☒

□ Digital Corruption DSS Discussion
□ Echostar
□ Channel tier packs

☒ UBBFriend: Email This Page to Someone!

☒ Post New Topic ☒ Post A Reply

profile | register | prefs | faq | search

next newest topic | next oldest topic

Author **Topic: Channel tier packs**

Stymie

☒ Posted 12-03-98 11:40 AM by Stymie ☒ Click Here to See the Profile for Stymie ☒ Click Here to Email Stymie ☒ Edit Message

I think it would be a nice idea if we created a channel list of known tiers.

Logging the card, I see that the IRD will not give you a channel until you issue the tier pack. This reminds me of challenge/password type entrances.

-Stymie

nipper

☒ Posted 12-04-98 04:18 PM by nipper ☒ Click Here to See the Profile for nipper ☒ Click Here to Email nipper ☒ Edit Message

RETURN 00 00 03 E7 INSIDE A CHANNEL SERVICE POLL. OPENS THE WORLD UP TO A CARD.

nipper

☒ Posted 12-05-98 01:01 AM by nipper ☒ Click Here to See the Profile for nipper ☒ Click Here to Email nipper ☒ Edit Message

TO CLARIFY THE ABOVE:

SEND THIS IN RESPONSE TO 20 SUB 08.
01 01 00 00 00 00 00 00 00 00 00 00 0D 81 4C 21 4C 21 00 00 03 E7 80 00 FF 00 FF 00

AFTER 4C 21: 00 00 (MIN CHAN 000)
03 E7 (MAX CHAN 999)

DR7
Administrator

☒ Posted 12-05-98 04:35 AM by DR7 ☒ Click Here to See the Profile for DR7 ☒ Click Here to Email DR7 ☒ Edit Message

Thanx again Nipper...you rock even though your a ugly lookin promo-dog ☒ ☒ ☒ ☒

StuntGuy

☒ Posted 12-05-98 10:25 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy ☒ Click Here to Email StuntGuy ☒ Edit Message

I don't think it's quite that easy...I modified a blocker to spoof commands 20/08 and 21/08 as follows:

20/08: 12 PCB 05 A0 01 01 90 00 CS
...Should make the IRD think there's 1 channel service pack to return

21/08: 12 PCB 20 A1 1C 01 01 00 00 00 00 00 00 00 00 00 00 0D 81 4C
21 4C 21 00 00 03 E7 80 00 FF 00 FF 00 90 00 CS
...Should make the IRD think channels 000 through 999 are valid.

If I put the card in alone and tune to a station I'm authorized for, then insert the card with the blocker, I get picture and audio until I try to change channels, at which point everything freezes after about 6 seconds, and I need to pull the blocker/card to get control back.

Are you sure it's 0D 81 and not 0D 61? According to the logs I've got, for all of its valid channel service polls, my subscribed CAM returns 0D 61. Also, what're bytes 5 and 6 of the data field? (01 01 00 00 xx xx)? On my subscribed CAM, I don't get 00 00 there...I get something that appears to be loosely related to the minimum channel number. Also, for min and max channel number, my subscribed CAM often returns a value that's > 999...are these aliases for programming packages?

-s

[This message has been edited by StuntGuy (edited 12-05-98).]

nipper

☒ Posted 12-05-98 10:39 AM by nipper ☒ Click Here to See the Profile for nipper

☒ Click Here to Email nipper ☒ Edit Message

THE TIER MUST BE PLACED INSIDE PIECE OR NOTHING. THE GUIDE IS OPNED NOW.

StuntGuy

☒ Posted 12-05-98 02:13 PM by StuntGuy ☒ Click Here to See the Profile for StuntGuy

☒ Click Here to Email StuntGuy ☒ Edit Message

Ah...that would explain it, then.

-s

uniwiz
Junior Member

☒ Posted 12-06-98 05:49 PM by uniwiz ☒ Click Here to See the Profile for uniwiz

☒ Edit Message

StuntGuy,

Thanks for the disassembly of the blocker.hex

It had a few errors to fix before I could assemble it. Works nice and the info you gave is very helpful. Nice job.

I have a question on this 20/08 command?
Is nipper saying the response we need to send must be in the 20/08 packet?
Did you get it to work StuntGuy?

DataPimp
Member

☒ Posted 12-06-98 07:10 PM by DataPimp ☒ Click Here to See the Profile for DataPimp

☒ Edit Message

uniwiz,

I have the avrtools thing that I downloaded from atmel.com, I was wondering though, i can't open it in the studio, it says it's to large, i could compile it via the command line though, where is the .lst file that is needed?

uniwiz
Junior Member

☒ Posted 12-06-98 08:05 PM by uniwiz ☒ Click Here to See the Profile for uniwiz
☒ Edit Message

The file is avrasm.exe, the command line should look like this:

```
avrasm -i c:\avrtools\block.asm block block.hex
```

Nipper in answer to StuntGuy's question
does the packet go into the 21/08 packets or does go after the 20/08 packet IE 12 PCB 20 A0 1C 01 01 00 00 00 00 00 00 00 00 00 0D 81 4c 21 4c 21 00 00 03 e7 80 00 ff 00 ff 00 90 00 CS ??

uniwiz
Junior Member

☒ Posted 12-06-98 09:15 PM by uniwiz ☒ Click Here to See the Profile for uniwiz
☒ Edit Message

StuntGuy,

I get 0D 65 ......

