



DOCSIS: Insecure By Design

Free Anonymous Internet Using Modified Cable Modems

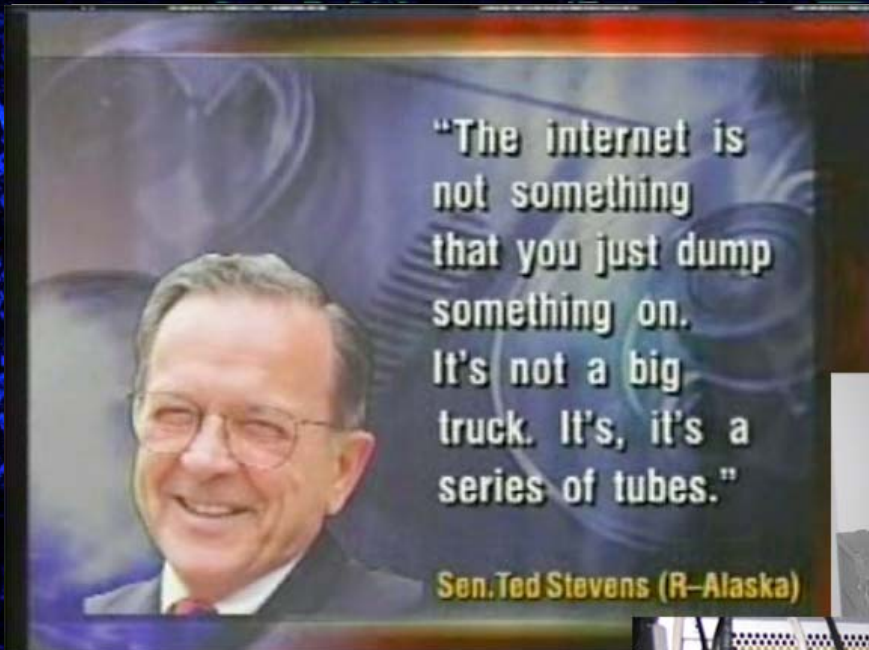
http://www.soldierx.com/defcon16speech/docsis_insecure_by_design-blake_durandal.ppt

Blake Self
bitemytaco
DevDelay



Sponsored by SOLDIERX - <http://www.soldierx.com>

Humor



Maybe Ted Stevens has a series of hacked modems and a drop amp at his place. Could this be the reason he thinks that the internet is a series of tubes?





Background

- Personal
 - Conducted SIPRNET Administration and Red Team Penetration Testing for the USMC.
 - I currently do research for SERC (Software Engineering Research Center), an NSF Industry/University Cooperative Research Center.
- Speech
 - A much shorter version of this presentation was given at the Spring 2008 SERC Showcase.
 - Various people (such as Durandal from SOLDIERX) have used the methods in this Defcon presentation to put and keep modems online.





What This Speech Will Cover

- Requirements (for our examples)
- Network Overview
- Anonymous Access
 - Gaining service with a non provisioned MAC address
- Cloning a HFC MAC linked to an ISP account
- How Anonymous You Really Are
 - How close ISPs can pinpoint your location as well as techniques to catch people abusing/stealing service
- Firmware Overview
- Hardware and Security
 - Specifications, firmware disassembly, current and future security solutions





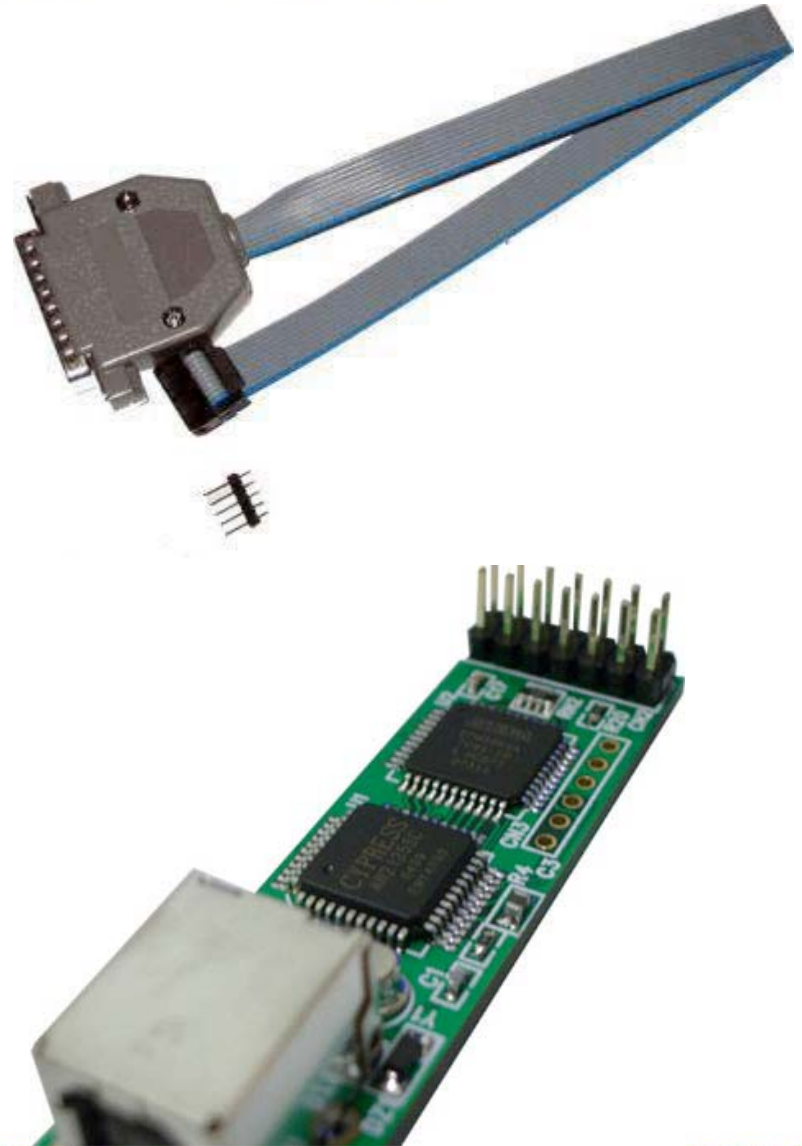
Requirements

- What do you need for our examples?
 - Coaxial connection to the cable company
 - JTAG cable
 - MIPS EJTAG (Enhanced Joint Test Action Group)
 - - USB Cypress or FTDI based JTAG (Fast)
 - - Parallel buffered/unbuffered JTAG (Slow)
 - SB5100/5101 cable modem
 - Other modems can be modified
 - Soldering Skills + 10 pin header
 - YouTube is an excellent resource for soldering reference
 - Applications for flashing the firmware onto a modem
 - Parallel - Schwartze Katze by tcniso.com
 - USB - USB JTAG from usbjtag.com



