Flashing the Jolla C2 using the Unisoc flash mode

This information was originally in a forum post: https://forum.sailfishos.org/t/flashing-the-jolla-c2/21020/3

The Jolla C2 contains a Unisoc UMS9230 (Tiger T606) SoC. All Unisoc SoCs implement a special USB flashing protocol in their boot ROM, which can be entered by pressing the Volume Up and Power keys. This provides a way to reflash the phone even if a broken bootloader was flashed.

This flashing interface is usually used with Unisoc's flashing software to flash PAC files containing the entire factory image for the phone and a loader signed with device-specific keys. However, the signature check can be bypassed on this SoC, and tools have been developed to allow flashing partitions directly with an unsigned loader.

Initial Setup

Follow these steps to set up your environment for flashing the Jolla C2:

1. Download https://github.com/TomKing062/spreadtrum_flash and build it using make (for Windows users, a prebuilt .exe is available in the ums9230 unlock archive, but please note that the examples below assume a Unix-like system)
2. For Linux users: set up udev rules if you want to run the flashing commands with normal user permissions. See this README for more information.
3. Download the ums9230_universal_unlock.zip archive from here and extract it into the main spreadtrum_flash directory (required files are `custom_exec_no_verify_65015f08.bin`, `fdl1-dl.bin` and `fdl2-dl.bin`)
4. Obtain a bootloader image for the Jolla C2 / Reeder S19 Max Pro S, from one of the following places:
   - from an archive with images: the file will be named `uboot_a.img`, `uboot_a.bin` or `lk.bin`
   - **or** from the phone directly by using `fdl2-dl.bin` temporarily (make sure to read about the side effects in the "Troubleshooting" section):

```
./spd_dump \
    exec_addr 0x65015f08 \
    fdl fdl1-dl.bin 0x65000800 \
    fdl fdl2-dl.bin 0x9efffe00 exec \
```

```
    r uboot_a reset
```

Flashing partitions

To flash partitions to the device, use the following command:

```
./spd_dump \
    exec_addr 0x65015f08 \
    fdl fdl1-dl.bin 0x65000800 \
    fdl <path to your FDL2 file> 0x9efffe00 exec \
    w <partition name> <image path> \ # This line can be repeated for multiple partitions
    reset
```

It is recommended to use the device-specific bootloader as the FDL2 unless you are flashing a critical bootloader partition (splloader or uboot). The device-specific bootloader does not allow flashing these partitions, while fdl2-dl.bin from the exploit package does. See the "Troubleshooting" section for the expected side effects of using it.

Flashing Sailfish OS

This should also work with a Reeder S19 Max Pro S: see https://forum.sailfishos.org/t/installing-sailfish-to-reeder-s19-max-pro-s/21873/20

Get the Sailfish OS images from https://releases.sailfishos.org/images/. Assuming they are unpacked into a directory named SailfishOS, run these commands to flash them:

```
simg2img SailfishOS/sailfish.img001 sailfish.img
simg2img SailfishOS/fimage.img001 fimage.img
./spd_dump \
    exec_addr 0x65015f08 \
    fdl fdl1-dl.bin 0x65000800 \
    fdl fdl2-dl.bin 0x9efffe00 exec \
    w uboot_a SailfishOS/lk.bin \
    w uboot_b SailfishOS/lk.bin \
    w dtbo_a SailfishOS/dtbo.img \
    w dtbo_b SailfishOS/dtbo.img \
    reset
# Hold down the volume up key while the phone reboots!
./spd_dump \
    exec_addr 0x65015f08 \
```

```
fdl fdl1-dl.bin 0x65000800 \
fdl SailfishOS/lk.bin 0x9efffe00 exec \
w boot_a SailfishOS/hybris-boot.img \
w boot_b SailfishOS/hybris-boot.img \
w vendor_boot_a SailfishOS/vendor_boot.img \
w vendor_boot_b SailfishOS/vendor_boot.img \
w userdata sailfish.img \
w super fimage.img \
reset
```

Troubleshooting

The flashing tool cannot connect to the phone:
Make sure to boot into flashing mode using Volume Up + Power. You should not see anything on the screen!

The command fails with timeout or connection errors:
Restart the flashing mode by holding the Volume Up and Power keys for 7 seconds. This is usually required if a command is interrupted.

The phone reboots when the Volume Down key is pressed!
This is a **side effect** of using `fdl2-dl.bin`. This behavior disappears after the phone is shut down completely.

The phone reboots while flashing or dumping large partitions:
This is typically also caused by `fdl2-dl.bin`. Use the device-specific bootloader instead.

Revision #5
Created 29 January 2025 17:35:06 by Affe Null
Updated 23 February 2026 14:59:42 by Affe Null