

Cable Modem Security

An Independent Investigation

Travis H.

Work in Progress

Why Investigate Cable Modems?

- Very popular networking technology for “last mile”
- Modems themselves sold as “black boxes” with no user-configurable settings
- Actually very capable devices
- But all the neat stuff is usually only available to the ISP
- Security properties are not well known
- So? Time for research!

Disclaimer

- The author is studying this from a research standpoint
- The cable modem I use has not been modified in any way
- Uncapping is considered theft of service and will get you blacklisted
- All identifiers (IPs, MACs) have been altered

Terminology

- HFC** Hybrid Fiber & Coax - the cable company's network
- CPE** Customer Premises Equipment - your cable modem
- CMTS** Cable Modem Termination System - the cable company's equipment that talks to your modem, also called a "headend"

Early Days

- Motorola CyberSURFER modems
- LANCity modems
- Early cable modem equipment had compatibility problems
- Industry organized into Multimedia Cable Network Systems (MCNS) Partners

DOCSIS Standard

- Solution: Data Over Cable Service Interface Specification (DOCSIS)
- Equipment certified by company called CableLabs
- Modems (CPE) as well as Cable Modem Termination Systems (CMTS)
- DOCSIS standard is pretty tight, but implementations vary in security

- http://www.cisco.com/en/US/tech/tk86/tk168/technologies_tech_note09186a0080093d79.shtml

- TODO: describe this more

Generalities

- Modem has two sides:
 - 1 Ethernet side
 - 2 Hybrid Fiber-Coax (HFC) side
- Each side has independent MAC address

Modem Boot Sequence

- 1 Use DHCP to get an address and a config file name
 - 2 Use TFTP to download the config file from the TFTP IP address configured in the firmware
 - 3 Config file specifies the parameters of the connection, including download/upload speeds
 - 4 Modem starts to pass layer 2 traffic back and forth between its two interfaces like a bridge
- NOTE: IP address your modem gets is not the same one your computer gets

Introduction

- Cable service providers silently rate-limit modems to certain upload speeds
- Called “capping”
- Many people wish to have higher speeds, trick their modems into supporting higher bandwidth
- This is called “uncapping”
- Later on companies started capping download speeds
- This is so they could sell tiered service (price discrimination in disguise)

LANCity Cable Modems

- Employee of cable provider UPC in NL discovered an uncapping exploit
- Apparently involved manipulation of ARP table
- Company fired him when he disclosed his discovery
- Distributed the hack as FuckUPC.exe

SB2100

- General Instruments SB2100 (Surfboard) one of the first DOCSIS cable modems
- Internal web server on 192.168.100.1 displayed config file name and TFTP IP address
- May actually be at <http://192.168.100.1/logs.html> which is a long list of all the diagnostics logs
- Using this, users could then download their modem's config file via TFTP

Arp Poisoning

- Arp tables map IP addresses to **interface** and MAC address
- There is only one global arp table, not one for each interface
- Thus, by inserting entries into the arp table, you control which **interface** the modem uses
- This is a bit like routing, only at the Ethernet level

Installing Your Own Config File

- Set up a TFTP server with the same IP address as the real TFTP server
- Edit the config file you downloaded to have no caps
- Poison the modem's arp table by pinging it during the bootup process
- The modem then downloads the modified config file from your server
- You are now uncapped

Why Was This Possible?

- The security features of DOCSIS were disabled in the modem by default
- Ethernet bridge open during bootup process (“registration”)
- “CMTS checksum”, a HMAC-MD5 checksum of the config file and a secret phrase known only to ISP, was disabled

Gaining Access to SNMP

- Most ISPs did not set the public community string
- SNMP values include e.g. TFTP IP address and config file name
-

Releasing the HFC Side IP

- At least one firmware automatically does a DHCP RELEASE on the IP it obtained
- Prevents anyone from accessing the HFC side of the modem (SNMP, etc)
- May also make your ISP think that you're not online (speculation)
-

Getting a VxWorks Command Shell

- TCN-ISO firmware gives the client side a web interface
- Provides a web page where you can enter VxWorks commands
- Is similar to the shell in Unix, but executes function calls rather than invoking separate programs
- Warning: Some TCN-ISO firmware images “phone home” with a packet of unknown contents

Watching the Ethernet Port

- Simply by running tcpdump on the interface connected to the cable modem, you can see some interesting traffic
- Suggested: `tcpdump -enls 2048 -i INTERFACENAME`
- That gets you MAC addresses as well as IPs

