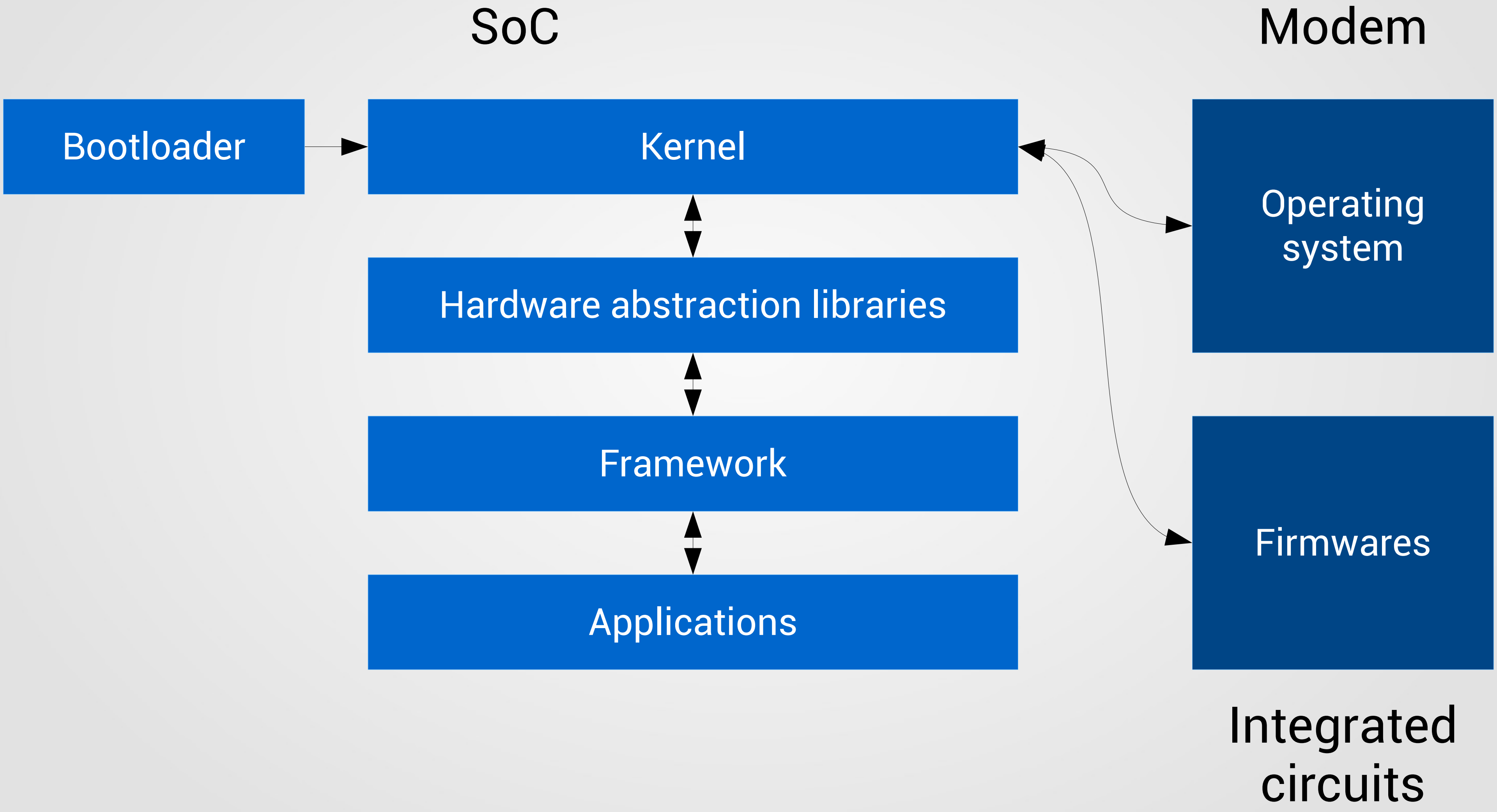
Software-side overview

Mobile devices: simplified overview



Software-side overview

Mobile devices: simplified overview



Software-side overview

Ideal scenario

Total freedom on telephony-enabled mobile devices:

- ✓ Free **hardware**
- ✓ Free **firmwares**
- ✓ Free **modem system**
- ✓ Free **bootloader**
- ✓ Free **system**

Ideal scenario

Total freedom on telephony-enabled mobile devices:

✓ Free **hardware**
✓ Free **firmwares**
✓ Free **modem system**
✓ Free **bootloader**
✓ Free **system**

Guarantees from mobile telephony operators:

✓ **Neutral** access to the Internet
✓ No **interception** of the data
✓ No collection of the users' **positions**

… but what is the reality today?

