Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Sniffing A Cable Modem Network: Possible or Myth?

There are a growing number of warnings from various sources regarding the security threats associated with cable modems. This paper focuses primarily on the threat of malicious users sniffing on a cable modem network. Most of these warnings about sniffing cable modem networks emphasize the fact that the physical media employed by the cable modem network is a shared medium. I contend that these warnings are unfounded.

Copyright SANS Institute
Author Retains Full Rights

AD

Sniffing A Cable Modem Network: Possible or Myth?
Dexter Lindstrom
March 5, 2002

1.0 Abstract

There are a growing number of warnings from various sources regarding the security threats associated with cable modems. This paper focuses primarily on the threat of malicious users sniffing on a cable modem network. Most of these warnings about sniffing cable modem networks emphasize the fact that the physical media employed by the cable modem network is a shared medium. I contend that these warnings are unfounded.

In order to substantiate my claim that network sniffing on a cable modem network is a negligible threat, I will cover some basic details on network sniffing and cable modem networks. Once the reader has a basic foundation of these two topics, a discussion of their technological relationship will be covered. This discussion will demonstrate the possibilities of network sniffing on a cable modem network.

2.0 Introduction

Today's modern society is beginning to become highly dependent on the Internet. As the dependency grows, users demand an increasing amount of bandwidth. Broadband Internet access has been growing steadily for years now and will continue to grow for the foreseeable future. As of December 2001, there were approximately 8 million cable modem subscribers in the United States.

These broadband Internet connections are a joy to the typical computer user. However, these connections also introduce the unsuspecting user to a growing number of security threats. Most of these threats involve direct attacks against broadband Internet connections with their "always on" state. Default OS configurations and poorly configured systems are extremely vulnerable. These are very real and tangible threats.

For the cable modem user, there is an additional area of threat called network sniffing, which many prominent security organizations publicize. This rather benign threat is undeservedly included with its darker, more nefarious siblings of direct attack vulnerabilities. For example, CERT has the following statement on a web page covering home network security, "because of this shared medium topology, cable modem users may experience slower network performance, and may be more susceptible to risks such as packet sniffing …" (http://www.cert.org/tech_tips/home_networks.html). Many other security and network organizations have similar admonitions; some with elevated tones of paranoia.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

3.0 Network Sniffing Overview

(Note: This section is not intended to be a thorough discussion of network sniffing. For an excellent and comprehensive paper on network sniffing, please visit http://secinf.net/info/misc/sniffingfaq.html.)

Network Sniffing is a method of eavesdropping on computer network communications. A simple analogy is wiretapping a telephone call or intentionally listening to a private conversation in a room. Because network sniffing is an eavesdropping technology, ascertaining useful information means patiently waiting for the private parties to exchange such information. Picture a law enforcement agent sitting in a van with headphones on, patiently waiting for a suspect to incriminate himself on a telephone call. This can be a long and possibly unsuccessful method of gathering useful information. Network sniffing is no different. For example, acquiring passwords transmitted in clear text is subject to luck and/or patience.

Network sniffing is based on electrical properties. In order for a network device to send data to another network device, an electrical signal is propagated along a conducting medium. Any device connected to the physical medium receives this signal. Normally a network card is configured to disregard any signals not intended for its host. However, a network card can be configured for 'promiscuous' mode, where all signals are retained for inspection.

Many devices can act as network sniffers, such as computers, routers, or switches. Network sniffers were originally designed to aid technologists in troubleshooting or enhancing network architectures. But alas, in addition to their beneficial characteristics, they can be used by miscreants for eavesdropping on private communications. But there is hope, network sniffers are limited in their use as a hacker tool because they require a physical connection to the network medium.

Certain network mediums are more at risk because of their design and types of use. I suggest that the two primary network topologies most susceptible to sniffing are Ethernet and Token Ring. This is because the vast majority of network hosts are connected via these topologies, thus providing easy physical access to the network layer. (Switched Ethernet provides a greater level of security than non-switched Ethernet, but can still be subverted in several ways.) I'm assuming here that the vast majority of Internet backbone devices (Ethernet and Token Ring) are located in highly controlled areas and have very restrictive system access. Thus, the potential for a hacker to commandeer one of these coveted network devices and enable promiscuous mode would be extremely difficult.

