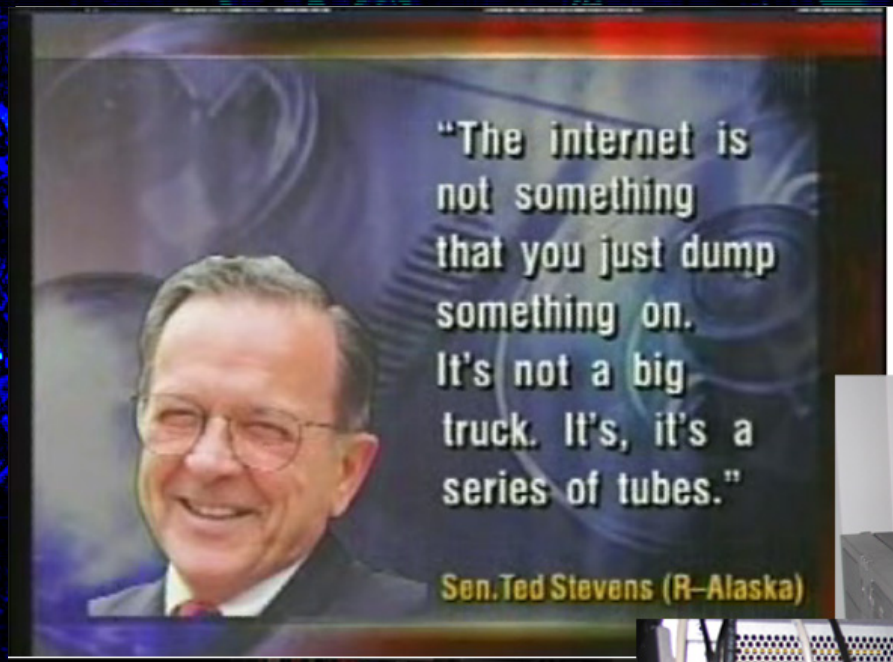
Hacking DOCSIS For Fun And Profit

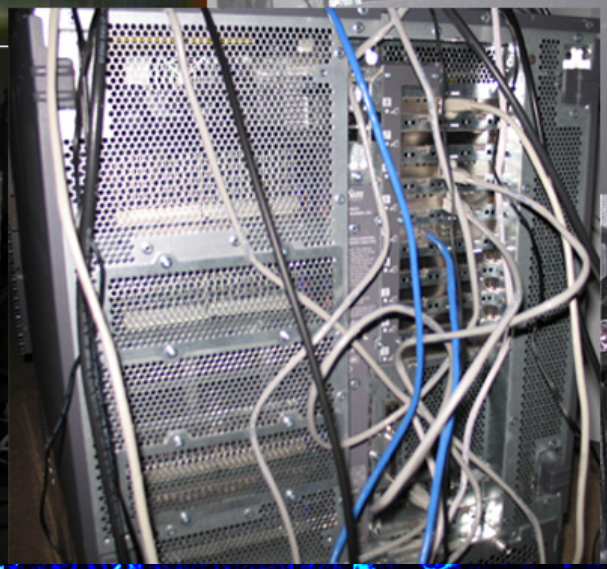
http://www.soldierx.com/defcon18/hacking_docsis_for_fun_and_profit-blake_bitemytaco.ppt

Blake Self
Bitemytaco (SBHacker.net)

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
  - I currently do research for S^{2}ERC (Security and Software Engineering Research Center), an NSF Industry/University Cooperative Research Center.
  - Bitemytaco is one of the root admins at SBHacker (http://www.sbhacker.net)
- Speech
  - We covered DOCSIS 2.0 and below at Defcon 16 with devDelay.
  - Our last speech led to a plethora of people to come to SBHacker and discuss modem technology (including employees at the various ISPs)

What This Speech Will Cover

- Requirements (for our examples)
- Previous Speech Overview
  - Anonymous access
  - Cloning HFC MAC linked to an ISP account
  - How anonymous you really are
  - Previous Firmware
- DOCSIS 3.0
  - Changes from the ISPs and Hackers
- Packetcable
  - How VOIP got owned
- United States vs Modem Hackers – Criminal Cases
  - Who all got a visit from the party van after our last speech?
- New Tools and Firmware
  - A review of all of the fancy new tools and firmware
- The Future
  - Botnet problems, the law, and future security solutions

