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

Denis 'GNUtoo' Carikli and David 'dllud' Ludovino

February 4, 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

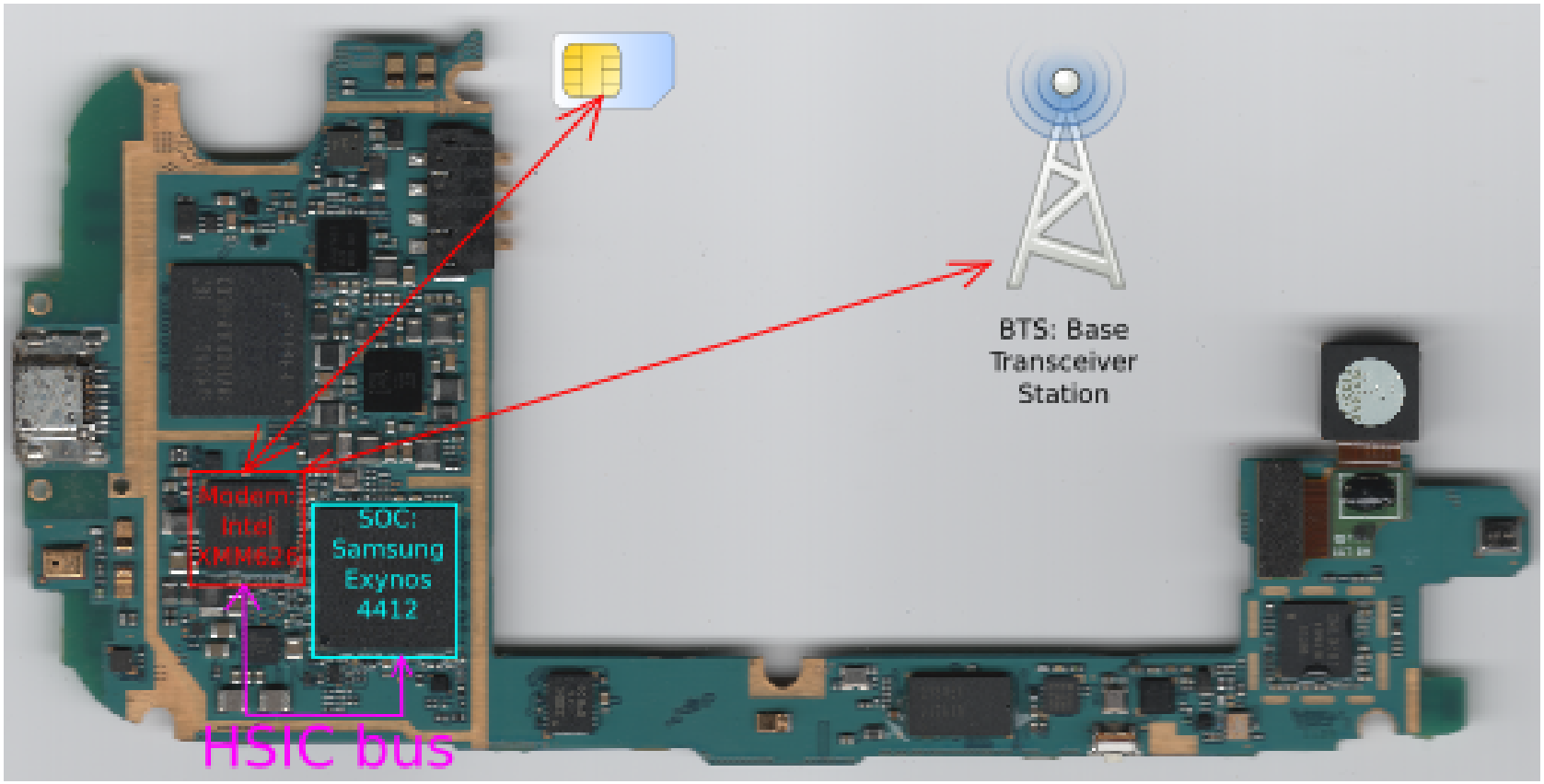
Quick Facts

- 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 $\sim$ 10 devices (smartphones and tablets)
- $\sim$ 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
  - $\rightarrow$ run on devices that:
    - Lack keyboard
    - Have capacitve 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 substainability

- SOCs, WiFi chips, smartphones and tablets
  - Write the code that work as fast as possible
  - Support as many hardware features as possible
  - $\rightarrow$ Varying code quality
  - $\rightarrow$ 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 $\leftrightarrow$ Android framework $\leftrightarrow$ HAL $\leftrightarrow$ 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)
- $\rightarrow$ 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...

$\rightarrow$ [[Peer pressure]] and advertizing

$\rightarrow$ Employment (exploitation?)

You need to be reeeeachable at all timesssss.

Dave: okay okay, I finally bought a smartphone.

