Replicant: software freedom and Privacy/security on mobile devices

Paul Kocialkowski
paulk@replicant.us

Sunday 16 August 2015

Mobile devices

Mobile devices are **everywhere**: phones, tablets…

- Full computers (**hardware**, **systems**, **applications**)
- Possible to use **free** software

Mobile devices

Mobile devices are **everywhere**: phones, tablets…

- Full computers (**hardware**, **systems**, **applications**)
- Possible to use **free** software

Why free software?

- 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

Mobile devices are **everywhere**: phones, tablets…

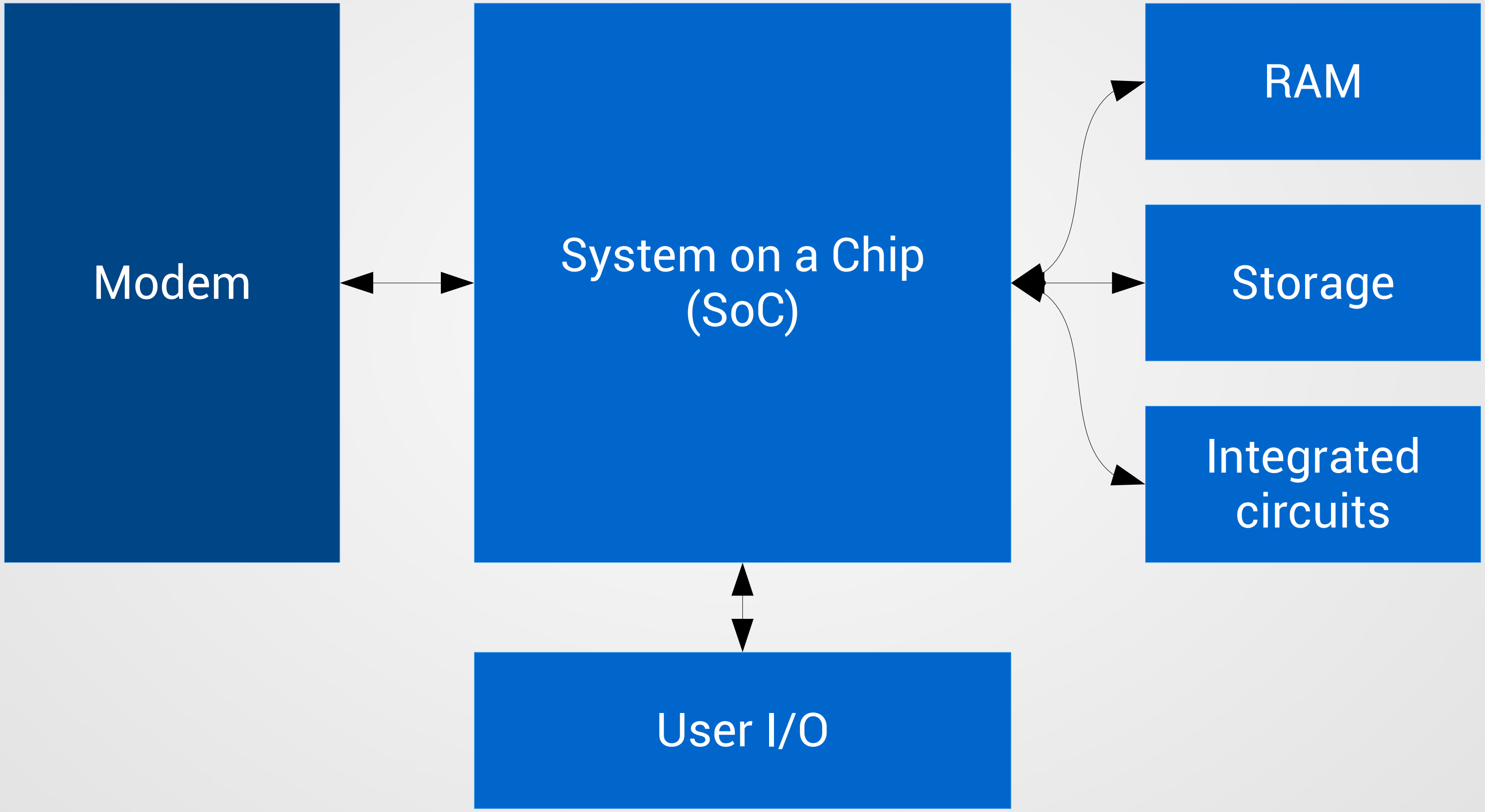
- Full computers (**hardware**, **systems**, **applications**)
- Possible to use **free** software

Why free software?