ARP Requests

- Arp requests by CMTS headend to Customer Premise Equipment (CPE)
- 17:14:52.198585 **00:14:f1:bc:12:51** ff:ff:ff:ff:ff:ff 0806 60: arp who-has 72.31.156.15 tell **72.31.171.1**
- 17:14:52.308686 **00:14:f1:bc:12:51** ff:ff:ff:ff:ff:ff 0806 60: arp who-has 91.34.136.77 tell **91.34.136.1**
- Most common type of packet you'll see
- Observation: despite **last IP** being different, **src MAC** was always the same
- Conclusion: One CMTS headend with multiple IP address aliases on single interface
- By analyzing these you can build up list of IPs and a good idea of the netmasks

OUIs

- SRC MAC was **00:14:f1:bc:12:51**
- First 3 octets form IEEE OUI[6]
- Can look up the OUI to find out that Cisco made this equipment
- Thus, this is a Cisco CMTS headend

Arp Thoughts

- All we see is arps from CMTS headend to CPE
- Probably to determine if the IP address is no longer in use and can be reclaimed/reallocated
- What happens if we respond to the CMTS arp requests ourselves?
- Might be able to hijack traffic to other customers with arp poisoning

DHCP Response for CPE Fixed Fields

- DHCP Responses are fairly common:
- 17:20:00.848855 **00:14:f1:bc:12:51** ff:ff:ff:ff:ff:ff 0800 368:
12.34.160.1.67 > 255.255.255.255.68: xid:0x5fe5b027
flags:0x8000 **Y:61.86.83.229 G:12.34.160.1 ether**
00:1e:90:12:34:56
- Based on src MAC, this is also coming from Cisco CMTS headend
- Y = “your” (client) IP address
- G = relay agent IP address, used in booting relay agent - note it is same as src IP
- Client ethernet address is there, OUI tells us its manufacturer is Elitegroup Computer System Co.

DHCP Response for CPE Vendor Fields

- ... vend-rfc1048 DHCP:ACK **SID:12.34.160.1 LT:51918 SM:255.255.240.0 DN:"city.company.com" DG:12.34.80.1 NS:89.12.23.127,89.12.23.128 RD:Y**
- SID = server identifier (IP address of DHCP server), LT = lease time (secs)
- SM = subnet mask. DN = domain name, DG = default gateway, NS = name servers

DHCP Response for CPE Thoughts

- Include a wealth of information
- OUIs in MACs give you manufacturer names
- IP addresses and netmasks for clients
- Name servers
- Domain names
- Gateway IPs

DHCP Responses for Cable Modems

- Basically similar but have the following fields:
- file
"filename_2.bin@DkGp6Og_AnYi8eM1gO5hjjWc6nh+q2k7"
... TFTP:"12.34.47.160"
BF:"filename_2.bin@DkGp6Og_AnYi8eM1gO5hjjWc6nh+q2k7"
- The config file has a dynamically-generated name
- This is to prevent people from hard coding a fixed-name config file with higher bandwidth caps
- Also makes it more difficult to TFTP the config files

Dynamic Config File Thoughts

- filename_2.bin@DkGp6Og_AnYi8eM1gO5hjjWc6nh+q2k7
- The config file is appended with a “@” and 32 characters of what could be a base-64 encoded value

Watching the Ethernet Observations

- Everything we have seen is from CMTS to CPE
- We don't see responses sent upstream from CPE to CMTS
- There are two distinct channels; upstream and downstream
- Upstream traffic is not rebroadcast on the downstream channel

Scanning the Subscriber Network

- According to a recent 2600 article, a large cable modem provider does not change their SNMP community strings.
- Based on the eavesdropping, you can create a relatively comprehensive list of subscriber modem IPs
- You might be able to access SNMP on modems other than your own.
- TODO: if I ever get results on this, I'll put them here.

For Further Reading I



Der Engel

Hacking the Cable Modem

No Starch Press, 2006.



Brian McWilliams

Cable Modem Hacking Tricks Uncapped Online

<http://www.securityfocus.com/news/353>



Kevin Poulsen

Cable Modem Hacking Goes Mainstream

<http://www.securityfocus.com/news/394>



Kevin Poulsen

Cable modem hackers conquer the co-ax

<http://www.securityfocus.com/news/7977>

For Further Reading II



CableLabs DOCSIS site

<http://www.cablemodem.com/>



IEEE OUI tables

<http://standards.ieee.org/regauth/oui/index.shtml>



RFC 2131 - DHCP

<http://www.isi.edu/in-notes/rfc2131.txt>



Surfboard Hacker Forum

<http://www.sbhacker.net/forum/>