U-Boot

porting and maintaining a bootloader for a multimedia SoC family

Who ?

- 14y Kernel & Firmware Hacker
  - Entirely Ported Linux & custom boot chain on custom ARM SoCs
  - Worked with SoC design team
- 5y BayLibre Engineer
  - Writes support for Amlogic Mainline Linux & U-Boot
- 2y1/2 Amlogic U-Boot Custodian Maintainer
  - 47 Pull Requests since January 2019

What ?

- Amlogic provides a line of Multimedia SoCs
  - Originally designed for low-cost Digital TV / Set-top-box market
- First Single Board Computer with the Odroid-C1
- The following Odroid-C2 became Famous
  - 4xCortex-A53 up to 1.6GHz
  - USB2, Ethernet 10/100/1000
  - HDMI 2.0
  - eMMC, SDCard, 40pin header
  - 2GiB DDR
- The last Odroid-N2+ is much better !
  - 2xCortex-A53@1.8GHz + 4xCortex-A73@2.2GHz
  - USB3.0
  - HDMI 2.1
  - 4GiB DDR

Software Support Status

Amlogic provides an open source vendor kernel tree

- Was 3.14 for Odroid-C2
- The latest is 4.9 for Odroid-N2+
- Driver code doesn't follow kernel frameworks
  - There is a clock driver, almost unused
  - Since 2017, Amlogic re-used some mainline drivers (with some heavy changes)
  - Display & Decoder/Encoder code is completely custom
  - Drivers are almost not reusable
- DT is completely custom, not reusable
  - Hard to understand for newcomers

Software Support Status

- U-boot is derived from v2015.01 (!!!!!!)
  - But with a lot of code backported from recent u-boot
  - Melting pot of firmware code and DM code
  - Custom eMMC partition format based on NAND
  - Custom multi-DT boot flow
  - Custom USB Device flash protocol
    - For curious people: https://github.com/superna9999/pyamlboot/blob/master/PROTOCOL.md
  - Drivers are not reusable

Software Support Status

- Amlogic has now a v2019.01 based U-Boot
  - Supports only new SoCs
  - Still too old
  - Vendor code is the same as the v2015.01 version
  - Still not usable as maintainable codebase

Software Support Status

- SoC Boot flow
  - Amlogic uses TF-A, PSCI & SCPI since S905
    - Was mandated by ARM for new Armv8 platforms
    - They used a custom boot flow for their Armv7 platforms
  - Amlogic provides binaries only for:
    - BL2: DDR controller and system PLLs Inits
    - BL30: SCP Firmware running on the Cortex-M3
    - BL31: EL3 Runtime Firmware
    - BL32: Secure-EL1 Payload (optional)
  - Build from Amlogic U-Boot Souce
    - ACS: DDR controller and system PLLs Settings
    - BL21: Board specific power Init
    - BL301: BL301 open-source loadable part of BL30

Software Support Status

- SoC Boot flow
  - The provided boot flow handle full scrambled and signed secure boot
  - Used for Digital TV products
  - Not Documented...

Software Support Status

- Upstream Status of ARMv8 SoCs (S905 to A311d)
  - Great Linux coverage
  - Great U-Boot coverage
  - Partial TF-A (BL31) is upstream
    - BL2/BL30 are very complex to reverse-engineer
    - Complex undocumented DDR init
    - Tricky and undocumented system PLL init
    - Would need documentation to do a clean job

Software Support Status

- Great Linux coverage
  - See my other talks
  - TL;DW(atch)
    - Basic system support is complete
    - Basic I/O support is complete
    - Partial Multimedia support
      - Lacks all advanced Digital TV features (HDR, 3D, …)
      - Entirely lack Video Encoders support
      - Partial Video Decoder support (basic H264, VP9, no HEVC)
  - → http://linux-meson.com

Software Support Status

- Great U-Boot coverage
  - System support is complete
  - Basic I/O is complete
    - PWM has been merged
  - Advanced I/O is partial
    - Ethernet OK
    - USB OK
    - SD/eMMC OK
    - *NAND is missing*
    - *PCIe/NVMe is missing*
  - Video Output is partial
    - *DSI output is Ongoing*

