DR7 Discussion Forums - nASTY iO iNSiDE bLOCKeR
Login @DR7 E-mail Signup @DR7 E-mail

Email This Page to Someone!
Show a Printable Version

DR7 Discussion Forums > General Information Discussion Forum
nASTY iO iNSiDE bLOCKeR < Last Thread   Next Thread >
Author Thread

nipper
Guest

Registered: Not Yet
Posts: N/A
ALL THESE ROUTINES WERE ALMOST DIRECT TRANSLATIONS FROM THE ROM. THE
2 TABLES ARE USED IN THE REAL CARD AND WE SIMPLY PORTED THE
CONVERSION OF THE REFERENCE INTO THE BLOCKER.

'NIPPER THE BUTTLICKER' IS ALSO THEIR TEXT. IN THE CAM DUMP, WE
SIMPLY SHOWED YOU WERE KEYS WERE LOCATED. NOTE THEIR ARE 2 POSSIBLE
CHANNEL DECRYPT KEYS USED. OFFSETS 28h AND 30h (KEYS FLOW IN ORDER).

ENJOY!

11-12-1998 12:47 PM

StuntGuy
Guest

Registered: Not Yet
Posts: N/A
Okay, that's truly sad...I mean, I'd assume their programmers were a
little on the lazy side, but that's BAD.

-s

P.S. How about sharing some info on how to get an EEPROM dump?

11-12-1998 08:06 PM

masa
Guest

Registered: Not Yet
Posts: N/A
Funny thing you should ask, StuntGuy.
Now, weather or not this proves to be of any
use or not, it is still rather interesting, and because I have had
some time off from work (injury), I have had far too much time on my
hands. I have gone into the EchoStar's IRD Memory Dump & Diagnostics
screen. Upon entering that screen, I have started a manual type dump
of everything in the IRD's memory. I have also already dumped a hex
file of the card. It was 512 bytes large. Interesting how much NVRAM
that it holds. I would have thought it might hold more than that,
but at the beginning of the card dump, shows the familiar for
letters. "BUFA". These same letters are shown in the IRD's System
Information Screen under SOFTWARE Version and Boot Strap Version. If
anyone would like a copy of this dump, I would be more than happy to

share it with SCG or any of you other guys out there that might want
to examine it. I don't know what kind of use it is to anyone, but it
seems to be a program for something, stored in the card's NVRAM. If
I'm going down the wrong track by dumping this stuff, someone should
tell me before i go too far past the IRD dump (now at 18k).

Masa

11-14-1998 03:42 AM

biatch
Guest

Registered: Not Yet
Posts: N/A
How can I get into the diagnostic menu?
whatyou have sounds like the data from the 24C08 or the 24C16
depending on you system.
buda

11-14-1998 04:34 AM

StuntGuy
Guest

Registered: Not Yet
Posts: N/A
Yeah, the NVRAM stuff on the receiver's screen (biatch: go to the
diagnostics menu, then hit INFO-right arrow-left arrow) is the IRD's
EEPROM, not the card's. The EEPROM in the card is at least 4096
bytes long. what's really interesting is looking at the differences
in the NVRAM stuff in various receivers...I've got a couple of 1000s
I'm using for experiments, and their NVRAM is pretty worthless. I've
got a 5000 and a HDSR-100U that both have things like favorite
channel lists in the IRD EEPROM, etc. Lots of stuff stored in there
in straight ASCII, too.

I'm guessing that "BUFA" is a signature that the E* people use to
allow them to know that the EEPROM is initialized.

-s

11-14-1998 12:33 PM

biatch
Guest

Registered: Not Yet
Posts: N/A
Stundgyt,
or "BAKA"
Buda

11-16-1998 02:55 AM

pasha

Guest

Registered: Not Yet
Posts: N/A
how we can get this second key???
-Pasha

03-26-1999 09:39 AM   IP: Logged

johnyaya
Guest

Registered: Not Yet
Posts: N/A
nipper, any chance that i can get a copy of the cam dump? please,
please, please...

03-26-1999 01:00 PM   IP: Logged

Ben Dover
Guest

Registered: Not Yet
Posts: N/A
If you look, this stuff is FOUR MONTHS OLD.

(Four months? Is that all?????)

Anyway, these guys are long gone, mainly due to petty squabbles.
(Note that they don't have any "member" info under their names. They
haven't been on since the board shutdown/restart.)