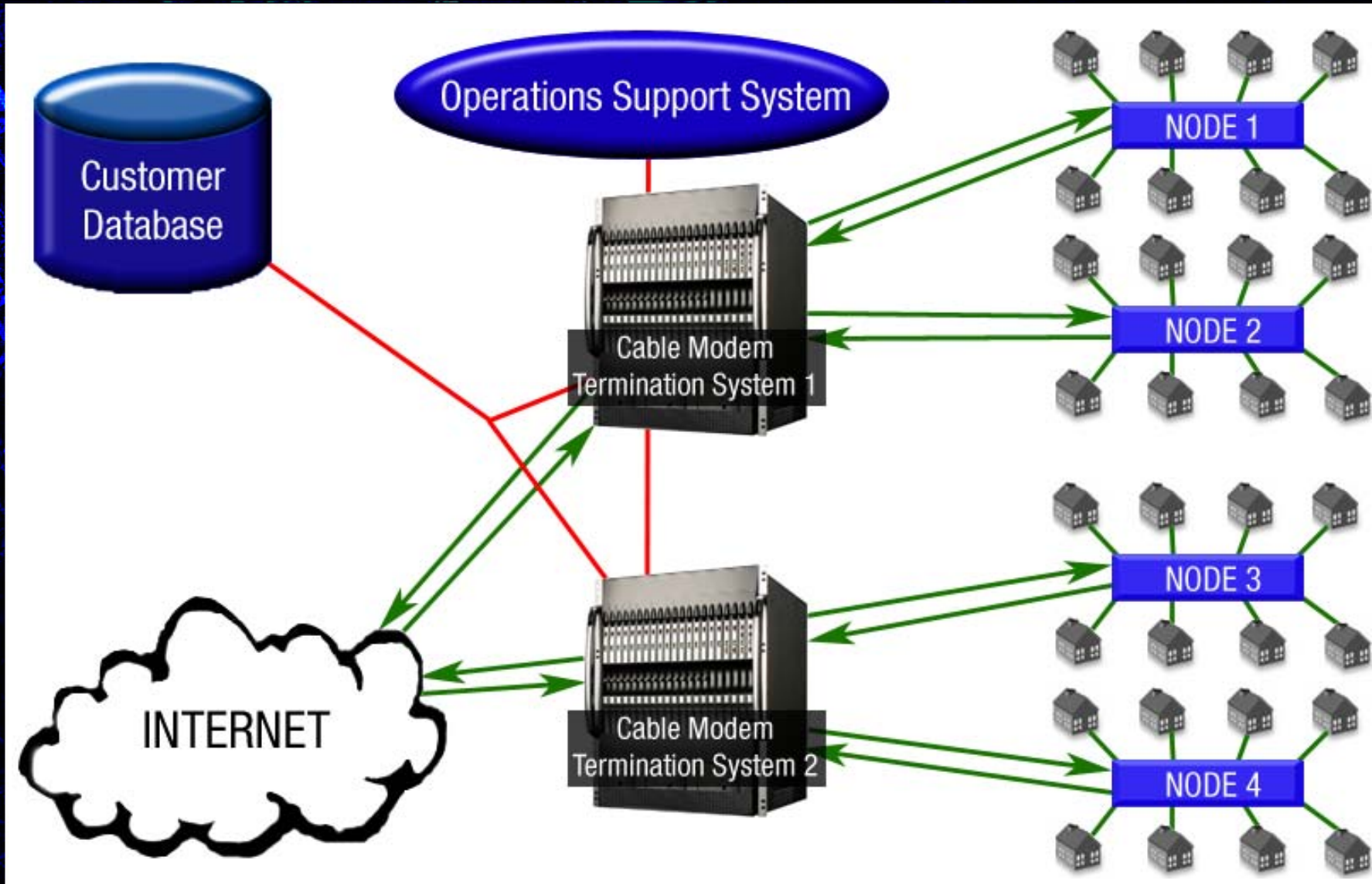
Requirements

- What do you need for our examples?
  - Coaxial connection to the cable company
  - SPI/JTAG cable
    - SPI/JTAG (Serial Peripheral Interface/Joint Test Action Group)
      - USB Cypress or FTDI based SPI/JTAG(Fast)
      - SPI/Parallel JTAG buffered (Slow)
  - SB6120/SBV6220/DPC3000 cable modem
    - Other modems can be modified
  - Soldering Skills
    - YouTube is an excellent resource for soldering reference
    - Solder wires directly to SPI flash chip
  - Applications for flashing the firmware onto a modem
    - USBJTAG NT
    - Haxomatic
    - SPI Programmer

