Unleash The Power Of Your Echostar

A Beginners Guide To Hacking E*

By Jazzercz

Version 1.1 - January 30th, 1999

Introduction

There are many ways to hack Echostar and get all of the channels. All information contained in this document was obtained from the www.dr7.com web site. Unfortunately the information is spread over many files and forums which makes it difficult for beginners to comprehend. This document will bring together this disperse set of information into a beginners cookbook on how to perform the hack. Of the many methods (Single AVR, Dual AVR, BAT cards, etc...), my favorite is the single AVR method. This is what I will document here.

I am not an expert at this by any means. I am a novice. I have just spent untold hours reading the forums and documents which are available. Hopefully this document will reduce the time you need to get started. If you have any questions, or want to know more, please post your questions to the Echostar forum on www.dr7.com. I don't have the time, nor the knowledge to answer everyones questions.

This technology is changing so fast, that this document is out-of-date five minutes after it has been written. After you have read this document, it would behoove you to go to DR7's web page and spend quite a bit of time reading the Echostar forum to get a current view of things.

Overview Of Terms

First, let me give you an overview of terms and abbreviations which are used in this document and in the forums.

Term	Definition
E*	Echostar
IRD	The big black box which you plug your cables into.
CAM	The "credit card" you slide into the front of the IRD. The CAM is also known as as Smart Card. Refer to http://www.dr7.com/smartfaq.htm or http://www.smartcard.co.uk/tech1.html for more info about smart cards. The CAM is sometimes referred to as the plastic.
E*C	Echostar chat - www.dr7.com click on chat forum and then click on the echostar section
ECM	Electronic Counter Measure - The ability for the echostar company to send a satellite signal which will determine that your IRD has been hacked and to somehow disable your IRD from working.
DAT	enabler/blocker board. It is a long card with some components on it which you stick in your slot where your CAM normally goes. It serves as a replacement for the CAM.
8515	Short name for AT90S8515-8PC - An ATMEL microprocessor which is used in this hack. This chip contains an 8 bit RISC CPU with 8K flash memory, 512 by bytes of Sram. The 8515 comes in many varieties. The one which is u 8PC.
AVR	The ATMEL family of AT90 microprocessors

CASE NO.
SA CV 03-950 DOC (JTLx)
ECHOSTAR SATELLITE CORP., et al.,
vs.
NDS GROUP PLC, et al.
DEFENDANT'S EXHIBIT 524
DATE ________________ IDEN.
DATE ________________ EVID.
BY ____________________
Deputy Clerk

EXH
C
9

Unleash The Power Of Your Echostar

A Beginners Guide To Hacking E*

By Jazzercz

Version 1.1 - January 30th, 1999

Introduction

There are many ways to hack Echostar and get all of the channels. All information contained in this document was obtained from the www.dr7.com web site. Unfortunately the information is spread over many files and forums which makes it difficult for beginners to comprehend. This document will bring together this disperse set of information into a beginners cookbook on how to perform the hack. Of the many methods (Single AVR, Dual AVR, BAT cards, etc...), my favorite is the single AVR method. This is what I will document here.

I am not an expert at this by any means. I am a novice. I have just spent untold hours reading the forums and documents which are available. Hopefully this document will reduce the time you need to get started. If you have any questions, or want to know more, please post your questions to the Echostar forum on www.dr7.com. I don't have the time, nor the knowledge to answer everyones questions.

This technology is changing so fast, that this document is out-of-date five minutes after it has been written. After you have read this document, it would behoove you to go to DR7's web page and spend quite a bit of time reading the Echostar forum to get a current view of things.

Overview Of Terms

First, let me give you an overview of terms and abbreviations which are used in this document and in the forums.

Term	Definition
E*	Echostar
IRD	The big black box which you plug your cables into.
CAM	The "credit card" you slide into the front of the IRD. The CAM is also known as as Smart Card. Refer to http://www.dr7.com/smartfaq.htm or http://www.smartcard.co.uk/tech1.html for more info about smart cards. The CAM is sometimes referred to as the plastic.
E*C	Echostar chat - www.dr7.com click on chat forum and then click on the echostar section
ECM	Electronic Counter Measure - The ability for the echostar company to send a satellite signal which will determine that your IRD has been hacked and to somehow disable your IRD from working.
DAT	enabler/blocker board. It is a long card with some components on it which you stick in your slot where your CAM normally goes. It serves as a replacement for the CAM.
8515	Short name for AT90S8515-8PC - An ATMEL microprocessor which is used in this hack. This chip contains an 8 bit RISC CPU with 8K flash memory, 512 bytes of eeprom, and 512 bytes of Sram. The 8515 comes in many varieties. The one which is used in this hack is an 8PC.
AVR	The ATMEL family of AT90 microprocessors

EXHIBIT 524
Rachel A. Fenner
CSR No. 6948
Date: 6/8/05
Guggenheim

How Does This Hack Work

This is a simplified overview of how it works. The steps below will make more sense once you understand the concept of how this hack works.

