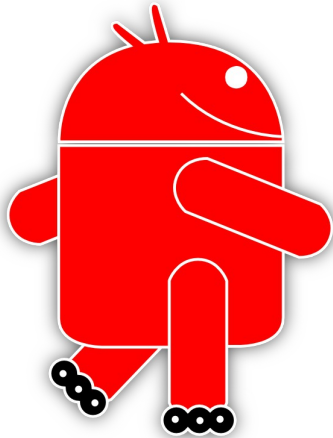


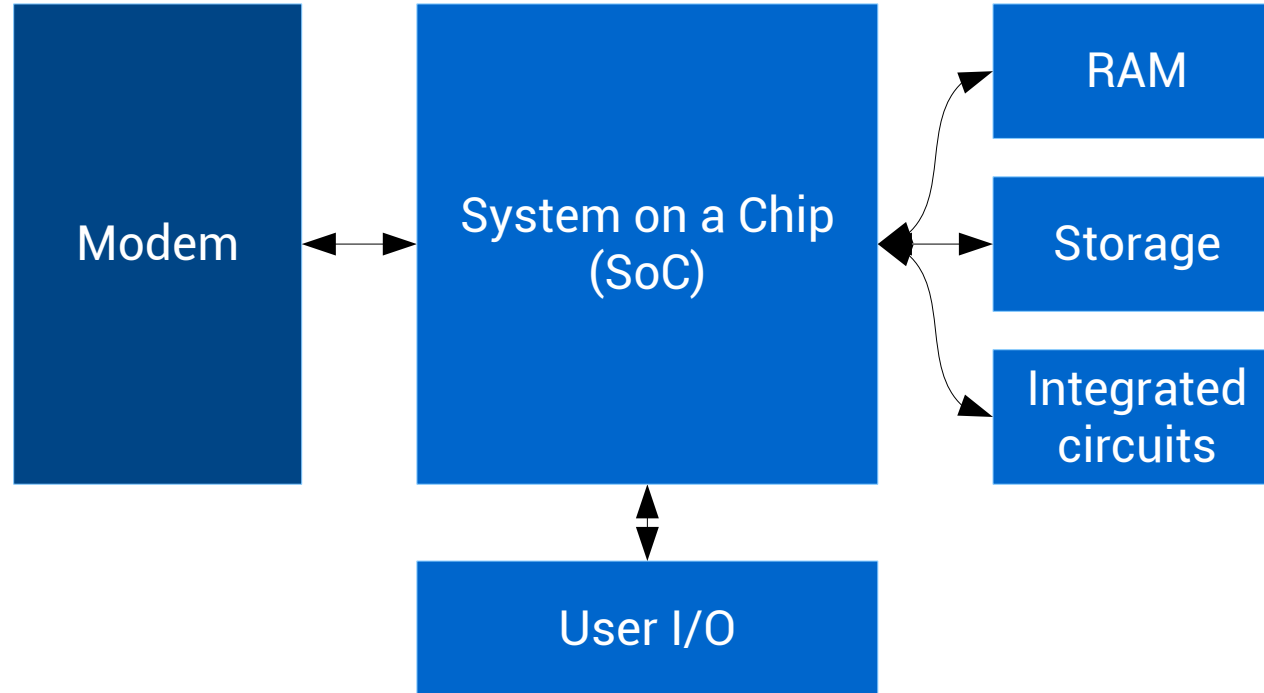
Replicant

software freedom on mobile devices



Paul Kocialkowski
paulk@replicant.us

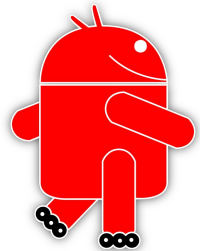
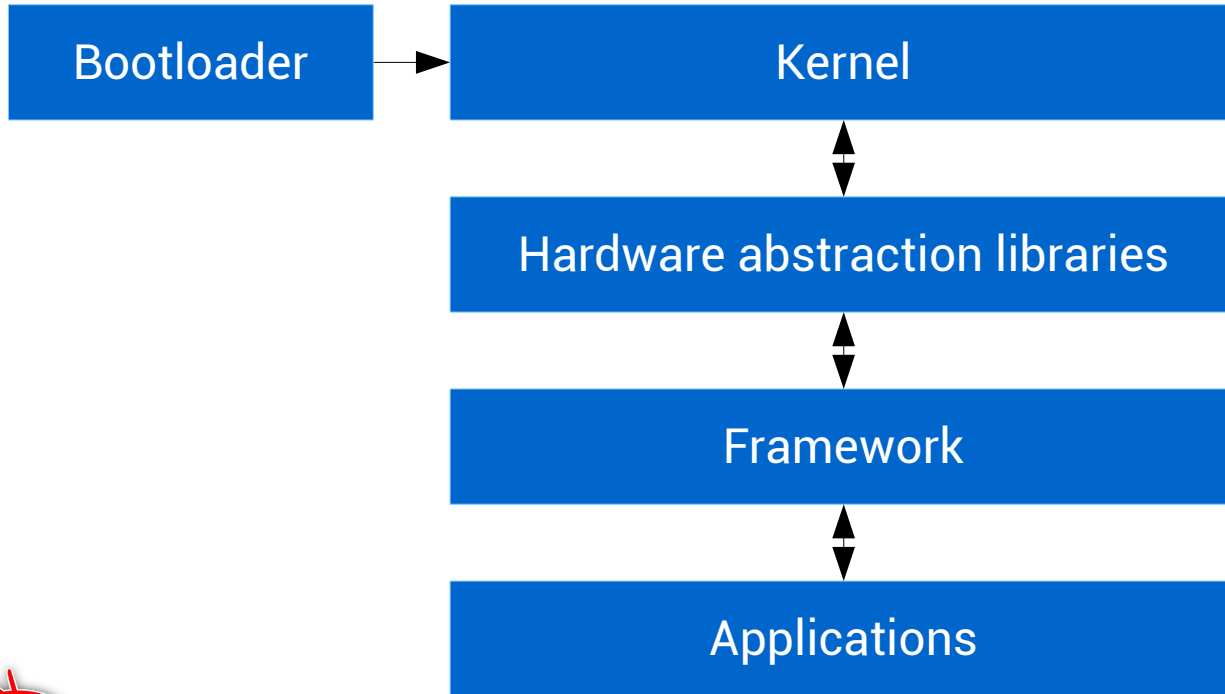
Simplified overview of mobile devices:



