Playing in a Satellite environment 1.2

Leonardo Nve Egea

lnve@s21sec.com

S21sec

La seguridad digital del futuro, hoy

ÍNDICE

1. INTRODUCTION

Satellite sniffing is something practiced long time ago. Since 2004 I have read several presentations explaining how to do it. What can we sniff? There are video feeds, audio and data connections.

Satellite communications are widespread since the mid-'60s, when in 1964 he conducted the first television transmission using this medium. The satellite's broadcast coverage is continental. Who uses this technology? Home and corporate communications with stations away from population centers (such as renewable energy stations), bases in other continents, companies with mobile units (ships or news), those who want a backup connection using this technology.

For these kinds of connections we use geostationary satellites, for our eyes they are always at the same place in the sky so we have not to move the antenna following them, this one is always pointing the same place.

2. DIGITAL VIDEO BROADCASTING (DVB)

Digital Video Broadcasting (DVB) is a suite of internationally accepted open standards for digital television. DVB standards are maintained by the DVB Project, an international industry consortium with more than 270 members, and they are published by a Joint Technical Committee (JTC) of European Telecommunications Standards Institute (ETSI), European Committee for Electrotechnical Standardization (CENELEC) and European Broadcasting Union (EBU) (Source: Wikipedia).

This suite is normally used to send video, audio or data; in Europe we use it to have satellite television, radio, Internet and other data links. DVB-S & DVB-S2 is the specification for satellite communications. These protocols are almost the same, DVB-S2 improves DVB-S. We are going to work with DVB-S.

We will use transponders (like channels in satellite comms), with the following parameters:

Frequency (C band or Ku). Ex: 12.092Ghz

Polarization. (horizontal/vertical)

Symbol Rate. Ex: 27500Kbps (basically the maximum speed allowed)

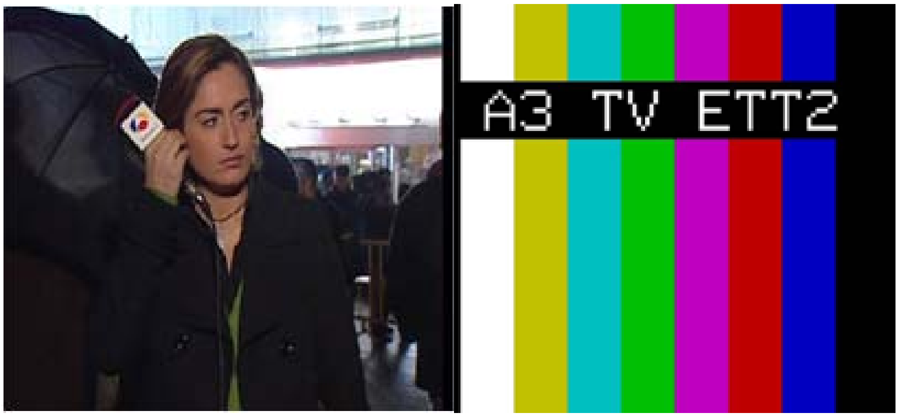
FEC. (Error control system)

Every satellite has many transponders onboard which are operating on different frequencies, in each one we can send multiple contents in little packets. Each packet have a Program ID, It permits different programs at same transponder with different components [Example BBC1 PIDs: 600 (video), 601 (English audio), 603 (subtitles), 4167 (teletext)].

Usually DVB is not encrypted, the content should provide the security.

3. DVB FEEDS

One use of the DVB protocol is to send video signals for live emissions, sports, news or digital TV. One example:



Hispasat Pre news feed (live news).

DVB video feeds are also used in military communications, and remember that DVB is not encrypted so, if they don’t encrypt it, everybody with coverage can see it, for example in June of 2002 (eight years ago) John Locker discovered how to watch NATO spy flights over the Balkans [1].

