

DOCSIS: Insecure By Design

Free Anonymous Internet Using Modified Cable Modems

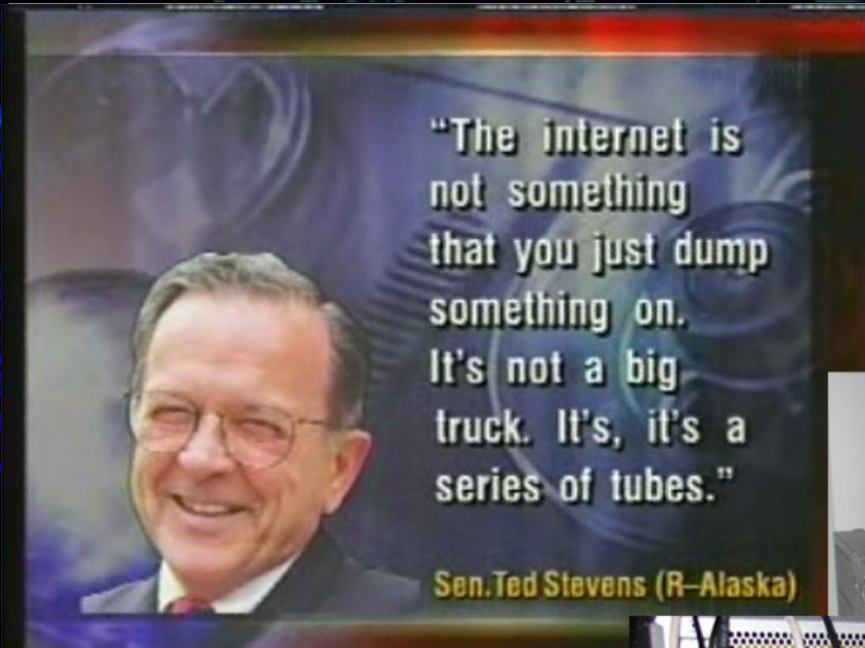
http://www.soldierx.com/defcon16speech/docsis_insecure_by_design-blake_durandal.ppt

Blake Self

Durandal of SOLDIERX



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
 - Started working in the security industry at the age of 17.
 - 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.
 - I have had various experts on this topic (such as bitemytaco from <http://www.sbhacker.net>) verify the information in this Defcon presentation.





What This Speech Will Cover

- Requirements (for our examples)
- Network Overview
- Anonymous Access
 - Gaining service with a MAC address not tied to an account
- Cloning a MAC Tied to an Account
- How Anonymous You Really Are
 - How close ISPs can pinpoint your location as well as techniques to catch people abusing/stealing service
- Breakdown of Hardware/Firmware (Durandal)





Requirements

- What do you need for our example?
 - Cable connection (to the cable company)
 - JTAG cable (MIPS EJTAG for our example)
 - EJTAG stands for Enhanced Joint Test Action Group
 - SB5100 cable modem (other modems can be modified, but this is the one that we're using for our example)
 - Soldering Skills
 - If you do not know how to solder, there are solderless adapters available from sites like <http://www.tcniso.net/shop/product.php?cat=2&page=1&product>
 - Application for flashing the firmware onto the modem (We use Schwarze Katze for Windows from TCNiSO)

