

Extending the lifetime of smartphones with Replicant, a fully free Android distribution

Denis 'GNUtoo' Carikli and David 'dllud' Ludovino

July 3, 2020

Introduction

Replicant:

- ▶ Fully free Android distribution approved by the FSF
- ▶ But the hardware it runs on is not...
- ▶ More details on hardware related freedom issues later

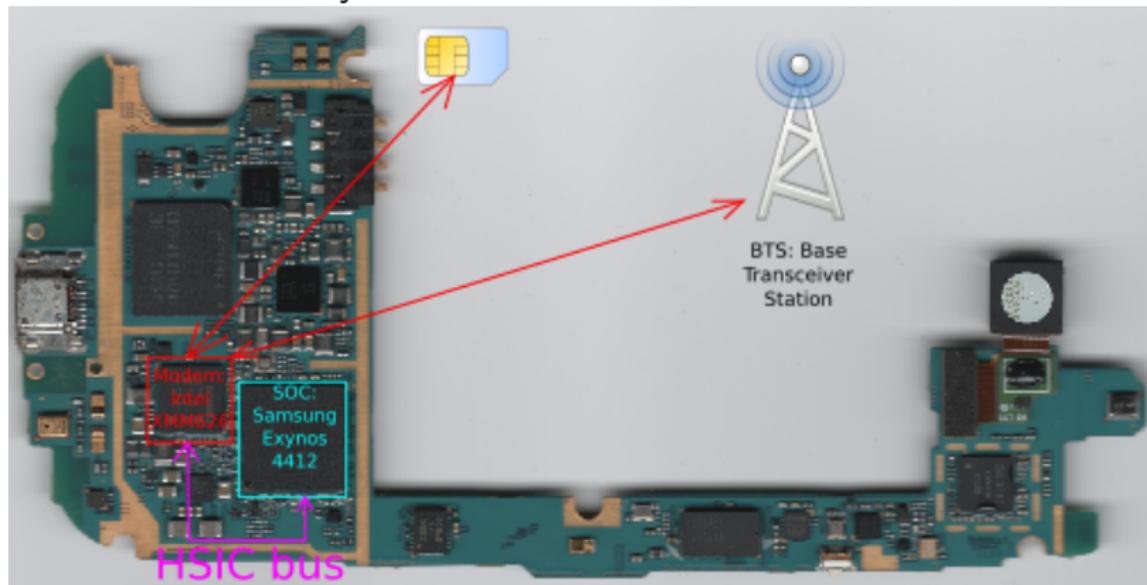
Quick Facts

- ▶ Website: replicant.us
- ▶ Exists since September 2009
- ▶ Currently based on LineageOS
- ▶ Android versions:
 - ▶ Replicant 6: Android 6, last security update: October 2017[?]
 - ▶ Replicant 9: Android 9, work in progress[?]
- ▶ Supports ~ 10 devices (smartphones and tablets)
- ▶ ~ 2 full time equivalent contributors and a big community

Minimum feature set required to support a device:

- ▶ Display working and graphics fast enough
- ▶ Sound working
- ▶ Be able to make calls
- ▶ etc
- ▶ GPS, Camera, and other non crucial hardware may not work, or work in later releases

A very short introduction on hardware:



- ▶ System on a chip
- ▶ Smartphones and the modem

Why Android?

▶ Advantages:

- ▶ GUI and applications adapted to big fingers
- ▶ → run on devices that:
 - ▶ Lack keyboard
 - ▶ Have capacitive touchscreen and no stylus
 - ▶ Have very small displays with very high number of pixel

▶ Issues

- ▶ Part of the GNU/Linux software architecture is light years away: package management and build system, graphics, audio, etc
- ▶ Huge unknown code from Google
- ▶ Meant to run proprietary software, not to empower users

Android: From time to market driven architecture to sustainability

- ▶ SOCs, WiFi chips, smartphones and tablets
 - ▶ Write the code that work as fast as possible
 - ▶ Support as many hardware features as possible
 - ▶ → Varying code quality
 - ▶ → Example: One driver rewritten 3 times
- ▶ Breaking Kernel API and ABI
 - ▶ It can take time (years) to bring in a new framework in Linux
 - ▶ Example of API breakage: HTC dream audio driver
 - ▶ Solution: Apps ↔ Android framework ↔ HAL ↔ Kernel
 - ▶ Getting better in Android: Trebble and Generic Kernel images

Ugly code is good (for freedom):

- ▶ Having the source code under free software licenses, even if the code quality is bad is crucial for freedom:
 - ▶ Hardware bringup is often made that way anyway
 - ▶ Things can be improved later: always be cleaned up later or if the code quality is too bad, rewritten from scratch
 - ▶ Having the source code under a free software license is very important
 - ▶ Worst case: use the source code as documentation or reverse engineer it (add prints)
- ▶ → We depend on that source code

[OK] Listened to the background introduction.

[OK] Listened to the background introduction.
Starting second part about sustainability.

Part II: Smartphones lifetime

What I'm about to tell you is subversive...

<subversive>

Once upon a time...

Dave didn't want to buy a smartphone...

"Nearly all Present-day cell phones are Stalin's dream"

Richard Stallman[1]

But...

- [[Peer pressure]] and advertizing
- Employment (exploitation?)

Dave bought an Android smartphone off the shelf.
The smartphone has a removable battery.

Two years later...

Dave buys a new battery.

Dave doesn't want to destroy the planet

Two years later...

Dave was living happily ~~ever~~ after and forgot about his smartphone
(and all the backdoors...).

Dave faints...

Part III: The Phantom Menace

Dave panicks and removes the battery.