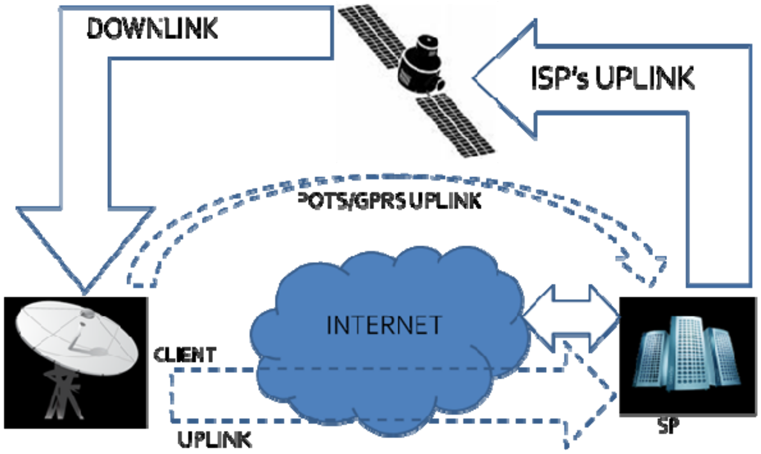
Again, in 2009, DoD admitted that insurgents intercepted the video feeds by taking advantage of an unprotected communications link between UAV and a US surveillance center [2].

Capturing feeds is old there are a lot of information about these [3].

4. IP SATELLITE LINK

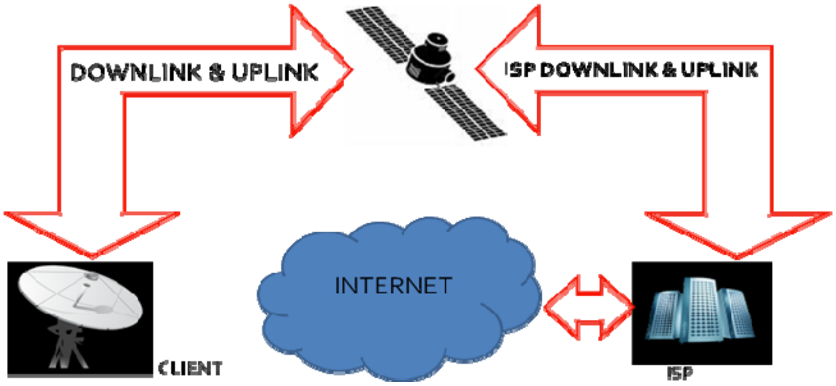
A satcom can be use to have a intranet or internet connection, there are two possible infrastructures:

Satmodem one:



The uplink is a low speed connection directed to the sat provider or through Internet tunnelized to it.

Satellite Interactive Terminal (SIT) or Astromodem one:



The uplink is through satellite (using DVB-RCS protocol).

Anyone with coverage can sniff the DVB Data packets and normally these are unencrypted, so anyone can sniff these IP packets, no matter if these are for video broadcasting, Intranet communications or Internet communication. But, only the client downlink, we can´t can sniff uplink because it is DVB-RCS and the hardware is not COTS.

The minimum hardware and software to sniff data (and feeds) we need:

- A satellite antenna with the LNB. I used one for Ka-Band.
- The data to point it
- Skystar 2 DVB Card (I used the PCI one) this one is for DVB-S for DVB-S2 we need Skystar 2 HD or Skystar HD2.
- Linux (I used Fedora and Ubuntu)
- linuxtv-dvb-apps
- DVB analyzer (dvbsnoop)
- Wireshark

You can find all of these for only 70$!!!! (ebay support this sentence ;)

5. HOW TO SNIFF

Once the antenna and the card is installed and linuxtv-dvb-apps compiled and installed, the process is:

1- Tune the DVB Card

2- Find a PID with data

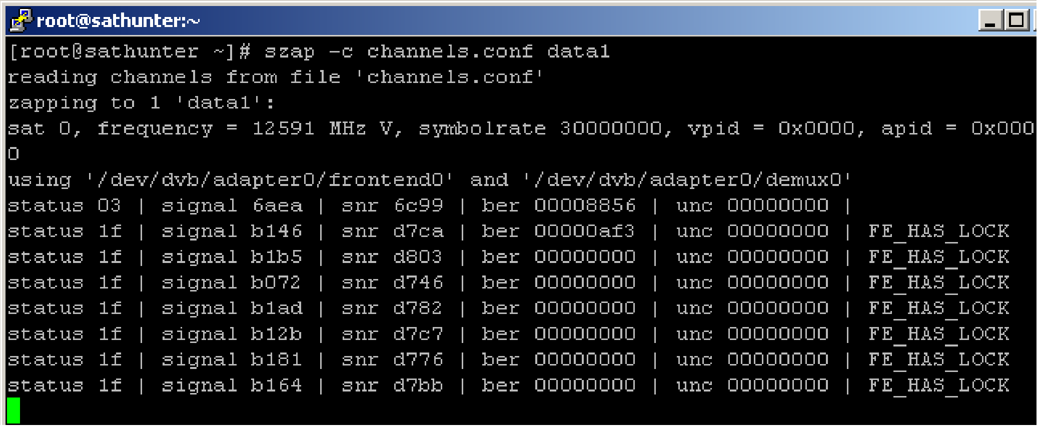
3- Create an Ethernet interface associated to that PID