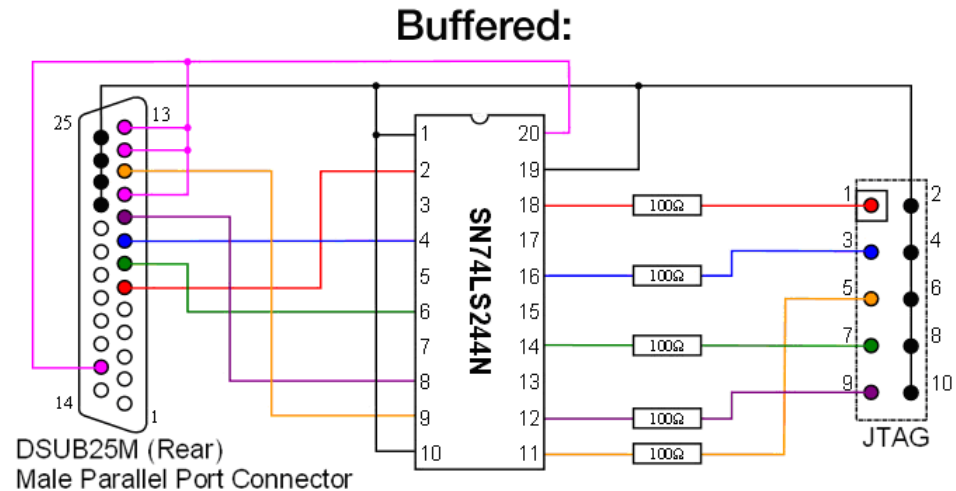
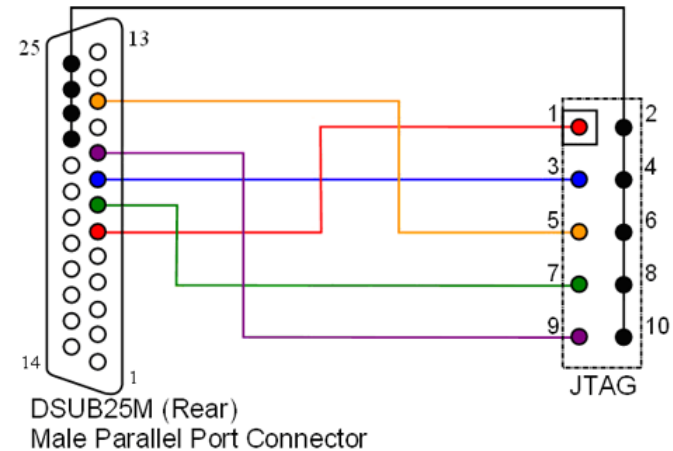




Requirements In Depth

- Cable connection
- EJTAG Cable
 - Easy to make
 - Available online

MIPS EJTAG Cable Schematics





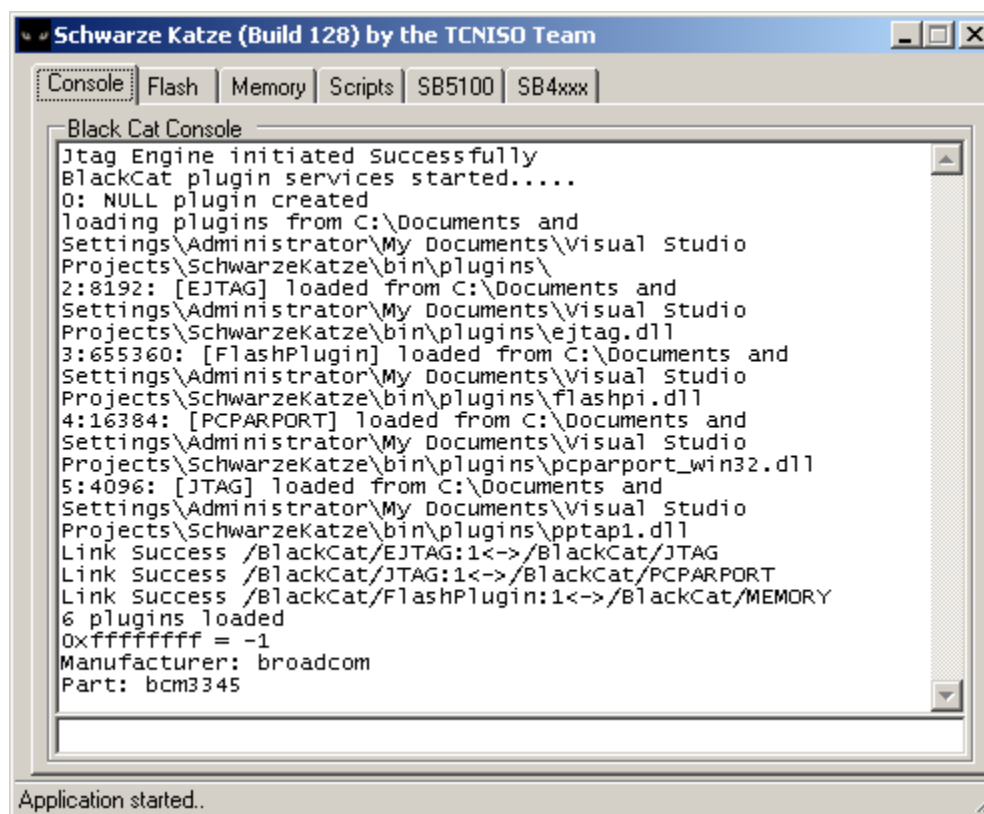
Requirements In Depth (cont'd)