- 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

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

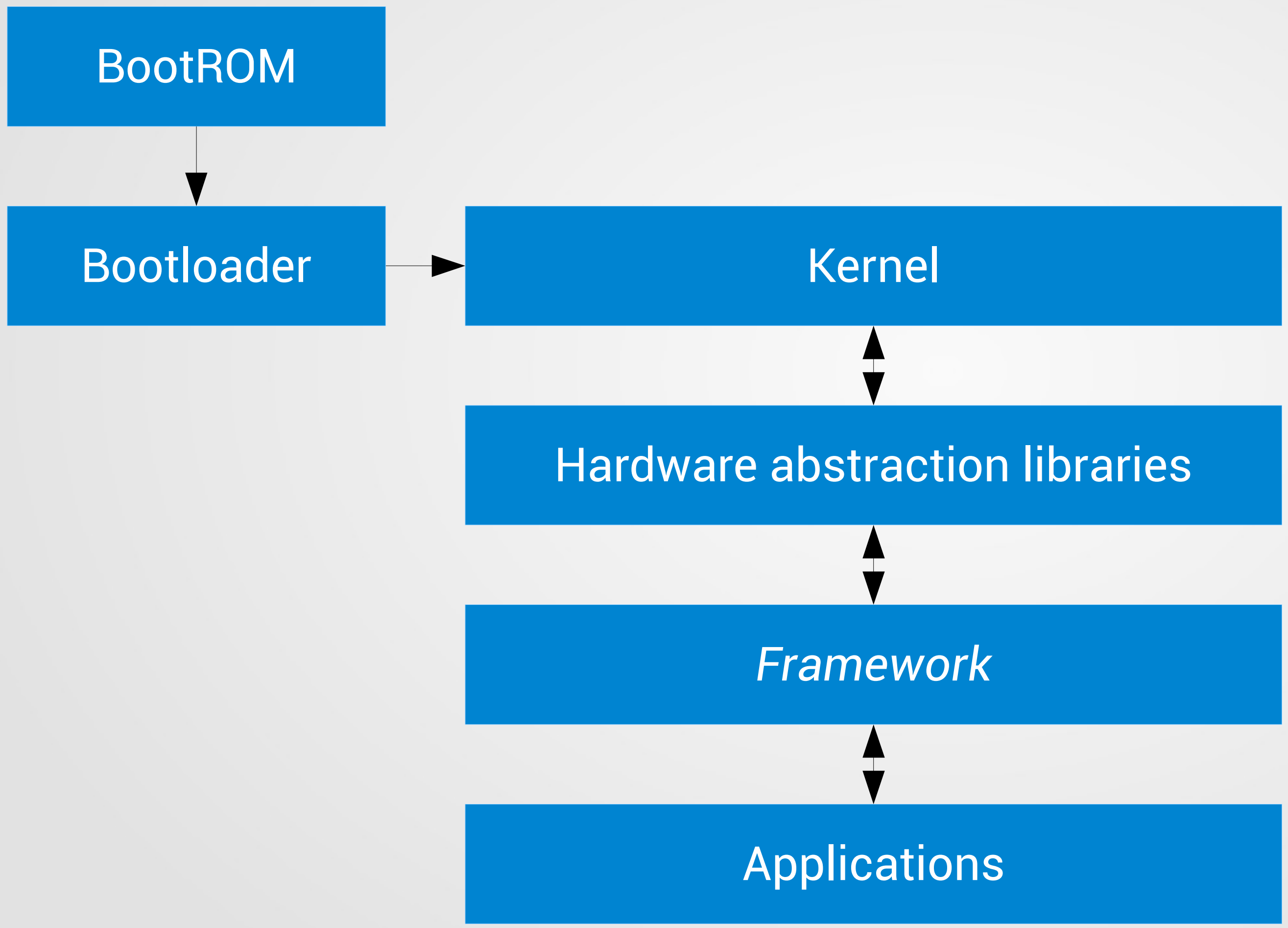
Mobile devices: simplified overview



Hardware-side overview

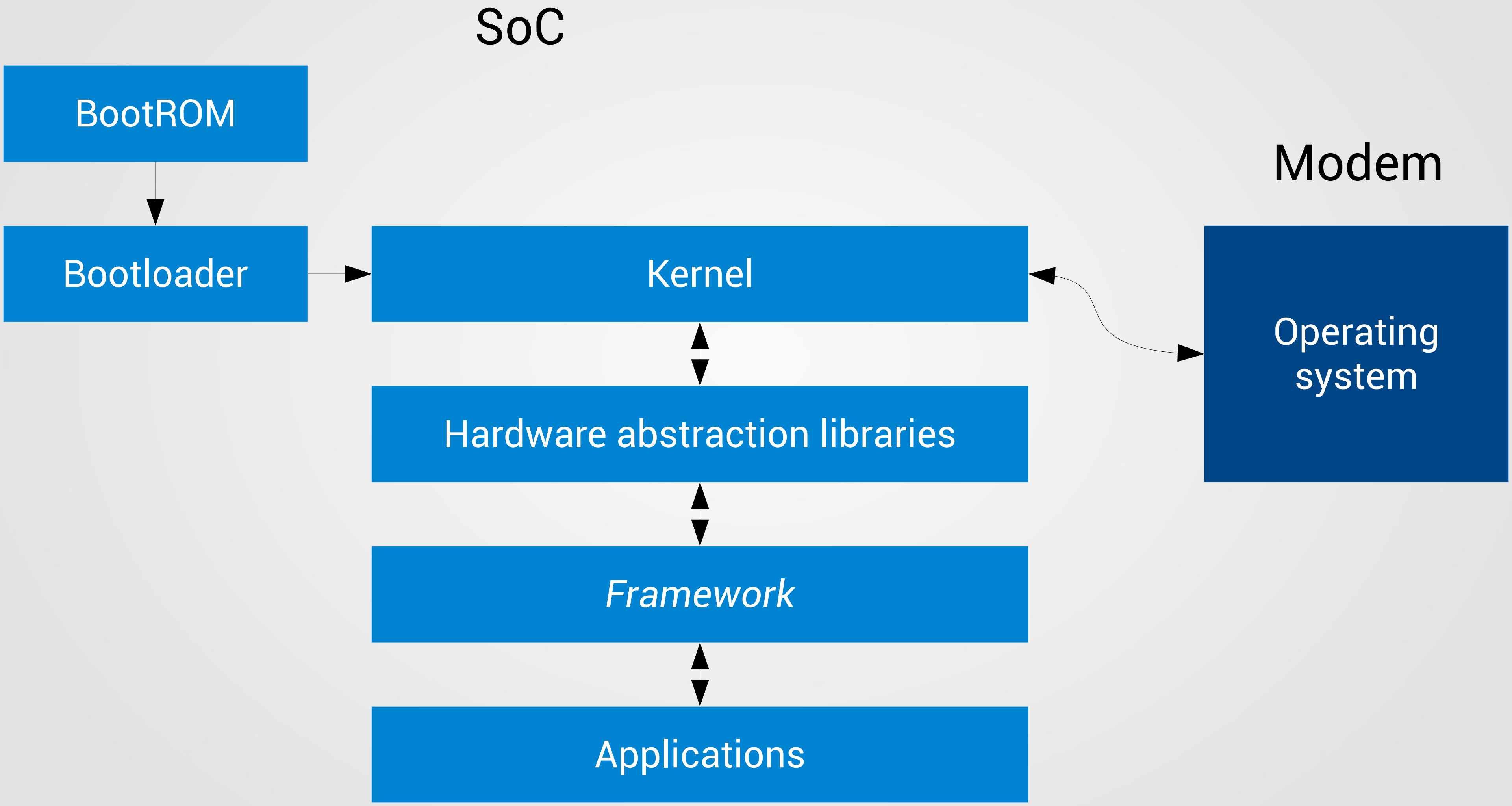
Mobile devices: simplified overview

SoC



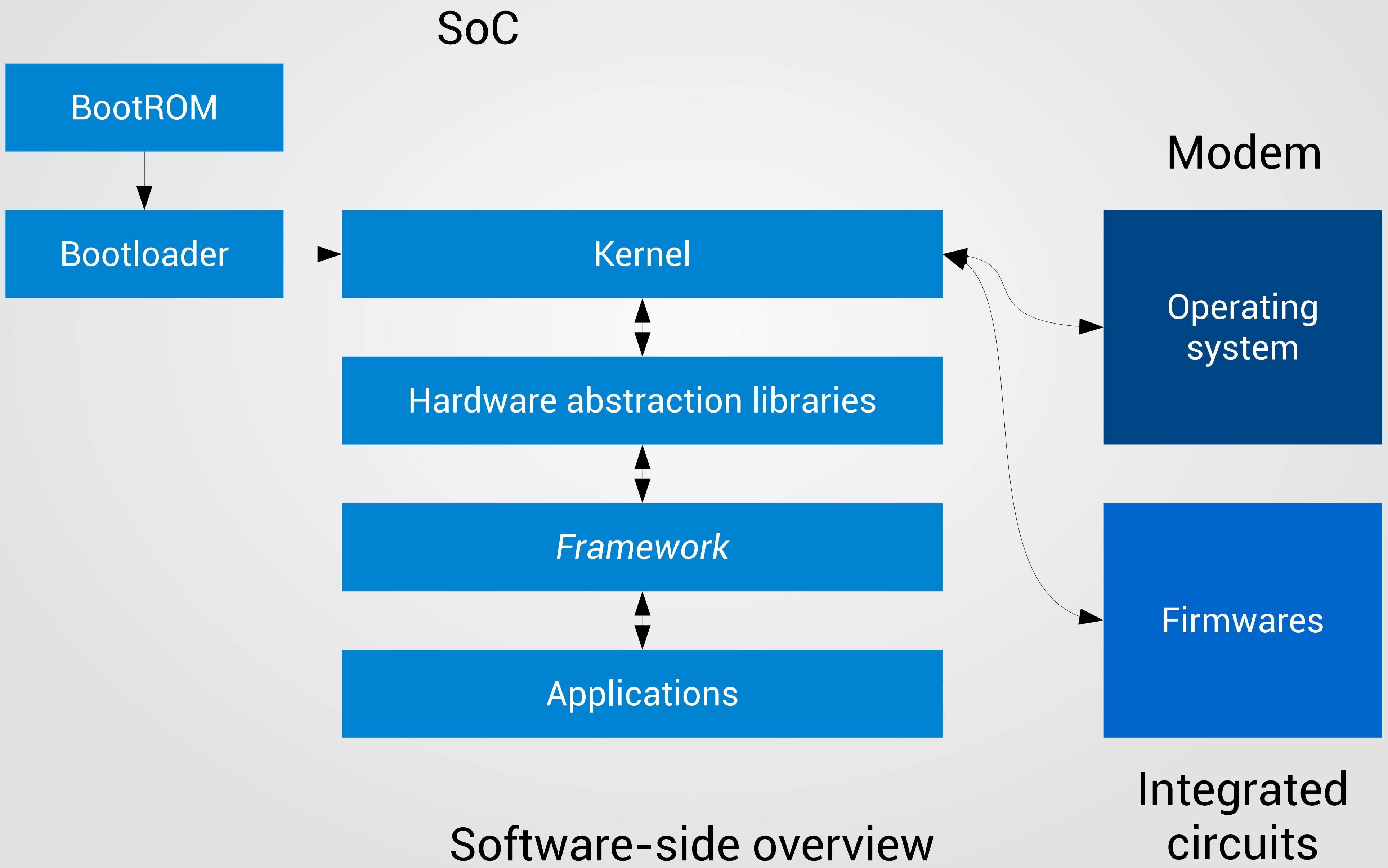
Software-side overview

Mobile devices: simplified overview



Software-side overview

Mobile devices: simplified 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**.

Free hardware

Free hardware doesn't exist today, or barely:

- Modifying is nearly **impossible** (new batch)
- **Printed circuits** designs are sometimes free in **free** and documented formats?
- **Expensive** for an individual
- **Integrated circuits** are not free hardware

- 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 (or hard) 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**

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**:

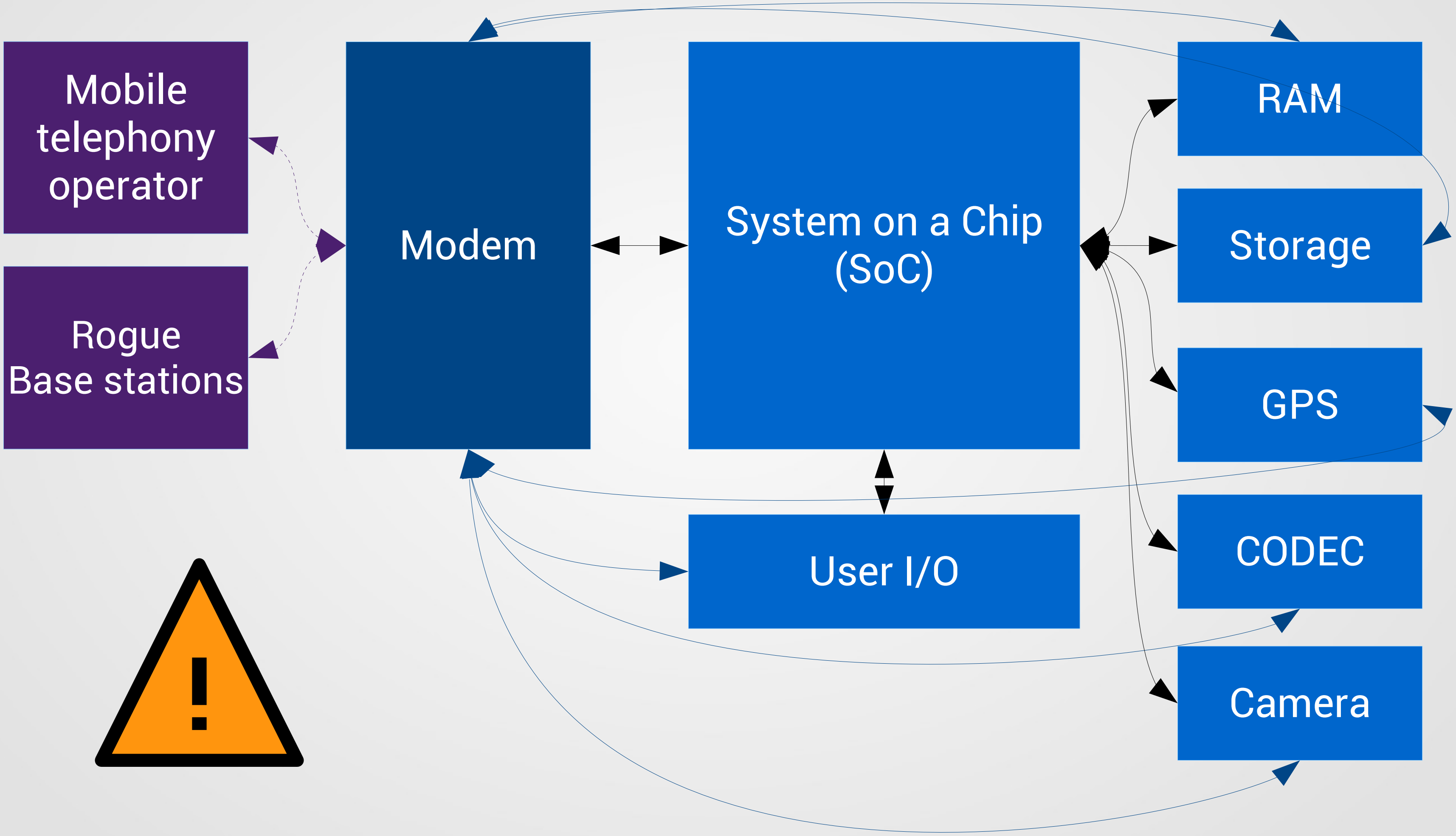
- **Nearly always** connected to the GSM network
- **Remote control**
- **Direct access** to more or less **critical** parts

Modem isolation

Workaround for security/privacy: modem isolation.