In respect to cable modems, the threat of network sniffing is seeded with the idea that the cable modem network is a shared medium. In section 5.0, I will discuss why I believe this to be partially untrue.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

4.0 Cable Modem Network Architecture

(Note: As with the previous section, this overview should not be considered a comprehensive guide to cable modem networks. Cable modem networks are highly complex due to the juxtaposition of many technologies. I refer the curious reader to the links in the references section for excellent sources of information on cable modem technology.)

A cable modem is a device residing at a customer site, which provides access to a computer network; in most cases the network in question is the Internet. Access to the Internet is accomplished on a physical medium that was originally intended for (and still primarily used for) television broadcasting. This cable infrastructure was coined as CATV – community antenna television.

Television signals, whether terrestrial or cable based, are modulated on high frequency carrier waves. Each TV channel is modulated in a 6 MHz channel between the frequencies of 42 MHz and 850 MHz (the range used varies among cable service providers). A television 'tunes' to the desired frequency and demodulates the original TV signal from the carrier wave. This is identical to lower frequency broadcasts like AM and FM radio (note that the FM frequency spectrum - 88 MHz to 108 MHz - is sandwiched in the range used for TV broadcasts). The modulation of TV signals on carrier waves allows many distinct signals to propagate along the same physical medium simultaneously (the medium for terrestrial broadcasts is the atmosphere).

The function of the cable modem network is to send and receive data signals across the CATV network. However, the cable network was designed for one-way communication. Hence, before a cable modem can function, the cable networks must be retrofitted for upstream (return path) communications. These network upgrades have been done in many metropolitan areas and efforts continue on older networks. The earliest upgrades were intended to address requirements for acquiring data from cable TV set top boxes, such as pay-per-view movies that have been viewed. This data is collected at the cable 'headend' – central CATV distribution point. It is only in the recent past that the requirements for the return path have changed dramatically. The downstream data path is typically in the higher frequencies (550 MHz and above). The cable companies use the lower frequencies for TV broadcasting because most modern TV receiving equipment is 'cable ready', meaning they have tuners prepared for these broadcast channels.

The relatively small amount of data originally collected from customer homes may have lead designers to use the lower end of the radio frequency spectrum for the return path (5 MHz – 42 MHz). This portion of the RF spectrum is inherently prone to ingress noise (e.g., electrical appliances, HAM radio transmissions, etc.). More than likely, the designers chose this portion to avoid sacrificing a more valuable VHF or UHF channel. In terms of data bandwidth, the typical upstream channel can handle in the range of 500 Kbps to 10 Mbps (depending on a number of factors). The total downstream bandwidth for a single channel is almost invariably 27 Mbps. More channels may be allocated by the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

cable company depending on the number of homes serviced by a single distribution point. Both of these figures represent total bandwidth values; not what a customer is allocated.

