Weaknesses in Satellite Television Protection Schemes

or

“How I Learned to Love The Dish”

A presentation by

A

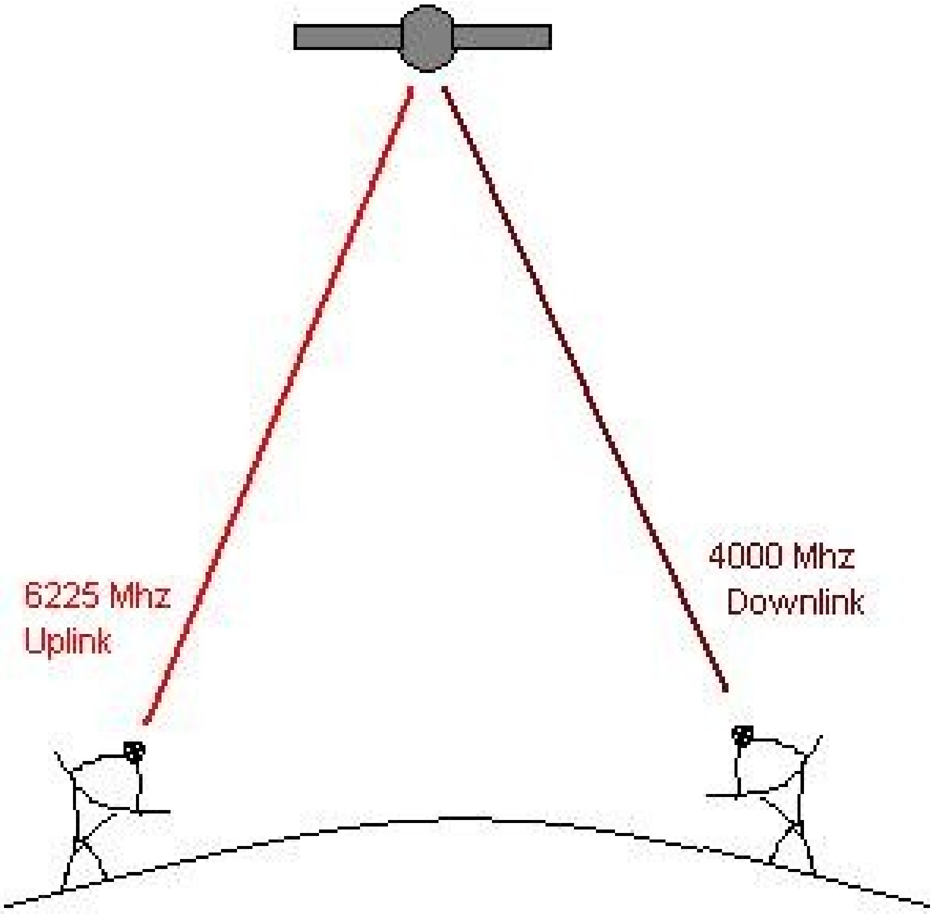
Defcon 12
July 30,2004
Las Vegas

Legal Warning!

- Many topics covered may be illegal!
- “Except as otherwise specifically provided in this chapter any person who - intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a). - http://www4.law.cornell.edu/uscode/18/2511.html
- “No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.” 47 U.S.C. §553 (a)(1)- http://www4.law.cornell.edu/uscode/47/553.html
- “Doing things that big corporations don't want you to do is illegal and immoral.” A's take on the DMCA
- Check out “DMCA, Then and Now” by Dario D. Diaz, Sunday at 11:00am for more info about the DMCA

How Do Comm Satellites Work?

- Convert the frequency of incomming signals from earth to the output frequency and point the signal back at earth