Tune the DVB Card

The tool we must use is szap and we need the transponder's parameters in a configuration file. For example, for “Sirius-4 Nordic Beam":

# echo “sirius4N:12322:v:0:27500:0:0:0" >> channels.conf

And now use szap:



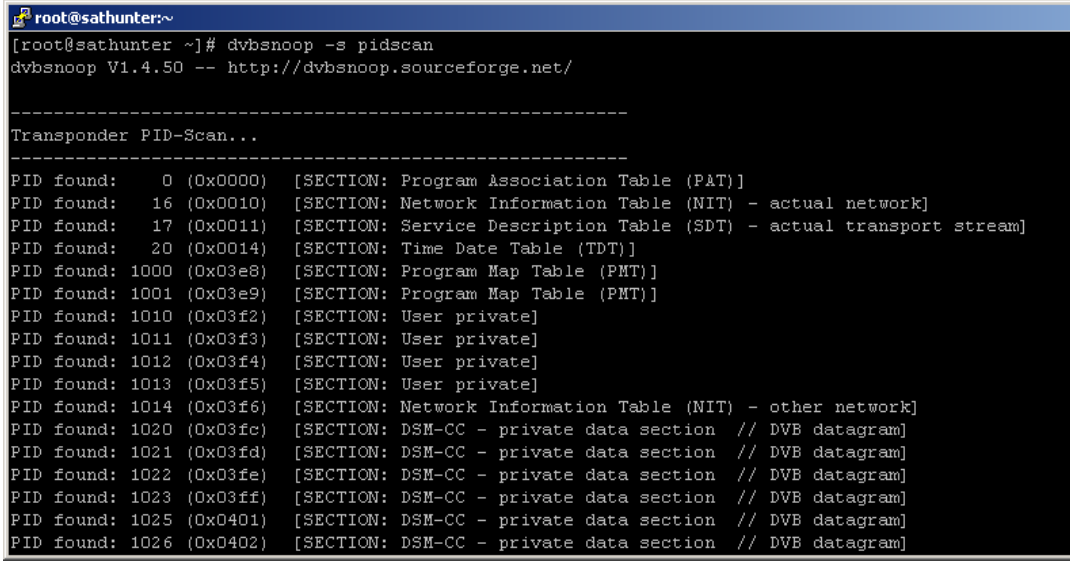
```
[root@sathunter ~]# szap -c channels.conf data1
reading channels from file 'channels.conf'
zapping to 1 'data1':
sat 0, frequency = 12591 MHz V, symbolrate 30000000, vpid = 0x0000, apid = 0x000
0
using '/dev/dvb/adapter0/frontend0' and '/dev/dvb/adapter0/demux0'
status 03 | signal 6aea | snr 6c99 | ber 00008856 | unc 00000000 |
status 1f | signal b146 | snr d7ca | ber 00000af3 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b1b5 | snr d803 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b072 | snr d746 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b1ad | snr d782 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b12b | snr d7c7 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b181 | snr d776 | ber 00000000 | unc 00000000 | FE_HAS_LOCK
status 1f | signal b164 | snr d7bb | ber 00000000 | unc 00000000 | FE_HAS_LOCK
```

The FE_HAS_LOCK means that we have tuned it correctly.

The transponder parameters can be found around Internet [4] or scanning the satellite, refer to Adam Laurie presentation [3].