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



Requirements In Depth (cont'd)

- Program the SB5100 using Schwarze Katze.



```
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.d11
3:655360: [FlashPlugin] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\flashpi.d11
4:16384: [PCPARPORT] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\pcparport_win32.d11
5:4096: [JTAG] loaded from C:\Documents and
Settings\Administrator\My Documents\Visual Studio
Projects\SchwarzeKatze\bin\plugins\pptap1.d11
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..
```



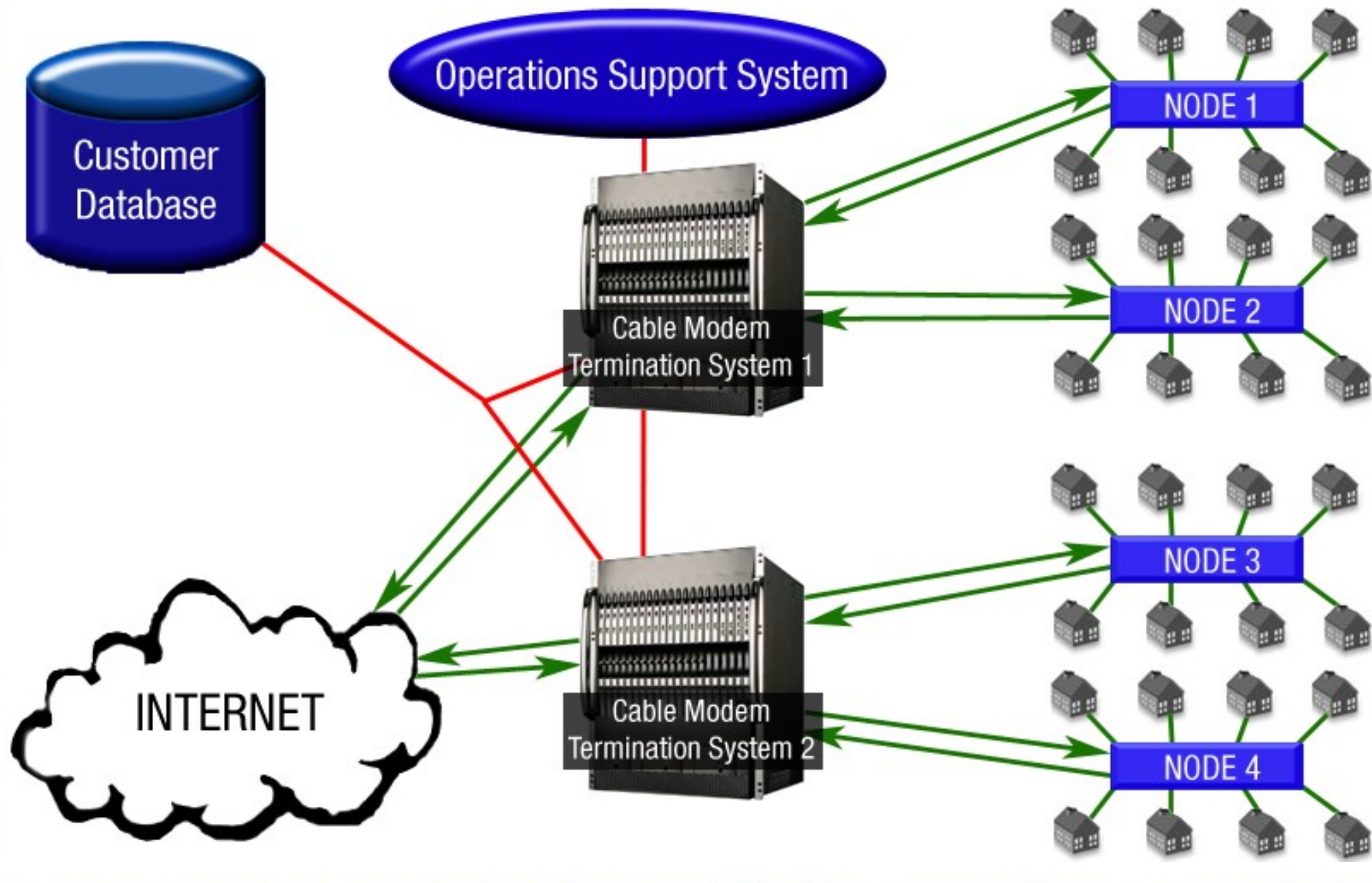

Modified Firmware

- Abilities of SIGMA X2 build 142 firmware:
 - Change the MAC Address
 - Change the serial number
 - Firmware upgrade blocking
 - Reboot disable
 - Force network access (ignore unauthorized messages)
 - Remove ISP filters (ports blocked at modem level)
 - Specify configuration file filename and TFTP server IP address
 - Upload and use a configuration file
 - Control of SNMP (Simple Network Management Protocol)
 - Broadcom CLI access
 - Full shell access to VxWorks (unix-like OS on sb5100)





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 plug a modem into the Comcast network that does not have an account, the only page that comes up is a Comcast page asking you to sign up for service.
- We found that you can generally connect into the computer hooked up to the modem – but you cannot connect out from the computer.
- Changing the DNS server gives you the ability to connect out (some of the time).
- Removing filters via the Broadcom CLI removes port blocking at the modem level.
 - *Commands to turn the filters off:*
 - cd /
 - cd snmp
 - filters off
 - write



Faster Speeds

- Anonymous access is good, but faster anonymous access is better.
- In order to increase speeds, you can specify a faster configuration file to use or upload your own.
- You can specify a TFTP server IP address, but on Comcast almost every TFTP 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 screenshot displays the SIGMA-X2 web interface. At the top, there is a navigation bar with links for [Main](#), [SIGMA](#), [WebShell](#), and [Advanced](#). The main content area is titled "SIGMA-X2" and contains several configuration sections:

- Config Changer:** A table with five rows, each containing a configuration option, its current state, and a "Change" button.

Disable firmware updates:	Enabled	<input type="button" value="Change"/>
Factory Mode:	Disabled	<input type="button" value="Change"/>
Configuration page changeable:	Enabled	<input type="button" value="Change"/>
Reboot disabler:	Enabled	<input type="button" value="Change"/>
Force network access:	Enabled	<input type="button" value="Change"/>
- Telnet Daemon:** Includes fields for "Embedded Telnet Server" (Enabled), "Login" (soldierx), and "Password" (soldierx), each with a "Change" button.
- Hardware Changer:** Includes fields for "MAC" and "Serial", each with a "Change" button.
- Firmware Changer:** Includes fields for "Filename" and "IP", with a "Download" button.

Below the configuration sections, there is a footer that reads "SIGMA-X2 build 142 - Developed by [TCNISO](#), 2008".