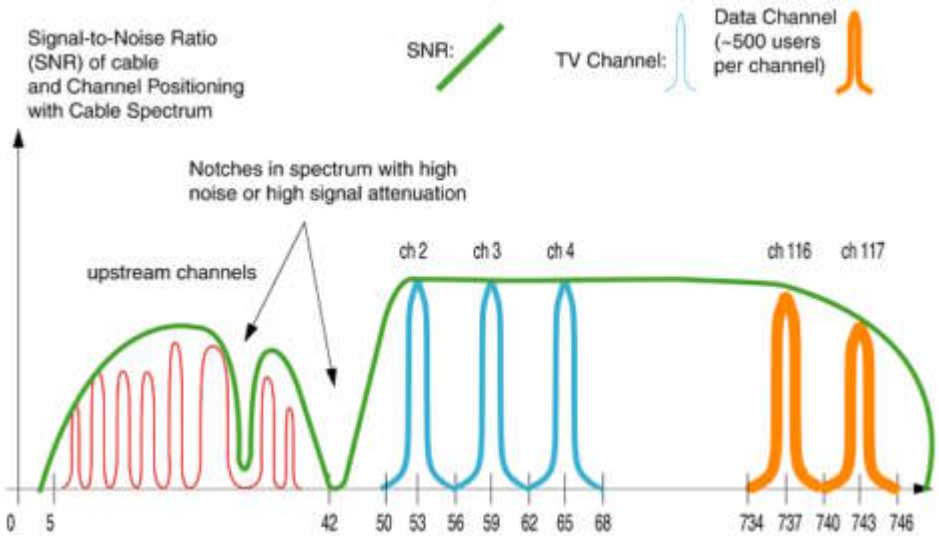

Figure 1 (http://ewh.ieee.org/r4/chicago/ed-cas-ssc/meet010522.html)

On the surface, the cable modem has a simple function: MOdulate network data on the upstream channel and DEModulate network data on the downstream channel. Hence, the term cable modem. Actually, the cable modem is a bit more complicated than this simple statement. It acts in most cases as a bridge connecting two disparate network topologies – the cable modem network and the customer's equipment. And in some cases the cable modem can act as a router (many PCs connected to the same cable modem).

The cable modem has two connections. The first is the F-channel connector in which the coaxial cable from the cable company is connected. (As previously mentioned, cable networks are highly susceptible to interference, which is reduced by using high pass filters. These filters must be removed for the connection to the cable modem.) The second type of connection is to the local CPE host (consumer premise equipment). This is typically a 10 Mbps Ethernet connection, but USB connections are becoming increasingly popular. Typical CPE devices are inexpensive firewalls, routers and PCs.

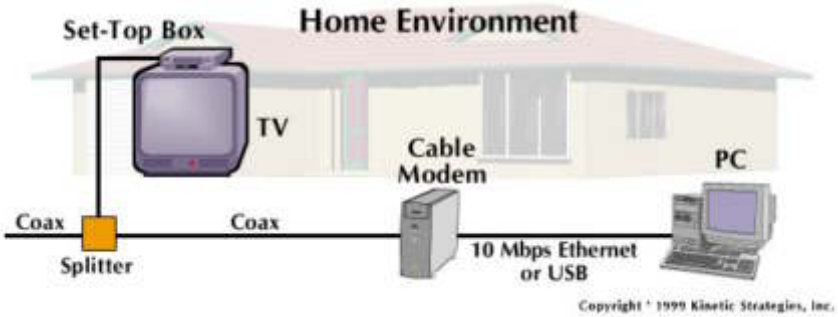

Figure 2 (http://www.cabledatacomnews.com/cmic/home.html)

On the other side of the cable modem network, there is a device called a Cable Modem Termination System (CMTS). The upstream path traverses the coaxial and often times

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

fiber networks back to the cable company's Headend. At this junction, the receiving device for the data communications is the CMTS. The CMTS is the interface between the cable modems and the Internet IP network.

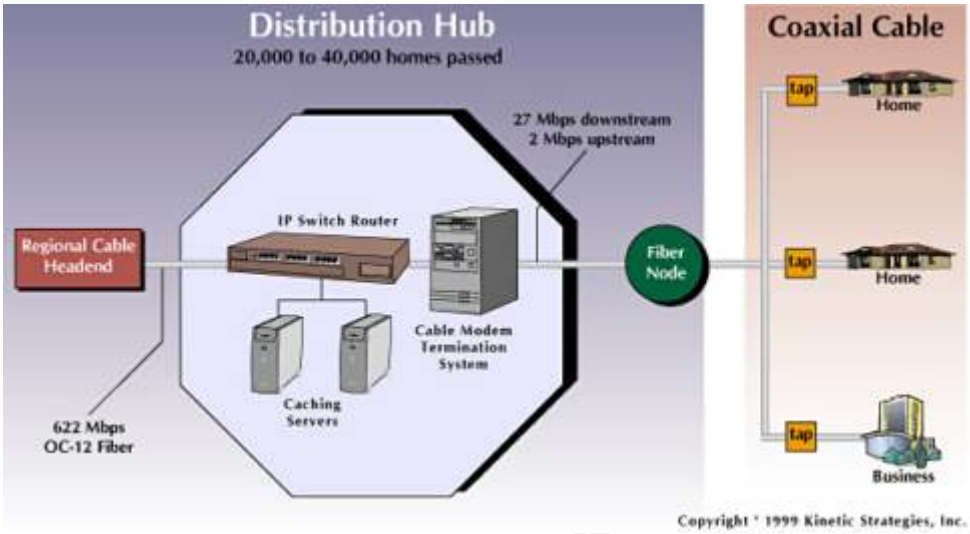

Figure 3 (http://www.cabledatacomnews.com/cmic/hub.html)