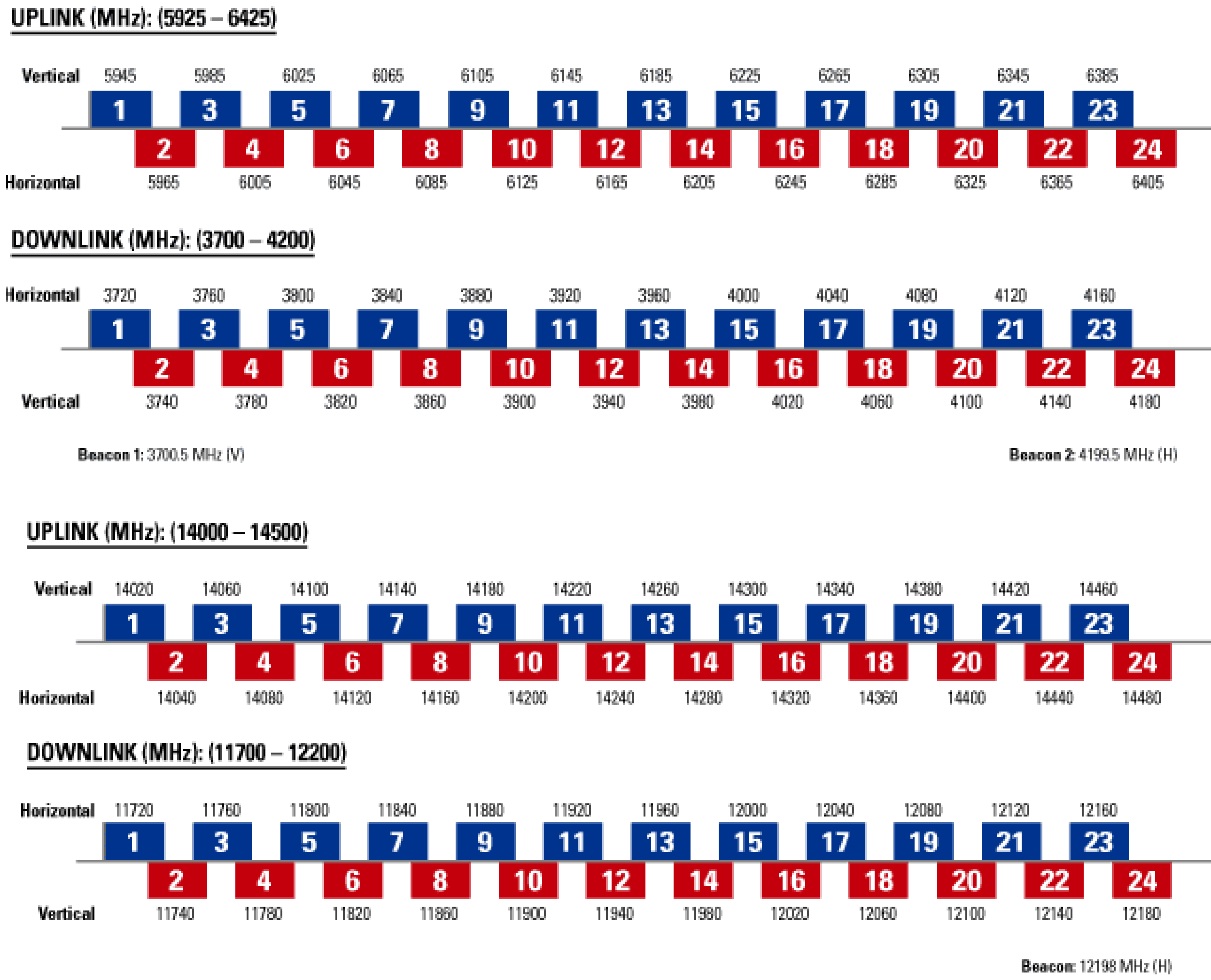
SATELLITE vIDEO tECHNOLOGY

Quazi Layered Approach

- Physical - Radio Level
  - Frequency
    - C-Band
    - Ku-Band
    - KA-Band
  - Oribital location
  - Footprint

