Replicant - Issue #2027

Investigate Ithor / thor and samsung u-boot for Tizen

05/07/2020 06:01 AM - Kurtis Hanna

Status:	New	**Start date:**	05/07/2020
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	Replicant 6.0	**Spent time:**	0.00 hour
Resolution:		**Grant:**	
Device:	Unknown		

Description

We already know of a method by which we can replace s-boot and replace it with u-boot, but it requires opening up the device and shorting a touch point on the logic board.

We have been looking for a method by which we can replace s-boot via software only techniques. One such technique might spring from the work being done here: https://github.com/oranav/i9300_emmc_toolbox

Another option, if heimdall by itself doesn't prove in the end to be enough, might be Ithor.

This upstream u-boot ODROID exynos4412 repo shows that Ithor/thor is enabled:
https://gitlab.denx.de/u-boot/u-boot/blob/master/configs/odroid_defconfig

It was suggested to Wolfgang in the last email of this thread that he should use Ithor to "convert" an i9300 to an RD-PQ/Trats2 board to get u-boot on the device: https://patchwork.kernel.org/patch/9345815/

Ithor is free software, but the i9300 doesn't have Ithor support by default.

On post #77 here https://forum.xda-developers.com/showthread.php?t=2482563&page=8 it is claimed that a modified kernel with access to the mmcblk0boot0 partition was used to flash a modified version of s-boot, which was dumped from a RD-PQ, that included u-boot with Ithor enabled in it. Much of the same information is reiterated by the same author in this post:
https://forum.xda-developers.com/showthread.php?p=64794497#post64794497

It is my understanding that once you can use Ithor with your device, you can then very easily flash any image that you'd like onto the emmc using the free software program Ithor. At least that is the suggestion after reading to the end of this section of a Tizen wiki:
https://wiki.tizen.org/Exynos#Creating_the_image_manually

https://wiki.tizen.org/images/b/bd/Lecture-1.pdf has some information about creating updated versions of u-boot-mmc.bin, which might come in handy.

History

#1 - 05/18/2020 02:18 AM - Denis 'GNUtoo' Carikli

If we had a fully free software u-boot it could be installed with cat or dd, after booting an upstream Linux kernel.

CONFIG_USB_FUNCTION_THOR=y seem very interesting. I'll check but from the name it looks like it implements the same protocol than heimdall.

If that's the case, then it may enable us to simplify **a lot** the installation instructions of Replicant as we would be able to use heimdall with u-boot too.

I'd like to also be able to use the CONFIG_DISTRO=y that enables to use syslinux config file, like what is used in Parabola.

It may be possible to make everything work together, to enable different users to reuse their GNU/Linux or Android knowledge.

If my memory is correct, in Barebox, which is also a free software booloader like u-boot, you can configure fastboot or DFU to flash files in a filesystem.

Edit: Last summer, I also looked how to export mmcblk2boot0 and mmcblk2boot1 in u-boot and I didn't find how to do it, so I'm unsure how mmcblk2boot* could be made accessible through heimdall.

#2 - 05/18/2020 02:32 AM - Denis 'GNUtoo' Carikli

Thanks, it looks like the protocol used by Heimdall and Odin.

Thanks to this bugreport we now know the name of that protocol, which is really handy.

#3 - 05/18/2020 03:27 AM - Kurtis Hanna

This suggests that there is a version of s-boot that was used on Samsung's Tizen when running on the Galaxy S2 and S3 https://wiki.tizen.org/TM1

I've seen forum posts where people have successfully put Tizen's version of s-boot on their i9300, which then gives them u-boot with lthor, but I don't have the links handy. They used odin to change the s-boot version without being required to open up the phone and short the test point.

#4 - 05/21/2020 06:16 PM - Kurtis Hanna

Here's one of the forum posts I'm referring to. The same author posted a fair bit about this on xda forums too.
https://developer.tizen.org/forums/general-support/retail-i9300-and-tizen-rd-pq-firmware

#5 - 05/22/2020 06:11 PM - Kurtis Hanna

Here's Tizen's lthor repo on github: https://github.com/tizenpdk/lthor

Here's another write up on the Tizen forums:
https://samsung.tizenforum.com/platform/flashing-tizen-to-android-device/msg14383/?PHPSESSID=c3lu20sksk88ptliggf40a47s1#msg14383

Here's a write up that includes a lot of info about lthor and an exynos4412 ODROID dev board:
https://wiki.tizen.org/How_to_Build_and_Load_Tizen_on_Odroid_U3

Here's the post on xda that seems to explain exactly how to install the version of s-boot that includes u-boot and lthor without needing to open up the phone and short a resistor. https://forum.xda-developers.com/showpost.php?p=68146979&postcount=77

I think that if we can figure out how to get this tizen version of s-boot we can then use lthor to completely remove s-boot and replace it with an up-to-date version of u-boot (with the proprietary BL1 blob).