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

Cable Network Overview

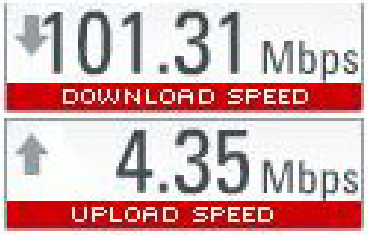


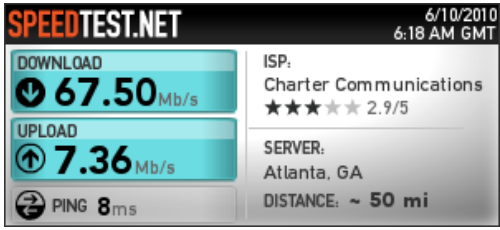
Anonymous Internet Access

- For our example of anonymous internet access, we will be using Comcast.
- Why Comcast?
  - According to Alex Goldman's research on isp-planet.com, 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

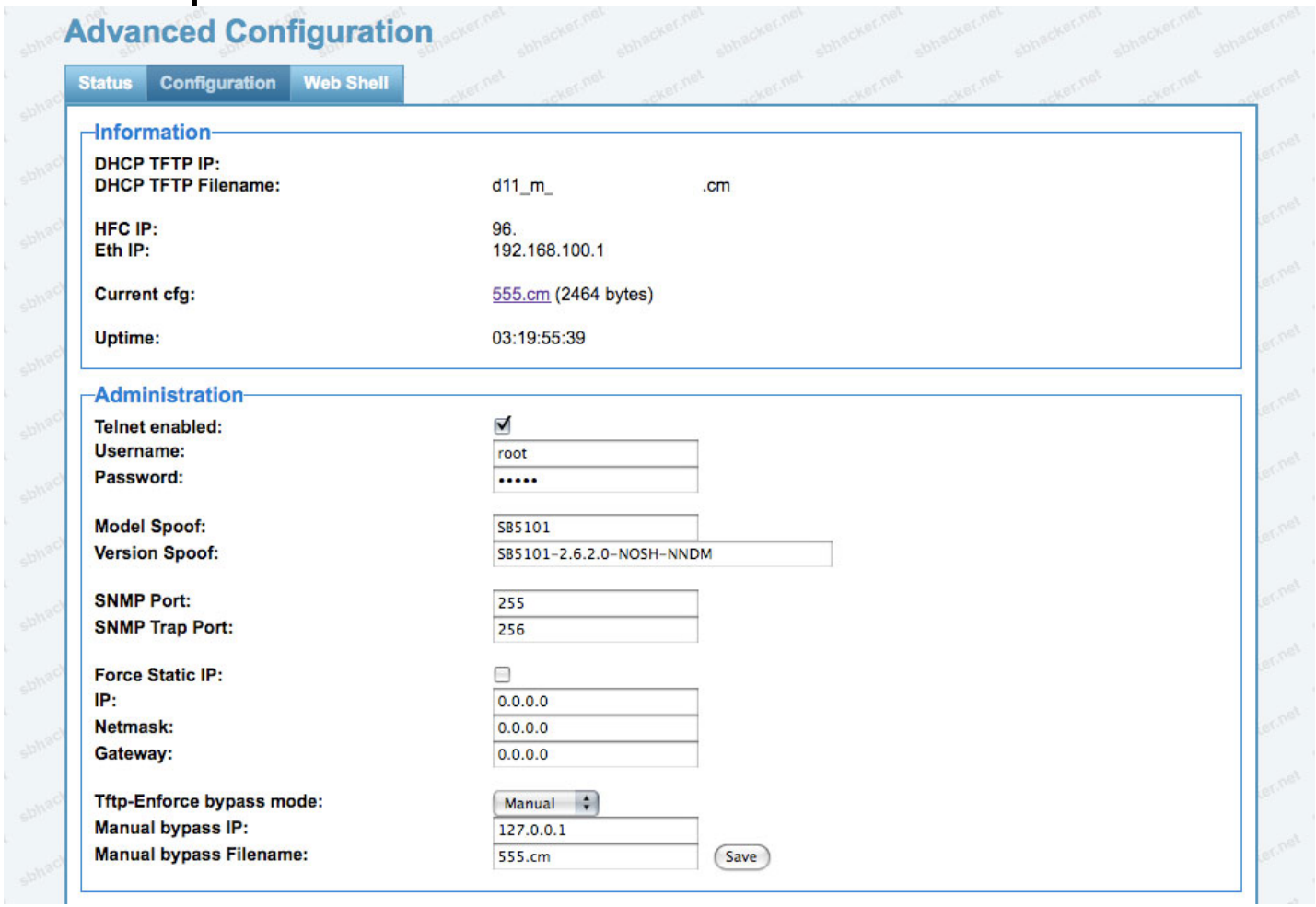
- Anonymous access is good, but faster anonymous access is better.
- In order to increase speeds, you can force a faster configuration file from the ISP, served locally or from configs stored in flash memory.
- You may specify a TFTP server, Comcast uses static instead of dynamic configs and each server 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 example is from Haxorware on the SB5101



