Booting XNU on the Raspberry Pi

by Cian Martin Bohan

Twitter: @cianmarbo
GitHub: THePr0gram3rMastr

Contents:

1. Disclaimer

I am not responsible for any damage that may be caused to your Raspberry Pi, SD Card, Mac or anything that may be damaged as a result of following this tutorial. I did not create any of the below tools and I am only providing a tutorial. This tutorial is not for the faint hearted and if you don’t know what XNU is and you are even the slightest bit unsure about what you're doing STOP. This isn’t for you.

A few notes before you begin:

- I made this tutorial based on my own experience and research.
- I never actually got to test this on an actual Raspberry Pi.
- It only supports the Raspberry Pi 1 and possibly the Zero.
- Section 10 is incomplete and will require research and what's written is NOT ACCURATE.
- There may be power consumption issues when running on a Raspberry Pi.
- There is a mediocre chance that this may not work.
- This tutorial requires the Mac OS X Operating System.
- Make sure you have the Xcode Command Line Tools and the iOS SDK installed on OS X.

2. Installing the CTF Tools

Install the CTF Tools by running the following commands in Terminal:

```
$ curl -O http://opensource.apple.com/tarballs/dtrace/dtrace-11.tar.gz
$ tar zxf dtrace-118.tar.gz
$ cd dtrace-118
$ mkdir -p obj sym dst
$ xcodebuild install -target ctfconvert -target ctfdump -target ctfmerge
ARCHS="x86_64" SRCROOT=$PWD OBJROOT=$PWD/obj SYMROOT=$PWD/sym DSTROOT=$PWD/dst
```

3. Installing Homebrew

Install Homebrew by running the following command in Terminal:

```
$ ruby -e "$(curl -fsSL
https://raw.githubusercontent.com/Homebrew/install/master/install)"
```

4. Installing Mac Ports

Install Mac Ports on your computer by going to http://www.macports.org/install.php and choosing the version of Mac OS X your computer is running.

5. Installing the GNU Tools for ARM Embedded Processors

Install the GNU Tools for ARM Embedded Processors by downloading the file for OS X at https://launchpad.net/gcc-arm-embedded/+download

Open Terminal and type:

```
$ cd /usr/local
$ sudo tar xjf ~/Downloads/gcc-arm-none-eabi-4_9-2014q4-20141203-mac.tar.bz2
```

Now check if the tools are fully functional by running the following Command:

```
$ /usr/local/gcc-arm-none-eabi-4_9-2014q4/bin/arm-none-eabi-gcc --version
```

The output should be similar to this:

```
arm-none-eabi-gcc (GNU Tools for ARM Embedded Processors) 4.9.3 20141119
(release) [ARM/embedded-4_9-branch revision 218278]
Copyright (C) 2014 Free Software Foundation, Inc.
This is free software; see the source for copying conditions.  There is NO
warranty; not even for MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
```

6. Installing image3maker

Install image3maker by running the following commands:

```
$ mkdir -p ~/Projects/DarwinARM/Work; cd ~/Projects/DarwinARM/Work
$ git clone https://github.com/darwin-on-arm/image3maker.git
$ cd image3maker; make
$ sudo install -s -m 755 image3maker /usr/bin/image3maker
```

7. Installing GenericBooter

Install GenericBooter by running the following command:

```
$ git clone https://github.com/darwin-on-arm/GenericBooter.git
```

8. Downloading required files

Download xnu-master.zip and extract the files:
https://drive.google.com/file/d/0B3gKfvJ8g_0ZeExDOFVtalZNOTg/view?usp=sharing

Download ramdisk-master.zip and extract the files:
https://drive.google.com/file/d/0B3gKfvJ8g_0ZeII3S2tpVkdhMnM/view?usp=sharing

9. Creating a Bootable image

Open Terminal and type:

```
$ cd (wherever you unzipped the xnu-master folder)/xnu-master/
$ sudo make
$ sudo make TARGET_CONFIGS="release_arm_raspberrypi"
```

Now run the following commands:

```
$ cd GenericBooter
$ make menuconfig
$ sudo image3maker -t krnl -f ../(wherever you unzipped the xnu-master folder)
/xnu-master/BUILD/obj/RELEASE_ARM_RASPBERRYPI/mach_kernel -o images/Mach.img3
$ sudo image3maker -t rdsk -f ../(wherever you unzipped the ramdisk-master
folder)/ramdisk-master/ramdisk.dmg -o images/Ramdisk.img3
```

10. Booting XNU

*THIS SECTION IS INCOMPLETE AND WHAT'S WRITTEN IS INACCURATE!

To boot XNU on the Raspberry Pi format the first partition of your SD Card and place the uImage we created using the steps above into that partition. Insert the SD Card into the slot and boot the Raspberry Pi. Enter the following commands when prompted:

```
fatload mmc 0 0x6b726e6c /uImage
setenv bootargs rd=md0 debug=0x16e serial=3 -v symbolicate_panics=1
bootm 0x6b726e6c
```

If all goes well, you should be greeted with a `login:` prompt. Type `root` and you're done! If you encounter any problems just read back over the tutorial to see if you overlooked anything.

11. Useful Resources

- Darwin on ARM Project GitHub: https://github.com/darwin-on-arm
- Winocm's Blog: http://web.archive.org/web/20140625062552/http://winocm.com/
- Tutorial for booting on Apple A4 devices: https://www.theiphonewiki.com/wiki/Tutorial:Booting_XNU_on_A4_Devices
- XNU Wikipedia: https://en.wikipedia.org/wiki/XNU
- image3maker The iPhone Wiki: https://www.theiphonewiki.com/wiki/Image3maker
- YouTube tutorial on compiling and booting XNU on Apple A4 devices: https://www.youtube.com/watch?v=V-6W3tZfKps