Find a PID with data

dvbsnoop is a dvb stream analyzer and monitoring tool for DVB data transmission streams and related data streams. We can use it.



```
[root@sathunter ~]# dvbsnoop -s pidscan
dvbsnoop V1.4.50 -- http://dvbsnoop.sourceforge.net/

---------------------------------------------------------
Transponder PID-Scan...
---------------------------------------------------------
PID found:    0 (0x0000)  [SECTION: Program Association Table (PAT)]
PID found:   16 (0x0010)  [SECTION: Network Information Table (NIT) - actual network]
PID found:   17 (0x0011)  [SECTION: Service Description Table (SDT) - actual transport stream]
PID found:   20 (0x0014)  [SECTION: Time Date Table (TDT)]
PID found: 1000 (0x03e8)  [SECTION: Program Map Table (PMT)]
PID found: 1001 (0x03e9)  [SECTION: Program Map Table (PMT)]
PID found: 1010 (0x03f2)  [SECTION: User private]
PID found: 1011 (0x03f3)  [SECTION: User private]
PID found: 1012 (0x03f4)  [SECTION: User private]
PID found: 1013 (0x03f5)  [SECTION: User private]
PID found: 1014 (0x03f6)  [SECTION: Network Information Table (NIT) - other network]
PID found: 1020 (0x03fc)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1021 (0x03fd)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1022 (0x03fe)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1023 (0x03ff)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1025 (0x0401)  [SECTION: DSM-CC - private data section  // DVB datagram]
PID found: 1026 (0x0402)  [SECTION: DSM-CC - private data section  // DVB datagram]
```

DSM-CC – private data section // DVB datagram is a IP packet, so in this example we have IP packets over PIDs 1020,1021,1022,1023,1025 and 1026.

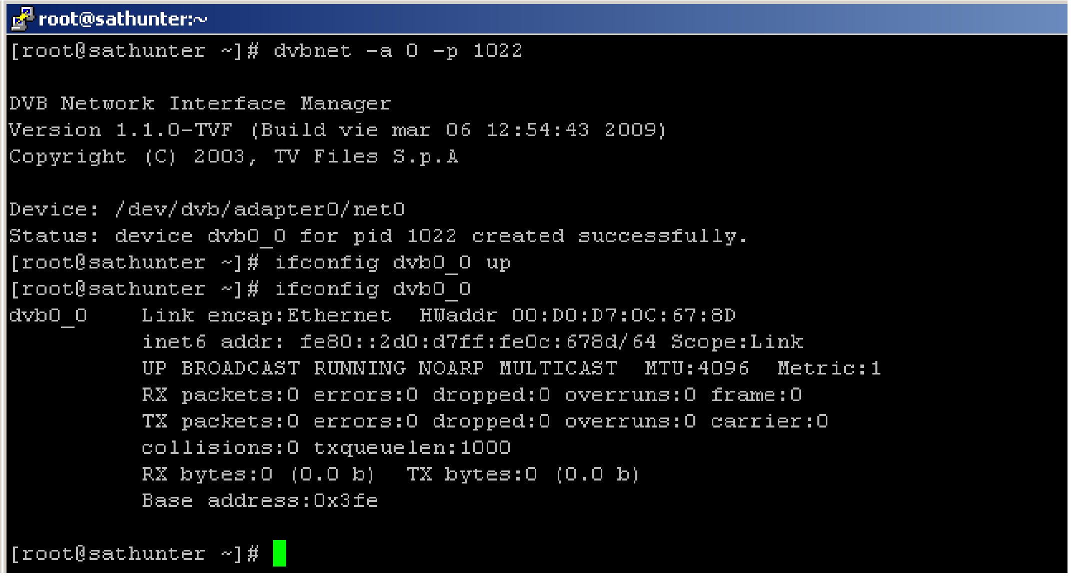
Create an Ethernet interface associated to that PID

Create an interface associated to a PID

```
#dvbnet -a <adapter number> -p <PID>
```