Techniques for Remaining Anonymous

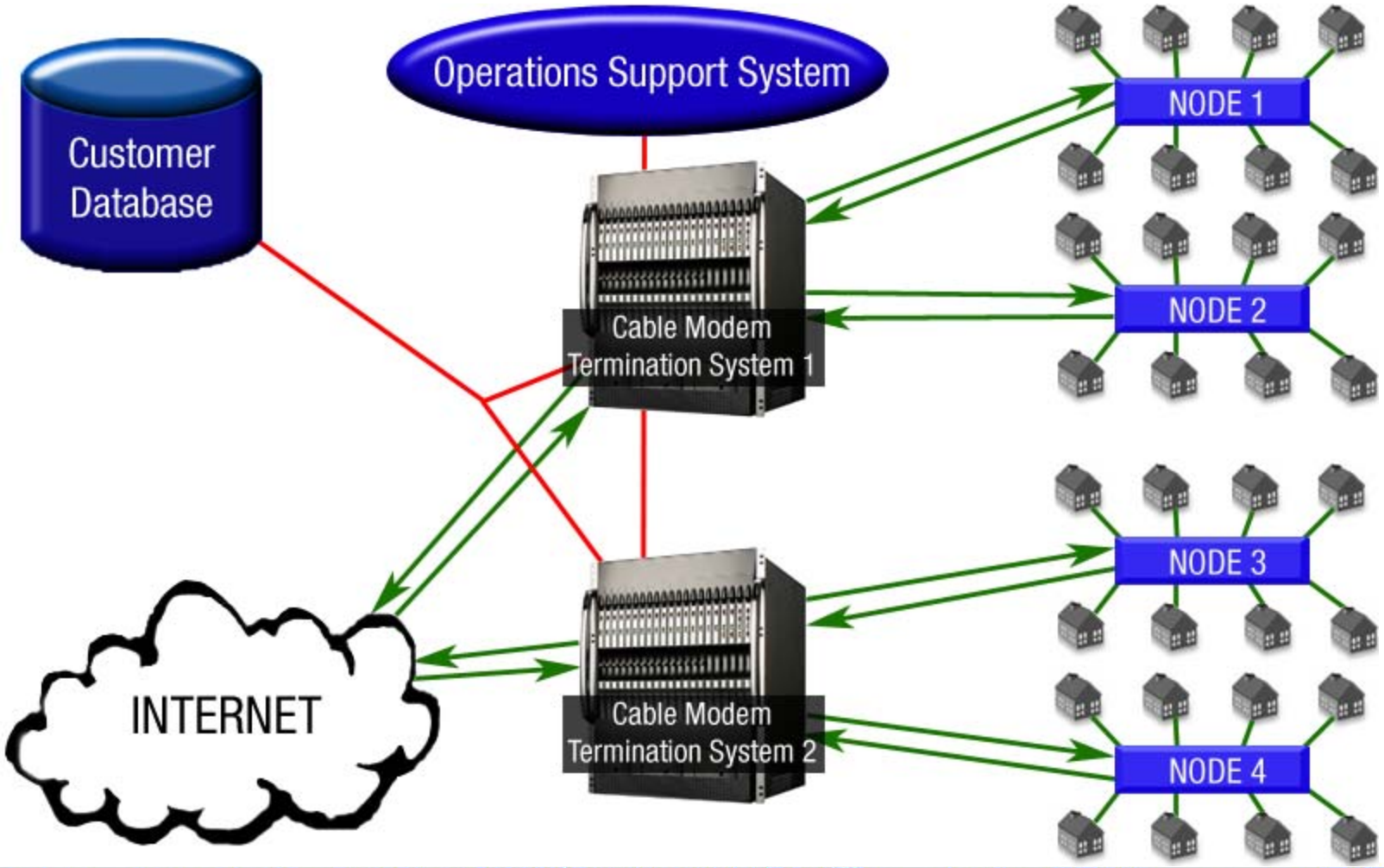
- Disable the SNMP daemon after registration
  - cd /non-vol/snmp
  - diag_disable_post_reg true
  - write
- Hide the Modem's HFC IP Address (You cannot hide CPE IP addresses)
  - cd /non-vol/snmp
  - hide_ipstack_ifentries true
  - write
- Hide Reported Software Version (system OID)
  - cd /snmp
  -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