Requirements In Depth

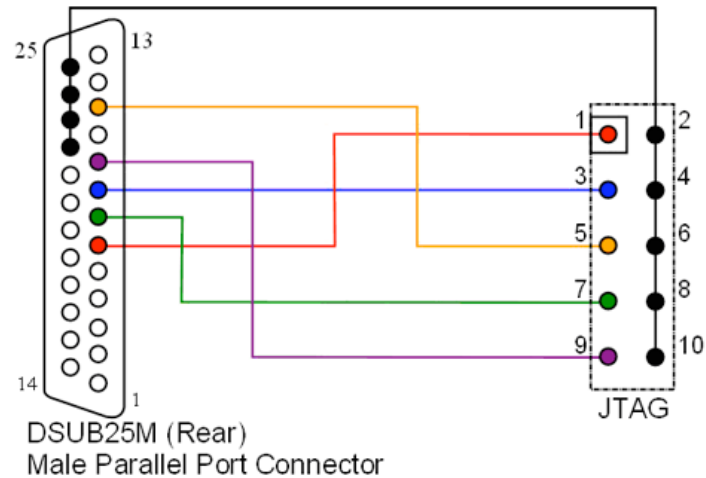
- Cable connection
- EJTAG Cable
 - Easy to make
 - Available online
- USBJtag
 - Difficult to make
 - Really fast



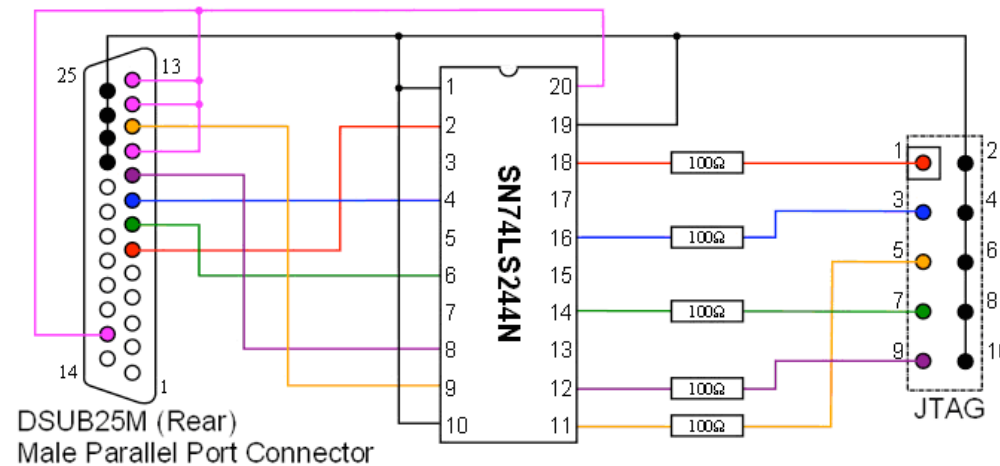
Requirements In Depth (cont'd)

MIPS EJTAG Cable Schematics

Unbuffered:

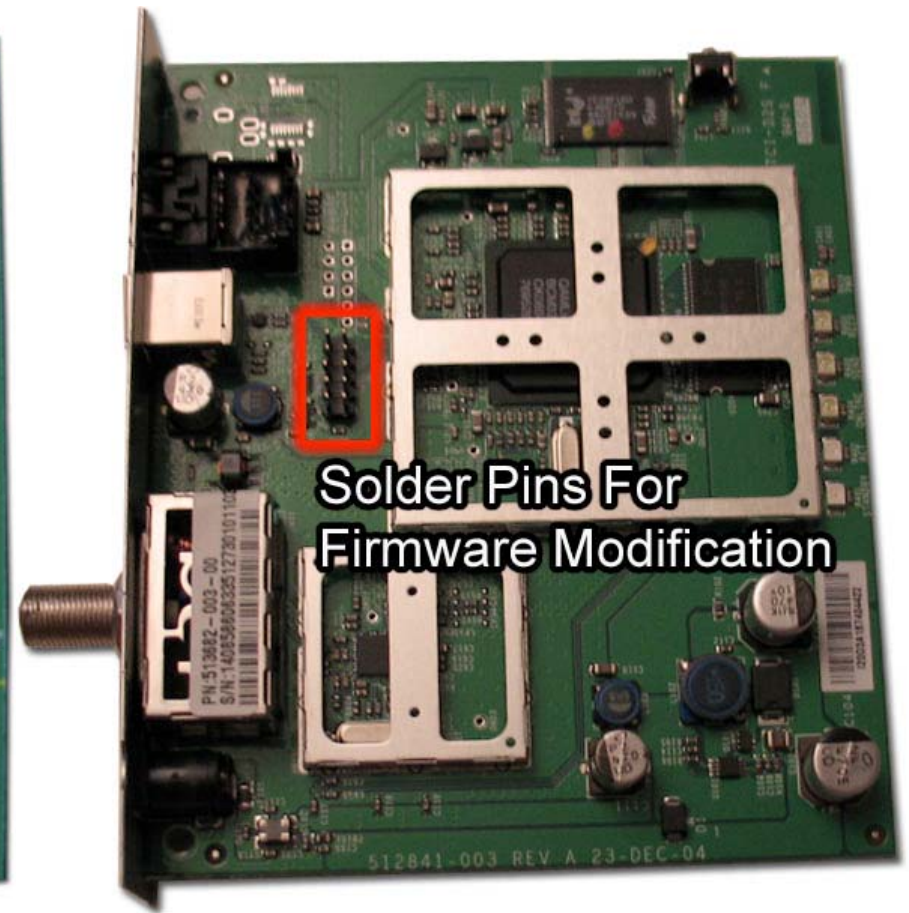


Buffered:



Requirements In Depth (cont'd)

- Modify the SB5100/5101 or buy a Premod
 - (available from sites like www.sbhacker.net)



Requirements In Depth (cont'd)

