Who’s yo DAHDI

An examination of HamVoIP theft

• Bryan Fields, W9CR
• 30-DEC-2019
• app_rpt is a plug-in for Asterisk
• Zaptel does hardware interfacing
• Combine with radio = AllStar
• Zapata became DAHDI
• Jim designed it all
Timing Alignment is important

Older hardware included this as the kernel lacked it. Newer kernels on Intel don’t have a problem.
Issues on ARM

• ARM - Acorn RISC Machine
• It’s the Raspberry Pi!
• Asterisk (newer asterisk) runs well, Older no so much (1.4 is allstar)
• Why?
  • Timing!
  • Intel has this fixed, and this can cause stuttering and such in the conference calls that app_rpt uses
  • Pickle Linux for the BeagleBoard-xM 2011 or so by Jim and N7PKT with the LoX interface
  • The first ports of code to it RPi
    • 2013 – RPi 1 B+ – 700 MHz single core ARMv6, 512mb ram (runs like ass)
    • 2013 – Beagle Bone Black – 1GHz ARMv7, 512mb ram, works well as IO is not a factor
    • 2015 – RPi 2 – 900 MHz quad-core ARMv7, 1gb ram – first serious contender, USB issues
    • 2106 – RPi 3 – 1200 MHz quad-core ARMv7, 1gb ram – worked well
Hi all,
Just an update, the Arch Linux version of allstar has been stable for 2 weeks now on the repeater VK2RCZ.
If you are happy to compile the allstar code, I have updated my modified version to https://github.com/anthcp/Arch-allstar.
You may still have to fine tune the makefiles like add a symlink for the ar library but it does show the code changes....
We will make a Live CD in the future sometime....

Regards

Anthony, VK2ACP

-------------- next part ---------------
An HTML attachment was scrubbed...
URL: <http://lists.keesles.org/pipermail/app_rpt-users/attachments/20130117/b7b89bea/attachment.html>
Porting to Arch Linux

Anthony, VK2ACP ports it and gets Zaptel/DAHDI running
Porting to ARM
First inquiries about Pi and BBB from Doug

[App_rpt-users] Asterisk and Allstar on the Raspberry Pi

Doug Crompton doug at crompton.com
Sat Apr 20 17:35:54 UTC 2013

• Previous message (by thread): [App_rpt-users] Voter Question
• Next message (by thread): [App_rpt-users] Asterisk and Allstar on the Raspberry Pi
• Messages sorted by: [date] [thread] [subject] [author]

I have been using the Pi for awhile on IRLP with great success. It runs without a hitch. I was curious if anyone is using or has explored the use of the Pi with Asterisk on Allstar? It seems like the requirements would be similar. I use a USB sound FOB and the standard TRLP controller board. The Pi GPIO drives the IRLP controller in place of the standard PC parallel port.

I suspect the URI radio adapter or equivalent is all I would need in the way of hardware for Allstar. I have experience with Asterisk as I have been using it in a residential PBX for almost 10 years.

73 Doug
WA3DSP
http://www.crompton.com/hamradio

-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.kaekies.org/pipermail/app_rpt-users/attachments/20130420/8269261a/attachment.html>

[App_rpt-users] Beagleboard Black and Allstar

Doug Crompton doug at crompton.com
Thu Apr 25 23:21:34 UTC 2013

• Previous message (by thread): [App_rpt-users] A completely off-topic request
• Next message (by thread): [App_rpt-users] Beagleboard Black and Allstar
• Messages sorted by: [date] [thread] [subject] [author]

What are thoughts on using the Beaglebone Black in place of the Beagleboard for Allstar? It is about 1/3 of the price and it looks like it has as much or more capability.
http://beagleboard.org/Products

73 Doug
WA3DSP
http://www.crompton.com/hamradio

-------------- next part --------------
An HTML attachment was scrubbed...
URL: <http://lists.kaekies.org/pipermail/app_rpt-users/attachments/20130425/9560176e/attachment.html>

Doug Crompton doug at crompton.com
Thu Jun 26 05:02:00 UTC 2014

- Previous message (by thread): [App_rpt-users] Question
- Messages sorted by: [ date ] [ thread ] [ subject ] [ author ]

Hello and welcome to the first public release of Allstar on the BeagleBone Black. This represents months of trial and error testing which first started with the Raspberry Pi back at the beginning of the year and was finally successful on the BBB platform. We have had several beta versions out now for over two months with many testers and we had very good reports. There is more to be done but this is a working system that will allow many to get rid of their energy consuming PC’s with constantly running hard drives and have an Allstar system that fits in the palm of your hand.

