



Linux on the Go: Modems

Camden Bruce

A bit about me

- PINE64 Community manager
- Student at EIT in Hawke's Bay
- I love Linux on mobile devices

What is Linux on mobile?

- Running a mainline kernel on your phone
- Using a downstream Android kernel with Libhybris/Halium compatibility layer

Linux & Modems

- Modems are typically used as a USB dongle
- ModemManager & NetworkManager work together to automatically set up discovered modems.
 - KDE and Gnome support ModemManager
- Sailfish and Ubuntu Touch use oFono and ConnMan

1. Some business/enterprise laptop lines (like Thinkpads, Elitebooks, etc) have the option to include a cellular modem
- 2/2.1. KDE and Gnome can have modems configured directly in the settings for things like APNs, MMS and other modem related settings.
3. oFono is a telephony stack created by Nokia for their phones running Meego like the N9. It's very old now but is embedded deep into Sailfish so it continues to be used.

Enter, the PinePhone

- Open mobile Linux hardware
- Quectel EC25-G 4G Modem
- Very well supported device

Why PinePhone and Quectel EC25-G?

- The modem runs Android
 - Communication is possible through
 - ADB
 - Fastboot
- It's powerful
 - ARM Cortex-A7 @ 1.2 GHz
 - 256MB of RAM
 - It can run DOOM
- And most importantly ...
 - It has open firmware available to flash

1. The user can send AT commands through ADB and force the modem to reboot into flashing mode using Fastboot. It's very accessible and easy to communicate with the modem.
2. The modem uses a MDM9207 CPU which is one of Qualcomm's modem CPUs. This means we can play Doom or even run an entire web server.
3. We'll get into that in the next slide :)

Open modem firmware

- The Quectel EC25-G has an open firmware created by Biktor
- Improves on many things from the stock closed firmware
 - Signal tracking support
 - Call recording support
 - Internal call and sms support
 - Internal sms logging
 - Ability to downclock the CPU for improved battery life while sleeping
 - 0 binary blobs in userspace
- Though there are still a couple of closed source binaries :(
 - ARM TZ (Trust Zone)
 - ADSP firmware (Applications Digital Signal Processor) for processing audio.

1. Can be found here: https://github.com/the-modem-distro/pinephone_modem_sdk

2.

2.1. Get notified whenever the modem switches tower

2.2. Done internally

2.3. You can call the modem to test it

2.4. You can log SMS messages internally on the modem

2.5. The open modem firmware has a minimum 100Mhz speed for the CPU. The stock is 800Mhz so this change drastically improves battery life.

2.6. Both closed source blobs are on the modem itself.

3. While unfortunate trustzone on Qualcomm is closed due to potential IP and security through obscurity reasons

Why this is so special

- Modem firmware isn't supposed to be open due to
 - Regulatory and Government regulations
 - FCC, radio communication standards
 - Patents
 - Nobody with the open firmware has a license to use the technology anymore. Which is illegal.
- It gives users the power to do things they shouldn't
 - Hardware cloning/spoofing
 - Ability to (in theory) flood towers with data (to behave erratically).

1.

1.1. To prevent malicious things from happening on cellular networks companies aren't allowed to make their firmware open for cellular modems.

1.2. Due to patents and legal obligations from manufacturers you aren't allowed to modify the firmware of modems in a way that will disrupt normal cellular frequencies or disrupt cellular traffic

2. These are the illegal parts that can get you charged or potentially jailed.

Why hasn't anyone done anything then?

- Simple ... nobody has done anything publicly malicious yet.
- Therefore, there isn't a good reason for companies to go after it yet.
- PineStore don't endorse or ship the firmware by default
 - This is 100% due to legal reasons.
 - Could potentially get the PinePhone banned from being sold in many countries.

1/2. Self explanatory

3.1. The open firmware is a modification of the stock firmware, therefore the PinePhone cannot be sold. There are legal implications that I do not understand.

To conclude

- Buy a PinePhone
- Open cellular modem firmware gives the opportunity to improve on crappy bug ridden stock firmware
- Open cellular modem firmware is in a legal gray area
- If anybody does anything malicious with it, it's joever

Thank you for listening!