Now that the physical connectivity of the modem is defined, the functionality of the cable modem can be discussed. For the downstream data, the cable modem has a tuner (just like a TV) that tunes to the appropriate 6 MHz downstream channel (42 MHz – 850 MHz). The cable modem demodulates the signal, extracts only the portion of the downstream data that is destined for it, and then converts the data into an Ethernet or USB signal. The upstream channel works in a similar, but reverse order: 1) an application on the CPE device sends data to the Internet, 2) the cable modem receives the Ethernet (or USB) signal and modulates the data onto the upstream carrier frequency, and 3) negotiates channel access with the CMTS to send the data. Consequently, the connection appears to be an Ethernet connection to the local user or CPE device, but is actually nothing like Ethernet between the cable modem and the CMTS.

Cable modems work within the framework of the DOCSIS (Data Over Cable Service Interface Specification) standard. The original standard is 1.0, the current standard is 1.1 and the future version is 2.0. A mix of DOCSIS 1.0 and 1.1 is currently in use by cable providers. The DOCSIS standard dictates the interaction between the cable modem and the CMTS and between the cable modem and the CPE. In short, DOCSIS specifies every aspect of the cable modem functionality. In addition to the cable modem functionality, the standard also outlines the specifications for the CMTS equipment.

When a cable modem is turned on it proceeds through a number of initializations steps. First, the cable modem scans the downstream frequency range (42 MHz to 850 MHz) for the channel containing the network data. Now the upstream data frequency is extracted from the downstream data. Once the upstream channel is determined, the cable modem can request a DHCP address from the CMTS (this follows the standard DHCP discover,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

offer, request, acknowledgement sequence). Once the cable modem has an IP address, it contacts a ToD (time of day) server to synchronize its clock with the CMTS). Next it contacts a TFTP (trivial file transfer protocol) for a configuration file. This file governs the parameters that the cable modem uses to communicate. Some of the parameters the configuration file sets are: 1) the downstream and upstream frequencies (even though this information is ascertained during the initialization sequence, the frequencies can change at a later time), 2) the upstream and downstream bandwidth limits (typical caps may be DS=1.5 Mbps and US=128 Kbps), 3) control parameters that enable the cable modem to communicate on the upstream channel (often called time slots), 4) the modulation scheme (QAM, QPSK, etc), and 5) symbol rate (the number of bits per transmission cycle). At this point the cable modem is fully initialized with its own IP address and other IP configuration parameters.

A component of the DOCSIS 1.1 standard called Baseline Privacy Interface + (BPI+) is bi-directional encryption between the cable modem and the CMTS. This is accomplished using a digital certificate chain, where Verisign manages and operates the DOCSIS Root CA on behalf of CableLabs. Each DOCSIS 1.1 compliant cable modem has a digital certificate stored in its firmware. This certificate is linked to the manufacturer's root CA which is linked to the DOCSIS Root CA.

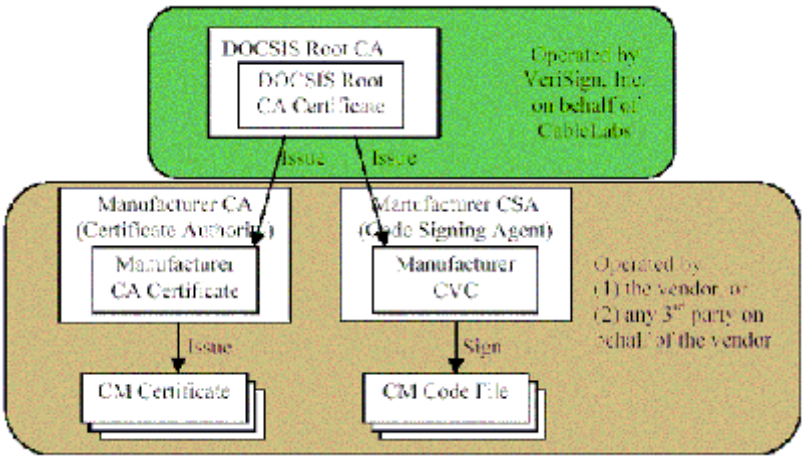

Figure 4 (http://www.cablemodem.com/downloads/DOCSIS_Digital_Cert_Instructions_011205.pdf)