This screenshot shows a specific configuration page for the TFTP config file. The title is "SIGMA-X2". The page indicates the current TFTP config file is [basic.cfg](#). There are three configuration options, each with a "Change" button:

- Firmware name reported:
- SNMP listen Port:
- Auto boot config file: **Enabled**

Below these options is a "Config Uploader" section with a file input field, a "Browse..." button, and an "Upload" button. At the bottom, it states "Current config stored: hacked.cfg (1010 bytes)".

You can either specify a file that exists and the server that it exists on (blank for your ISP's tftp server) or you can upload your own.





Techniques for Remaining Anonymous

- Disable Reading the Modem with SNMP
 - cd /
 - cd snmp
 - view_v1v2 Noaccess
 - y
 - cd /
- Hide the Modem's HFC IP Address (You cannot hide CPE IP addresses)
 - cd /
 - cd non-vol
 - cd snmp
 - hide_ipstack_ifentries true
 - write
- Hide Reported Software Version (system OID)
 - cd /
 - cd snmp
 - delete sysDescr
 - write





Field Results

- Various members of SOLDIERX and other groups have reported high success rates with zero signs of detection
 - Durandal has a high use server that has been online for over 10 months
 - An anonymous individual has a machine on a business configuration that has been seeding torrents steadily for 6 months
 - Many people have as many as 8 modems running concurrently
 - In all of these scenarios, the individuals are paying for service. They are simply splicing their line to add additional modems