Also spoofing 20/08 didn't work.
The ird got around it by repeating the cmd's over and over. My reply packet (above) didn't seem to work.
I was thinking to catch 20/08 get the sum data add one. Then add my extra packet in the teir packets.
Would this work??

uniwiz
Junior Member

☒ Posted 12-06-98 10:17 PM by uniwiz ☒ Click Here to See the Profile for uniwiz
☒ Edit Message

Thanks guys!! Nipper you are the greatest!!
Got it to work. Sent DR7 the block.asm file.

All the channels show up in the listings!!

Still not authorized to get un subbed channels through.
Nice to see a breakthru.

StuntGuy

☒ Posted 12-07-98 08:07 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy
☒ Click Here to Email StuntGuy ☒ Edit Message

I'm sure that the packet Nipper posted needs to be in response to the 21/08 packet, but you also need to grab the 20/08 packet so that the IRD will think there's at least 1 channel service packet coming, even if the card wants to say "0".

UW: The 20/xx packet is a poll for presence of data from the IRD to the card. If the card responds saying that there's some non-zero number of entries for a particular data type (01=IRD info, 08=channel service, 11=PPVs, etc.), then the IRD will proceed with 21/xx packets which are requests for data of type xx.

On the blocker: Yeah...I didn't find out that it wouldn't assemble until after I had posted it and I tried to reassemble with my 20/08 21/08 spoof code. Sorry 'bout that...I'll be sending along an updated copy with some corrected comments soon.

-s

uniwiz
Junior Member

☒ Posted 12-07-98 07:27 PM by uniwiz ☒ Click Here to See the Profile for uniwiz
☒ Edit Message

OK,
I spoof 21/08 command and replace the first tier with 03 E7 packet.
All channels are listed only 2 channels "red", all music channels wide open
☒

I get "Card not authorized error" on unsubbed channels.
Spoofing the C0 command and having the blocker replying NAD PAC LEN 08 B0 04 04 00 00 06 sw1 sw2 CS the error goes away but the channel is blank.

Command 13 the CAM is not replying with data mostly zeros instead.

Any help on command 13?

Thanks

nipper

☒ Posted 12-07-98 08:33 PM by nipper ☒ Click Here to See the Profile for nipper
☒ Click Here to Email nipper ☒ Edit Message

---

21 POLLS OF RELEVANCE:

01: IRD INFORMATION (ZIPCODE,TZ,IRD#,IRD INFO)
08: PURCHASED SERVICES
0B: PURCHASED PPV'S

NOTE: 11 IS IRRELEVANT AND IS ONLY FOR CALLBACK INFORMATION AND NAGGING. 0B IS WHERE THE ENABLE OF A PPV IS COMING FROM.

StuntGuy

☒ Posted 12-08-98 08:12 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy
☒ Click Here to Email StuntGuy ☒ Edit Message

Nipper: Thanks man...that helps.

Uni: Hmm...so you intercept the first 21/08 reply, but not the 20/08? What happens with an unsubscribed card? As I mentioned above, I tried intercepting both 20/08 and 21/08, but I didn't get any useful results.

Maybe I'll take your advice and make a "smart" one that just tries to tack a final channel service pack on the end.

As far as the 13 packets go, it looks to me as though they base their return value on the data that was sent in an 03 packet. If you check your logs, I think you'll find that two packets before any 13 packet, there's an 03 packet.

-s

uniwiz
Junior Member

☒ Posted 12-08-98 03:55 PM by uniwiz ☒ Click Here to See the Profile for uniwiz ☒ Edit Message

---

SG,

I tried the idea you had with the 20/08 stuff.
Replacing the count with 01 and then inserting the reply to the 21/08 command.
It didn't work. It appears you must insert it into one of the 21/08 "real" packets. Didn't matter beginning or end. Also 81,61,85 all appear to work.
Thanks for the ideas.

Will check on the 03 stuff ☒
My logs always lose sync evey now and then.

StuntGuy

☒ Posted 12-09-98 08:07 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy ☒ Click Here to Email StuntGuy ☒ Edit Message

---

On the logger losing sync: Yeah...and given that the current SCP logger doesn't save the decrypted info to the log file, I'm thinking I'll probably release my logger...it'll provide the same long-term output, but it doesn't lose sync, it'll work with any parallel port, and it'll work in either byte- or nibble-mode.