Frequency

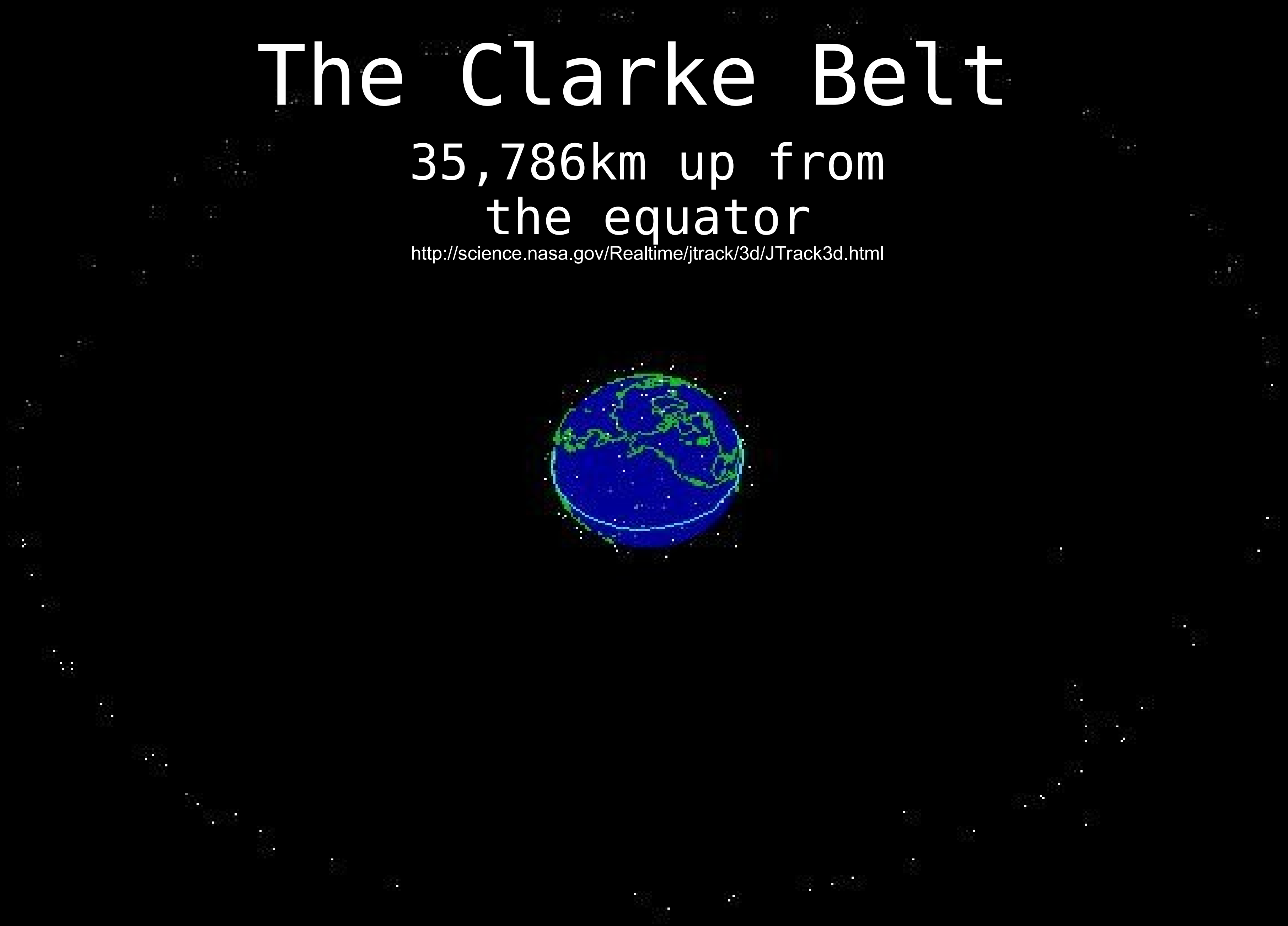
- The two major freqency bands are the c-band with a downlink of ~4Ghz and Ku-Band with a downlink of ~11Ghz


UPLINK (MHz): (5925 – 6425)
Vertical 5945 5985 6025 6065 6105 6145 6185 6225 6265 6305 6345 6385
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Horizontal 5965 6005 6045 6085 6125 6165 6205 6245 6285 6325 6365 6405
DOWNLINK (MHz): (3700 – 4200)
Horizontal 3720 3760 3800 3840 3880 3920 3960 4000 4040 4080 4120 4160
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Vertical 3740 3780 3820 3860 3900 3940 3980 4020 4060 4100 4140 4180
Beacon 1: 3700.5 MHz (V)
Beacon 2: 4199.5 MHz (H)
UPLINK (MHz): (14000 – 14500)
Vertical 14020 14060 14100 14140 14180 14220 14260 14300 14340 14380 14420 14460
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Horizontal 14040 14080 14120 14160 14200 14240 14280 14320 14360 14400 14440 14480
DOWNLINK (MHz): (11700 – 12200)
Horizontal 11720 11760 11800 11840 11880 11920 11960 12000 12040 12080 12120 12160
1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24
Vertical 11740 11780 11820 11860 11900 11940 11980 12020 12060 12100 12140 12180
Beacon: 12198 MHz (H)