#6 - 06/04/2020 05:59 AM - Denis 'GNUtoo' Carikli

Kurtis Hanna wrote:

> This suggests that there is a version of s-boot that was used on Samsung's Tizen when running on the Galaxy S2 and S3
> https://wiki.tizen.org/TM1
>
> I've seen forum posts where people have successfully put Tizen's version of s-boot on their i9300, which then gives them u-boot with lthor, but I don't have the links handy. They used odin to change the s-boot version without being required to open up the phone and short the test point.

Thanks.

The test points are only used for recovery when something goes wrong. Let's say I want to flash x-boot on the eMMC to do a test, or I have flashed a non-working u-boot and can't recover because the u-boot I flashed doesn't boot. Then shorting the test points documented in Exynos4Bootrom will just make the hardware boot on the microSD first instead of booting on the eMMC first.

However if we find their u-boot version, it might be interesting to understand where it is flashed:

- If it's flashed in the BOOT partition, then we could ship that u-boot right away in replicant >= 9, and then work with upstream to get support for the midas devices when u-boot is flashed in the BOOT partition or after some nonfree and non-redistributable BL1 too, in order not to step on the feet of the people that are working on that, and if we get a free BL1 one day, we'd already have some of the work done this way.
- If not it might still be interesting to look at how it boots, if they have a free software BL1 or not. Even if they don't have a free BL1, it give us new interesting information (more fields on the headers of the BL1, etc)

#7 - 06/04/2020 06:00 AM - Denis 'GNUtoo' Carikli

- Subject changed from Investigate lthor / thor to Investigate lthor / thor and samsung u-boot for Tizen

update bug title to reflect that we discuss about the tizen u-boot too

#8 - 06/04/2020 06:17 AM - Denis 'GNUtoo' Carikli

It might be possible to flash u-boot with heimdall, however it would require quite some work.

Part of mmcblk2boot0 seem to be read-only:

```
--- Entry #0 ---
Binary Type: 0 (AP)
Device Type: 2 (MMC)
Identifier: 80
Attributes: 2 (STL Read-Only)
Update Attributes: 1 (FOTA)
Partition Block Size/Offset: 0
```

```
Partition Block Count: 1734
File Offset (Obsolete): 0
File Size (Obsolete): 0
Partition Name: BOOTLOADER
Flash Filename: sboot.bin
FOTA Filename:

--- Entry #1 ---
Binary Type: 0 (AP)
Device Type: 2 (MMC)
Identifier: 81
Attributes: 5 (Read/Write)
Update Attributes: 1 (FOTA)
Partition Block Size/Offset: 1734
Partition Block Count: 312
File Offset (Obsolete): 0
File Size (Obsolete): 0
Partition Name: TZSW
Flash Filename: tz.img
FOTA Filename:
```

It's still possible to flash a different PIT, as this is read-write:

```
--- Entry #2 ---
Binary Type: 0 (AP)
Device Type: 2 (MMC)
Identifier: 70
Attributes: 5 (Read/Write)
Update Attributes: 1 (FOTA)
Partition Block Size/Offset: 34
Partition Block Count: 16
File Offset (Obsolete): 0
File Size (Obsolete): 0
Partition Name: PIT
Flash Filename: mx.pit
FOTA Filename:
```

But someone would need to write a procedure that is robust enough not to make users and developers break their devices.

Another option would be to patch the bootloader in memory with the exploits from the emmc_tooklit, however it's probably hard to find the location to patch if it's not already documented somewhere.

Currently flashing u-boot is done this way:

- People boot a recovery that has a kernel that doesn't hide the mmcblk0boot0 partition
- They flash the bootloader with that recovery

Doing a Replicant recovery just for that now is probably not very interesting as we don't have a free software BL1 anyway.

Also, the upstream kernel and replicant >=9 kernel gives access to the mmcblk0boot0 partition. So once we have a Replicant >=9 recovery, or even a Replicant >=9 image, and a free BL1, people could use it to flash u-boot.

#9 - 07/28/2020 12:52 AM - Kurtis Hanna

This patch suggests that upstream u-boot added some sort of support for Tizen's THOR a few years ago: "Enable Tizen's THOR download protocol support in U-Boot. It allows downloading images into memory and flash them to target device."
https://github.com/u-boot/u-boot/commit/c6c1ca100feaddd0003723f8a06102db1e521412#diff-43b97f93daa343987f97aa1cbb118680R148

#10 - 11/23/2020 08:35 PM - Kurtis Hanna

The most recent version of lthor seems to be 3.2.

A pre-compiled binary of it seems to be able to be downloaded here: https://download.tizen.org/tools/latest-release/Ubuntu_20.04/

The most up to date source code I could find is here: https://git.tizen.org/cgit/tools/lthor/