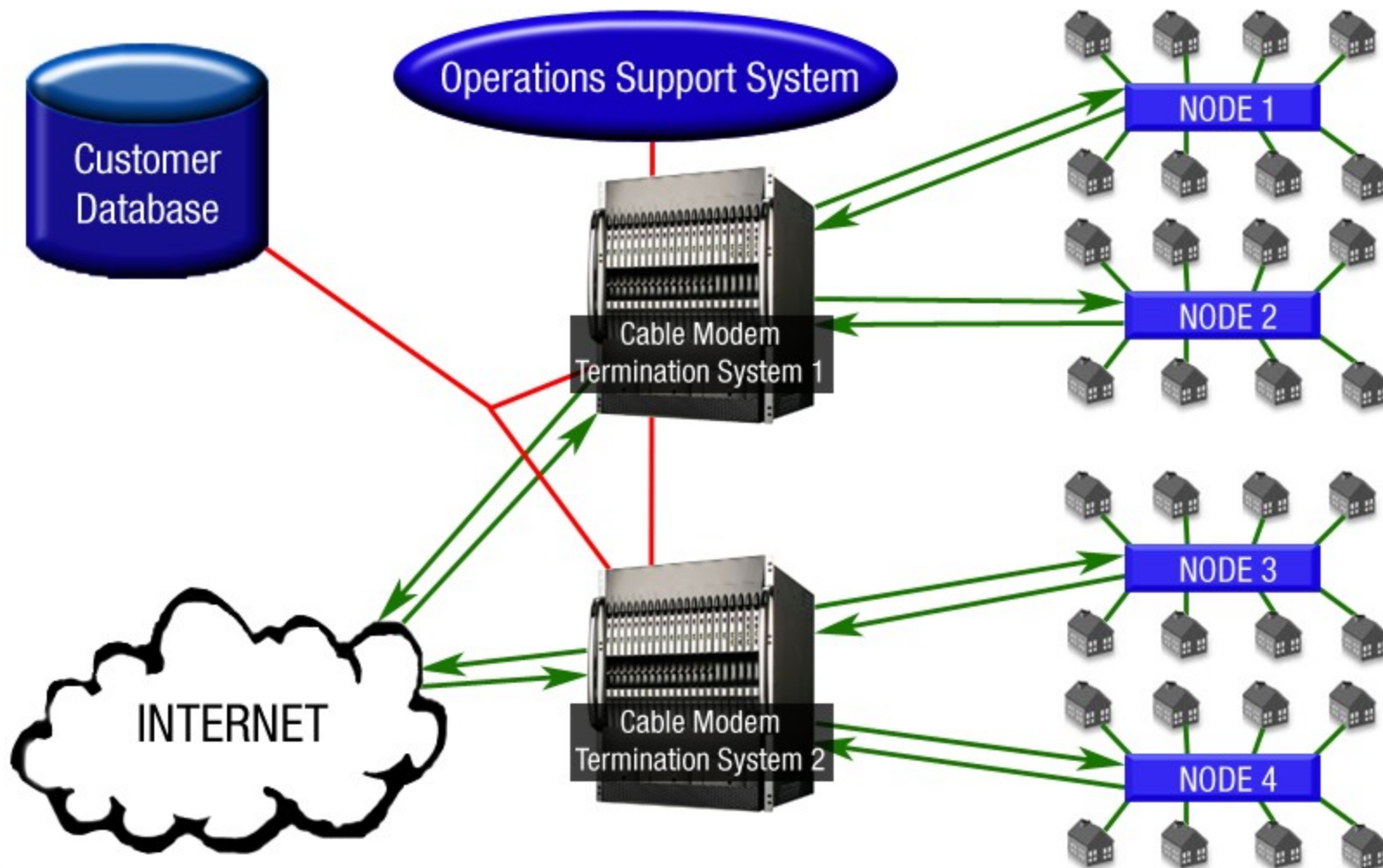
Cloning

- Cloning is where you use another customer's MAC address in order to get the same service they are paying for.
- Due to the way the system is setup, you have to use