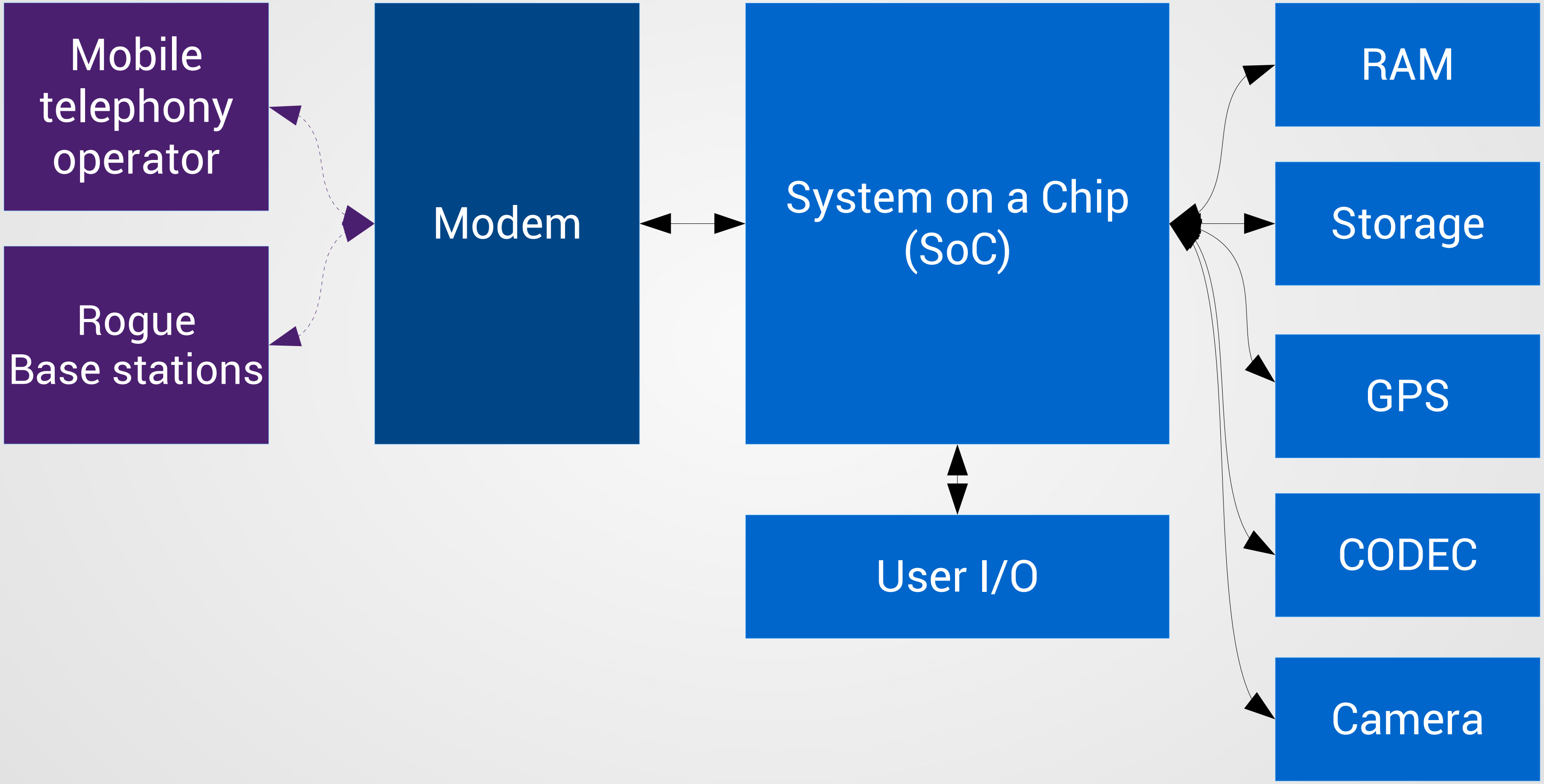
- Modem's access to the rest of the **hardware**
- Spying capabilities (GPS, microphone, camera)
- Ability to compromise the system (storage, RAM)

Modem isolation



Bad modem isolation

Modem isolation



Good modem isolation

Modem isolation

Workaround for security/privacy: modem isolation.

- Modem's access to the rest of the **hardware**
- Spying capabilities (GPS, microphone, camera)
- Ability to compromise the system (storage, RAM)

- Doesn't solve **freedom** issues
- Other means to **spy** on the user

Problem: how to check for **isolation**?

- Hints of a **bad situation**
- Platforms with **interated** modem
- Leaked **documentation**
- No **free hardware** !
- Good faith and **trust**

BootROM, bootloader

About the main processor :

- BootROM: non-free, read-only
- **Signature** checks
- **Non-replaceable** keys, rarely leaked
- Free **bootloaders** exist (U-Boot, etc)

Examples of good platforms:

- Freescale i.MX
- Allwinner
- TI OMAP (GP)
- nVidia Tegra (non-ODM)
- Rockchip ?

Operating system

The operating system coordinates the dance:

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

That's the most critical part for security/privacy!
Samsung Galaxy Back-door

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

Very important for free software as well!

Operating system

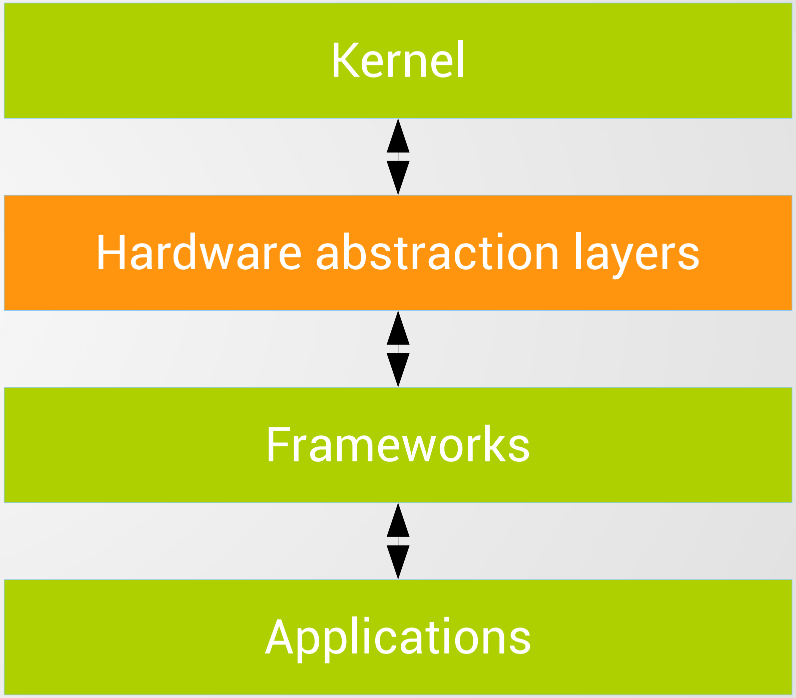
Operating systems for mobile devices:

Mostly-free systems:

- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- Open webOS

On most of these systems:

- Linux **kernel**
- **Proprietary** drivers
- Free **framework**
- Free base **applications**
- Various free **applications**



Free parts
Proprietary parts

Current situation

Overview of the current situation:

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

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

Replicant

> *“Replicant is a fully free Android distribution running on several devices, a free software mobile operating system putting the emphasis on freedom and privacy/security"*

- Pragmatic way for **software freedom** on **mobile devices**
- Started in mid-2010: **Openmoko FreeRunner** and **HTC Dream**
  AOSP, ***community*** *versions*
- **Fully free** version of Android
- **Ethical** project that **respects** users
- Functional and **usable** daily
- **Privacy** enhancements

Replicant development

Technical grounds:

- **AOSP** base at first
- **CyanogenMod** for more devices

Implications of a fully free system:

- **Remove** or **replace** proprietary parts:
  executables, libraries, firmwares
- Get rid of **malicious features**
  tracking, statistics, etc

Additional work:

- **Adapt** the system for the lack of proprietary components:
  graphics acceleration, firmwares loading
- "**Branding**", look and feel
- Maintenance, **security** updates

Replicant advancement timeline

December 2010	January 2011	April 2011	Summer 2011
Replicant 2.2			
HTC Dream	Nexus One	SDK	libsamsung-ipc

November 2011	January 2012	April 2012	September 2012
Replicant 2.3			
Nexus S (I902x)	Samsung-RIL	Galaxy S (I9000)	GTA04

November 2012	January 2013	April 2013	July 2013
Replicant 4.0			
Galaxy Nexus (I9025) Galaxy S 2 (I9100)	SDK	Galaxy Tab 2 10.1 (P51xx) Galaxy Tab 2 7.0 (P31xx)	Galaxy S 3 (I9300)

October 2013	January 2014	June 2014
Replicant 4.0	Replicant 4.2	
Galaxy Note (N7000)	Galaxy Note 2 (N7100), SDK	GTA04

Challenges in new devices

Samsung devices:

- RIL: **Samsung-RIL**, **libsamsung-ipc**, device-specific transport
  Rewrite during summer 2014

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

- Camera: preview, EGL
- Sensors: accelerometers, magnetic field sensors

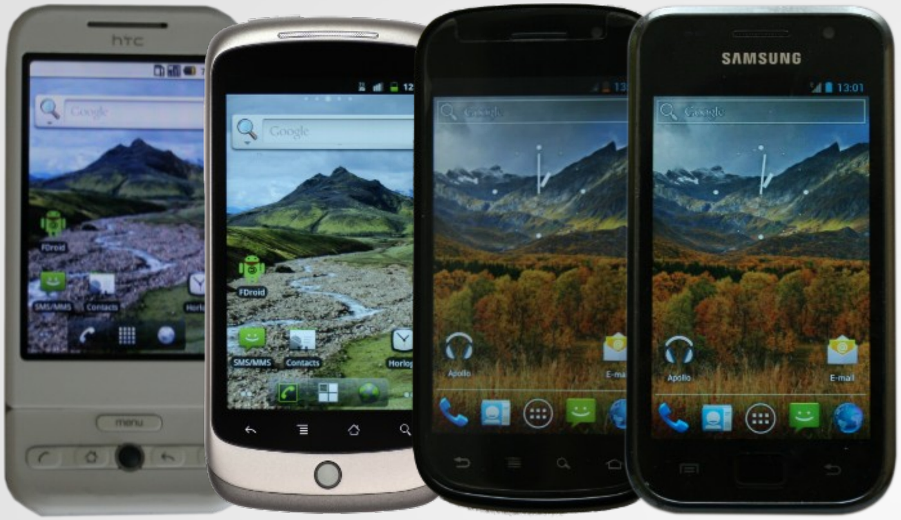
Galaxy S 2 (I9100), Galaxy Note (N7000):