Under normal operation, when you select a channel, the IRD sends a message to the CAM and asks the CAM if you have permission to watch the channel you selected. Even though the CAM looks like a credit card, the CAM is a little computer in itself. Once the CAM receives the permission request message, it does some calculations and sends back a message to the IRD informing the IRD if you are permitted to watch the channel or not. The IRD does what it is told.

This hack works by replacing the CAM with another computer, an 8515, which is programmed to act like a CAM. However, the 8515 is programmed to blindly give permission to all channels. In order for the 8515 to act like a CAM, the 8515 needs to be loaded with a program which emulates a CAM. The program is called **xfile**.

E* didn't make it easy for us. The CAM and the IRD communicate in encrypted messages which is unique to each IRD. In order for the 8515 to properly emulate the CAM in your specific IRD, it needs to know the secret key your IRD uses. Your IRD secret key is unique. This document will tell you how to find out your secret key.

The CAM looks like a credit card, but the 8515 looks like a normal computer chip. Therefore some circuitry is needed to make the 8515 interface with the IRD. One method is using a DAT board.

ECM

To date, E* has not transmitted an ECM. However, the ability to hack an E* system is only a little over a month old. Since an ECM has not been sent, there is no way to know exactly what they will/can do. Will they send an ECM which will make the current hack stop working? Will they send an ECM which will not only stop the current hack, but inhibit the IRD from working even with a subscribed CAM? Who knows?

The current conjecture is that the only thing that they can do to permanently screw up your IRD is to send codes which will overwrite an EEPROM in your IRD. If that happens, then you will need to remove your current EEPROM and replace it with an EEPROM with good data in it. This EEPROM uses a chip packaging called TSOP. People use the word TSOP to refer to this chip in the IRD. On http://www.dr7.com/echostartools.htm there are donated TSOP dumps of good EEPROMS which you can download and install in your IRD to return it to a good state. To get a good feel of what is involved, you can read http://www.dr7.com/chipremoval.htm which will describe the processes of removing and replacing the chip. This is a great document and contains photos which will show you the inside of an IRD and what the TSOP looks like. To do the chip removal yourself, you need to purchase an EEPROM programmer and maybe some adapters which could push the price well into the $300 range.

DR7 recommends that you perform the chip removal procedure so that you have an archive of your TSOP. He feels this is the best way to protect yourself against ECM's.

There has been some conjecture that the only way E* can update your IRD is when it is turned off. So, it probably would be a good idea to leave it on all the time.

Basically, an ECM could make things messy and the exact recovery process has not been identified at this time.

Disclaimers

Currently, not all boxes have been confirmed to be hackable. Refer to E*C for the latest information on this, but models 1000, 2350, 3000, 3500, 4000, 5000, and JVC DVHS have been successfully hacked.

The hack currently works, as of the date of this publication, but can be disabled by E* at sometime in the future of their choosing. If you plan on doing this hack to save money, you probably won't in the long run.

The legality or enforcement of this in your area is unknown by the author and no claims are made or implied by such. Contact your local law enforcement agency or lawyer for legal concerns and information.

There is nothing unique or novel in this document, it is just a rehash of what has already been disclosed in public forums.

New Dish Users

If you currently do not have an E* system, I would recommend that you purchase a 4000 with a dual LNB. The board inside the 4000 is more friendly to recovery from ECM's. The dual LNB is good for future expansion (i.e. more than one IRD).

Process

Overview of steps:

Here is a quick overview of the process.

1. Find your secret key
2. Get DAT board and parts -or- do an internal mod
3. Program the 8515 chip
4. Insert dat into IRD and have fun watching TV

Process Detail:

1. Find your secret key.

   In order for these hacks to work, you need to find the secret key which is contained in your IRD. The secret key is an 8 byte (16 hex digits) key which is unique to your IRD. There are two known ways to find your key:

   A. The safest (in terms of the ability to recover from an ECM) and most expensive way is to modify your IRD. DR7 recommends this method. You will require some soldering skills in order to do this. The process is to open your IRD, remove a tiny EEPROM which uses TSOP packaging, read the EEPROM with an EEPROM reader to get your secret key, and then write a new EEPROM and insert it into your IRD. Refer to http://www.dr7.com/chipremoval.htm for detailed information and pictures on how to accomplish this task. Since you have a copy of your TSOP, you can recover it in case of an ECM which alters your EEPROM so that it does not function. However, if you are not careful, you can harm your IRD, so this may be more risky than the next method.