the MAC address of a customer that is on a CMTS other than yours.
- This method is not as stealthy because your modem is now tied to somebody else's account.



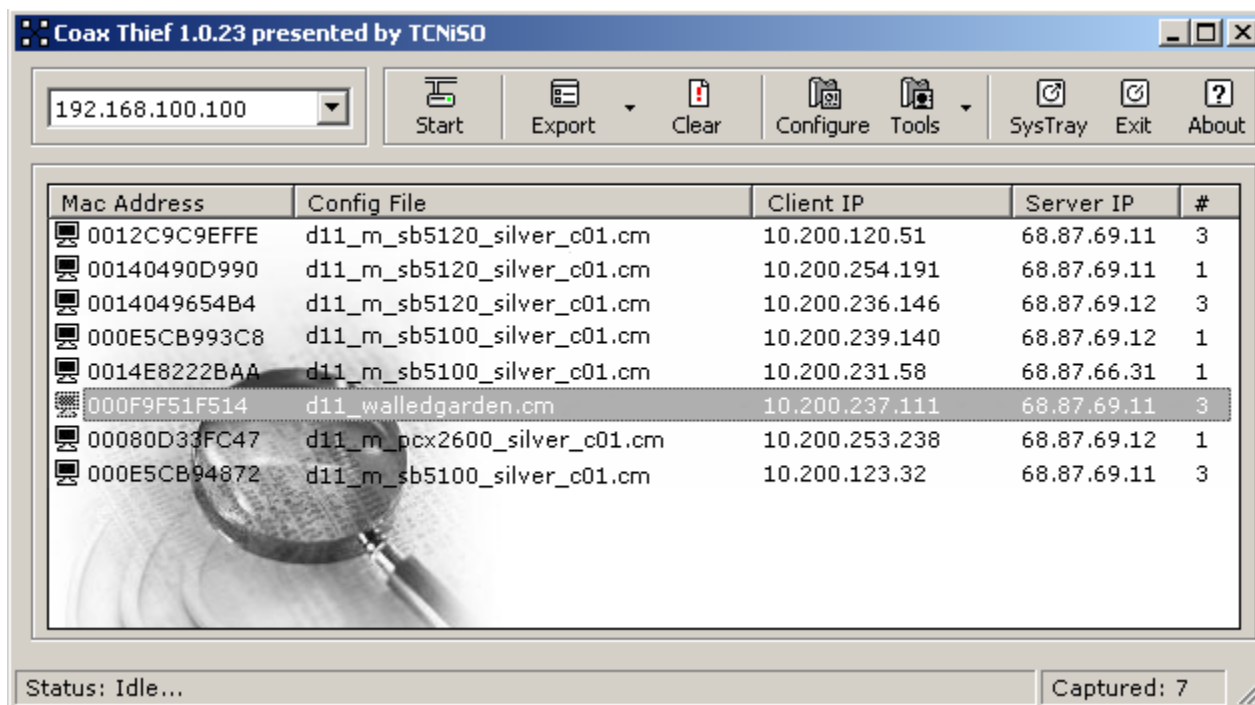
Cloning (Cont'd)