Hardware-side representation

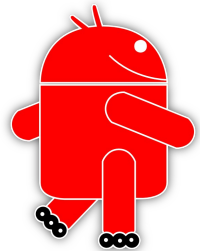
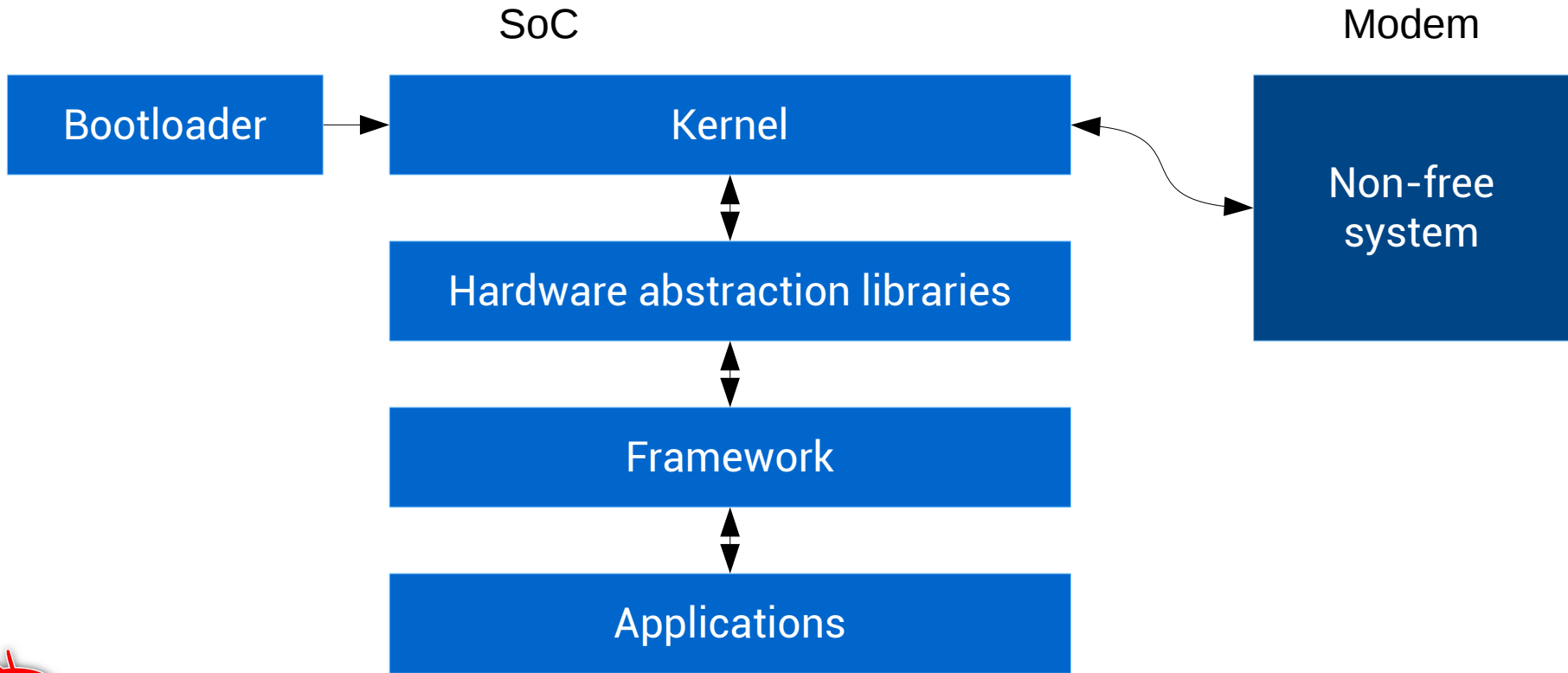
Simplified overview of mobile devices:

SoC



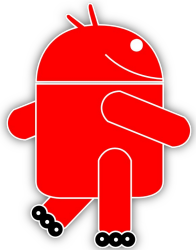
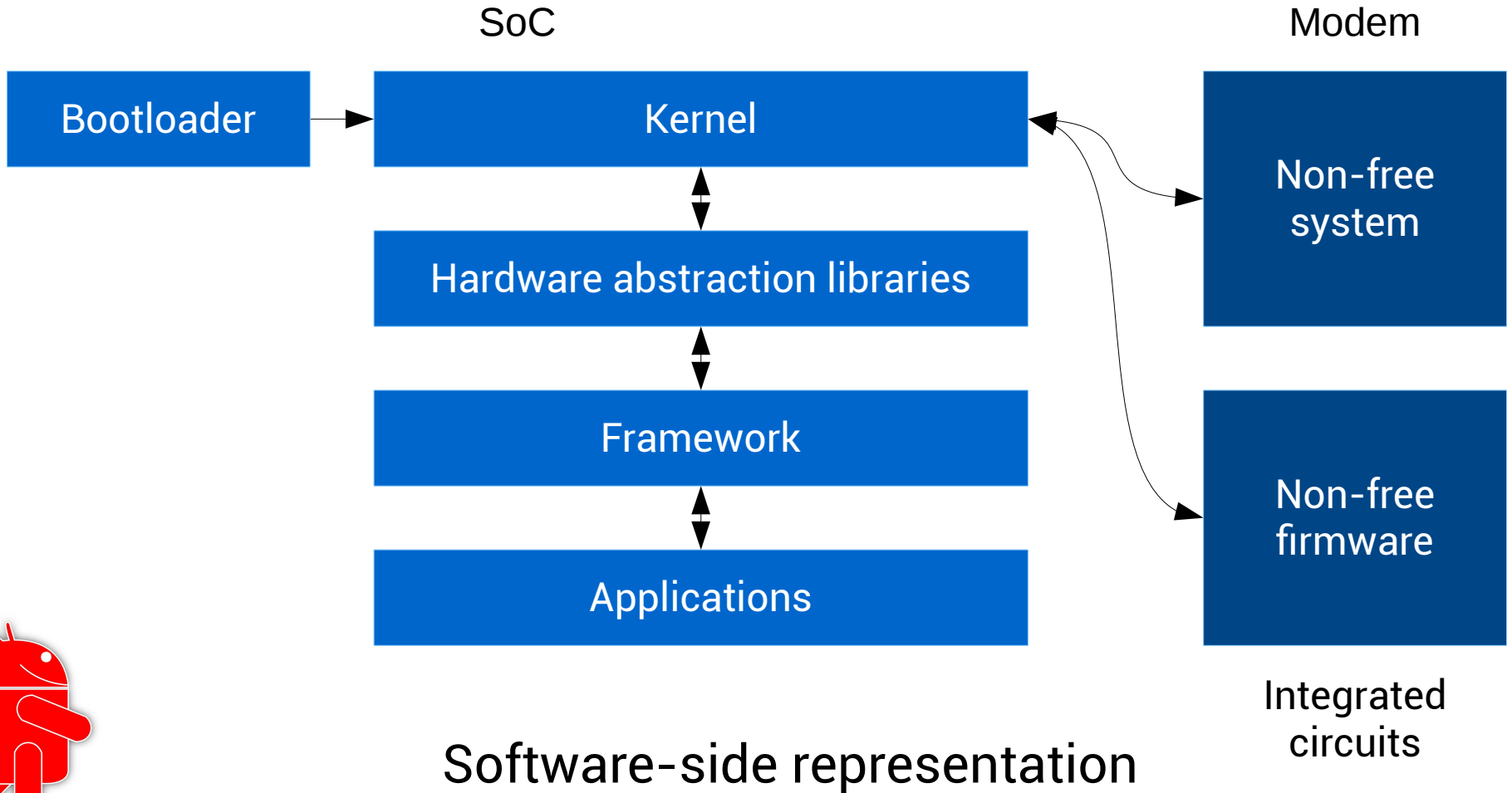
Software-side representation