Mobile telephony operators

Mobile telephony operators:

- ✗ Often apply **filters** on mobile data networks
- ✗ Keep track of **messages** and **calls**
- ✗ Often gather the **real time position** of users
- ✗ Often provide unlimited access to **security agencies**

All of that depends on the **operator**, **country**, **government**.

Mobile telephony operators

Mobile telephony operators:

- ✗ Often apply **filters** on mobile data networks
- ✗ Keep track of **messages** and **calls**
- ✗ Often gather the **real time position** of users
- ✗ Often provide unlimited access to **security agencies**

All of that depends on the **operator**, **country**, **government**.

Bottom line:

- Pretty bad situation
- Tendency: make things worse
- Very few technical workarounds
- Demand change!

Free hardware

Free hardware doesn't exist today, or barely:

- Modifying is nearly **impossible**: new batch
- **PCBs** sometimes have schematics (Arduino, Goldelico GTA04)
- Producing complete mobile devices PCBs costs **a lot of money**
- **Chips** are not free hardware

Bottomline:

- Totally free hardware doesn't exist yet
- When partially possible (PCBs), it's never as easy as:
  gcc -o code code.c

Firmwares

Regarding integrated circuits:

- **Proprietary** firmwares in **nearly every** integrated circuit
- Not always possible to **replace** the firmware
- Free firmwares are **hard** to write
- Free firmwares exist for very **specific hardware**
  examples: Arduino, BusPirate, Milkymist One
- Firmwares **liberated** by the **manufacturer**
  example: **ath9k_htc**

Bottom line:

- Most loaded firmwares are **proprietary**
- Situation is not improving

Modem system

Modem system:

- Free GSM stack: **OsmocomBB**
- Supported devices are **old**
- **OmsocomBB** needs a **host computer** to operate
- Software **certification** and public networks