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



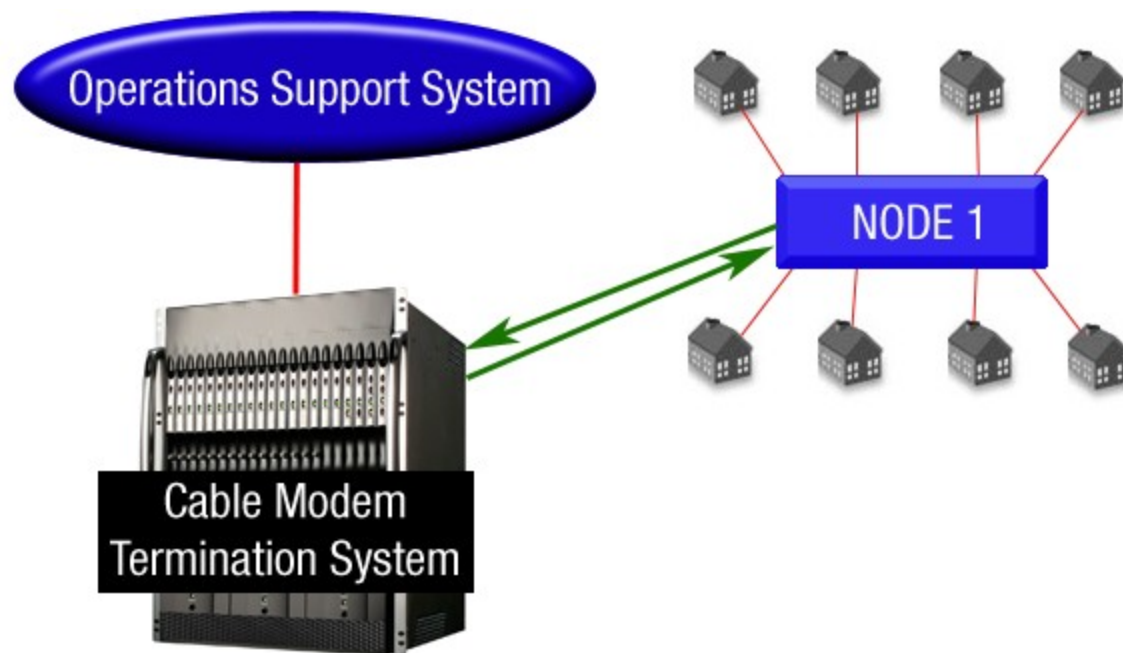
Getting MAC Addresses for Cloning

- MAC addresses are often traded in private ircs and on private forums.
- One free tool to sniff MAC address and configs is Coax Thief/CMSniff
 - Located at <http://www.tcniso.net/Nav/Software/Content/CoaxThief.rar>



How Anonymous Are You?

- The Operations Support System is unable to pinpoint a modem to an exact location due to the design of the legacy cable network.
- Currently, 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.
 - This technician will 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 check on lines that should not be connected in order to verify that they are not.
 - Many ISPs use colored tags to identify the account and service.





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)
- Uncapping on cloned MAC addresses
- 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
- 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.
- 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.





Thanks

- Thanks to bitemytaco of SBH (<http://www.sbhacker.net>) for reviewing the information in these slides.
- Anonymous network technicians that answered questions about OSS.
- Thanks to DerEngel of TCNiSO for starting mainstream cable modem hacking.
- Anonymous cable modem hackers that told me their stories and gave me enough information to verify it.