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.

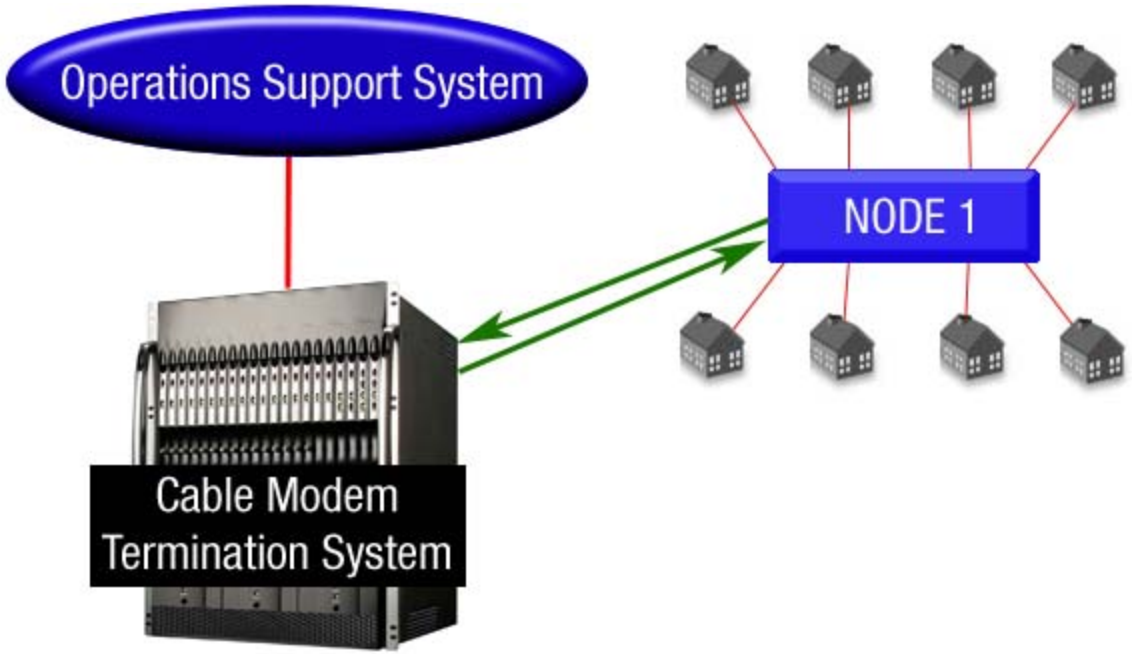


Obtaining Information for Cloning

- 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.