Part IV: The counter attack of the clones Replicants

Part IV: Breaking the chains

Part V: Back to the real world

Replicant 6 → More recent Android.

Requirements += Replacable battery:

- ▶ No need to rush to support the device
- ▶ The device lasts longer
- ▶ → In line with upstreaming longer term work.

Devices supported by Lineage 16 with a removable battery:

- ▶ Qualcomm MSM8*:
 - ▶ Fairphone: FP2
 - ▶ LG: G3 (many versions)
 - ▶ OPPO: Find 7a/s
 - ▶ Samsung: Galaxy Note 3 LTE (Many versions)
 - ▶ Samsung: Galaxy S III Neo (2 versions)
 - ▶ Samsung: Galaxy S5 Active
 - ▶ Samsung: Galaxy S5 LTE (Many versions)
 - ▶ Samsung: Galaxy S5 LTE Duos (Many versions)
 - ▶ Wileyfox: Swift
- ▶ Qualcomm APQ8*
 - ▶ Samsung: Galaxy S4 (Many versions)
 - ▶ Samsung: Galaxy S4 Value Edition (GT-I9515/L)
 - ▶ Samsung: Galaxy S4 Active
 - ▶ Samsung: Galaxy S5 LTE-A
 - ▶ Samsung: Galaxy S5 Plus
- ▶ Samsung Exynos 7580:
 - ▶ Samsung: Galaxy S5 Neo

Limiting freedom, privacy and security attacks:

- ▶ Isolated modem:
 - ▶ Modem not in the SOC.
 - ▶ No shared memory (RAM) between the modem and the SOC.
 - ▶ HSIC: USB-like, the host control re-enumeration.
 - ▶ MIPI: Should be OK, not extensively reviewed.

Devices supported by Lineage 16 with a removable battery:

- ▶ ~~Qualcomm MSM8*:~~ Modem in the SOC
 - ▶ ~~Fairphone: FP2~~
 - ▶ ~~LG: G3 (many versions)~~
 - ▶ ~~OPPO: Find 7a/s~~
 - ▶ ~~Samsung: Galaxy Note 3 LTE (Many versions)~~
 - ▶ ~~Samsung: Galaxy S III Neo (2 versions)~~
 - ▶ ~~Samsung: Galaxy S5 Active~~
 - ▶ ~~Samsung: Galaxy S5 LTE (Many versions)~~
 - ▶ ~~Samsung: Galaxy S5 LTE Duos (Many versions)~~
 - ▶ ~~Wileyfox: Swift~~
- ▶ Qualcomm APQ8*
 - ▶ Samsung: Galaxy S4 (Many versions)
 - ▶ Samsung: Galaxy S4 Value Edition (GT-I9515/L)
 - ▶ Samsung: Galaxy S4 Active
 - ▶ Samsung: Galaxy S5 LTE-A
 - ▶ Samsung: Galaxy S5 Plus
- ▶ Samsung Exynos 7580:
 - ▶ ~~Samsung: Galaxy S5 Neo Modem ↔ SOC: shared memory~~

Hmmm

- ▶ → No Exynos with removable battery and isolated modem.
- ▶ → All the devices supported by Replicant 6.0 have been dropped.
- ▶ → We'd like to support the devices longer...
- ▶ The APQ* also look interesting, we would need to do more research on it:
 - ▶ Isolated modem?
 - ▶ Upstream support for the SOC?
 - ▶ Nonfree bootloader (~ BIOS+GRUB) (signed?)
 - ▶ Probably way more work needed (different modem, more upstreaming work).
- ▶ We also took the decision when LineageOS didn't support these.

Part III

Already supported by Replicant 6.0:

- ▶ Galaxy SIII (I9300): Good upstream status, modem support lacking, and other small fixes to do.
- ▶ Galaxy Note II (I9300): Good upstream status, modem and display support lacking.
- ▶ Galaxy SIII 4G (I9305) and Galaxy Note II 4G (N7105): Different modem.

Making devices more sustainable:

- ▶ → Upstream Linux → We can support them longer.
- ▶ → Most Replicant users and developers already have one.
- ▶ → Known hardware that works and can still be bought second hand.
- ▶ Remaining issues:
 - ▶ RAM size and new Android versions.
 - ▶ Nonfree bootloader.

Main blocker: Nonfree bootloader

- ▶ Nonfree → Incentive to drop the device.
- ▶ Partially free u-boot port → can't redistribute the nonfree part.
- ▶ Research to understand if we can make it fully free (XBOOT).
- ▶ Stock bootloader incompatible with Linux...

Upstream Linux bootloader requirements
Documentation/arm/Booting (since 2003):

The MMU must be off.

Instruction cache may be on or off.

Data cache must be off.

Some funding later...

Replicant 9.0:

- ▶ Galaxy SIII booting, modem initialized.
- ▶ Still work to do (testing, audio, networking, etc.).
- ▶ Slowed down by conferences and other Replicant work (XBOOT, Replicant 6, etc).

Future directions:

- ▶ Finish the research on XBOOT.
 - ▶ <https://github.com/xboot/xboot>
- ▶ Look into devices like the PinePhone and the Librem5.
- ▶ Share more work with GNU/Linux upstream (OFono, other hardware support libraries).

Licenses:

- ▶ The SIM card and BTS pictures comes from https://en.wikipedia.org/wiki/File:Gsm_network.png and are under the GFDL 1.2 or the Creative commons Attributions-Share ALike 3.0 Unported.
- ▶ This presentation: CC-BY-SA 4.0 International.
- ▶ The Galaxy SIII picture: CC-BY-SA 4.0 International.



<https://stallman.org/archives/2011-nov-feb.html>