B. The easiest way is to get into a special screen on your IRD and find the key. This is the path I took. For some models, the location of the key has been already found for you. Refer to http://www.dr7.com/echostar/memorymap.txt for a list of locations. To get into your memory dump, you need to press menu and then get into the diagnostics menu and once in the diagnostics menu press the following keys on your remote:

```
Push INFO
Right Arrow -> (browse)
Left Arrow <- (theme)
```

you should now be in a memory dump screen.

To navigate the screen, press Theme to get over into the left hand address window. You can enter addresses by pressing numbers on your keypad and/or the up/down arrows. Once you enter your address, you can press select to display the memory at your address. When entering your address, make sure that you pad zeros on the front of the address. For example, if you are going to FBB0 (sometimes written as $FBB0, just ignore the $), you would enter it as 0000FBB0 . The keypad only has numbers, so to enter letters, you need to press the up or down arrows to roll through the values. Once you play with this a little, you will get the hang of it.

On the top part of the screen, the dump will appear. The lines are similar to:

```
0000FBB0  00123234 45657898 A134BC54 1203EC23
0000FBC0  12434556 AB4532BC 3245BDE4 45BEDC95
  ..ETC..
```

For a 4000, the secret key to a subscribed system is located starting at FBB8. (A new, just out of the box, never exposed to the datastream 4000 has it's secret key located at 9FD0FFF4) In the above display, 0000FBB0 is the address on which the first line starts. FBB8 is the address starting at the 8th byte (counting from zero) into the line. Each byte is 2 hexadecimal numbers. So, FBB0 = 00, FBB1 = 12, FBB3 = 32, etc... FBB8 = A1. The secret key is 8 bytes (16 hex digits), so the secret key in the above example is: A134BC541203EC23

For those not familiar with hexadecimal addresses, once you get past 9, the numbers are replaced by letters as follows: 10 = A, 11 = B, 12 = C, 13 = D, 14 = E and 15 = F. For Example, FBBD would be the 13th byte on the line, or the hex value 03.

For more information, refer to E*C and look for the posts, *Where in the Memory Map did you find your keys - Part 1, Part 2 and part 3.*

2. Get a DAT board and parts -or- do an internal mod

There are 3 ways to get the 8515 to interface with the IRD.

A. DAT Board

I know of four locations where you can get these boards. They are:

- http://www.dr7.com/products.htm
- http://freeyellow.com/members6/eblocker/
- http://members.xoom.com/DualDATPlus/ddp.html
- http://www.geocities.com/TelevisionCity/6312/board.html

I make no claims to the reliability of these sites. Caveat Emptor (Buyer Beware)!

You have several options. You can purchase assembled boards. You can purchase a bare board and then purchase the parts (8515 chip, resistors, wires, etc...) from other locations. Or, they can sell you the complete kit with all parts. Choose which method you feel safest with. The more you do, the cheaper it is and the more you learn.

If you are really ambitious, you can even etch your own card. Schematics and PCB layouts for the card are available on http://www.dr7.com/echostartools.htm.

B. Internal Mod

There is another option which does not require you to purchase a DAT board at all. All you need is an 8515 chip, a 40 pin socket and some wires. This is by far the least expensive way of doing things... less than $10. However, you will need to open your IRD and do some soldering to install it.

Basically what you do is directly connect ISO Slot Connections to the 8515 via wires. You connect them as follows:

```
C1 - Pin-40 (VCC)
C2 - Pin-9 (RST)
C3 - Pin-19 (CLK)
C5 - Pin-20 (GND)
C7 - Pin-10 (I/O)
```

That is, slot C1 goes to Pin 40 on the 8515, Slot C2 to Pin 9, etc... Make sure you use a socket so you can easily remove the 8515 for program updates. Refer to E*C topics *Internal AT90S8515 mod - instructions here - Part 1 and Part 2* for more info. HeeD pioneered this innovative method.

C. Combination Method - Advanced User

The components on a dat board usually include a 4066 chip, some resistors, a socket, an 8515 and a LED. You can combine HeeD's method and use a bare DAT board and only an 8515, a socket, and a few wires. This hybrid method will provide the convenience of a DAT board, reduce the cost of the dat board, require less parts to scrounge up, and takes less time to build. Trace out the lines on the PCB and add jumpers where appropriate so that the ISO pads are connected as described above. Dat boards already have most of the connections in place. So only 2 or 3 (depending on the DAT Board) jumper wires are required.