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)

Previous 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

DOCSIS 3.0

- DOCSIS 3.0 is essentially DOCSIS 2.0 with channel bonding, native IPv6 support, and “enhanced” security and encryption features.
- Channel Bonding:
  - Minimum requirement of 4 bonded channels for both downstream and upstream on modems and CMTS.
  - Maximum speeds for a modem in 4x4 config are approximately 160mbps downstream and 120 mbps upstream (EuroDOCSIS 3.0 uses 8mhz wide DS channels instead of 6mhz and supports about 200mbps downstream in 4x4 configuration)
  - The specification does not limit the number of bonded channels so the speed possibilities are endless (for example, current 8x4 offerings support over 320mbps downstream)
- Chipsets:
  - Puma5 chip – 4 DS + 4 US channels, ARMv6 arch, runs on Linux
  - Bcm3380 – 8 DS + 4 US channels, MIPS arch, runs on eCos

DOCSIS 3.0 Modems

- puma5:
  - OS: MontaVista Linux
    - Motorola SB6120 and SBV6220
    - Cisco DPC3000
    - Arris WBM760A TM702G
    - Netgear CMD31T
- bcm3380:
  - OS: eCos
    - Motorola SBG6580
    - Cisco DPC3010
    - Thomson DCM475 / TCM470

Current ISP DOCSIS 3.0 Offerings

- Comcast
  - Comcast is the leader in widespread D3 deployments. D3 is a direct competitor to FiOS and other FTTx services.
  - 50/10 residential and 100/10 business packages. Hacked SB6120s easily pull 120mbps downstream and 15mbps upstream.
- Charter
  - 60/5 residential with 100/10 and 75/5 business packages coming soon.
- Cablevision/OOL
  - 101 mbps download
- Time Warner/Road Runner
  - D3 in New York City only, nationwide rollout soon.
- Europe
  - Some European cable companies are already offering 8-channel bonded deployments with downstream speeds in the 150-300 mbps range.

Packetcable

How VOIP got owned.

United States vs Modem Hackers – Criminal Cases

- **Cablehack.net**
  - Tom Swingler aka Mastadogg
    - Arrested in early 2008.
    - First major FBI bust of a cable modem hacker, received heavy media attention.
    - Snitched on by Dshocker.
    - Case was dismissed after 6 months without any official reason.
    - Mastadogg snitched on MassModz
- **TCNiSO.net**
  - DerEngel
    - Arrested October 2009.
    - Regarded as the “godfather” of cable modem hacking.
    - Snitched on by Dshocker.
    - Currently out on bond awaiting trial.

United States vs Modem Hackers – Criminal Cases

- **MassModz.com**
  - Matthew Delorey
    - Arrested February 2010.
    - Blatantly advertised pre-configured modems to steal service from Comcast.
    - Raided after being snitched on by Mastadogg.
    - Expected to plead guilty
- **Various Small Busts**
  - Mostly located in South Florida where theft of service is rampant.
- **All of the current arrests have involved theft of service. Using modems for diagnostic purposes is still completely legal. Another key factor in the majority of arrests has been snitches.**

STOP SNITCHING

- **And now a brief message from Stephen Watt (Unix Terrorist)**

New Tools and Firmware

- Haxorware and sbh alpha (unnamed)
  - Still the leading firmware, will most likely continue to be for quite some time.
  - Community of over 66,000 users at SBhacker.net
- Haxomatic
  - Hardware and software to flash newer modems
- Misc tools by Rajkosto at http://haxorware.com/6120stuff.html
- Usbjtag.exe by usbjtag
- Tom's jtag utility

The Future

- With the extremely high bandwidth of D3 modems, there is a big concern about users being targetted for the purpose of botnets.
  - Previous upstream was 256kbps to 2mbps
  - D3 average is 5-10mbps and increasing constantly
- With the previous modem busts, there is a possibility that law enforcement will continue to crack down on modem hackers.

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

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.
- rajkosto, devDelay, Bad_Ad84, |DTOX|, Scanman1, bmhoff, spender, sn4ggl3, pirrup, cisc0ninja, the_ut
- Anonymous cable modem hackers who share their stories with enough information to verify.
- Manufacturers for creating such insecure hardware and software.
- SBhacker.net
- Soldierx.com

Q/A

- Questions?