

Forum:[Hack Forums](#)

Thread: [Honeywell Lyric Alarm System/Controller Question](#)

cslim - September 23, 2019, 7:55 pm

I'm fairly new at the hardware hacking game. I have a quick question for anyone who's pretty well versed with obtaining firmware dumps for analysis.

So back in January I moved into a new house...it was advertised as a smart home. At the time I was told that it came with a slew of zwave switches and outlets. Unknown to me at the time, these devices were set up to communicate with a Honeywell Lyric Alarm system.

As soon as I moved in, I removed everything in the house from the Honeywell Lyric because I wasn't a fan of how I had to make a Total Connect account, the shitty voice capability of the device, and I already had a Samsung SmartThings Hub with an Alexa Show and multiple Echos.

I called the company who installed this shit in my house and they said that they were not allowed to give me the installer code to modify the set up of the system. This basically made it so I have a basic device sitting on my wall that really does nothing.

The other day, I decided F it and took it apart. After doing some more research, I attempted to find any type of debugging ports associated with the hardware and could not find it.

I'm looking for anyone who can assist me. I will take photos soon and upload.

The only data I can find online about the circuit board is the following:

Type: BTI ML-2 94-V0

Honeywell part number: 200-01526

Any help would be much appreciated!!

Thanks!

HyperPhobic - September 23, 2019, 8:12 pm

(Sep 23, 2019 07:55 PM)cslim Wrote: [\[CITE\]](#) I'm fairly new at the hardware hacking game. I have a quick question for anyone who's pretty well versed with obtaining firmware dumps for analysis.

So back in January I moved into a new house...it was advertised as a smart home. At the time I was told that it came with a slew of zwave switches and outlets. Unknown to me at the time, these devices were set up to communicate with a Honeywell Lyric Alarm system.

As soon as I moved in, I removed everything in the house from the Honeywell Lyric because I wasn't a fan of how I had to make a Total Connect account, the shitty voice capability of the device, and I already had a Samsung SmartThings Hub with an Alexa Show and multiple Echos.

I called the company who installed this Clay Davis in my house and they said that they were not allowed to give me the installer code to modify the set up of the system. This basically made it so I have a basic device sitting on my wall that really does nothing.

The other day, I decided F it and took it apart. After doing some more research, I attempted to find any type of debugging ports associated with the hardware and could not find it.

I'm looking for anyone who can assist me. I will take photos soon and upload.

The only data I can find online about the circuit board is the following:

Type: BTI ML-2 94-V0
Honeywell part number: 200-01526

Any help would be much appreciated!!

Thanks!

I'd be interested in helping! I have some experience working with honeywell SCADA. I can find you technician manuals, they should have diagrams for whatever you need. I'll try to find a potential privilege escalation vector for you.

cslim - September 23, 2019, 8:18 pm

That would be amazing! Thank you so much! I'll upload some photos of the board shortly.

HyperPhobic - September 23, 2019, 8:19 pm

(Sep 23, 2019 07:55 PM)cslim Wrote: [CITE](#) I'm fairly new at the hardware hacking game. I have a quick question for anyone who's pretty well versed with obtaining firmware dumps for analysis.

So back in January I moved into a new house...it was advertised as a smart home. At the time I was told that it came with a slew of zwave switches and outlets. Unknown to me at the time, these devices were set up to communicate with a Honeywell Lyric Alarm system.

As soon as I moved in, I removed everything in the house from the Honeywell Lyric because I wasn't a fan of how I had to make a Total Connect account, the shitty voice capability of the device, and I already had a Samsung SmartThings Hub with an Alexa Show and multiple Echos.

I called the company who installed this Clay Davis in my house and they said that they were not allowed to give me the installer code to modify the set up of the system. This basically made it so I have a basic device sitting on my wall that really does nothing.

The other day, I decided F it and took it apart. After doing some more research, I attempted to find any type of debugging ports associated with the hardware and could not find it.

I'm looking for anyone who can assist me. I will take photos soon and upload.

The only data I can find online about the circuit board is the following:

Type: BTI ML-2 94-V0
Honeywell part number: 200-01526

Any help would be much appreciated!!

Thanks!

cant find anything on that board :o post pics pls

cslim - September 23, 2019, 8:38 pm

So I guess I have to wait till I have more posts before I post links or images :(

Is there any other way I can send you the photos?

I have an album created on imgbb dot com.

So quick update. Since I can't post photos, I started doing some digging and found out that the Honeywell Lyric Controller uses an SPI EEPROM chip for its firmware...or at least I think. The chip number is 95256WP K7348. I was able to look-up the chip diagram and think I have a good idea of how to link the chip to my Raspberry Pi 4 with flashrom.

I'll post any updates after hooking it all up.

Does this sound like the right first avenue of approach?

cslim - September 25, 2019, 7:21 am

So I've made a diagram of all the chips on the board. I've been able to identify every chip and its datasheet. After identifying the SPI EEPROM chip, I realized I was missing the hardware I needed to pull the firmware data. I've ordered a SIP Clip, which should hopefully be here on Thursday.

I plan to pull the firmware off using the SIP Clip connected to my Raspberry Pi 4 using flashrom followed by binwalk.

Once the firmware is pulled and properly extracted I'll post an update if anyone is interested.

Where I definitely will need help is identifying possible root account passwords associated to the device after executing binwalk.

Does anyone have any good material that I could research to figure this out?

Thanks!!