The web page I have created gives very detailed instructions on how to download, install, and configure your BBB for use with Allstar. The web page is:

hamvoip.org

There you will find a link to download the image and also to join the arm-allstar email list. Please try to address questions specific to the BBB and Allstar to the arm-allstar list and not the apt-rpt list.
It has quite sadly become painfully necessary to "Officially" and publicly state that this release is *NOT* an "Official" Allstar release. It has not been sanctioned by me or the Allstar network. It is something that this person is doing completely independently.

I am not in any way trying to infer that there is anything "right" or "wrong", or anything else about it, merely that is in an independent operation and I/we are not in any way responsible for its contents and/or use.

Jim WB6NIL
Hi Jim and everyone,

I think Doug probably meant "officially released" since we've had several beta-test releases over the last 6 weeks or so.

I'm unfortunately not surprised by your comments, but, am disappointed. As the father of the AllStar project, you should be grinning from ear to ear that your baby has grown to the point that other developers are helping to build your network without requiring any of your time.

I, for one, hope this isn't another fork in the road. I hope it's just another step in the evolution of this already fantastic radio/repeater control and VoIP solution you envisioned.

As a software developer and project manager with decades of experience, one thing I've had to painfully learn is that everybody has their own vision for how a piece of software or a system should function. You can't stifle this creativity. Rather, you have to embrace it and direct it. If the system works reliably, inter-operates (with AllStar) compatibly and is being (pro)actively supported, then you smile and say: Good job guys! We need this feature next! Or, how about finding a solution for that issue???

This shouldn't be a competition. Let's work for a common goal.

73, David KB4FXC
On Wed, 24 Sep 2019, Skyler F wrote:

> Dahdi only runs well on a raspberry pi with Dahdi_Hrtimer.
> What does this do? How was this written? What is the reason why without
> this the raspberry pi has unreliable audio timing versus a normal
> computer?
> Other audio applications like audio / video streaming seem to run fine so
> why did you guys have to write something special for asterisk on the pi?
> Thanks
> Skyler

From: David McGough <kb4fxc@inttek.net>
Date: Wed, Sep 25, 2019 at 8:22 PM
Subject: Re: What does dahdi_hrtimer do?
To: Skyler F <electricity440@gmail.com>

Skyler,

I've spent literally hundreds of hours fixing timing issues in AllStar;
Too much to even begin to try and describe in an e-mail. The dahdi_hrtimer
code is one part of all the fixes. The HRTimer driver was cobbled together
by me.

This driver simulates (with lower resolution) the HPET timer functionality
which X86 PC's have included in their design since about 2005. The ARM
processor does not have any equivalent timer. So, I'm taking advantage of
the ARM SDC counter found in the Broadcom SoC chips. The counter is
free-running at 1MHz, with a 64-bit incrementing accumulator (so overflows
are not a concern). I've adapted this timing source to the needs of
AllStar / Asterisk---and, it works wonderfully.

As for why other audio/video applications work on the RPi?? Well, the
demands of simply playing (or recording) an audio or video stream are
simpler than what AllStar / Asterisk is doing. Asterisk is real-time
mixing and perhaps transcoding audio from multiple sources. Each of these
sources will have slightly different timing (meaning the stream bit rate
will be a little fast or slow). An highly accurate clock is required to
merge these streams, regenerating the frame timing in the process. Without
this, you end up with pops, clicks, etc. What's happening underneath the
covers is non-trivial.
What could this be?
It’s part of DAHDI, no?

- First we boot it up and look around at the kernel modules
What could this be?
It’s part of DAHDI, no?