Activate it

```
#ifconfig dvb0_<iface number> up
```

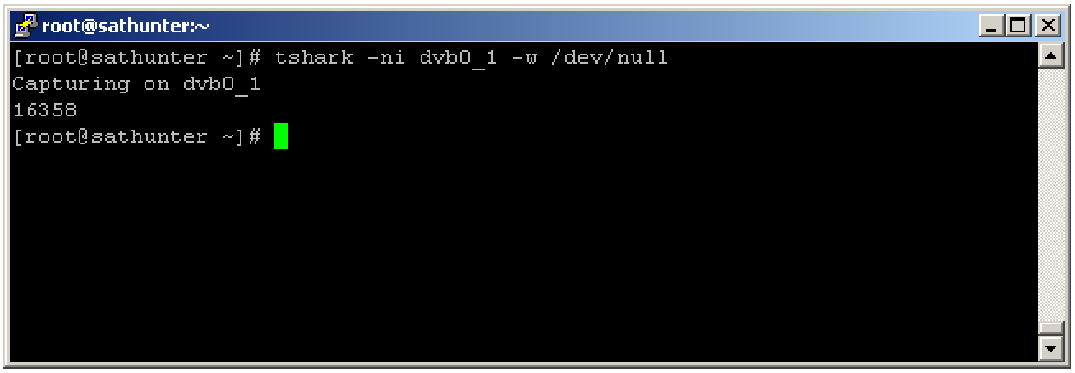


```
[root@sathunter ~]# dvbnet -a 0 -p 1022

DVB Network Interface Manager
Version 1.1.0-TVF (Build vie mar 06 12:54:43 2009)
Copyright (C) 2003, TV Files S.p.A

Device: /dev/dvb/adapter0/net0
Status: device dvb0_0 for pid 1022 created successfully.
[root@sathunter ~]# ifconfig dvb0_0 up
[root@sathunter ~]# ifconfig dvb0_0
dvb0_0    Link encap:Ethernet  HWaddr 00:D0:D7:0C:67:8D
          inet6 addr: fe80::2d0:d7ff:fe0c:678d/64 Scope:Link
          UP BROADCAST RUNNING NOARP MULTICAST  MTU:4096  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0x3fe

[root@sathunter ~]#
```

You can do it more time, then you will have dvb0_1, dvb0_2,...

Sniffing

Now, Wireshark is our friend



```
[root@sathunter ~]# tshark -ni dvb0_1 -w /dev/null
Capturing on dvb0_1
16358
[root@sathunter ~]#
```

6. ACTIVE ATTACKS

You can only sniff the downlink only so you will have only one way of the communication. With this we have a lot of possible attacks.

DNS spoofing

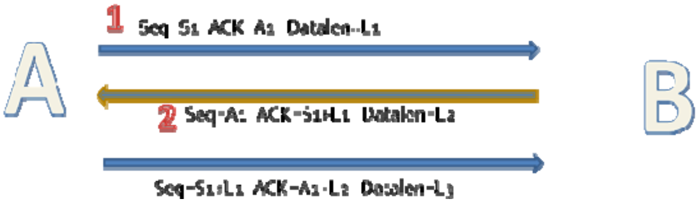
Remember what someone needs to make a successful DNS spoofing attack:

- The DNS Request ID
- The UDP Source Port
- The Source IP
- The Destination IP
- The Name/IP asking for

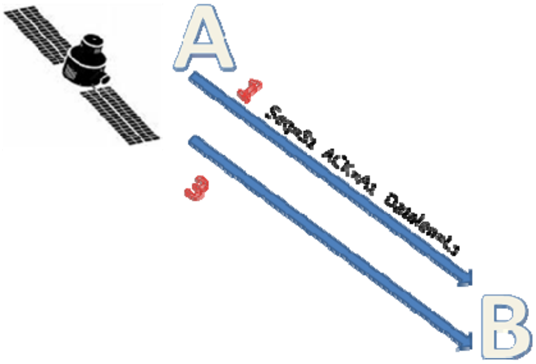
So, when we sniff a DNS request we have all these information. In some infrastructures these packets can be at the downlink of a client then we can send a false response and take control over that connection.