When a DOCSIS compliant cable modem is initialized, one additional step is the authentication of the cable modem. The authentication and encryption is based on 56-bit triple-DES and X.509 certificates and key pairs. This authentication component mitigates the potential for unauthorized network access.

5.0 Cable Modem Networks and Sniffers

As stated in the introduction, there are many sources of security warnings stating that cable modem users are at a greater risk of network sniffing because the network is a shared medium. It is my contention that these claims are ill conceived. I will qualify this statement with the circumstances that network sniffing is limited to a typical cable

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

modem connection with a typical CPE device (PC with any operating system). Or in other words, an average user enabling their PC as a network sniffer on the cable modem network.

Let me restate that the downstream signal from the CMTS is received by each and every cable modem. It is the function of the cable modem to disregard all the data not intended for it. Additionally, DOCSIS 1.1 systems employing BPI+ have the data encrypted. Consequently, only the appropriate cable modem should be able to decrypt the signal with its locally stored digital certificate. (As of this writing 56-bit Triple-DES encryption has not been broken.) While the downstream channel security is not full proof, it is a very good measure of privacy.

This small window of opportunity involves an extremely knowledgeable user performing many arduous tasks to subvert the cable modem's filtering system for the downstream data. One possible technique to accomplish this is to create a special cable modem configuration file, normally received from the cable company's TFTP server during initialization (and periodically refreshed during system up time). This rogue configuration file would then have to be loaded into the cable modem. Because the cable modem only accepts a configuration file from the TFTP server designated in its DHCP offer, the industrious hacker would have to trick the modem into accepting the modified file from a new source (or a spoofed source). The ability to perform these actions is widely discussed on cable modem newsgroups and is relatively inconclusive. I have not seen any concrete processes that arm a user to override the cable company's config file. It's worth noting that the impetus of the config file changes in these newsgroup postings is not to enable network sniffing, but to alter the upstream and downstream bandwidth limits set by the cable company's configuration file.

Another newsgroup topic, which is rather infrequent, is the enabling of a Promiscuous Mode setting on cable modems. There have been steps outlined for using SNMPSET to enable promiscuous mode; provided the read-write community name set within the cable modem is known (and very often it is 'private'). I have tried this on my own cable modem without success. In my case, the SNMPSET command returns a success value, but the promiscuous mode is never actually changed. I am inclined to believe that this extremely obscure threat may be possible, but a DOCSIS 1.1 cable modem network with BPI+ enabled would mitigate a hacker from sniffing the downstream channel.

While the downstream channel is vulnerable to a possible, but unlikely sniffer attack, the upstream channel is virtually impenetrable. The upstream channel's frequency is set in the configuration file received by each cable modem from the CMTS. The range of frequencies for the upstream channel is 5 - 42 MHz (downstream range is 42 - 850 MHz). Access to the upstream channel for each cable modem is allocated in time slots by the CMTS. Each cable modem is given a number of time slots to use for sending data through the cable modem data network. When a CPE device sends data, the cable modem receives the signal (Ethernet or USB), modulates the signal onto the carrier wave (upstream frequency), and spends some of its 'time slots' to get network access.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Each cable modem is designed to receive/demodulate on one range of frequencies (50-850 MHz). Likewise each cable modem is designed to send/modulate on another range of frequencies (5-42 MHz). Consequently, all consumer brand cable modems on this shared network have no way of demodulating the upstream data because their demodulating circuitry is strictly for the downstream frequencies! Only the CMTS is equipped to demodulate the upstream frequencies.