- Program the SB5100/5101 using Schwarze Katze/USB JTAG

```
USB JTAG Version 0.24 http://www.usbjtag.com Testing:SB510X User:devDe
File Tools SB5100 Testing Help
D F B
-detect
IDCODE 0334817F
Broadcom BCM3348
IMPCODE 800908
DMA supported
Found Address= 9fc00000 Intel 28F160C3B
-getram 9fc00000 200000
HFC Mac Address: 00:0E:XX:XX:XX:XX
Ethernet Address:00:0E:XX:XX:XX:XX
CPE USB MAC Address:00:0E:XX:XX:XX:XX
Serial: 118003XXXXXXXXXXXX40000
Factory MIB: on
Output Ram Boot cfg Image0 Image1 log
-detect
-getram 9fc00000 200000
Ready Jtag Connected DEBUG OFF
```

```
Schwarze Katze (Build 128) by the TCNISO Team
Console Flash Memory Scripts SB5100 SB4xxx
Black Cat Console
Jtag Engine initiated Successfully
BlackCat plugin services started.....
0: NULL plugin created
loading plugins from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\
2:8192: [EJTAG] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\ejtag.dll
3:655360: [FlashPlugin] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\flashpi.dll
4:16384: [PCPARPORT] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\pcparport_win32.dll
5:4096: [JTAG] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\pptapi.dll
Link Success /BlackCat/EJTAG:1<->/BlackCat/JTAG
Link Success /BlackCat/JTAG:1<->/BlackCat/PCPARPORT
Link Success /BlackCat/FlashPlugin:1<->/BlackCat/MEMORY
6 plugins loaded
0xffffffff = -1
Manufacturer: broadcom
Part: bcm3345
Application started..
```



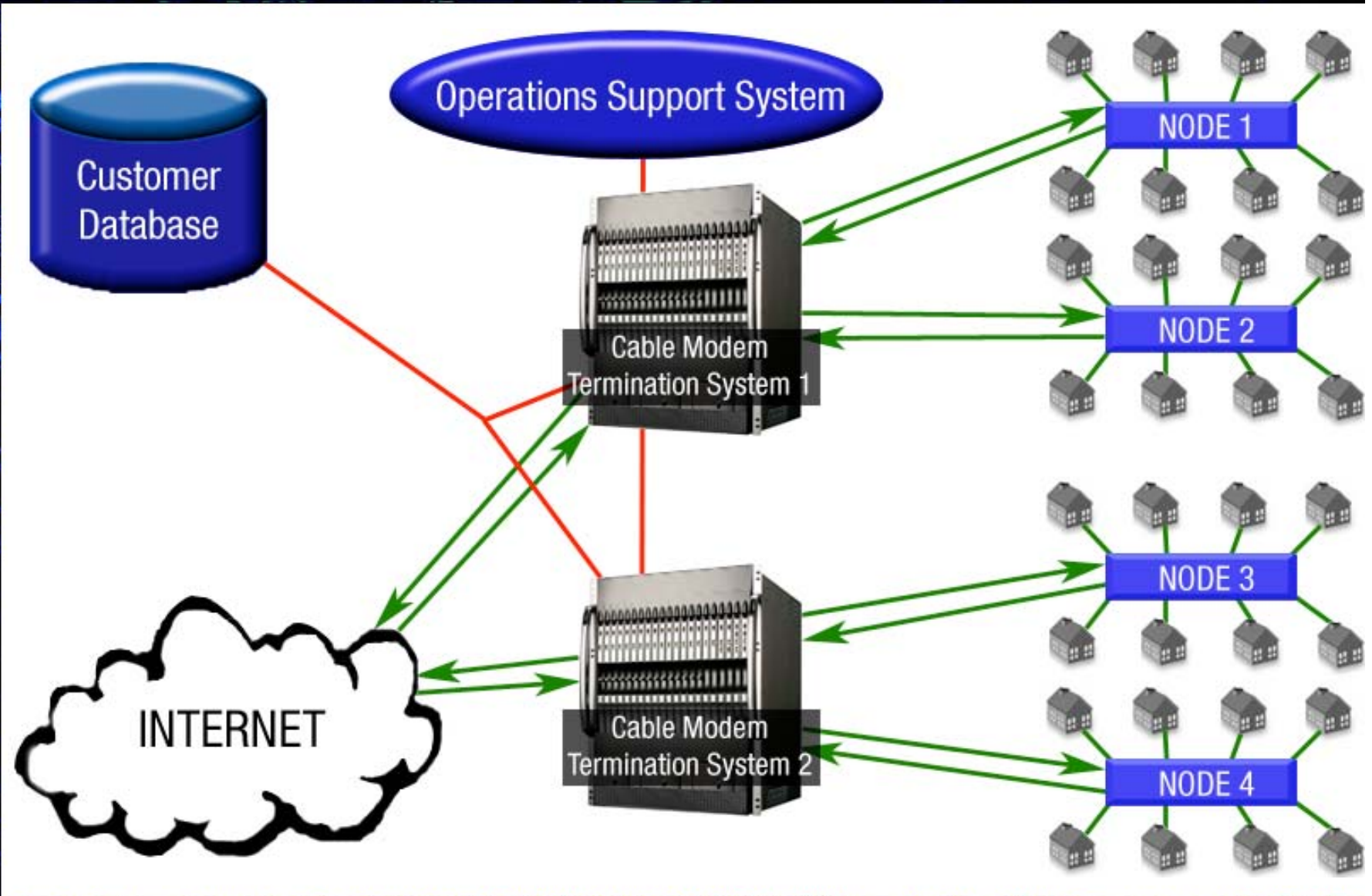


Modified Firmware

- Features of Sigma X2/Haxorware:
 - Enable factory mode
 - Change all associated MAC Addresses
 - Change serial number
 - Disable ISP firmware upgrade
 - Disable reboots
 - Force network access (ignore unauthorized messages)
 - Disable & Set ISP filters (ports blocked at modem level)
 - Specify config filename and TFTP server IP address
 - Force config file from ISP, local TFTP or uploaded flash memory.
 - Get & Set SNMP OID values and Factory mode OID values
 - Broadcom CLI access through serial connection or telnet
 - Full shell access to VxWorks/eCos (unix-like OS)
 - Upload, flash and upgrade firmware