Modem system

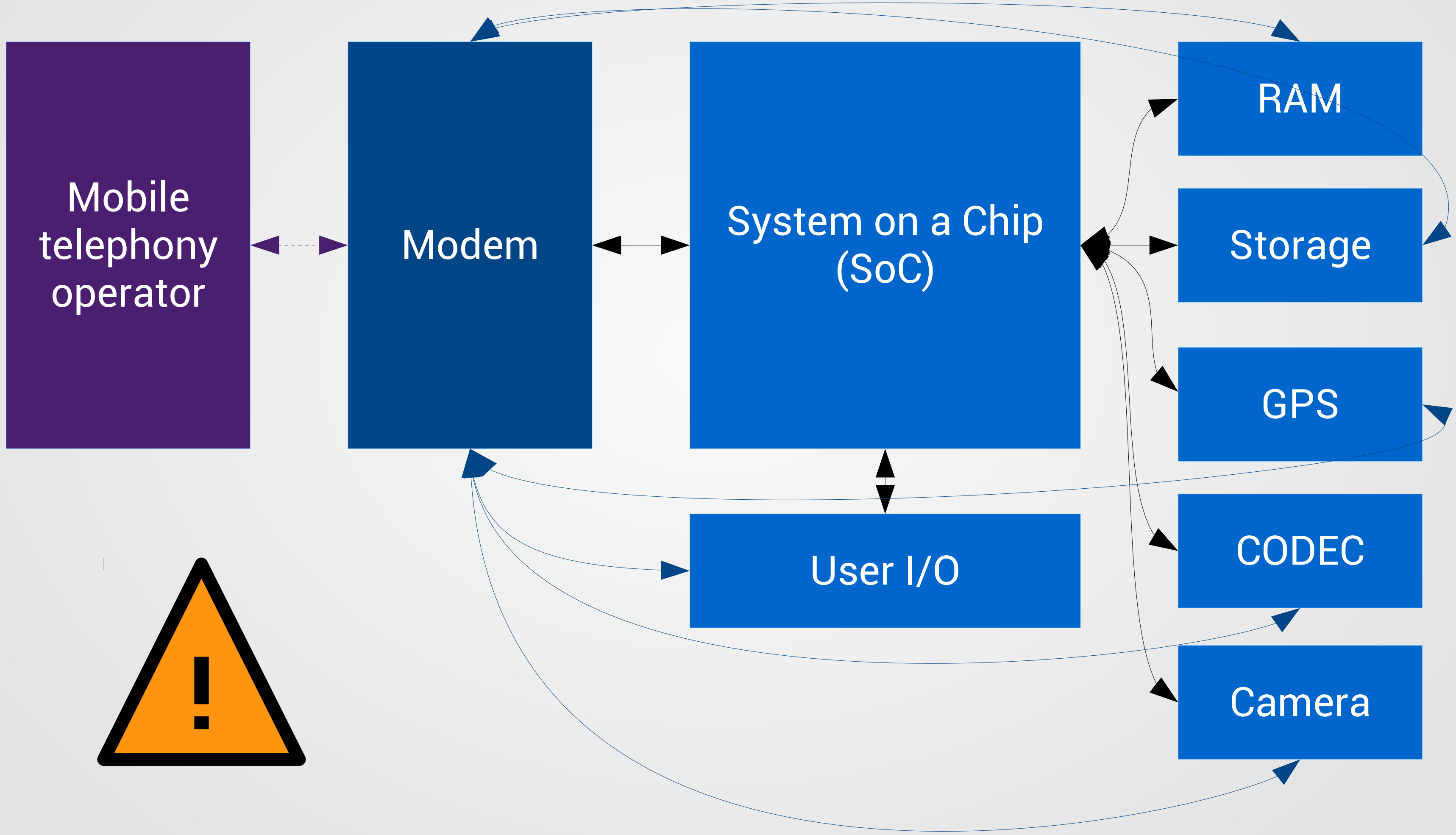
Modem system:

- Free GSM stack: **OsmocomBB**
- Supported devices are **old**
- **OmsocomBB** needs a **host computer** to operate
- Software **certification** and public networks

Crucial part for **security/privacy**:

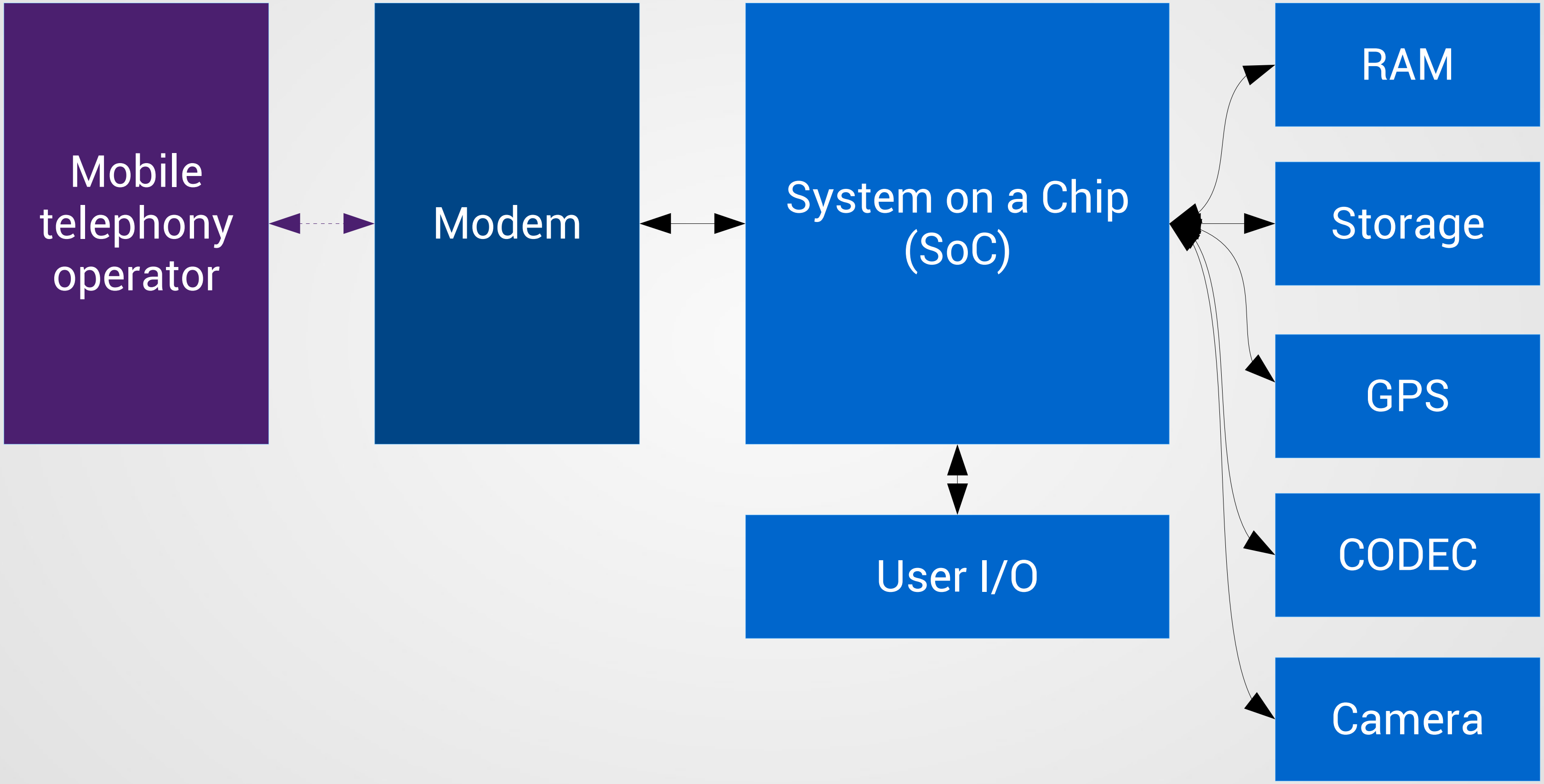
- **Nearly always** connected to the GSM network
- **Remote control**
- **Direct access** to more or less **critical** parts

Modem isolation



Bad modem isolation

Modem isolation



Good modem isolation

Modem isolation

Workaround for security/privacy: modem isolation.

- Ensures it cannot access **more than necessary**
- Ensures the modem cannot be used to spy
- Doesn't solve freedom issues
- There are still other ways to spy

Problem: how to make sure it's isolated?

- Leaked datasheets
- No free hardware
- Hints that it's bad: Linux kernel, datasheets, all-in-one
- Good faith and belief for the rest

Modem isolation

Bottom line:

- **Smartphones** use **proprietary** modem software
- **Hard** to improve the situation
- Modem **isolation** helps but is hard to figure out **reliably**
- Avoid obviously **bad platforms**

Note about **feature** phones:

- **Inexistent** modem isolation
- **Proprietary** software is in charge of **everything**

Bootloader

Back to the SoC, starting with the bootloader:

- The situation is **different** for every **platform**
- Primary and secondary bootloaders
- **Signature** checks, non-replaceable keys

Examples of good platforms:

- Allwinner Ax (when released or community-supported)
- TI OMAP (GP)

Bottom line:

- Good **platforms** exist
- **Signature** checks are very common
- Most high-end devices use **proprietary** bootloaders

Operating system

The operating system coordinates the dance:

- Access to every integrated circuit (I/O, camera, microphone, GPS)
- Access to the user's data
- Handles the user's communications

That's the most critical part for security/privacy!

- Direct interaction with the user:
  modifications, understanding, improving
- Knowledge about communication with the hardware

Very important for free software as well!