The Clarke Belt

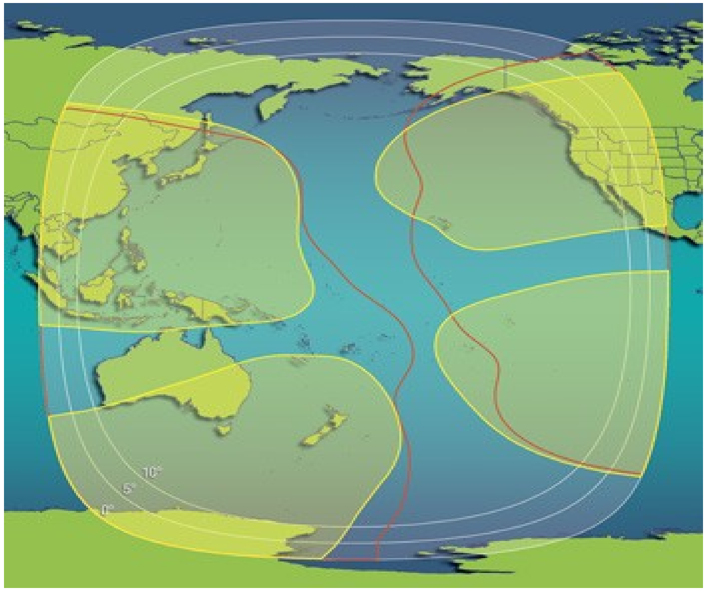
35,786km up from the equator

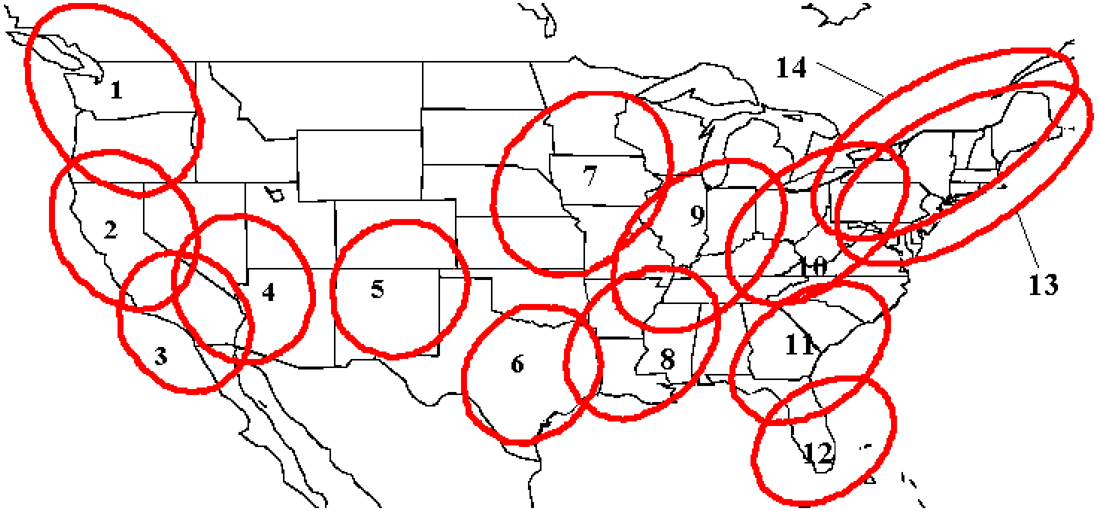
http://science.nasa.gov/Realtime/jtrack/3d/JTrack3d.html



Footprint

- The Footprint, or coverage area could be as large as a hemisphere or as small as a city.





SATELLITE vIDEO tECHNOLOGY

Quazi Layered Approach

- Encoding
  - Analogue
    - NTSC
    - PAL
  - Digital
    - BPSK
    - QPSK
    - 8Psk
    - 16QAM

SATELLITE vIDEO tECHNOLOGY

Quazi Layered Approach

- Transport System - All MPEG Based
  - DCII
    - Owned by Motorola
    - Closed standard
  - DSS
    - Only used in North America
  - DVB
    - Open Standard
    - Most used
  - ISDB
    - Only used in Japan

SATELLITE vIDEO tECHNOLOGY
Quazi Layered Approach

- Protection Systems
  - DCII
    - Mediacipher
      - Unbroken
  - DSS
    - Videogaurd
    - Has been defeated many times http://www.dssdirect.tv/history_of_dss_testing_23_ctg.htm
  - DVB
    - Open Standard so many different systems have been used

SATELLITE vIDEO tECHNOLOGY
Quazi Layered Approach

- Popular DVB Protection Systems
  - Nagravision 1 - Defeated
  - Aladin {Nagravision2} Partial Defeat
  - PowerVu - ?
  - Irdeto 1 - Defeated
  - Irdeto 2 - Partial Defeat
  - Seca 1 - Defeated
  - SECA 2 - Defeated
  - ViaAccess - defeated
  - Conax - Partial Defeat

SATELLITE vIDEO tECHNOLOGY

Quazi Layered Approach

- ContenT Layer
  - Audio
    - Musicam (MP2)
    - AC3
  - Video
    - MPEG2 - Many Variables
      - Resolution
      - Bitrate
      - Aspect Ratio
      - Sampling Rates
        - 4:2:0
        - 4:2:2
  - Data
    - TimecodE
    - Program Guide

Programing Options

- Legal
  - Dish Network (with subscription)
  - Directv (with subscription)
  - Programing from around the world
  - PBS on AMC3
  - Music on Dish Network and BeV
  - Local Stations that are FTA
  - WildFeeds
  - Backhauls
- Illegal
  - Dish network (without subscription)
  - Directv (without subscription)

Applied Use

Where are the weaknesses?