Cable Network Overview





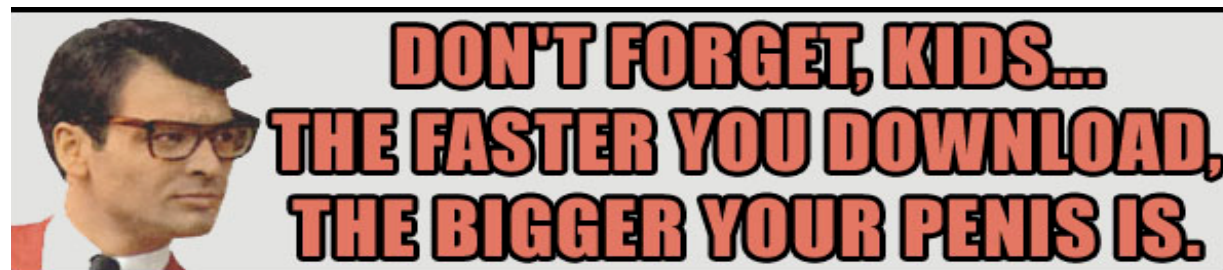
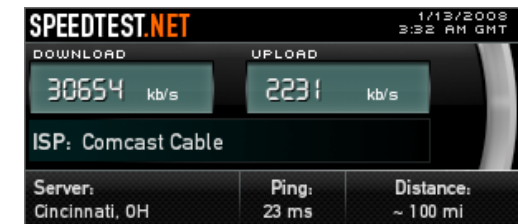
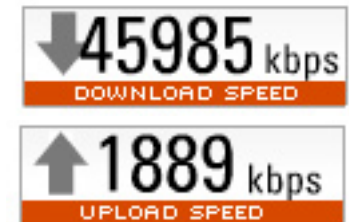
Anonymous Internet Access

- For our example of anonymous internet access, we will be using Comcast.
- Why Comcast?
 - According to Alex Goldman's research on [isp-planet.com](http://www.isp-planet.com), as of the fourth quarter of 2007 - Comcast is the second most used ISP in the United States, and the number one used ISP using DOCSIS. (<http://www.isp-planet.com/research/rankings/usa.html>)
- If you hook a non-provisioned modem into the Comcast network, the only page that comes up is a Comcast page asking you to sign up for service.
- You can generally connect inbound to the computer that is hooked up to the modem but you cannot connect outbound from the computer.
- Changing the DNS servers gives you the ability to connect out (some of the time). Forcing a config file at this point is all that is necessary to increase the service class for a non provisioned modem.
- Disabling SNMP filters in the console removes port blocking at the modem level and allows a user to poll other modems for useful information on ISP that allow SNMP polling through the entire HFC network:
 - `cd /snmp`
 - `filters off`
 - `type` and return yes for changes to take immediate effect



Faster Speeds

- Anonymous access is good, but faster anonymous access is better.
- In order to increase speeds, you can force a faster configuration file from the ISP, served locally or from configs stored in flash memory.
- You may specify a TFTP server, Comcast uses static instead of dynamic configs and each server has the same configuration files.
- Some example configuration files that Comcast uses:
 - DOCSIS 1.0
 - d10_m_sb5100_speedtierextreme2_c05.cm = 16/2
 - d10_m_sb5100_showcase_c01.cm = 55/5
 - d10_m_na_c05.cm = 0/0 (unrestricted)
 - DOCSIS 1.1
 - d11_m_sb5100_speedtierextreme2_c05.cm = 16/2
 - d11_m_sb5100_showcase_c01.cm = 55/5
 - d11_m_na_c05.cm = 0/0 (unrestricted)



Changing the Configuration File

- Navigate to <http://192.168.100.1:1337>
- The examples pictures are from Sigma X2 on the SB5100

http://192.168.100.1:1337/

es

Main - SIGMA - WebShell - Advanced

SIGMA-X2

Disable firmware updates:	Enabled	Change
Factory Mode:	Disabled	Change
Configuration page changeable:	Enabled	Change
Reboot disabler:	Enabled	Change
Force network access:	Enabled	Change

Config Changer

TFTP IP: Config name:

Telnet Daemon

Embedded Telnet Server: Enabled

Login: Password:

Hardware Changer

MAC: Serial:

Firmware Changer

Filename: IP:

SIGMA-X2 build 142 - Developed by [TCNISO](#), 2008

You can either specify a file that exists on ISP server, local server or upload and serve a file from flash memory. Forcing you own custom config file is not generally possible.

Main - SIGMA - WebShell - Advanced

SIGMA-X2

TFTP config file: [basic.cfg](#)

Firmware name reported:

SNMP listen Port:

Auto boot config file: Enabled

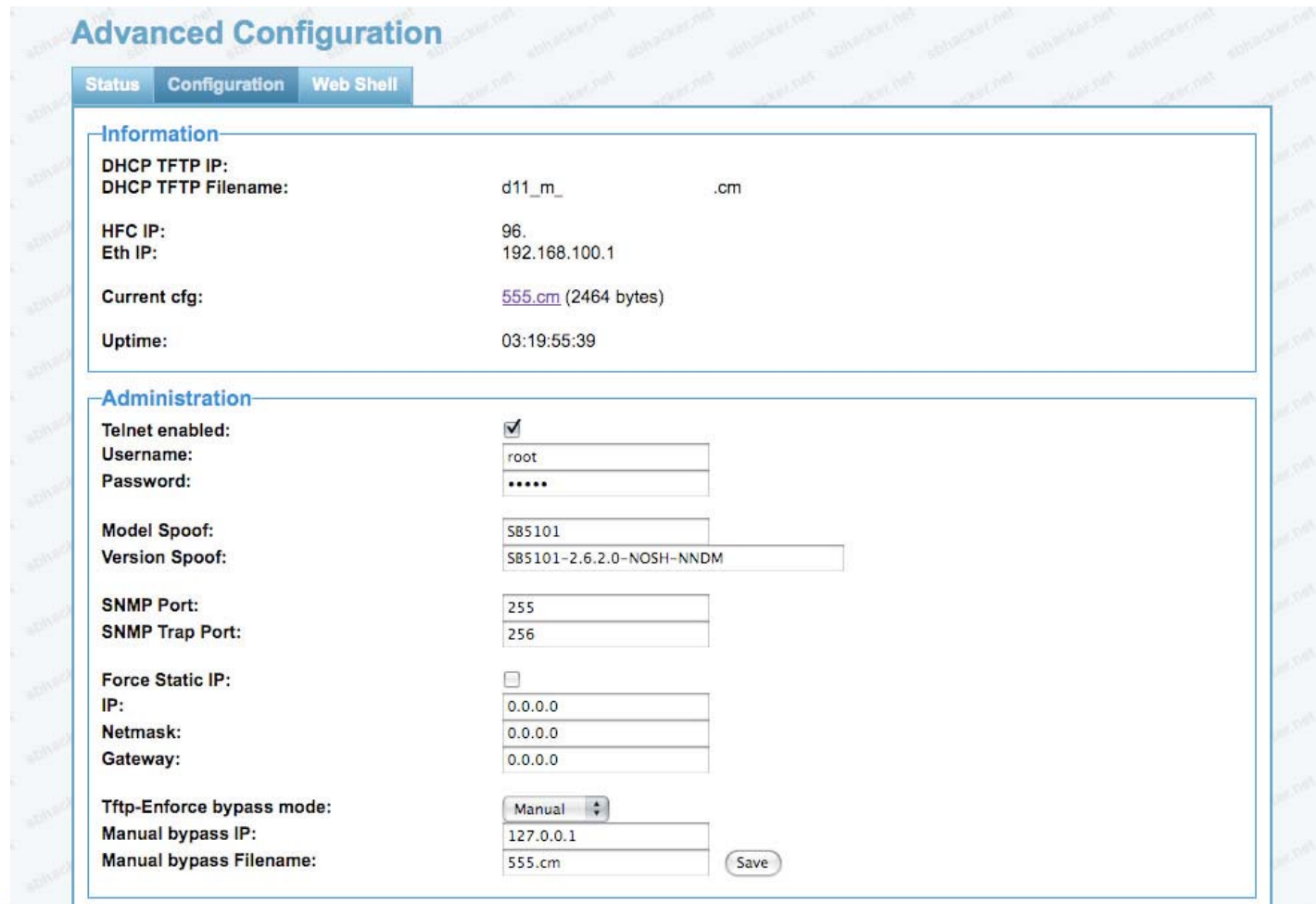
Config Uploader

Current config stored: hacked.cfg (1010 bytes)



Changing the Configuration File

- Navigate to <http://192.168.100.1:1337>
- The example is from Haxorware on the SB5101



The screenshot shows the 'Advanced Configuration' web interface. It has three tabs: 'Status', 'Configuration', and 'Web Shell'. The 'Configuration' tab is active. The interface is divided into two main sections: 'Information' and 'Administration'.

Information Section:

- DHCP TFTP IP: (empty)
- DHCP TFTP Filename: d11_m_ .cm
- HFC IP: 96.
- Eth IP: 192.168.100.1
- Current cfg: [555.cm](#) (2464 bytes)
- Uptime: 03:19:55:39

Administration Section:

- Telnet enabled:
- Username: root
- Password: *****
- Model Spoof: SB5101
- Version Spoof: SB5101-2.6.2.0-NOSH-NNDM
- SNMP Port: 255
- SNMP Trap Port: 256
- Force Static IP:
- IP: 0.0.0.0
- Netmask: 0.0.0.0
- Gateway: 0.0.0.0
- Tftp-Enforce bypass mode: Manual
- Manual bypass IP: 127.0.0.1
- Manual bypass Filename: 555.cm

A 'Save' button is located at the bottom right of the Administration section.



Techniques for Remaining Anonymous

- Disable the SNMP daemon after registration
 - `cd /non-vol/snmp`
 - `diag_disable_post_reg true`
 - `write`
- Hide the Modem's HFC IP Address (You cannot hide CPE IP addresses)
 - `cd /non-vol/snmp`
 - `hide_ipstack_ifentries true`
 - `write`
- Hide Reported Software Version (system OID)
 - `cd /snmp`
 - `delete sysDescr`
 - `write`
- These and other settings can be hard coded into or set by firmware for a desired result submitted to the CMTS.





Field Results

- Various anonymous cable modem hackers have reported high success rates with zero signs of detection
 - Durandal has a machine on a business configuration that has been seeding torrents steadily for over a year
 - Many people have as many as 8 or more modems running concurrently
 - In all of these scenarios, the individuals are paying for service. They are simply splicing their line to add additional modems