TCP hijacking

Reminder how TCP synchronization works:



If we want send a false packet we need now the state of the connection (Seq, Ack and Datalen of the previous packet). This graph in a satellite environment is:

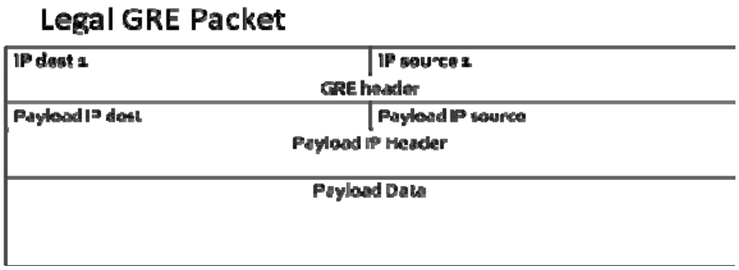


When we can sniff the 1 packet, we can send a 2 packet back to A and take the control over that TCP connection, with a thinking a little you can find a method to inject a packets back to B but you will not see the response.

Attacking GRE

This attack is based on a phenoelit’s one [5]. Generic Routing Encapsulation (GRE) is a point to point tunneling protocol which can encapsulate almost any protocol, for example, PPP protocol or IP; we are going to attack IP tunneling.

GRE is stateless; to inject a packet inside a tunnel you only need to know GRE header´s parameters, we can sniff it!

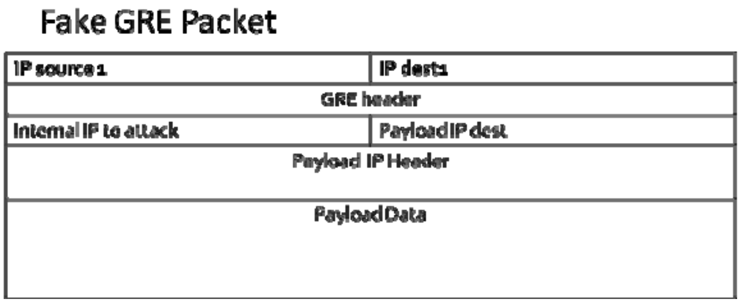

Legal GRE Packet

IP dest 1 | IP source 1
GRE header

Payload IP dest | Payload IP source
Payload IP Header

Payload Data

If we want to inject a packet inside the LAN and also get the response, we send (over Internet) a packet like:



Fake GRE Packet

IP source 1	IP dest1
GRE header	
Internal IP to attack	Payload IP dest
Payload IP Header	
Payload Data	

With this packet, if the internal host sends any response, this will be encapsulated in a GRE packet to IP dest 1 that we can sniff (remember that it is a Satellite connection's IP). IP dest 1 must be an Internet routable IP of course and you ISP must allow IP spoofing.

This technique can be extrapolated to IP over IP tunneling.

7. HOW TO SCAN THE NSA AND CANNOT BE TRACED

Now, with all this information is easy to deduce that if you can capture a satellite connection you may have an anonymous connection to the Internet.

Let´s see how. We need a Satellite connection IP and the destination MAC address, sniffing we have this information. Now, we configure our DVB interface with that hardware and IP address, and netmask /32 because we don’t want send packets using this interface (we can´t). This is going to be our downlink.

We need an uplink and it will be through Internet. We can configure our internet interface with that IP, and with some routing tricks (hardcoding MAC address of the gateway) all is done. Of course our ISP must allow IP spoofing.

Now we send packets with an IP address which is not ours and we receive with a not traceable interface because an entire continent can see that packet!

This is a too easy to exploit and a too serious issue, because anyone can do whatever he wants on Internet using this ‘vulnerability’. If a French satellite IP attacks one computer in US (for example), where is the attacker? Spain? Italy? Morocco? ...

8. CONCLUSION

Satellite communications must be considered insecure. With this technology in our sky, an anonymous connection is possible.

A lot of attacks can be made, I just talked about only few level 4 and level 3 attacks, many kinds of Denial of Service are possible. We need a thorough study on the security of the protocols encapsulated in DVB.

My research now focuses on techniques to trace illegal users, inject data directly to satellite (DVB-RCS protocol).

9. REFERENCES

[1] http://news.bbc.co.uk/2/hi/programmes/newsnight/2041754.stm

[2] http://online.wsj.com/article/SB126102247889095011.html

[3] http://www.blackhat.com/html/bh-dc-09/bh-dc-09-archives.html#Laurie

[4] http://www.fastsatfinder.com/transponders.html

[5] http://www.phenoelit-us.org/irpas/gre.html

*[Pamplona . San Sebastián . Barcelona
Madrid . Sevilla . México DF . Buenos Aires]