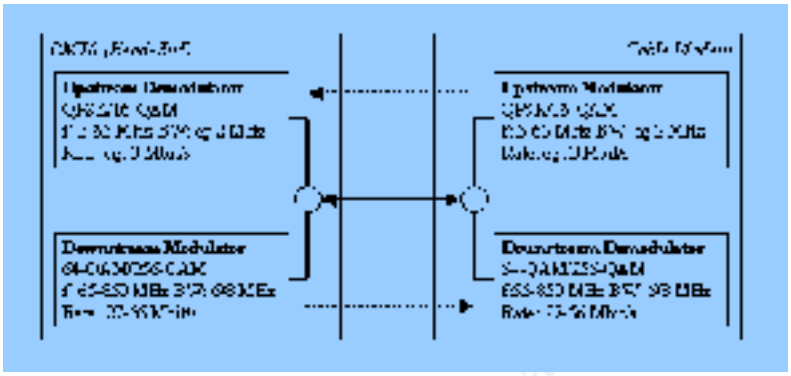

Figure 5 (http://www.cable-modems.org/tutorial/01.htm)

One of the most typical uses of a sniffer device is to eavesdrop on communications to catch user id and password information. Telnet, FTP, POP3, SNMP are some examples of upper layer protocols that send account and password information in clear text. These passwords are sent from the client to the server and thus cannot be sniffed on a cable modem network (upstream data) because the passwords are encapsulated in the upstream data.

There is the possibility that highly specialized equipment exists to sniff the upstream channel. It is my belief that the cable service providers may have such equipment designed for troubleshooting purposes; permitting the sniffing of both downstream and upstream data. This equipment is most likely expensive hardware, not readily available to average users (if it exists at all). As an indication that such equipment may not exist, Cisco's CMTS documentation depicts connecting a network analyzer to the CMTS for troubleshooting, not the customer site. This suggests that troubleshooting be done at the Headend and not the customer site.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

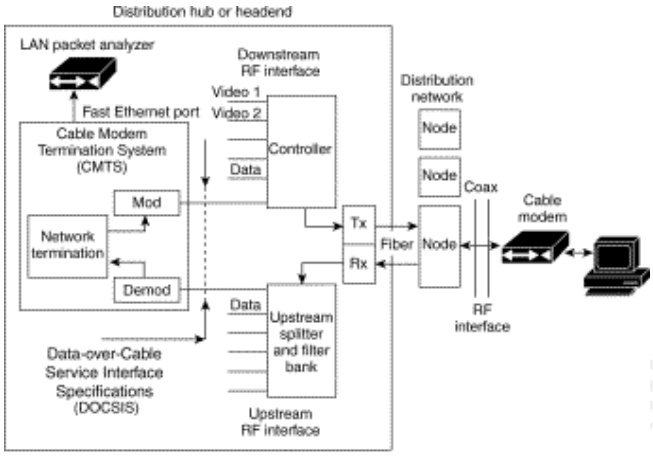

Figure 6 (http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_cmon.htm)

In the scenario that a user enables promiscuous mode on their CPE device, the captured frames will include the CPE's inbound and outbound data, broadcast frames, and multicast frames. While some of the broadcast frames may seem useful, most of the information extracted could be ascertained by simpler methods (like ARP broadcasts). When enabling network sniffing on my home CPE, what is captured is my own network traffic, a lot of ARP requests from the local router (no replies), and a few sporadic DHCP frames (offers and acknowledgements). This is all relatively useless information.

Many prominent cable service providers (including mine – AT&T) have blocked ports that they feel expose their customers to possible attacks or unauthorized system access. For example, AT&T blocks ports 137, 138, 139 (Windows file and printer sharing) and ports 65 and 67 (DHCP ports). Blocking the Windows ports prevents consumers from opening network neighborhood and viewing (and possibly accessing) their neighbors computer systems (UDP 137 is used by WINS for registration and name resolution, UDP 138 is used by the MS computer browser function, and TCP 139 is used for RPC communications to the Server service).