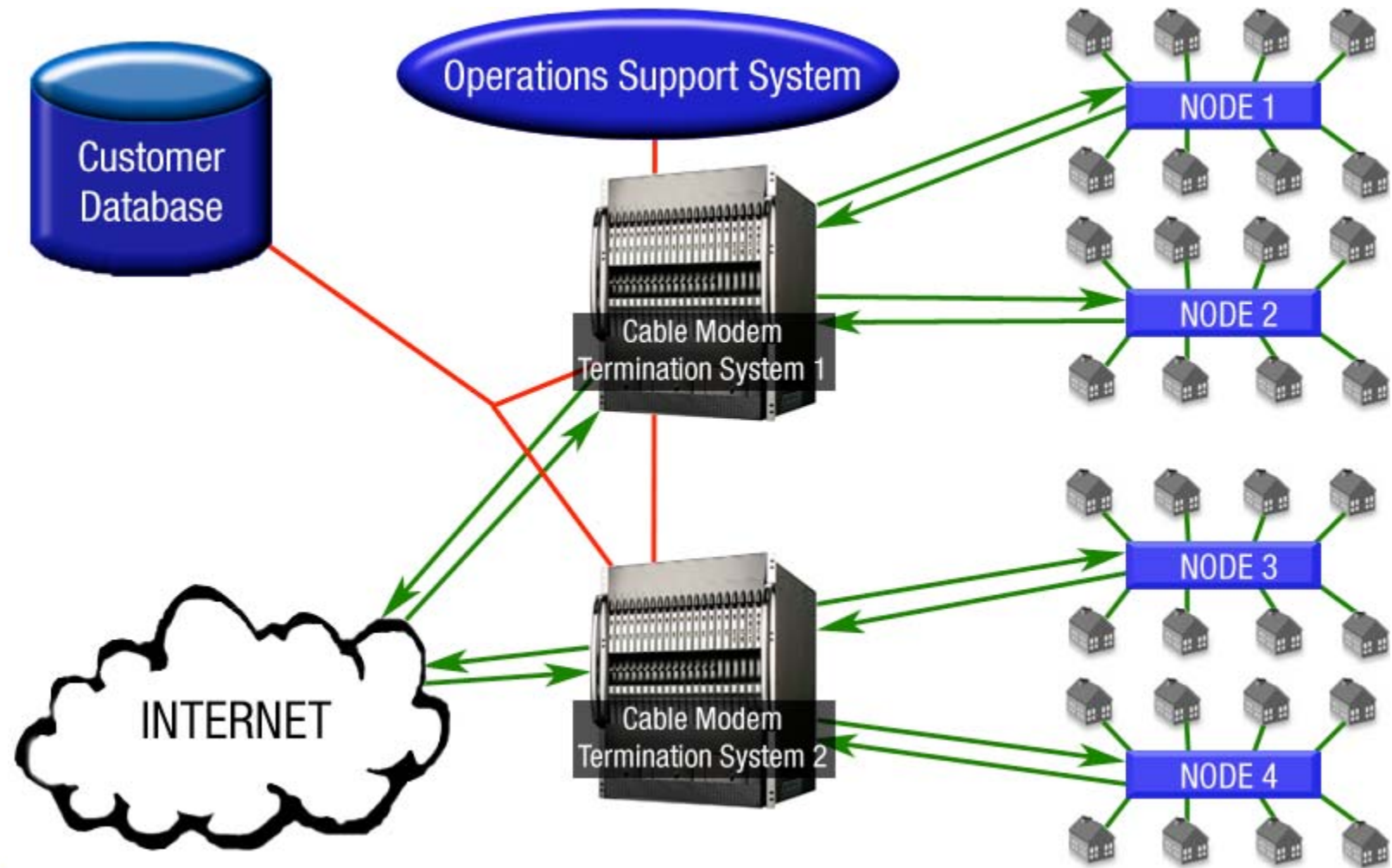
Cloning

- Basic Cloning involves specifying a provisioned HFC MAC address in order to get a class of service assigned to the MAC.
- Due to the broadcast nature of the network, you must use a HFC MAC address that is on a CMTS other than yours.
- This method allows you to then force any config file, but it associates your modem with someone else's account.



Cloning (Cont'd)

- The CMTS (Cable Modem Termination System) does not prevent the cloning of a MAC address from Node 3 to Node 1.





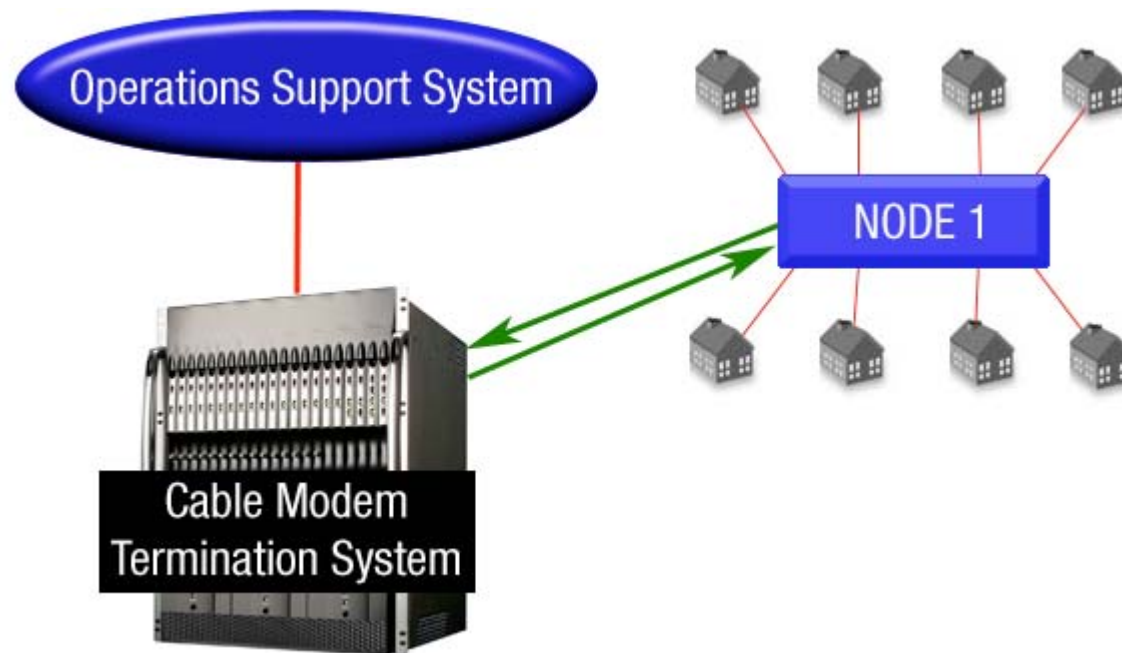
Obtaining Information for Cloning

- MAC addresses are traded privately on forums and IRC.
- Finding HFC MAC addresses on your node can be found by sniffing the DHCP packets that are sent from the CMTS to all modems.
- Wireshark can filter out broadcasted packets to easily assemble a list of HFC MAC's on a user's node.
- SNMP scanning the preferred method for obtaining HFC MAC's for multiple nodes with ISP's that allow it.
- Exact clones can be used by obtaining all identifying information from the modem including the HFC MAC, ETHER MAC, USB MAC, Serial, and all BPI+ Certificates.
- Exact clones are usually non-provisioned modems - the collective information simply allows the modem to pass initial authentication checks and gain network access. A faster config file would be forced to bypass the ISP assigned non-provisioned config that has a limited class of service.



How Anonymous Are You?

- The Operations Support System is normally unable to pinpoint a modem to an exact location due to the design of the hybrid fiber coax cable network.
- Usually, detection only goes as far as the node where the modem in question is located.





How Anonymous Are You? (cont'd)

- Some ISPs poll for poor signal levels.
 - Technicians would disconnect each line to find out which line is causing the signal loss.
 - You can prevent this by using an amp if your signal strength is too low. We personally like the BDA-S1 Broadband Drop Amp from Motorola.
 - The downstream should be between -15 and +15 dBmV and the upstream should be between -35 to -50 (Upstream is always negative).
- Many ISPs perform routine audits on lines that should not be connected in order to verify that they are not.
 - Most ISPs use colored tags to identify the account and service.
- Some ISP have adopted & implemented (at a cost) ROC
 - Regional Operating Centers: independently networked to each CMTS that collectively maintains a customer MAC database.





Throwing Up a Red Flag

- Not using previously discussed techniques for remaining anonymous.
- Excessive torrenting.
- FTP/Web Servers hosting Warez/Porn (or other types of heavily used services).
- Using cloned MAC addresses without discretion, committing fraud crimes etc.
- Splitting the connection too many times will weaken the signal and can cause techs to come out to check it.





Precautions to Take

- Do not transfer personal information over unencrypted connections....EVER!
- Keep an eye out for the party van (or cable technicians)
- Pay for service on one modem and have another one hooked up that is modified for anonymous internet
- Be careful with which HFC MAC addresses you clone
- Remove line identifiers to assist in anonymity (especially at apartment complexes)



Response From the SERC Showcase

- Anonymous Internet was not nearly as much of a concern as BPI/BPI+ in DOCSIS 1/1.1/2.0
 - The maximum privacy that is offered via encryption is 56bit DES.





Enter bitemytaco

The good, the bad and the excellent...