On the 21/08: Hmm...so you intercept one of the responses coming back from the CAM? Interesting. Maybe it's an issue of the IRD always wants to see more than one channel service pack. Definitely gotta do some more work on this.

-s

[This message has been edited by StuntGuy (edited 12-09-98).]

uniwiz
Junior Member

☒ Posted 12-09-98 04:42 PM by uniwiz ☒ Click Here to See the Profile for uniwiz ☒ Edit Message

---

Hmmm, I'm going to build the 20 pin logger version and see if it fairs better.

I could really use a better logger ☒
I'm puttng in some serious time on this.
Really appreciate all the help.

On 21/08, I think it's more of an issue that you need the correct number of packets.

On the command 13 issue, my command 03's seem to be coming in ok but the 13's are still 00 00 (empty).

Need to make a list of commands, I've started.
How bout the blocker being able to buy PPV's?
Haven't figured yet what's stopping that.
Anyhow it's all good stuff. Keep me posted on your logger.

[This message has been edited by uniwiz (edited 12-09-98).]

StuntGuy

☒ Posted 12-10-98 08:12 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy ☒ Click Here to Email StuntGuy ☒ Edit Message

---

On the 03/13 issue: That's because even though the 03 command is getting through okay, the card knows you're not authorized for the channel, so it doesn't provide the decryption key for the video back to the IRD in the 13 command.

On the logger: I'll probably work on it tonight and get a limited-functionality version released.

On the 20/08 / 21/08 thing: Yeah...I do that...when I spoof the 20/08 packet, I respond telling the IRD that there's 1 data item to return. Then, when it asks for the 21/08 packet, I send the one with 000/999. Locks the receiver up pretty good. OTOH, this could be a problem with some other space-saver mods I made, too.

On what's stopping the PPVs: Its the fact that the blocker blocks 00/01/02 commands. If you change the first command handler table at CHNDLRS so that the first three entries point at PASSIRD instead of C000102 (I'm assuming you're using my disassembly here), it should allow you to buy PPVs, but it'll no longer block deactivations and card updates. Keep in mind...this is just a guess...I haven't tried it out.

-s

Stymie

☒ Posted 12-10-98 10:28 AM by Stymie ☒ Click Here to See the Profile for Stymie ☒ Click Here to Email Stymie ☒ Edit Message

---

I think that should be okay stuntguy. If they use common/group/unique style management packs (logical way no?), the first pack offset (Cmd 00) would be common. If the box could uniquely send out uniquely signed packets to your card, that would tell us the inverse of the algorithm was tucked inside the onboard flash. I am very curious however as too what exactly is in the flash. Has anyone read out their flash?

DataPimp
Member

☒ Posted 12-10-98 04:42 PM by DataPimp ☒ Click Here to See the Profile for DataPimp ☒ Edit Message

---

StuntGuy,

Ok, If you want me to post it somewhere where ppl can get it, lemme know, eager to try it out and see if it helps ☒

DP

uniwiz
Junior Member

☒ Posted 12-10-98 08:05 PM by uniwiz ☒ Click Here to See the Profile for uniwiz

☒ Edit Message

SG,
On 20/08 the correct packet number must be there. You can replaced one or all the channel packets (21/08).
I never had lockups unless I program the commands wrong. I did each way you suggested.

On 03/13 I am still confused. That mean 20/08 is only good for opening the channels up to be listed. Authorization is provide via another command.

Yes it is save to assume I'm using your remarked code ☒ Willing to share any changes I've made.

On PPV I've tried freeing up each command 00, 01, 02 but still no help.

StuntGuy

☒ Posted 12-11-98 08:30 AM by StuntGuy ☒ Click Here to See the Profile for StuntGuy

☒ Click Here to Email StuntGuy ☒ Edit Message

On the logger: It should be up here now. I think I'm going to make a couple of changes to the way the filtering works, though...I woke up this morning not entirely happy with the limited (and slow) way I implemented the filter, so I'll probably make a configuration screen or something where you can just specify outright which IRD commands you want to log and which you don't. I'll also probably add some sort of "alarm on unusual packets" feature so that if any 00/01/02 packets come along, you'll get some indication that maybe now is the time to look at your log.

On channel service packets (20/08 / 21/08): Hmm...that's sort of interesting...I wonder how the IRD knows how many packets of channel service info the CAM will be providing ahead of time, because if I respond to the 20/08 with a "01", the IRD _should_ be expecting just a single packet for 21/08.

On the 13 and 03 commands: I'm thinking that what happens is that the 03 packet (or possibly the 00 packet) contains some sort of encrypted version of the decryption keys for the next N seconds of video and audio. The next 13 command that comes along is requesting the decrypted version of those decryption keys so that the IRD can use those keys to decrypt the video and audio.

-s

All times are PST (Can)

next newest topic | next oldest topic

□**To close this thread, click here (moderator or admin only).**

☒ Post New Topic ☒ Post A Reply **Hop to:** Echostar Go

Contact Us | Digital Corruption

☒