	S905	S905X S805X	S912 S905D	A113X	S905X2 S905D2 S905Y2	S922X A311D	S905X3 S905D3
Boards	Odroid-C2 Nanopi-K2 P200 P201	P212 Khadas-VIM LibreTech-CC LibreTech-AC	Khadas VIM2 Libretech-PC	S400	U200 SEI510	Odroid-N2 Khadas-VIM3	SEI610 Khadas-VIM3L Odroid-C4
UART	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pinctrl/GPIO	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Clock Control	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PWM	No	No	No	No	No	No	No
Reset Control	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Infrared Decoder	No	No	No	No	No	No	No
Ethernet	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-core	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Fuse access	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SPI (FC)	Yes	Yes	Yes	Yes	Yes	Yes	No
SPI (CC)	No	No	No	No	No	No	No
I2C	Yes	Yes	Yes	Yes	Yes	Yes	Yes
USB	Yes	Yes	Yes	No	Yes	Yes	Yes
USB OTG	No	Yes	Yes	No	Yes	Yes	Yes
eMMC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SDCard	Yes	Yes	Yes	Yes	Yes	Yes	Yes
NAND	No	No	No	No	No	No	No
ADC	Yes	Yes	Yes	No	No	No	No
CVBS Output	Yes	Yes	Yes	*N/A*	Yes	Yes	Yes
HDMI Output	Yes	Yes	Yes	*N/A*	Yes	Yes	Yes
CEC	No	No	No	*N/A*	No	No	No
Thermal Sensor	No	No	No	No	No	No	No
LCD/LVDS Output	No	*N/A*	No	No	No	No	No
SoC (version) information	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Software Support Status

- Great U-Boot coverage
  - All known Amlogic Single Board Computers are supported
    - Except ARMv7 ones… (Odroid-C1)
    - Waiting for Banana Pi BPI-M5 samples :-)
  - Generic Reference Designs are also supported

    Permits booting products based on Reference Designs
    - P200 (S905)
    - P212 (S905X)
    - Q200 (S905D, S912)
    - W400 (S905X2, S905D2, S905X3, S905D3, S922X, A311D)
    - S400 (A113D)

Software Support Status

- Great U-Boot coverage
  - Most drivers were ported from Linux
  - The U-Boot Driver Model helped a lot !
  - NAND driver is missing, the Linux driver exists
  - PCIe driver for NVMe support is missing
  - A few tweaks subsist
    - Ethernet PHY config is still static, this need to be cleaned
    - PHY Mux driver between Internal & external is missing

Software Support Status

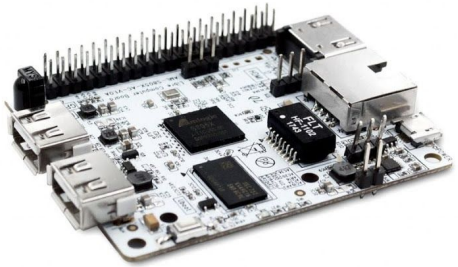
- Great U-Boot coverage
  - HDMI Output is supported
  - Display framework is pretty basic but works fine
  - MIPI-DSI Output is implemented
  - U-Boot dm-display EDID handling is primitive
    - Only handles detailed timings
    - Doesn't have Standard & established timings tables like Linux
    - Doesn't support HDMI VIC timings
  - Some monitors EDID don't have their native timing in the detailed timings table
  - → Can't support HDMI1.4 4K & HDMI2.0 4K timings

Software Support Status

- Great U-Boot coverage
  - UEFI support comes for free !
  - Great motivation to maintain support upstream
  - RNG is supported for Linux KASLR boot
  - Runtime Variables are still missing….
    - This could need per-board implementation (is possible)
    - Only a few board has an on-board SPI NOR flash

Software Support Status

- Used in Real products !
- Example:



La Frite | AML-S805X-AC
https://libre.computer

La Frite default SPI Flash bootloader is Mainline U-Boot !
Supports UEFI boot & eMMC flashing via USB Gadget