Simplified overview of mobile devices:



Software-side representation

Simplified overview of mobile devices:



Ideal mobile device and best case scenario:

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



Ideal mobile device and best case scenario:

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

Guarantees from mobile telephony operators:

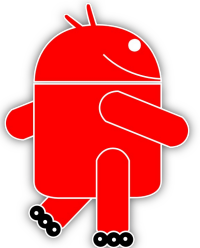
- ✓ **Neutral** access to the Internet
- ✓ No **interception** of the data
- ✓ No collection of the users **positions**



The actual situation today is far from ideal.

Firmwares:

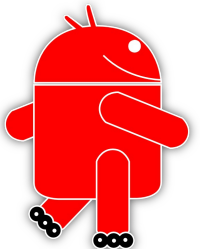
- **Proprietary** firmwares in **nearly all** integrated circuits
- Not always possible to **replace** the firmware
- Free firmwares are **hard** to write
- Free firmwares exist for very **specific hardware**
Exemples: Arduino, BusPirate, Milkymist One
- Firmwares **liberated** by the **manufacturer**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



The actual situation today is far from ideal.

Modem system:

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



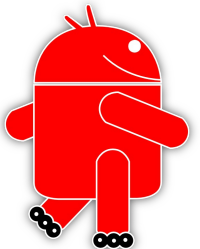
The actual situation today is far from ideal.

Modem system:

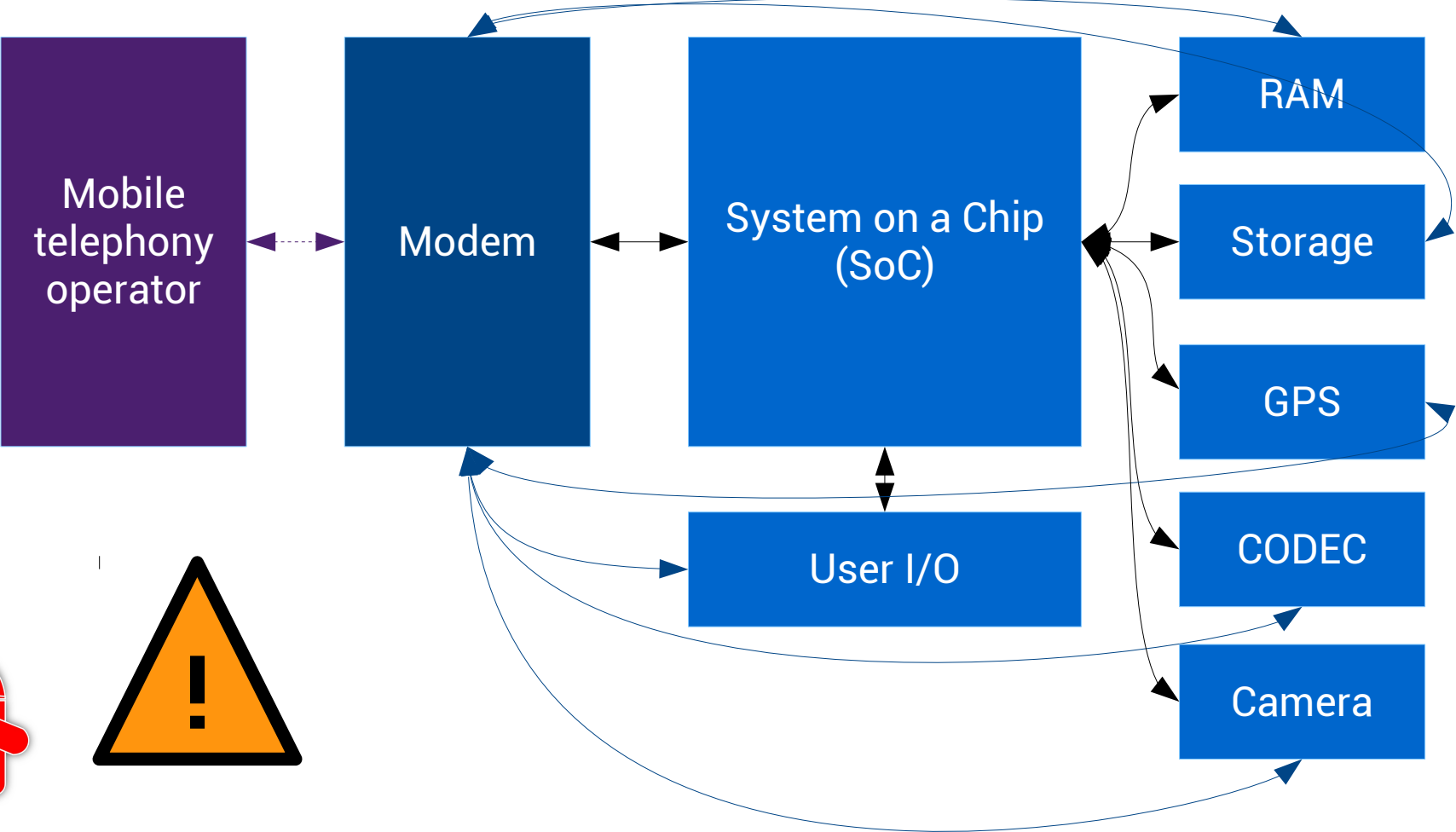
- Free GSM stack: **OsmocomBB**
- Supported devices are **old**
- **OsmocomBB** needs a **host computer** to operate
- Software **certification** and public networks