FIRMWARE OVERVIEW

```
jal    BcmAllocInit      move   $a1, $0           move   $a0, $v0         addiu  $sp, -0x10
nop                                         jal    memset           jal    dpadd           sw     $ra, 0x10+var_10($sp)
bnez   $v0, loc_8002979C  li     $a2, 0x78        move   $a1, $v1        jal    BcmFree
li     $v1, 0xFFFFFFFF   jal    sub_80029E64     b      loc_800293E8     li     $a1, 0xFFFFFFFF
la     $a0, dword_804C1260  nop                                         nop
```





Diagnostic Factory Firmware

Pros

- You may already have it, referred to as shelled firmware.
- Every bit as functional as hacked firmware if you know what you're doing.
- Stock firmware straight from the manufacturer.

Cons

- RTFM.
- May take some trial and error to configure for proper use.
- No GUI.





Sigma X2

Pros

- Works without too much trouble.
- Fairly decent list of firmware features.
- Based on altered versions of factory shelled firmware.

Cons

- Created by DerEngel's hired group of coders.
- You install a license to use it.
- Costs money
- Beware of possible backdoors and rebooting issues.





SB5100 MoD & SB5101 Haxorware

Pros

- Free alternatives to sigma (no licenses).
- Improved features for a changing world.
- Based directly off factory shelled firmwares.
- Stable!

Cons

- Still some bugs.
- So many features it can become confusing.





Haxorware & Proof of the Future

Hands down the most advanced firmware available for SB5101 or BCM3449 chipsets

Built from ECOS based SB5101 factory diagnostic firmware

Features of current build, beta 0.9.2:

- TFTP-enforce bypass
- Local TFTP: serve TFTP over the ethernet interface
- Autoserv & Client (upload and host configs from flash memory)
- Set static HFC IP, subnet and gateway
- Spoof vendor, model, version & change SNMP ports used
- Console webshell & telnetd with diagnostic output
- Webif authentication
- Firmware upgrade via webif
- Backup and restore complete flash & non-vol settings
- Skipped modem config checks





Enter devDelay

Make it simple, but not stupid....

HARDWARE & SECURITY





Abstract

- Presenter Background
- Objectives
- Cable modem hardware
- Trust Meets Encryption & Authentication
- Why and who is at fault?
- Perspectives
- Firmware Reversing
- The Future
- Problems & Solutions





Background Information

- Why should you listen to me?
- IT & IS Consultant
- Actively pursuing CISSP certification
- Active member & admin of SBH
- Assisted Rajkohaxor (The Serbian Prodigy) on development design, debugging and testing of Haxorware with financial backing from Bitemytaco of SBH





Objectives for Honest Discussions

Provide an open forum for users, hackers, professionals & law enforcement:

- Hacked modems exist, warrantless wiretaps legal?
- Used for anonymous, free or faster internet
- Virtually undetectable / Could be used for evil

Understand & evaluate Docsis networks as a viable telecommunications protocol:

- The nature of Docsis HFC networks & hardware
- Security flaws & Best practices
- Improper use and abuse by all parties
- How can we make it better & Can We Coexist?





What is a Docsis Cable Modem?

- Just another computer
 - Chipset: Broadcom BCM3348/BCM3349
 - Processor: 200MHz MIPS-32 core with MMU
 - RAM: 16-bit SDRAM bus with 8MB RAM (upgradeable)
 - Storage: 2MB Flash ROM
 - OS: RTOS (Real Time Operating System)
 - WindRiver's VxWorks
 - ECOS (Embedded Configurable operating system)
 - QNX (Microkernels are good)
 - Unix-like UI
 - X86 or MIPS flavors





Trust: Encryption & Authentication

BPI: Baseline Privacy Interface

- Methods for encrypting traffic between the cable modem and the CMTS at triple 56bit DES with 768/1024 bit key modulus

BPI+: Baseline Privacy Interface Plus

- Implemented in Docsis 1.1 Specs (Backwards compatible)
- Introduces X.509 v3 (RSA 1024bit) digital certificates & key pairs
- Authentication based on certificate hardware identity; validated when modem registers with a CMTS

Certificates, Keys & The 'trust ring'

- Stored in the non-vol settings of a modems firmware
- Contains: Public, Private, and Root Keys, CM & CA Certificates
- DOCSIS Root CA signs manufacturer CA intermediate certificate, manufacturer signs CM certificate. CMTS parses and verifies CM certificate, an identity based on HFC MAC





Why hacking modems is possible?

- **Hardware (blame the manufacturers)**
 - Absolutely no physical security
 - Common hardware components
- **Software (blame the developers)**
 - Initial hacks involved netboot/etherboot, enabling built in factory mode (implemented by the OS and enabled by setting a SNMP OID) or using stock (noisy) bootloaders.
 - Diagnostic firmware does the job, but better firmware with custom features is easy to make
- **ISP (blame the administrators)**
 - Improperly configured CMTS
 - Security flaws in CMTS IOS
 - Costs & Convenience





Perspectives: Role Playing

•Customers

- Protect and respect our privacy
- Provide us with quality but NOT limited service
- Stop charging more when you've failed...

•Hackers

- You might expect this
- We demand anonymous internet access (why not?)
- You make it so easy, it seems like it's on purpose
- Not my fault the network is not configured properly
- ...You WILL still have a problem

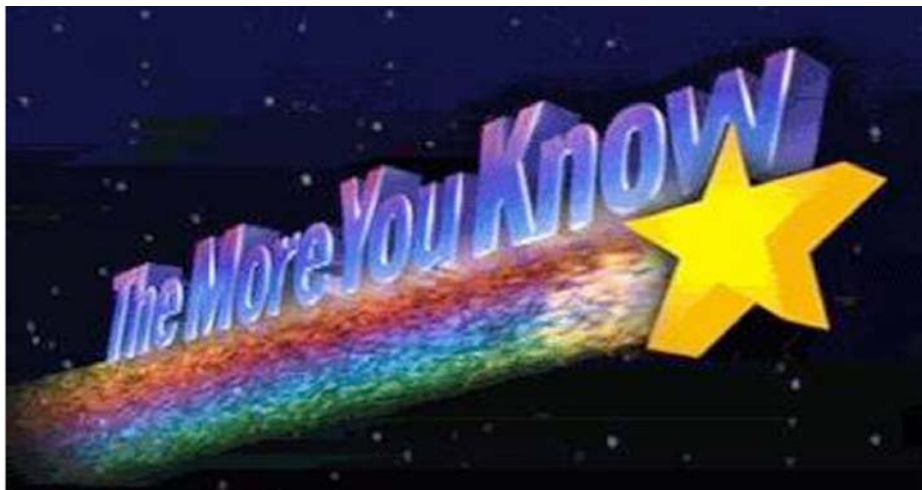
•ISPs

- We should probably just lie
- Let's cut corners to save money
- Unlimited user bandwidth bad (Customer monthly throughput < Profit)
- You can't do that on the Internets!
- Your information is being sold to the highest bidder



This firmware sucks!...