Operating system

Operating systems for mobile devices:

Mostly free systems:
- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- Open webOS

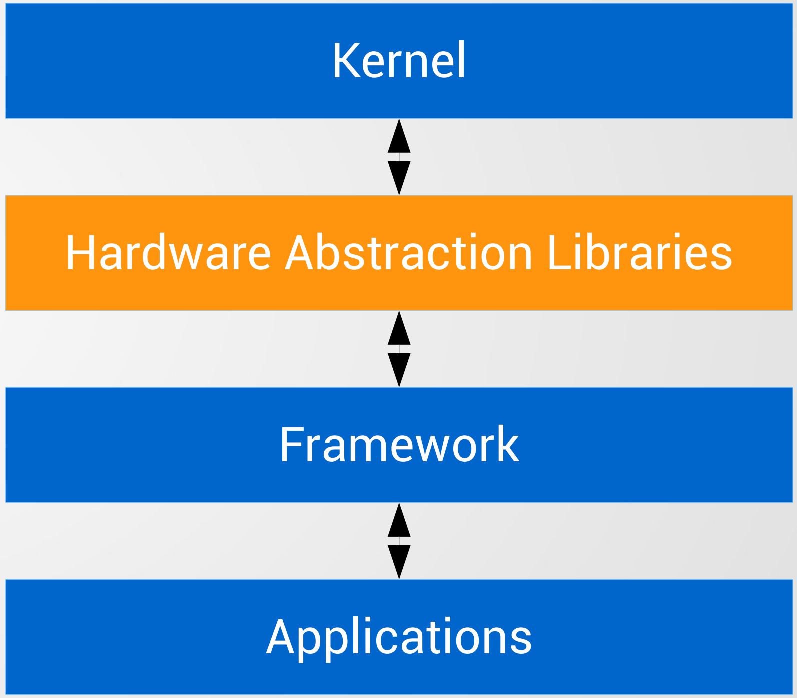
Mostly proprietary systems:
- Apple iOS
- Windows Phone

Operating system

Operating systems for mobile devices:

Mostly free systems:
- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- Open webOS

On most of these systems:
- Linux kernel
- Proprietary user-space drivers
- Free framework
- Free base applications



Free components
Proprietary component

Current situation

Overview of the current situation:

- ✗ No free hardware
- ✗ Non-free firmwares in integrated circuits
- ✗ Non-free modem systems
- ✓ Modem isolation (hard to figure out reliably)
- ✓ Free and unsigned bootloaders
- ✓ Mostly free systems

The situation isn't so great:

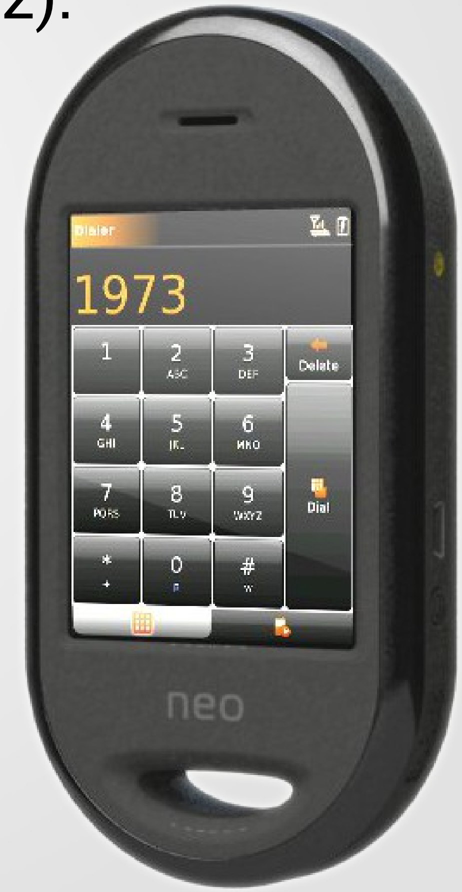
- If you care about freedom with no compromise or anything serious is at stake: **don't use any telephony-enabled device!**
- Else, you have to make compromises

Openmoko Neo Freerunner (GTA02)

Instead of giving up, let's push things **forward**!