Lets hope that these guys have been lurking in the background, since
they (and a few others) are the only real chance that we have of
surviving the next (first!) ECM.

03-26-1999 01:15 PM   IP: Logged

Ben Dover
Guest

Registered: Not Yet
Posts: N/A
And john, the CAM dump is posted in the Tools section... Echostar
Running Card Dump + Public Keys by Swiss Cheese Productions

03-26-1999 01:17 PM   IP: Logged

Beavis
Guest

Registered: Not Yet
Posts: N/A
Ben Dover,
didn't they leave due to the johnny satellites?

03-26-1999 02:44 PM   IP: Logged

johnyaya
Guest

Registered: Not Yet

Posts: N/A
thanks ben, i was hoping for something new...

03-26-1999 04:03 PM   IP: Logged

uniwiz
Guest

Registered: Not Yet
Posts: N/A
nipper you are a f**king genius!
4 months old and the answer is there.

hehehe

good job pasha

03-26-1999 09:28 PM   IP: Logged

pasha
Guest

Registered: Not Yet
Posts: N/A
unwiz,
we have to look all old posts TECH posts, some good info is here.
-Pasha

03-27-1999 01:10 AM   IP: Logged

Ben Dover
Guest

Registered: Not Yet
Posts: N/A
Beavis - No; I'm pretty sure it was one or two people pushing the
"put up or shut up" bit.

03-27-1999 03:23 AM   IP: Logged

All times are PST (US)

Forum Jump: Please select one: Category: The Reviews
  Conferences-------------------The SpawnDevices Loader ForumThe DishToys
  AVR3 ForumCategory: The Digital Satellite
  Hobbyist-------------------Receiver Problems & SolutionsEquipment
  Help/Support for New UsersMedia Programming & ReprogrammingMedia Repair
  Tips and TechniquesHobbyist FAQ'sHardware ForumInvalid Media and
  Extension MessagesEMU DiscussionSmart Cards Discussion(Non Satellite
  Related)HDTV(High Definition Television) Discussion and TipsSignal
  Disruption & InterruptionLatin DirecTV and Sky Mexico3rd Generation
  MediaGeneral DiscussionVideoCipherII C Band DiscussionCategory: TIVO and
  Replay Conferences-------------------General DiscussionTIVO
  Modification and BlessingCategory: The Ekko
  Hobbyist-------------------General Information Discussion
  ForumTechnical Discussion ForumReceiver & Modification
  DiscussionsPlastic Media Repair DiscussionLogger Device Discussion
  ForumCategory: The Definitive Home Theater-------------------Dolby
  Digital 5.1, 6.1 and 7.1DVD - Great Movies and Great ExperiencesHome
  Theater Help and TipsCategory: Home Theater
  Automation-------------------Touchscreen RemotesHardware & Software for
  Home AutomationCategory: Music In The Digital
  Domain-------------------MP3 Releases and TechniquesDVD AudioCompact

DR7 Discussion Forums - nASTY iO iNSiDE bLOCKeR.txt
Disc Releases & ReviewsCategory: Digital Photography & Editing
Software-------------------Photographic HardwareCategory: Small Office
Home Office-------------------Home Office NetworkingCategory: Personal
Computers & Computer Technology-------------------Personal Computers
(PC Compatible)MacIntosh DeskTops and LaptopsComputer Related
HelpCategory: NASDAQ and Digital Technology-------------------The
Technology MarketplaceCategory: Used Products for
sale-------------------Used Products: For sale or tradeCategory:
Satellite Politics-------------------We the Canadians...but everyone is
welcomedCategory: General Discussion-------------------Jokes from the
Members :)Dealer ComplaintsFrench Speaking Satellite DiscussionsDealer
Praise and CommentsIndividual Praise and Comments < Last Thread   Next
Thread >
Forum Rules:
Who Can Read The Forum? Any registered user or guest.
Who Can Post New Topics? Any registered user.
Who Can Post Replies? Any registered user.
Changes: Messages can be edited by their author. Messages can be deleted
by their author.
Posts: HTML code is ON. Smilies are ON. vB code is ON. [IMG] code is
ON.Admin Options:
Open / Close Thread
Move Thread
Delete Thread
Edit Thread

< Contact DR7 Support - DR7 - Feeding the Digital Mind >
Powered by: vBulletin Version 1.1.5
Copyright © Jelsoft Enterprises Limited 2000.
c2001 X-Factor Web Designs