Neo900

Crafting The Private Phone

Sebastian Krzyszkowiak

dos

http://dosowisko.net/

OHSW 2014
Garching, 29.11.2014
CC-BY-SA 4.0

http://neo900.org/stuff/ohsw2014/
Neo900

The truly open smartphone that cares about your privacy.

Merge of GTA04 and Nokia N900... and beyond

http://neo900.org/
Neo900

- TI OMAP3 DM3730 @ 1 GHz
- 1 GB RAM
- 512 MB NAND + 32/64 GB eMMC
- Cinterion PHS8/PLS8 modem (LTE)
- GPS/GLONASS
- Dualtouch resistive screen
- Modem sandbox and monitoring solution
- Hackerbus
- http://neo900.org/specs
The Hardware Problem

- I'm the admin of my PC. Why can't I be the admin of my phone as well?
- We don't use App Stores on PCs. Why should we need them on phones?
- We can choose from hundreds of systems to install on PC. Why can't we do that on mobiles as well?
Walled Gardens Explained:

A: Everyone here makes money.
B: Everyone here can go find themselves.
The Hardware Problem

Does a cellphone really differ so much from your average laptop?

It doesn't.

It's just smaller and more integrated.
The Hardware Problem

- Lack of documentation
- Closed components
- Porting – the neverending story
- Upstream? In your dreams.
- Planned obsolescence
- When you have to break into your own device in order to use it as you wish, **something is completely wrong!**
Privacy
How can your privacy suffer?

- Data on your storage gets damaged or destroyed
- Data gets leaked via:
  - The Internet
  - Other wireless technology
  - Removable media
- Your life gets spied on:
  - Location tracking
  - Audio/video eavesdropping
  - Logging your activities, collecting metadata
• Turns out a good, open, hackable device is a perfect first step towards better privacy.
Baseband processor

- A big, proprietary black box.
- Known to often be vulnerable.
- **All Your Baseband Are Belong To Us**
  Ralf-Philipp Weinmann, Black Hat conf 2011
Baseband processor

- Having control under the main operating system (like Android) is not enough
- Main problem with projects like Blackphone
Baseband processor

- The baseband is often tightly integrated with rest of the system
  - Direct connection to microphone
  - Direct Memory Access
Baseband processor
Baseband processor
Baseband processor
Baseband processor
Baseband processor
Baseband processor
Open baseband?

• Unfortunately, it's not going to happen for both economical and legal reasons.

• Basebands are cryptographically locked and any change in their firmware results in revocation of their certification, rendering them illegal to use in public networks.
OsmocomBB

- Open baseband firmware
- Runs on *Ti Calypso* (the same as in GTA01/02)
- **Illegal** to use as a phone outside the lab
- http://bb.osmocom.org
Open baseband?

• However, open baseband **does not** magically fix all the privacy problems.
The threats

- **Tracking**
  - Trilateration based (IPL, **OTDOA**, **E-OTD**, **U-TDOA**)
  - GPS-assisted (**RRLP**)
- **Eavesdropping**
- **Data leakage**
- **Security bugs in firmware, SIM cards**
- **Direct access to main RAM**
The threats

- GSM hacking
  - It's not hard to do fun rogue stuff with GSM.
  - Encryption (A5/1, A5/3) was broken long ago
    - It was actually deliberately weakened in specs to make live of governmental surveillance agencies easier.
  - Denial of Service attacks are easy
  - The only „protection“ is... illegality
Not solvable

- Eavesdropping of calls
- Eavesdropping of Internet connection
- Trilateration while connected to the network

It can (and does) happen outside of the device or is necessary for it to function. Aside from encryption, there's nothing we can do against it.
Neo900 concept

- **Counter-surveillance** rather than audit and trust
- Everything not 100% in control is **considered rogue**
- Rogue stuff is **sandboxed** and constantly monitored
Neo900 design

The baseband processor is locked into a cage
Neo900 design

• If the modem is compromised, the main system remains safe use the encryption, Luke

• If the modem is supposed to be off, but it isn't – we know that and react accordingly before anything bad happens

• If the GPS is in use when not requested – we know that but the antenna will be disabled anyway

• If the modem tries to record audio when not requested – we know that but it won't be able to do it
Neo900 design

- When modem act badly, user is notified and automatic hard reset via emergency_off line and/or hard shutdown by cutting power can be applied.
Neo900 concept

• This way, when something fishy is going on, software kicks off an alarm to make user do efficient measures to stop the threat:
  – Removing the battery
  – Destroying the device
  – Hiding it under the seat in bus and leaving

• With basic solutions like external power switch, user is not aware that his device has been tampered with.
  – ...but it can be used post-mortem
Neo900 design

• Our monitoring approach can also reveal some „rogue” activities from outside – like packet-storms on airports.

https://www.schneier.com/blog/archives/2014/04/gogo_wireless_a.html#c5459667
In the end, it's the user who gets the full control over how their device works and how it reacts to possible threats.

Staying secure may need some effort, but without it there's only false sense of security – which is even worse than no security at all.
Interesting resources

- https://srlabs.de/rooting-sim-cards/
- https://srlabs.de/gsmmap/
- http://events.ccc.de/congress/2008/Fahrplan/events/2997.en.html
SIMtrace

- Osmocom SIMtrace is a software and hardware system for passively tracing SIM-ME communication between the SIM card and the mobile phone.

http://bb.osmocom.org/trac/wiki/SIMtrace
Neo900: current status

- Almost 400 devices already „preordered”
  - That's twice as much as we needed to proceed
- Most of the design finished
- Schematics catching up with the design
- Sourcing is tough – components slowly fade away in the market
Neo900: current status

http://neo900.org/stuff/block-diagrams/
Neo900: next steps

- Sourcing the risk parts (like 1GB RAM)
- Ordering the cases
- BB-xM based proto_v2 expected in February
Thank you!

http://neo900.org/stuff/ohsw2014/
http://neo900.org/resources/

QA:
IRC - #neo900 on Freenode
http://webchat.freenode.net/?channels=neo900