Software Support Status

- U-Boot Upstream Development
  - Initial support was done by Beniamino Galvani (Thanks !)
  - Only a few non-Baylibre contributors
  - U-Boot process is close to Linux
    - Due to fewer reviewers, non-core patches are less reviewed
    - Has a dedicated mailing-list, easier to track patches
  - U-boot has a handy test suite to validate core code
    - “Sandbox” is U-boot as linux application
    - Can communicate with other Linux process
    - Can run unit tests coordinated from Python
  - U-Boot has a very complete CI
    - Test using Sandbox, only build-tests for other platforms

Software Support Status

- U-Boot binary must be packaged
- U-Boot is part of the TF-A boot chain (BI33)
- Amlogic used a variant of TF-A FIP format for GXBB
- Since GXL (S905X), Amlogic has their own format
  - Because they have to load numerous firmware
  - They added DDR init firmwares for the lastest SoCs
- Packaging tools are closed source
- Packaging process is not documented

Software Support Status

GXL/G12A/G12B/SM1 packaging

```
$ blx_fix.sh fip/bl30.bin fip/zero_tmp fip/bl30_zero.bin fip/bl301.bin fip/bl301_zero.bin fip/bl30_new.bin bl30
$ acs_tool.pyc fip/bl2.bin fip/bl2_acs.bin fip/acs.bin 0
$ blx_fix.sh fip/bl2_acs.bin fip/zero_tmp fip/bl2_zero.bin fip/bl21.bin fip/bl21_zero.bin fip/bl2_new.bin bl2
$ aml_encrypt --bl3enc --input fip/bl30_new.bin
$ aml_encrypt --bl3enc --input fip/bl31.img
$ $aml_encrypt --bl3enc --input fip/bl33.bin
$ aml_encrypt --bl2sig --input fip/bl2_new.bin --output fip/bl2.n.bin.sig
$ aml_encrypt --bootmk --output fip/u-boot.bin --bl2 fip/bl2.n.bin.sig --bl30 fip/bl30_new.bin.enc --bl31 fip/bl31.img.enc --bl33
fip/bl33.bin.enc
```

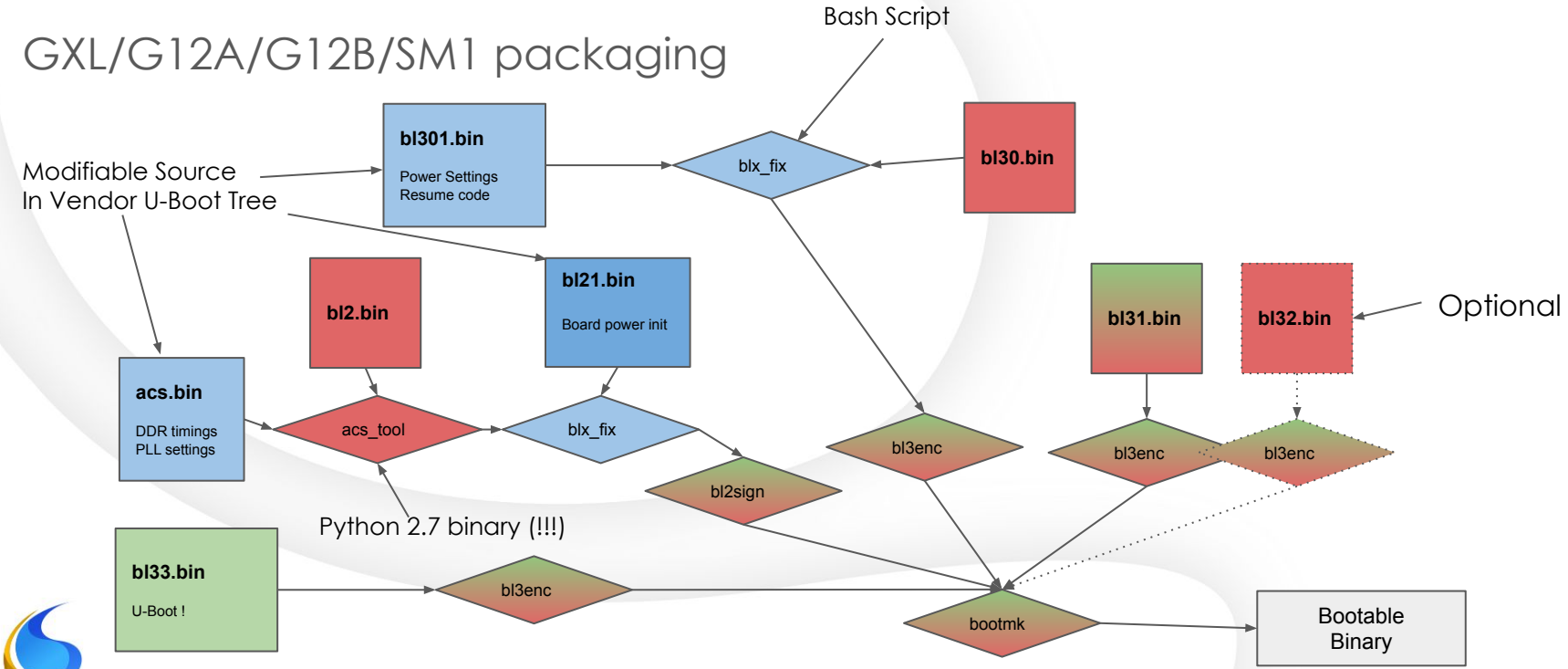
Pretty ugly...