Back in 2008, the Openmoko Neo Freerunner (GTA02):

- Free PCB design
- Isolated modem
- No loaded proprietary firmware
- Free bootloader
- Fully free GNU/Linux systems



Currently:

- Old device (400Mhz CPU, 128Mb RAM)
- Openmoko retired
- Community retired
- A few systems are still alive

Android and the HTC Dream

The same year, Google introduced Android and the HTC Dream:

- Proprietary bootloader
- Non-isolated modem
- Mostly free system with AOSP
- Proprietary hardware abstraction libraries

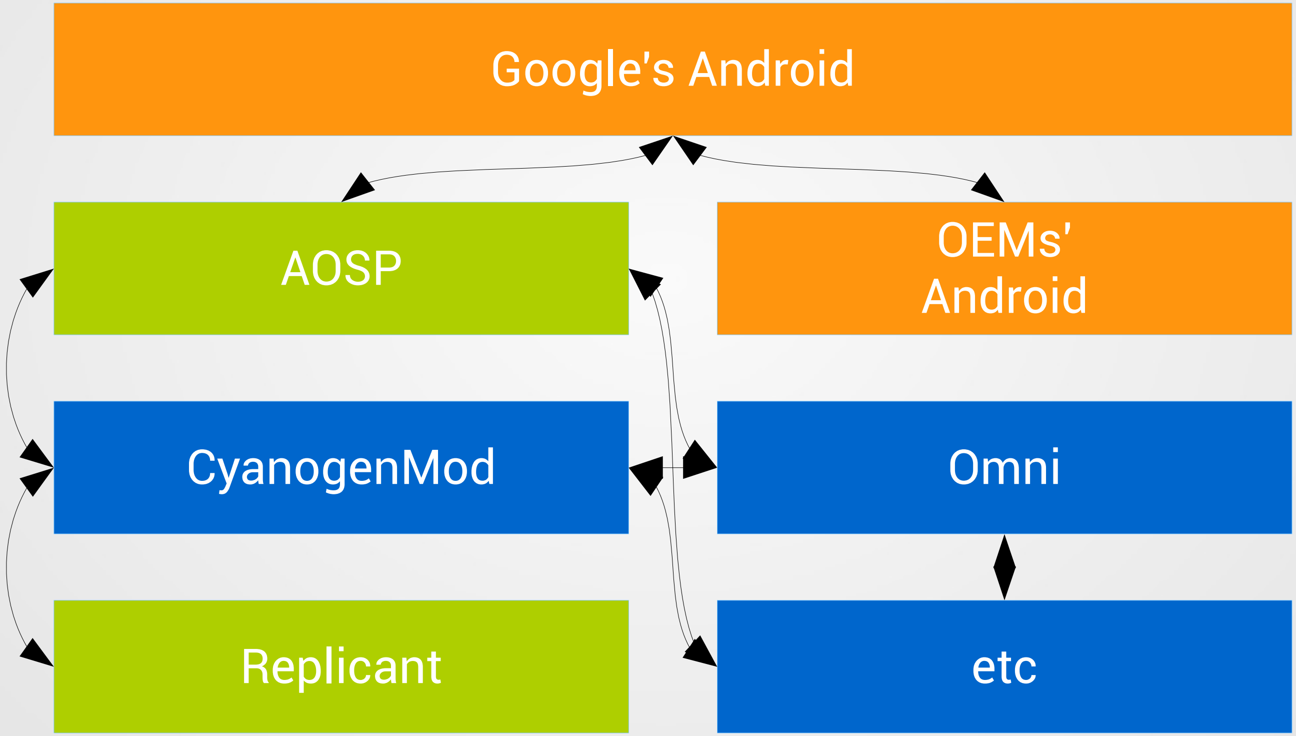
Not very good, but Android looked promising:

- Usable and stable interface
- Developed by a large group of people
- Large community of users and developers

Goal: freeing the HTC Dream. Replicant was born!

Taking a closer look at Android

Android is actually a family of operating systems:



Proprietary Android versions
Open source Android versions
Fully free Android versions

Taking a closer look at Android

Some facts about the Android Open Source Project:

- AOSP is nearly fully free software
- AOSP partially supports Google Nexus devices
- AOSP doesn't actually run on devices

To actually run on devices:

- Proprietary programs (HALs) and loaded firmwares are required

Community Android versions:

- Sometimes include proprietary applications
- Sometimes encourage Google applications
- Often include *malicious* features

Introduction to Replicant

Ideas behind Replicant:

- Make a fully free system out of Android
- Have something usable (graphics, audio, telephony)
- Replace or avoid proprietary parts
- Don't advocate the use of proprietary software
- Disable malicious features

Introduction to Replicant

Ideas behind Replicant:

- Make a fully free system out of Android
- Have something usable (graphics, audio, telephony)
- Replace or avoid proprietary parts
- Don't advocate the use of proprietary software
- Disable malicious features

Technically:

- Started as a derivative of AOSP
- Currently based off CyanogenMod (devices support)
- Ships with F-Droid, the free applications market

Replicant development

Development of Replicant:

- Currently 1 developer, on spare time
- Cleaning the CyanogenMod source code for Replicant: malicious features, adaptation for lacking functionalities
- Replacing proprietary HALs, with very little documentation
- Various fields: **audio**, **camera**, **modem**, **sensors**

Biggest part of the work on Replicant: reverse engineering

- Understanding how the proprietary components work
- Writing free software replacements

Complex tasks that Replicant doesn't deal with:

- Graphics acceleration (Freedreno, Lima)
- Firmwares
- Modem operating system

Replicant development

Over time, many free software replacements have been written:

- **RIL** (30000 lines, 9 devices)
- **Camera** (5500-10000 lines, 2 devices)
- **Audio** (4500 lines, 3 devices)
- **Sensors** (3000-4000 lines, 8 devices)

Working with other communities (teamhacksung):

- Including replacements
- Integrating Replicant's work in e.g. CyanogenMod
- Better for freedom
- Often technically better
- Porting to new versions of Android

Replicant support

As of today, Replicant 4.2 supports up to 12 different devices!

- Inherited CyanogenMod features and look
- Mostly Google Nexus and Samsung Galaxy devices
- Usable daily, with missing hardware features

Samsung Galaxy S 2 (I9100), Galaxy Note (N7000), Galaxy Nexus (I9250), Galaxy Tab 2 7.0 (P3100), Galaxy Tab 2 10.1 (P51xx), Galaxy S 3 (I9300), Galaxy Note 2 (N7100) :

- Proprietary and signed bootloaders
- Supposedly good modem isolation

Nexus S (I902x), Galaxy S (I9000):

- Proprietary and signed bootloaders
- Bad modem isolation

Replicant support

As of today, Replicant 4.2 supports up to 12 different devices!

- Inherited CyanogenMod features and look
- Mostly Google Nexus and Samsung Galaxy devices
- Usable daily, with missing hardware features

Goldelico GTA04:

- Free bootloader
- Supposedly good modem isolation
- Initial Android port
- Work in progress
- Well-documented protocols

Goldelico GTA04

In 2011-2012, Golden Delicious started the GTA04

- Motherboard replacement for the Openmoko FreeRunner (GTA02)
- Complete units available
- Other form factors

Reasonably efficient hardware:

- OMAP3 (DM3730), 800Mhz-1Ghz, 512Mb RAM
- GPS, sensors, Wi-Fi, bluetooth and more

Pretty good for freedom and security/privacy:

- Free bootloader
- Supposedly good modem isolation
- Friendly manufacturer
- Ships with Debian
- Community of users and developers: OpenPhoenux

OpenPhoenux

OpenPhoenux community:

- Dedicated to free software
- Aims to respect privacy
- Free hardware PCBs

Syndicates such projects:

- GTA04 and derivatives
- Neo900

More information:

- http://www.openphoenux.org/
- http://www.gta04.org/
- http://www.neo900.org/

Pre-order your GTA04A5 or Neo900!

Replicant

Replicant 4.2 0002 release:

- Initial support for the Goldelico GTA04
- Reduced dependency towards Google

A glance at Replicant's future:

- Stick to version 4.2 for a while
- Focus on devices that are good for freedom: GTA04, P970
- Support Wi-Fi-only tablets: Allwinner tablets, Kindle Fire, Nexus 7
- Integrate privacy and security enhancements

We need you to get involved!

- Replicant needs more than 1 developer
- Donations are welcome (devices are expensive)

Replicant

Learn more about Replicant:

- Website: http://www.replicant.us/
- Wiki/tracker: http://redmine.replicant.us/

Get in touch with us:

- Forums
- Mailing list
- IRC channel: #replicant at freenode

During the LSM/RMLL:

- Free Your Android Workshop (TD011, Polytech building)
- An overview of Replicant development (Wednesday, 9:40)
- ARM devices and your freedom (Wednesday 11:40)

That's all Folks!