The **modem** is one of the most important parts for **security!**

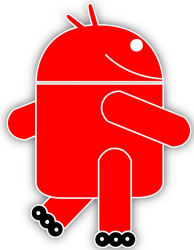
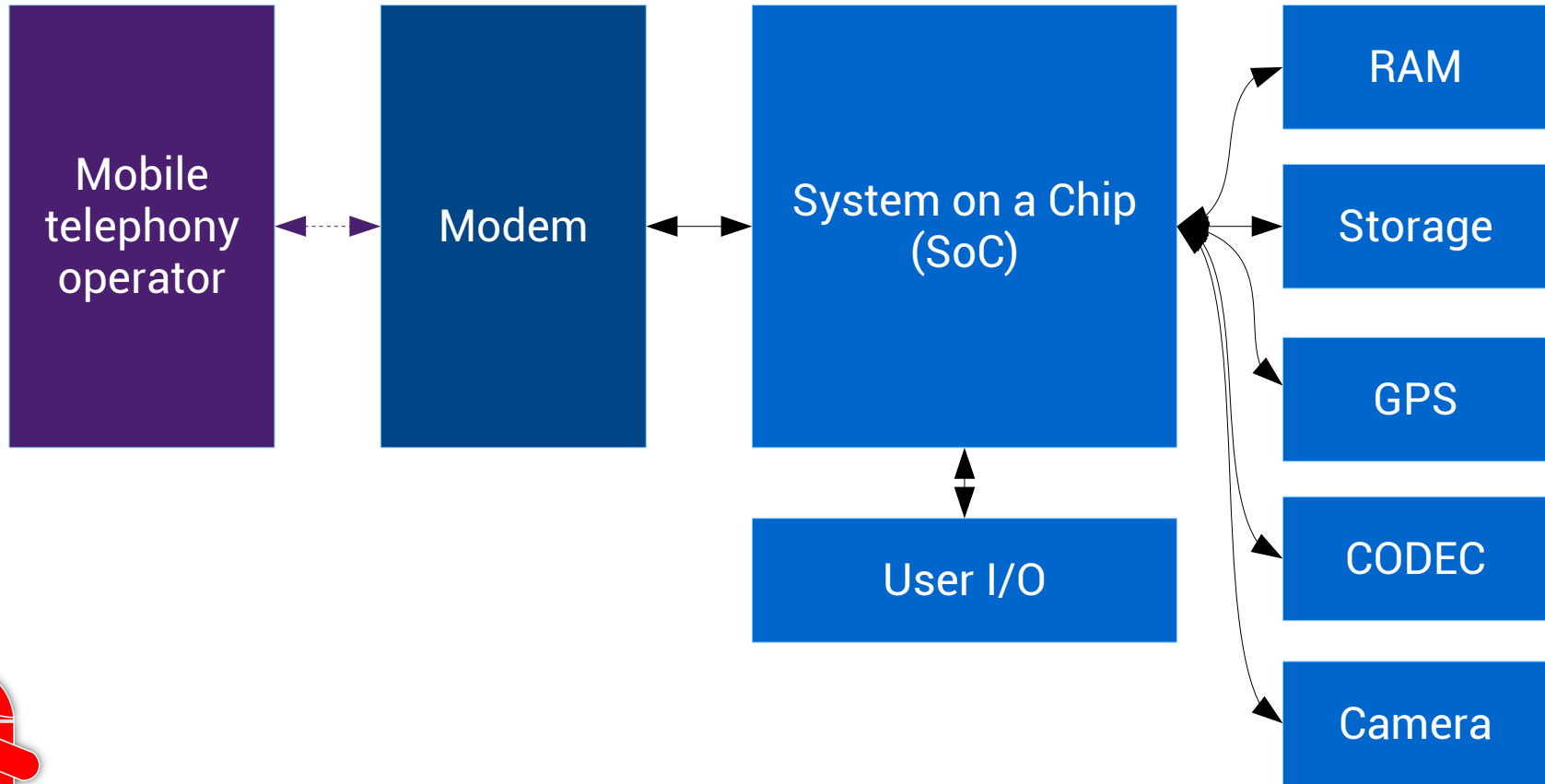
- **Nearly always** connected to the GSM network
- **Remote control**
- **Hardware access**

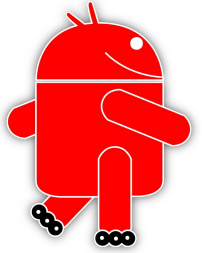


Bad modem isolation:



Good modem isolation:



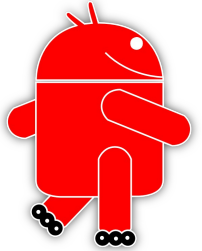


The actual situation today is far from ideal.

Bootloaders:

- Depends on the hardware platform:

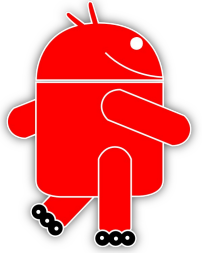
Platform	TI OMAP	Samsung Exynos	Qualcomm Snapdragon	Mediatek	Allwinner
Primary loader	Free (X-Loader)	Non-free	Non-free	Non-free	Free
Secondary loader	Free (U-Boot)	Possible (U-Boot, Coreboot)	Non-free	Free? (U-Boot)	Free (U-Boot)
Signature	Depends	Depends	?	Depends	No



The actual situation today is far from ideal.