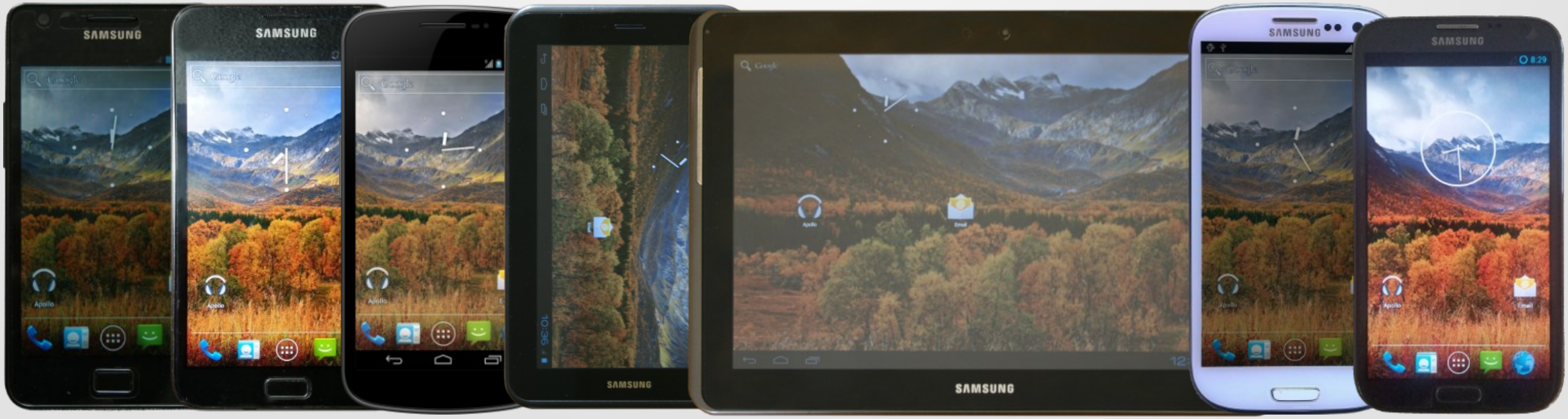
- Audio: Yamahell, **Yamaha-MC1N2-Audio**, **TinyALSA-Audio**
- Camera: **Exynos Camera**

Galaxy S 3 (I9300), Galaxy Note 2 (N7100):

- Camera: **Exynos Camera** rewrite, S5C73M3 interleaved format
- Sensors

Supported devices





Supported devices

Bad modem isolation

⚠

Supported devices

Proprietary and signed bootloaders

⚠

State of the Replicant project

Current state of the project:

- Lead by a **single** developer, on **spare** time
- Very few **external** contributions (security)
- Supports up to **12** different devices
  mostly Samsung Galaxy and Nexus devices
- Based on CyanogenMod 10.1, Android 4.2
- Funded thanks to **donations**

Recent achievements:

- Devices more **respectful** of **freedom**
- **Code source** situation
- **Security** updates

Challenges and directions for Replicant

Challenges for the future:

- Trust in **CyanogenMod**, OmniROM
- New **versions**, devices support
- Google applications and **AOSP**

Directions for the project:

- Next version : **4.4**?
- Support for more devices **respectful** of freedom and privacy/security
- Improvements for privacy/security

Future and projects for Replicant

Wiki updates :

- Devices evaluations, information:
  bootloaders, privacy/security, modem isolation
- Research about other devices
- **Documentation** about **uncompleted** projects (GPS, etc)

Privacy/security:

- **Security-oriented** version of Replicant?
  *breaking some **fonctionalities***
- Support for **modem-less** devices (Wi-Fi tablets)

Future and projects for Replicant

Supporting **better** devices:

- Free **hardware designs**
- **Documented** hardware
- Supposedly-good **modem isolation**
- Free **bootloader**
- Friendly chips for **free drivers**

OpenPhoenux community:

- **GTA04**, **Letux** devices
- **Neo900**

Mainstream devices:

- LG **Optimus Black** (**P970**)
- **Kindle Fire** (first generation)

Cheap chinese devices:

- **Allwinner** tablets
- **Rockchip** tablets

Other **form factors**!

Replicant

Learn more about Replicant:

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

Join the community:

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

The project needs you!

- Replicant deserves more than one developer
- Donations are welcome (devices are expensive)

That's all Folks!