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

This smartphone will self-destruct in 5 years

Dave: Why didn't I know that at the time of buying?

Two years later...

Hmmm

Dave: What?

I'm sorry Dave, your battery ran out.

Game Over: Buy a new phone.

Dave: Play again! Insert a new battery to continue!

Dave buys a new battery.

Uhhh consumers like Dave are tiring me...

Dave: I'm a humain beeing!

Uh oh.

Hmmm

Dave: What now?

I'm sorry Dave, your smartphone ran out of software support.

Dave: Shiiit

Dave doesn't want to destroy the planet

Dave:

~~No passaran~~

~~You shall not pass~~

I shall not buy a new smartphone.

Dave: I can still run Android apps.

Securityyyy....

Dave: my smartphone is full of backdoors anyway.

Dave: You're part of my threat model.

Shit they become more and more clever.

Hmmm?

I'm sorry Dave, the Android apps don't support your old Android version.

Dave: Shiiit

Dave: Fuck you, I'll install LineageOS.

I'm sorry Dave, you will loose your data in the process.

Dave:
I'll migrate the data myself.
DIY is great !

Dave Dave please remain with us...

Dave: I don't trust you. Fuck off!
Leave me alone!

Two years later...

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

I'm sorry Dave, LineageOS dropped support for your smartphone.

Dave faints...

Dave: How is that possible?

Knock Knock Dave...

Do you want the red pill [y/N]?

Do you want the red pill [y/N]? Y

Dave: Fuck yes I want the red pill!

Part III: The Phantom Menace

Dave, you've been living in a dream...

Until recently the Linux kernel in your phone was very heavily modified...

Our informations are scarse and sometimes outdated...

But we deduced that in 2008 the device and chip manufacturers did that to improve the time to market...

But who care about time to market when most of the humans will die with 2 degrees?

HAL: Warning: Anarcho-ecolo-communist terrorist detected

Dave: Good idea!

Kernel panic: error -1: Operation not permitted

So they abstract the kernel in libraries that are often nonfree.

Like the libril which implements the modem protocol, and in some cases a backdoor too...

Dave: Shiit...

Dave: So they own us?

In some way yes, but we have the devices, so we can still fight back.

For instance we have greater assurance of not being recorded, but if you left your phone on, they know where you are.

Shit.

Dave panicks and removes the battery.

You trapped me!
Because we're at the same location, they know I'm in the resistance now!

I don't use a smartphone so they don't know where I am.

By the way: Welcome to the Resistance.

Part IV: The counter attack of the ~~clones~~ Replicants

How to fight back? Do I need a ~~light saber~~ soldering iron?

I've no definite answer on that, many things were tried in the past.

Revolutions, assasinations, armed conflicts, theft, strikes, teaching, living in remote communities, regicides, and even making a bank.

But besides remote communities and self-management spaces within the system, we didn't get rid of abuse of power yet.

I meant for smartphones.

I'm sorry Dave, as of today smartphones can't respect your freedom.

They track you with a deadly precision.

Our sources indicated us 10 or 20 meters for GSM and 3G.

But replacing more and more nonfree software by free software limits the damage.

We have several fully free software GNU/Linux distributions and even Replicant, a fully free Android distribution.

Replicant is almost as old as ~~the Matrix~~ Android.

So if I've a supported device that has a removable battery, will it last longer with Replicant?

Not yet.

Part IV: Breaking the chains

Some smartphones have longer software support...
But they have batteries that cannot be easily removed...

Others are meant to be repaired...
But the software support is bad...

So we lost?

There are many many smartphones being produced each years...

What you must learn is that these rules are no different than rules of a computer system.
Some of them can be bent, others can be broken.

Most modern smartphones have non removable batteries!
It's hopeless!

Free your mind...

Do you think that the number of smartphones has anything to do with their strength?

Right, but how?

We're going to hangup on this political system, and then show these people what thoses in power don't want them to see. We're going to show them a world without power. A world without forced rules or controls, borders or boundaries. A world where anything is possible. Where we go from there, is a choice I leave to the people.

Part V: Back to the real world

Replicant 6 $\rightarrow$ More recent Android.

Requirements $+=$ Replacable battery:

- No need to rush to support the device
- The device lasts longer
- $\rightarrow$ 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 $\leftrightarrow$ SOC: shared memory

Hmmm

- $\rightarrow$ No Exynos with removable battery and isolated modem.
- $\rightarrow$ All the devices supported by Replicant 6.0 have been dropped.
- $\rightarrow$ 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 ($\sim$ 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:

- $\rightarrow$ Upstream Linux $\rightarrow$ We can support them longer.
- $\rightarrow$ Most Replicant users and developers already have one.
- $\rightarrow$ 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 $\rightarrow$ Incentive to drop the device.
- Partially free u-boot port $\rightarrow$ 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