• First we boot it up and look around at the kernel modules

```
[root@booty ~]# lsmod | grep dahdi
dahdi_hrtimer          16384  0
dahdi                 229376  69 dahdi_hrtimer
crc_ccitt             16384  1 dahdi
```

WOW, with it loaded!

```
[root@booty ~]# dahdi_test -c 20
Opened pseudo dahdi interface, measuring accuracy...
99.992% 99.993% 99.986% 99.991%
--- Results after 20 passes ---
Best: 99.994% -- Worst: 99.984% -- Average: 99.990017%
Cumulative Accuracy (not per pass): 99.990
```
What could this be?
It’s part of DAHDI, no?

- Lets rmmod it and see

```
[root@booty ~]# rmmod dahdi_hrtimer
[root@booty ~]# dahdi_test -c 20
Opened pseudo dahdi interface, measuring accuracy...
99.458% 98.676% 98.519% 99.618% 99.621% 99.622% 98.519% 99.620%
99.618% 99.653% 99.600% 98.536% 99.620% 99.613% 99.449% 99.619%
99.620% 99.445% 99.619% 99.453%
--- Results after 20 passes ---
Best: 99.653%  --  Worst: 98.519%  --  Average: 99.374804%
Cumulative Accuracy (not per pass): 99.963
```

Yea, that’s kind of normal for the RPi.

```
[root@booty ~]# cat /proc/sys/kernel/tainted
5120
```

Bits 10 and 12 are set, but the kernel is still all GPL:
So let’s decompress it and look at it:

```
 gunzip /usr/lib/modules/4.19.65-1-ARCH/dahdi/dahdi_hrtimer.ko.gz
```

Readelf

Oh, it’s got debugging symbols!

It’s GNU GPL code or so it says to the kernel!

`.text` (the code) is only 360h or 864 bytes

Let’s strip it and see
Remember John David is much smarter than us.

Where’s the SOURCE!

- So let’s decompress it and look at it.
- `gunzip /usr/lib/modules/4.19.65-1-ARCH/dahdi/dahdi_hrtimer.ko.gz`
- `Readelf`
- Oh, it’s got debugging symbols!
- It’s GNU GPL code or so it says to the kernel!
- `.text (the code) is only 360h or 864 bytes`
- Let’s strip it and see:
• So lets decompress it and look at it
• gunzip /usr/lib/modules/4.19.65-1-ARCH/dahdi/dahdi_hrtimer.ko.gz
• Readelf
• Oh, it's got debugging symbols!
• It's GNU GPL code or so it says to the kernel!
• .text (the code) is only 360h or 864 bytes
• Lets strip it and see:
• OhWhoa! Misspellings, I <3 misspellings
• It’s initialize not initialize
• GOOGLE SEARCH!
  • “Unable to intialize DAHDI driver”
Remember John David is much smarter than us.
Where’s the SOURCE!

- So let's decompress it and look at it:
  - gunzip /usr/lib/modules/4.19.65-1-ARCH/dahdi/dahdi_hrtimer.ko.gz
- Readelf
- Oh, it’s got debugging symbols!
- It’s GNU GPL code or so it says to the kernel!
- .text (the code) is only 360h or 864 bytes
- Let's strip it and see:
  - OhWhoa! Misspellings, I <3 misspellings
- It’s initialize not initialize
- GOOGLE SEARCH!
  - “Unable to initialize DAHDI driver”
WTF, it’s not just Dummy, is it?
dahdi_dummy is for timing only

- This hasn’t been needed as dahdi has it built in, and Jim built the dummy driver in 2001
- Wait, only on intel. This be ARM.
- John David didn’t just copy it and rename it
- Well let’s look at the timer interface
Can we compile dummy on ASL1.01? Lets see if it works.

- Grabbed the code and compiled on ASL
  - Have to enable it in /usr/src/asl-dahdi-linux-2.11.1/linux/drivers/dahdi/Kbuild
- It built, so lets try it!
- Hell look at that:
Can we compile dummy on ASL1.01?

Let's see if it works.