3. Program the 8515.

In order for this hack to work, you need to insert a program into your 8515 chip. Before inserting the program, the program needs to be modified to contain your secret key. Here is what you need to do:

A. Obtain the program, xfile.hex, from http://www.dr7.com/xfile.zip

Note: There is a new version of xfile, version 1.02, which is on DR7's site. It is a little more complicated to install. Once you go through installing xfile, then you may want to go back and get version 1.02 to try. I haven't noticed anything different between the two though.

B. Edit xfile.hex using your favorite text editor and insert your secret key at the bottom of the file where the numbers, 1122334455667788 are located. The 2nd to last line looks like:

```
:0E0E7000000000000000112233445566778810
```

if your secret key is A134BC541203EC23 make the line look like:

```
:0E0E7000000000000000A134BC541203EC2310
```

The 10 which is at the end of the line is a check sum value for that line and will need to be recomputed now that you changed that line.

C. Recompute your .hex file line checksums, using hexcsum program which can be found at: http://www.dr7.com/echostar/hexcsum2.zip - refer to the readme file contained in the .zip file for more instructions.

You now have your xfile program tailored to your specific IRD. Next you need to load your program into your 8515 chip. To do that you need a programmer. There are two ways:

A. Purchase one

There are many that you can purchase. The cheapest one I have found is the ATSTK200 for $50 which is manufactured by ATMEL and can be purchased from a variety of sources including www.marshall.com. The ATSTK200 also comes with one 8515 chip included. If you get this, it would be a good idea to purchase a 40 pin ZIF socket (around $10) for easy insertion and removal of the 8515 into the programmer. The ATSTK200 does not come with a power supply. You will need a power supply with a standard 2.1mm barrel connector. It can be AC (7-12V) or DC (9-15V). I used a transformer off of an old 14.4k modem.

B. Build one

It costs about $12 in parts from Radio Shack to build one. Refer to E*C topic *Another donated AVR programmer and Schematic* for more info on building one. The home site for this do-it-yourself programmer is at http://www.qsl.net/ba1fb/. You can also go to http://www.dr7.com/echostartools.htm and find some other AVR programmers.

In any case, you need to load your program into your 8515 using a programmer. Refer to the instructions which come with your programmer, but for the do-it-yourself programmer located at http://www.qsl.net/ba1fb/, here are some tips:

a. The programmer's name is FBPRG16
b. Start FBPRG16 and set the option of 8515, no lock bits, don't program eeprom, and RC off. Then exit the program.
c. Start the program again, but pass it the name of your tailored xfile.hex which has your secret key. For example:

```
FBPRG16 MYXFILE.HEX
```

This will invoke the programmer and automatically load your tailored myxfiles.hex into your 8515. If the program reports that it has verified the chip, then everything is ok. If not, something is wrong... Your on your own here. You may be able to get help from E*C.

Take your programmed 8515 and insert it on your DAT card (or in the 40 pin socket for the internal mod). On the 8515, there is a triangle mark. This points to pin #1. On one side of the socket in which you are going to insert your 8515, there is a notch, or maybe a dot pointing to pin #1. If there is a notch, the triangle side of the chip and the notch side are on the same side. If there is a dot, then the triangle pin goes in the hole with the dot.

4. Insert your DAT into your IRD. There are two physically possible ways to insert the DAT. Make sure you insert it so that the 8 contacts on the DAT are down. If you look at your CAM, you will see that it has the same 8 contacts and they are down when you insert it. The DAT does not need a separate power source as it draws it's power from the IRD.

   If you do this and all you get is the preview channel, CD Channels, the video guide is all grey, but the channels are black, that means you don't have the right secret key, or you inserted it wrong.

That's it, enjoy the newly unleashed power of your E*.

Additional Topics

What is the difference between jethro2 and xfile?

The chip removal document makes reference to jethro2. Jethro2 is an earlier hack than xfile and was the one which was available when the chip removal document was written. Jethro2 requires that your DAT also have an ISO slot on it in which you insert your CAM into. The DAT is inserted as normal into your IRD. This way, the DAT is electronically between the IRD and the CAM. The code in jethro2 does some of the processing required itself, and passes along some of the other processing to the CAM to perform. Xfiles.hex does all of the processing and does not require the CAM.

IRC Channel

The IRC channel which discusses echostar is #dishnetwork on irc.c-plusnet.com:6667.

Sources For Components

- www.ied.pios.com - A source for 8515's and other components
- www.insight-electronics.com - A source for 8515's, ATSTK200 8515 programmer and other components
- www.marshall.com - A source for 8515's, ATSTK200 8515 programmer and other components
- www.jameco.com - A source for electronic components
- www.jdr.com - A source for electronic components
- Iguana Labs - A source for an 8515 programmer and 8515 chips
- www.xtronics.com - Pocket Programmer - A cheap eeprom programmer
- Arlabs - A popular eeprom programmer
- Arrows - A source for electronic components