Various so-called **free** systems:

- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- ...



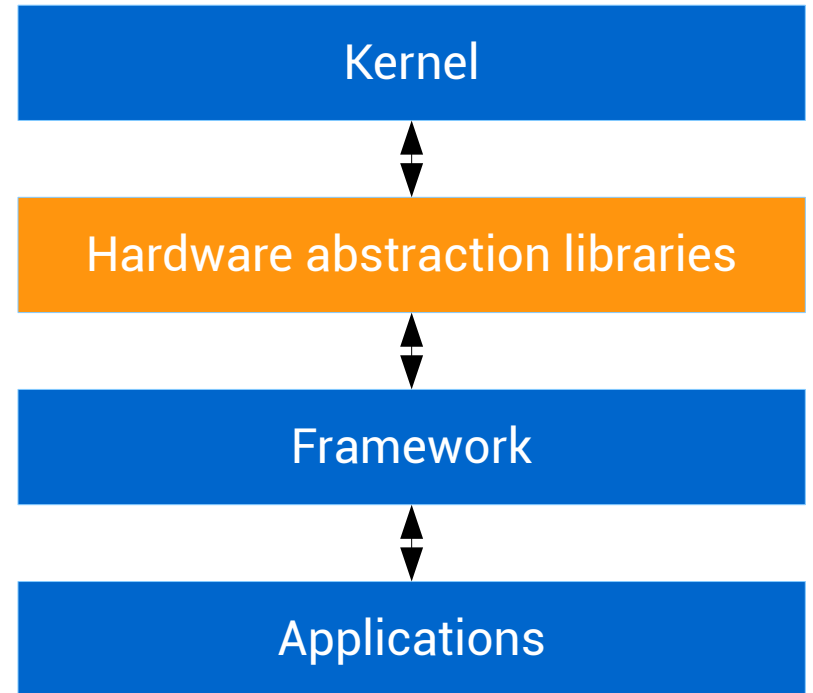
The actual situation today is far from ideal.

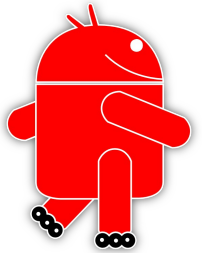
Various so-called **free** systems:

- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- ...

Free components

Proprietary components





The current situation:

- ✗ Locked hardware
- ✗ Non-free firmwares
- ✗ Non-free modem systems
- ✓ Modem isolation is possible
- ✓ Free and unsigned bootloaders exist
- ✓ Free system?

Bottomline:

- 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

Taking a closer look at free systems, back in 2008:

OpenMoko:

- Free hardware design
- Isolated modem
- Free bootloader
- Fully free GNU/Linux systems

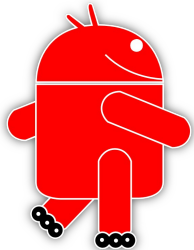


Taking a closer look at free systems, back in 2008:

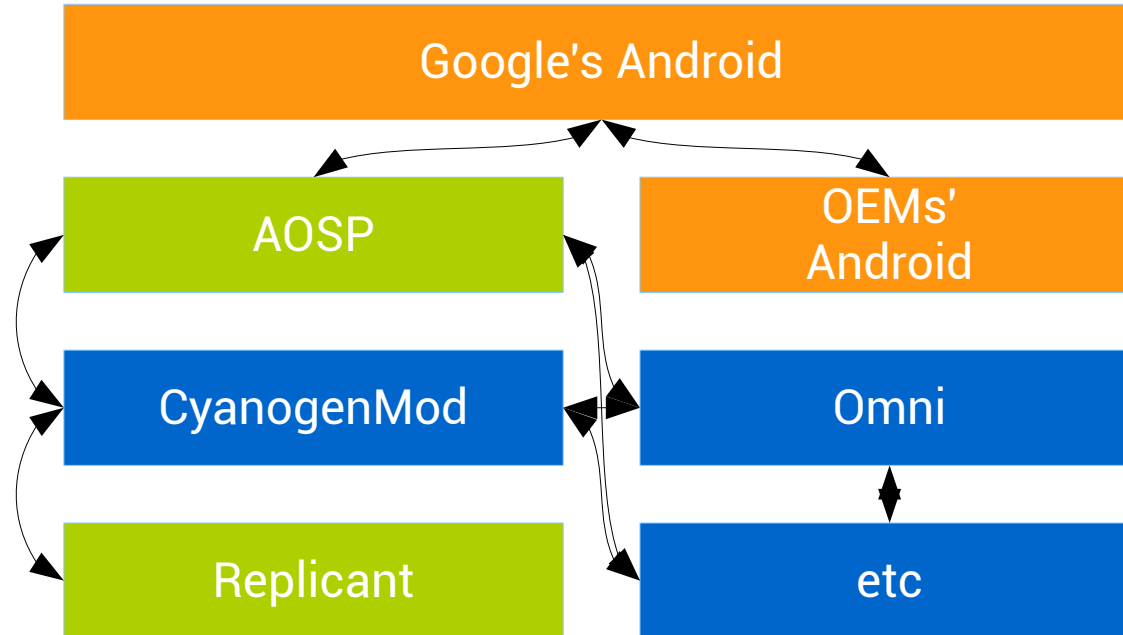
Android and the HTC Dream/Google G1/ADP1

- Proprietary bootloader
- Unisolated modem
- Free system with AOSP (android.git.kernel.org)
- Proprietary hardware abstraction libraries

Goal: freeing the HTC Dream. Replicant was born!



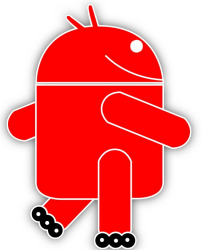
Android is actually a family of operating systems:



Proprietary Android versions

Open source Android versions

Fully free Android versions

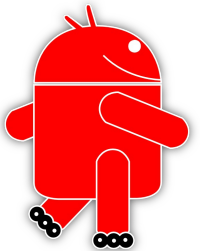


“ Replicant is a fully free version of Android running on several devices “

- AOSP doesn't run on devices

Other community Android versions:

- Proprietary libraries
- Proprietary firmwares
- Sometimes proprietary applications
- Sometimes encourage Google applications
- Often include *malicious* features



“ Replicant is a fully free version of Android running on several devices “

- Replicant is based upon CyanogenMod
- Proprietary libraries replaced or avoided
- Proprietary firmwares not distributed
- Malicious features removed
- F-Droid: free software market with free software applications

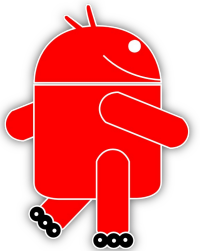


“ Replicant is a fully free version of Android running on several devices “

- Aims to be usable on actual devices
- Most of the work: replacing proprietary components
- Lots of code to write, little documentation
- Various aspects: **audio, camera, modem, sensors, etc**

Complex tasks, not dealt with:

- Firmwares
- Graphics acceleration, 3D



“ Replicant is a fully free version of Android running on several devices “

Most of the work:

- Understanding proprietary components
- Writing free software replacements

Working with other communities (teamhacksung):

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



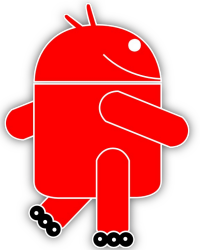
“ Replicant is a fully free version of Android running on several devices “

Learn more about Replicant:

- Website: <http://replicant.us>
- Wiki/tracker: <http://redmine.replicant.us>

Get in touch with us:

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





That's all Folks!



Text and diagrams:

- © Paul Kocialkowski, CC BY-SA 3.0

Pictures:

- **Android robot:** © Google, CC BY 3.0
- **Replicant robot:** © Mirella Vedovetto, Paul Kocialkowski, CC BY-SA 3.0
- **Openmoko Neo FreeRunner.** © FIC/OpenMoko, CC BY-SA 3.0
- **F-Droid logo:** © William Theaker, Robert Martinezi, CC BY-SA 3.0
- **Other pictures:** © Paul Kocialkowski, CC BY-SA 3.0