Software Support Status

- GXBB packaging tools has been reverse-engineered
  - https://github.com/afaerber/meson-tools
  - Until last year, only supported GXBB (S905)
- GXL later on
  - https://github.com/repk/gxlimg
- G12A/G12B/SM1 recently
  - https://github.com/angerman/meson64-tools
  - New SoCs has loadable DDR init code

Software Support Status

GXL/G12A/G12B/SM1 packaging



Software Support Status

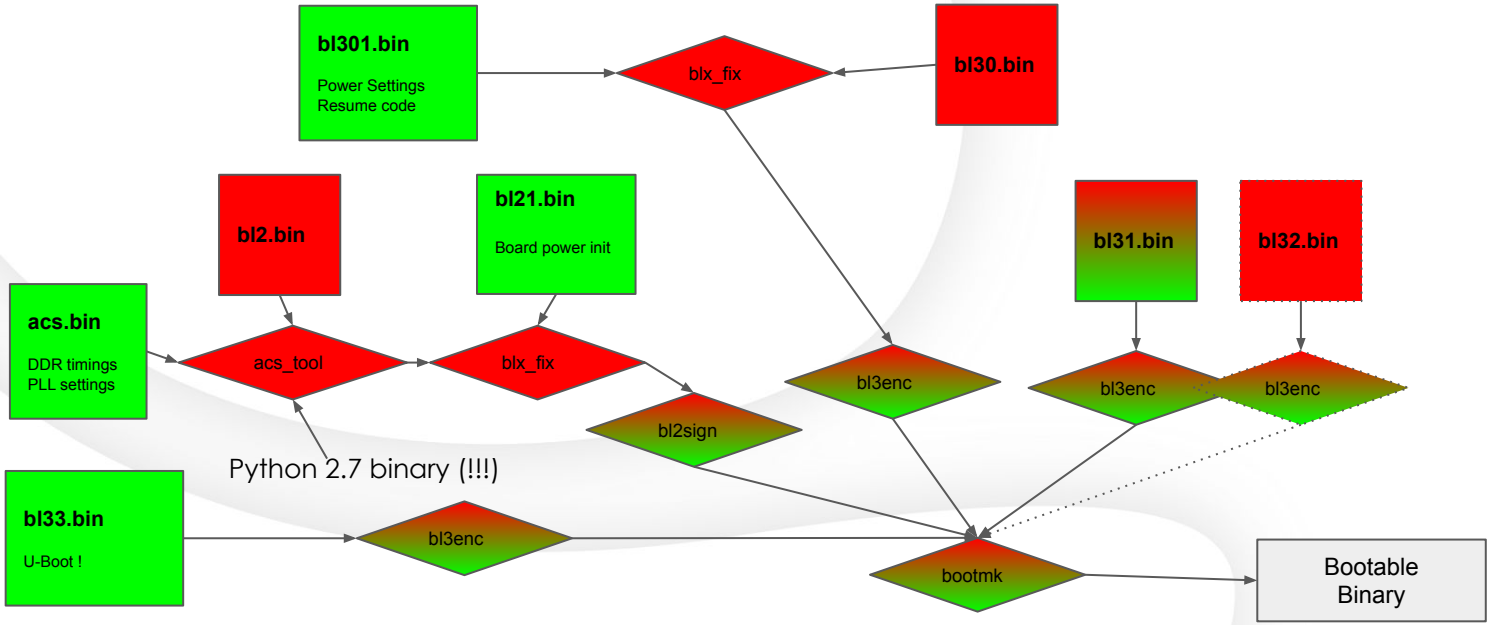
- Building bootable binary could trigger legal issues
  - bl2/bl30/bl32 binaries has finally a licence
    - Buildroot rejected due to lack of earlier licence terms
  - Acs.bin, bl21.bin & bl301.bin are part of the Vendor U-Boot source
    `arch/arm/cpu/armv8/gxl/firmware/bl21` → bl21.bin
    `arch/arm/cpu/armv8/gxl/firmware/acs` → acs.bin
    - Now have a clear licence: GPL2+
  - Still no clear licence terms for bl301.bin
    `arch/arm/cpu/armv8/gxl/firmware/scp_task` → bl301.bin
    - Some has GPL2+ headers, some none
- These could be moved out of vendor U-Boot
  - In a separate repo ? in Mainline U-Boot ?