- DSS - Directv
  - History of weak protection
  - Recently turned off the Hu stream
  - P4 Rumored to be defeated
  - One strength is that they have control over the hardware that is compatable with the DSS system
  - Outside of the scope of this talk.
  - A lot of information on the web.

Applied Use

Where are the weaknesses?

- DVB-S
  - Used by Dish Network and Bell Express Vu in North America
  - “Plastic Hacking”
    - Reprograming access cards
      - Very little hardware needed
      - Software is available online
  - Emulation
    - Similar to Plastic, but a computer is used to control what data is transferred between the IRD and the access Card
  - AVR
    - HaRDWARE That goes inbetween the access card and the card slot in an attempt to control what data is transferred between the IRD and the access Card

Applied Use

Where are the weaknesses?

- DVB-S (continued)
  - DVB-S PC interface devices
    - PCI or USB devices that allow a pc with the correct software to view DVB programing.
      - Software exisits that emulates the access control Hardware
  - FIRMWARE HACKING
    - PRACTICE OF ALTERING THE FIRMWARE OF A dvb-S ird SO THAT IT INCLUDES ACCESS CONTROL HARDWARE EMULATION SOFTWARE

Applied Use

Where are the weaknesses?

DVB-S PC Interface Devices

Applied Use

Where are the weaknesses?

- VideoCipher 2
  - Analogue system still used for content delivery in North America
  - Involves modifying the descrambler module
  - Check internet for details

Applied Use

Where are the weaknesses?

- Using a Legal Subscription to get digital copies
  - While not techincaly signal theft, if you circumvent a copy protection deVICe, you are breaking US law
  - PVR devices (like TiVo) Store programing digitaly on their storage media
    - There are Many hardware and software hacks available for the different types of PVR devices
  - Digital Outputs
    - Audio
    - Firewire?
- Find Another Source
  - There is a free to air station for Every major network in the USA
  - Wildfeeds

Getting STarted

- Used but Usefull hardware can be obtained for little to no cosT
  - Ask friends and family
  - Look in your own area
    - Residential ares built in the 70s and 80s are a great source
    - industrial/commercial areas
  - Swap meets and flee markets
- No need to break the law and steal hardware, there is plenty out there that people will give you.

Getting STarted

Getting STarted

Getting STarted

Getting STarted

- Used IRDs are often very useful
  - Analogue
    - Limited Use
    - Check for videocipher 2 module
  - Digital
    - Most digital IRDs are good
    - Check out the technology they are using by looking for logos
    - Primestar IRDs are useless but the dishes are great
- Do your homework before you spend money!

Where to Get More Info

- http://www.directv.com/
- http://www.dishnetwork.com/
- http://www.expressvu.com/
- http://ekb.dbstalk.com/
- http://www.satforums.com/
- http://www.faqs.org/faqs/Satellite-TV/TVRO/
- http://www.dvb.org/
- http://www.lyngsat.com/
- http://coolstf.com/mpeg/

Thanks

- My Father for introducing me to sat back in the day!
- My Mother for saying that she will come bail me out of jail if I get arrested at defcon, But only if it is because of what I spoke on! ;)
- The guys at dc801 and 2600slc esp OldskoolS and Adrenaline for teaching me about various sat topics!
- Grifter for getting me that gig last week so that I could afford to come to vegas for defcon!
- The EFF for keeping the internet free! And if I do get arrested for speaking on this, Legal assistance, I hope.
- All the Defcon staff for putting on such a great conference year after year!
- The current US administration for reminding us how great the freEdoms we once had were.

Legal Warning!

- Many topics covered may be illegal!
- “Except as otherwise specifically provided in this chapter any person who - intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication.” 18 U.S.C. § 2511(1)(a). - http://www4.law.cornell.edu/uscode/18/2511.html
- “No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law.” 47 U.S.C. §553 (a)(1)- http://www4.law.cornell.edu/uscode/47/553.html
- “Doing things that big corporations don't want you to do is illegal and immoral.” A's take on the DMCA
- Check out “DMCA, Then and Now” by Dario D. Diaz, Sunday at 11:00am for more info about the DMCA

Weaknesses in Satellite Television Protection Schemes

or

“How I Learned to Love The Dish”

A presentation by

A

Defcon 12
July 30,2004
Las Vegas