Enter Durandal

Cable Modem Hardware

Or How I Learned to Relax and
Love the Surfboard





Abstract

- Presenter Background
- WHYTO versus HOWTO
- SB5100 – Just another Computer
- Currently Available Firmware and Features
- Firmware Reverse Engineering
- Firmware Modification





Abstract - Translated

- Why you should listen to what I have to say
- Why you shouldn't listen to random people on forums
- Why you shouldn't panic
- How to avoid obsolescence by not being dumb
- Proof it doesn't take an angel to impress people





Background Information

- Active in the underground community since 1998
- Arabic Linguist 2002-2004
- JETS trainer under some of the most respected leadership in Army Intelligence 2003-2004





HOWTO vs WHYTO

HOWTO

- Tells you how to do something in a methodical, step by step method, allowing one to perform a task without understanding it.

WHYTO

- Tells you why something is a certain way, creating the underlying understanding necessary to perform a task.





HOWTO vs WHYTO Outcome

HOWTO

- Individual can follow simple steps, but cannot operate independently, or perform anything not specifically discussed in HOWTO.

WHYTO

- Individual is capable of operating independently and to the fullest ability of available equipment, including the application of knowledge to situations not specifically mentioned in any document or briefing.





If you fail, you can always do social engineering consulting....

SB5100 HARDWARE: WHY YOU ALREADY HAVE IT WRONG





What does a SB5100 Consist Of?

- A cablemodem is just a computer, so you're already halfway there:
 - Chipset: Broadcom BCM3348
 - Processor: 200MHz MIPS-32 core with MMU
 - RAM: 16-bit SDRAM bus with 8MB RAM (upgradeable)
 - Storage: 2MB Flash ROM
 - OS: WindRiver VxWorks (UNIX-esque RTOS)





Trust

- Due to the nature of the DOCSIS infrastructure, most of the burden associated with authentication is placed solely on the cable modem.
- Even if DOCSIS 23985 comes out next year, it stands to reason that if you can undermine all the countermeasures put into the cable modem, you're still online while all the kids are waiting for someone to make a firmware update.





Advice is like assholes...

SB5100 FIRMWARE OVERVIEW





SB5100 Factory Firmware

Pros

- You probably already have it
- It's every bit as functional as anything else out there if you know what you're doing
- There's very little chance of a surprise visit from the local ISP.

Cons

- You have to have two braincells to rub together
- Everyone in forums will tell you it has to be flashed to some other firmware
- Instead of having a nice GUI to change settings with, you have to use that icky command line.





Sigma X2 – The Lips of an Angel

Pros

- Works without too much trouble
- Made by someone who wrote a book

Cons

- That somebody was DerEngel
- You have to pay for it
- Claimed to come with “value-added features” (backdoors)
- Since it, and everything else that goes with it (you’ll need a licensed copy of schwartzekatze as well), requires a valid license, the idea of anyone actually paying for it so they can steal service defies all logic.





Sigma Stealth

Pros

- Cracked version of TCNiSO's firmware, meaning you save money.
- Usually has fixes to things DerEngel broke.
- All around stable firmware.

Cons

- Some versions are even harder to unpack than DerEngel's firmware, raising speculations as to the intentions of the author.
- With a name like Stealth Edition, you're bound to get caught.






Considerations

- If you simply want free internet access, the FERCSA-modified firmware is about as easy as it comes, requiring no knowledge of underlying commands.





Since your firmware can't possibly be worse than anything else out there...

DISASSEMBLING THE FIRMWARE





Tools Needed

- Image of firmware you wish to disassemble
- CMImageTool by BOLTAR
- LZMA.EXE
- WinHex
- IDA Pro Advanced
- JTAG cable and software (optional)





Obtaining Firmware

- Two types of firmware images:
 - Compressed .bin files (usually packed and compressed)
 - ROM dump images (already unpacked)





Q/A

- Questions?