Software Support Status

Amlogic Binary Distribution Licence

Software Support Status

GXL/G12A/G12B/SM1 packaging



Software Support Status

- Partial TF-A (BL31) is upstream for GXBB (S905)
  - First ArmV8 SoC
  - AES/SHA Accelerator are non-functional
  - Boot ROM has flaws
  - “Amlogic S905 SoC: bypassing the (not so) Secure Boot to dump the BootROM”
  - Upstream TF-A is partial
    - Doesn’t support Suspend/Resume
    - Doesn’t support Secure Boot (AFAIK untested)

Software Support Status

- Partial TF-A (BL31) is upstream for GXL (S905X/S905D)
  - Third generation ArmV8 SoC (GXTVBB for TVs is second)
  - AES/SHA Accelerator are functional, secure boot should be secure
  - Upstream TF-A is partial
    - Doesn't support Suspend/Resume
    - Doesn't support Secure Boot (AFAIK untested)
    - Doesn't support GXM (S912) variant for 8xCortex-A53
      - Doesn't support enabling second Cortex-A53 cluster

Software Support Status

- Partial TF-A (BL31) is upstream for AXG (A113D)
  - Fourth generation ArmV8 SoC, variant for Audio Applications
  - AES/SHA Accelerator are functional, secure boot should be secure
  - Upstream TF-A is partial
    - Doesn't support Suspend/Resume
    - Doesn't support Secure Boot (AFAIK untested)

Software Support Status

- Partial TF-A (BL31) is upstream for G12A (S905X2/S905D2)
  - Modern(ish) generation ArmV8 SoC
  - AES/SHA Accelerator are functional, secure boot should be secure
  - Upstream TF-A is partial
    - Doesn't support Suspend/Resume
    - Doesn't support Secure Boot (AFAIK untested)
    - Doesn't support G12B (S922X/A311d) variant
      - Doesn't support enabling second Cortex-A73 cluster
    - Doesn't support (yet) SM1 variant
      - Only difference from BL1 is the CPU model: Cortex-A55

Missing Features

- Secure Boot
  - These SoCs are designed for Secure products
  - Real-World secure boot is really complex
  - Tools are private, closed source & undocumented
  - Secure eFuse Map is undocumented, **bad fuse map could brick the device**
  - eFuse programming sequence is undocumented
  - But, only BL33 trusted boot would be enough !
- Unified Open Source boot tools
  - Today 3 different tools
- Full Open Source TF-A
  - Not sure this will happen one day...

Missing Features

- U-Boot Support
  - NAND
  - PCIe
  - Old ARMv7 SoCs support
  - EFI Runtime Variables
- Testing
  - Regular and complete boot testing is missing
  - We need a true CI to boot-test on major boards