DISASSEMBLING THE FIRMWARE



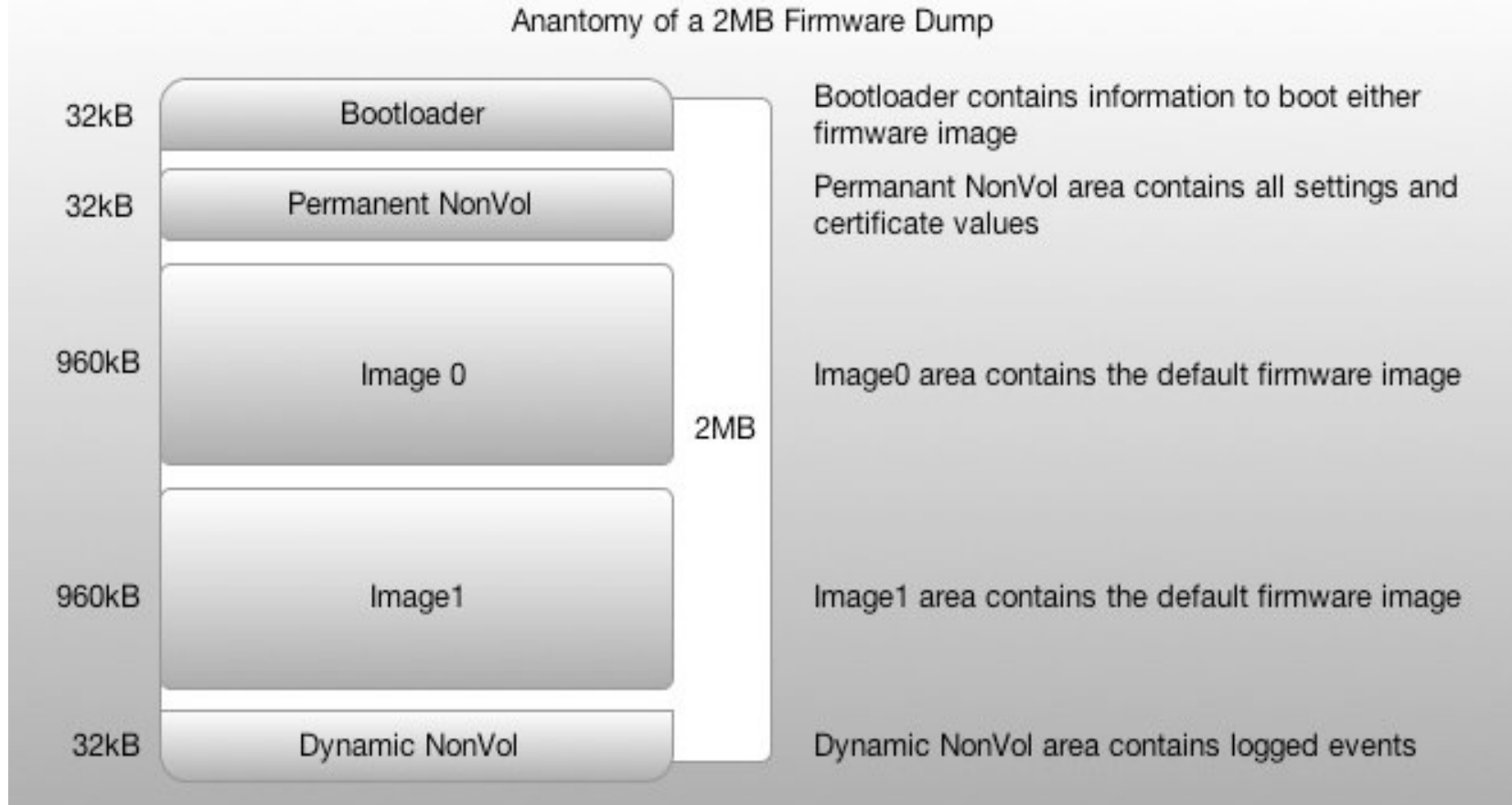


Firmware Images

- Three types of firmware images:
 - Signed & Compressed (PKCS#7 & binary)
 - Compressed binary image
 - RAM dump images (uncompressed & raw)
- A dump image is loaded in IDA Pro for reversing work or manipulation.
- Current firmware uses VxWorks or ECOS, both are coded in MIPS-32 assembly (fun for the whole family).



Anatomy of the flash contents





Reverse & Disassemble Tools

- Unsigned firmware binary images
- LZMA, CMImageTool by BOLTAR or other custom applications
- Your favorite hex editor
- IDA Pro Advanced
- Your favorite compiler (write your own)
- Serial console cable
- Jtag (optional)
- Vacation from real life & a lot of patience





The Future

- Better firmware
- ISP lockdowns
 - Craigslist is full of morons
- Docsis 3.0
 - More speed, essentially the same security
 - Advanced class of service mappings
- Purposefully designed anonymous networks
 - In a perfect world, this would be a priority





Problems & Some solutions

BPI+

- Crack 56bit DES or X.509 v3 RSA? (time, money and more time)
- Corporate espionage
- Self signed certificates
- Reverse current bpimanager & built in self signing functions

Cloning Detection

- Exact/Perfect clones can usually bypass this
- Network access can be gained on the majority of ISP as long as authentication is passed, cloning isn't exactly necessary
- If you still can't force a config to get network access, firmware modification is usually the answer.

The situation for ISPs preventing unauthorized access still looks very bleak for several reasons





Remember this stuff

- Anonymous / Fast Internet on Docsis networks
- Equipment used
- Cloning and Perfect Clones
- How to stay anonymous
- Firmware flavors & features
- Why it's possible
- Hardware & Security
- BPI+
- Development & reversing is kind of easy
- Security changes can be defeated
- Future plans are just as insecure





Thanks

- Anonymous network technicians that answered questions about OSS.
- Thanks to DerEngel of TCNiSO for essentially starting mainstream cable modem hacking.
- Anonymous cable modem hackers who share their stories with enough information to verify.
- Manufacturers for creating such insecure hardware and software.
- ISPs like Comcast whose walled garden is more like an wide open picket fence.
- Where da moviez at? & friends



Q/A

- Questions?