- Grabbed the code and compiled on ASL.
  - Have to enable it in /usr/src/asl-dahdi-linux-2.11.1/
dahdi-linux/drivers/dahdi/Kbuild.
- It built, so let's try it!
- Hell look at that:
  - This is not exact, the code is larger here in ASL1.01 (3e8 vs. 360 for hr)
  - It is a different Kernel.
  - Can we compile on HamVoIP and compare?
Dahdi from ASL on HamVoIP
Nate’s port is working

• Nate and Stacy got dahdi compiling on the newer kernel for the Pi 4
• I grabbed it and compiled it on HamVoIP
• Stripped of symbols, the files are the same size!
• Well that doesn’t mean they are the same, lets look in IDA
Dahdi from ASL on HamVoIP
Nate’s port is working

- Holy shit, it’s the same damn code.
- The only differences are it was renamed and authors removed
- John David’s M.O.
- Lol, I spent more time on this video
- Lets look at the assembled code
  Just to be sure there’s nothing hidden in his kernel module
- `objdump -d dahdi_hrtimer.ko-stripped`
Dahdi
from ASL on
HamVoIP
Nate's port is working
• Holy shit, it's the same damn code.
• The only differences are it was renamed and authors removed
• John David's M.O.
• Lol, I spent more time on this video
• Let's look at the assembled code
Just to be sure there's nothing hidden in
his kernel module
Dahdi from ASL on HamVoIP

Nate's port is working

• Holy shit, it's the same damn code.
• The only differences are it was renamed and authors removed
• John David's M.O.
• Lol, I spent more time on this video
• Let's look at the assembled code

Just to be sure there's nothing hidden in his kernel module
Dahdi from ASL on HamVoIP

Nate's port is working

- Holy shit, it's the same damn code.
- The only differences are it was renamed and authors removed
- John David's M.O.
- Lol, I spent more time on this video
- Let's look at the assembled code
- Just to be sure there's nothing hidden in his kernel module
Dahdi from ASL on HamVoIP
Does it do the same thing?

- It’s 100% the same code at the ASM level
- But does it do the same thing?
Dahdi from ASL on HamVoIP
Does it do the same thing?

• It’s 100% the same code at the ASM level
• But does it do the same thing?
• Yes
Dahdi from ASL on HamVoIP

Does it do the same thing?

- It’s 100% the same code at the ASM level
- But does it do the same thing?
- Yes
Dahdi from ASL on HamVoIP
Does it do the same thing?

• It’s 100% the same code at the ASM level
• But does it do the same thing?
• Yes

```
[root@booty ~]# asterisk -r
Asterisk 1.4.23-pre.hamvoip-V1.5.4-03-app_rpt-0.327-10/22/2019, Copyright (C) 1999 - 2019 HamVoIP.org and others. Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details. This is free software, with components licensed under the GNU General Public License version 2 and other licenses; you are welcome to redistribute it under certain conditions. Type 'core show license' for details.
-----------------------------------------------------------------------------------------------------------------------------
Connected to Asterisk 1.4.23-pre.hamvoip-V1.5.4-03-app_rpt-0.327-10/22/2019 currently running on booty (pid = 323)
Verbosity is at least 3
booty*CLI> dahdi show status
Description             Alarms    IRQ  bpviol  CRC4
DA kernel (source: HRtimer)  1        UNCONFIGUR  0    0
booty*CLI> quit
[root@booty ~]# dahdi_test -c 20
Opened pseudo dahdi interface, measuring accuracy...
99.991% 99.993% 99.992% 99.990%
--- Results after 20 passes ---
Best: 99.993% -- Worst: 99.981% -- Average: 99.990274%
Cumulative Accuracy (not per pass): 99.990
```

Installed
dahdi_dummy.ko
Summary

• John David McGough, KB4FXC is a thief.
• There is no way to spin this other than he is passing off others work.
• This isn’t an isolated incident.

• Internet Technologies, Inc. customers beware!

• I reached out to the listed author, and he had no idea about it.
John David McGough, KB4FXC is a thief.
There is no way to spin this other than he is passing off others work as his own
This isn’t an isolated incident.

• Internet Technologies, Inc. customers beware!
  • I reached out to the listed author, and he had no idea about this, no permission was granted for it.
  • *Asterisk on Arch was created by others*

• Wait! How do I enable this on my ASL1.01 RPi node?
  • [https://wiki.w9cr.net](https://wiki.w9cr.net)
Questions?