Although general network sniffing gleans very little information from a cable modem network, there are several alternative methods a determined hacker could use to sniff a cable modem connection. These include MAC spoofing, using ARP games, configuring the local CPE device with the MAC address of the router or a targeted cable modem user, ICMP redirection (where the hacker's CPE becomes a 'man in the middle' receiving data from host A, then forwarding it to host B), and MAC duplicating (I cannot find information on whether a CMTS will allow this type of behavior, but I'll assume it's possible). These are all methods of 'hacking' that involve changes to the network or hosts; they are not simply eavesdropping on private communications.

For example, if I configure my home PC (CPE) to have the same MAC address as the local router, I will receive all the network frames destined for the router. This would cause a significant and immediate change in network utilization, where the service provider may be alerted. Another similar type of threat is to duplicate the target hosts MAC address. In this case, the hacker is only seeing network traffic destined for the

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

target host. Neither of these threats is specific to cable modem technology. These can be performed on a DSL connection with the same effects.

6.0 Conclusion

The intent of this paper was to address the perception that a shared cable modem network is innately vulnerable to network sniffing attacks. These perceptions are based on notions that the cable modem LAN is as simple as an office Ethernet LAN. It is the author's belief that these perceptions are unfounded. I believe I have demonstrated why the cable modem network is not a simple Ethernet LAN and therefore not subject to the same types of general network sniffing. The most important concept to remember about the cable modem network architecture is the separate channels used for upstream and downstream traffic. This mitigates the possibility of a user sniffing any upstream data because cable modems are designed to send data on one channel and receive data on another.

A great deal of research was done trying to find documented cases of sniffing a cable modem network and none were found. Also thoroughly researched were the types and possibilities of network sniffing and how they could work with a cable modem. I was overwhelmed with the amount of information found on the Internet regarding cable modem networks, but was simply unsuccessful gleaning any information on sniffing these networks.

In the scope of security for a cable modem user, network sniffing is probably the least threatening. There are a number of other vulnerabilities of far greater magnitude. These include poorly configured Windows PCs with File & Print Sharing turned on, default installations of popular web server software, and unnecessary services and daemons running to name a few. In the end, a cable modem user should not be worrying about his neighbor sniffing his passwords.

7.0 References

Cable Television Laboratories, Inc.. "A CableLabs White Paper". 2002.
http://www.cablelabs.com/about_cl/pubs/cableNII.html

Ostergaard, Rolf V.. "What is a Cable Modem?". 2002.
http://www.cable-modems.org/tutorial/index.htm

Cable Television Laboratories, Inc.. "Cable Modem FAQ". 2002.
http://www.cablemodem.com/FAQs.html

Cable Datacom News published by Kinetic Strategies, Inc.. "Overview of Cable Modem Technology and Services". 1999.
http://www.cabledatacomnews.com/cmic/cmic1.html

Cable Television Laboratories, Inc.. "Cable Data Modems – A Primer for Non-Technical Readers". April, 1996.
http://www.cablelabs.com/about_cl/pubs/Cablemodem.pdf

Majeti, Venkata. "Cable Modem: Technology & Applications Part 1". May 22, 2001.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

http://ewh.ieee.org/r4/chicago/ed-cas-ssc/meet010522.html

Tzolkin Corporation. "Most Commonly Asked Cable Modem and xDSL Questions". November 11, 1999.
http://www.cablemodeminfo.com/CableModemFAQ.html

Wiebo Westerhof. "Cable Modems Frequently Asked Questions". 2001.
http://www.cable-modems.co.uk/faq/

Cable Datacom News published by Kinetic Strategies, Inc.. "Cable Modem Market Stats & Projections". March 1, 2002.
http://www.cabledatacomnews.com/cmic/cmic16.html

Limb, John O.. "Cable Modem Technology". January 1999.
http://www.hoti.org/papers/017.doc

International Engineering Consortium. "Cable Modems: Current Technologies and Applications". November 17, 1999.
http://www.onforum.com/pubs/cable_modems.html

Chapman, John T.. "Multimedia Traffic Engineering For HFC Networks". 1999.
http://www.cisco.com/warp/public/cc/so/cuso/sp/hfcn_wp.pdf

Cisco Systems. "Two-Way Data Headend Architecture". March 28, 2000.
http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cr72hig/cr72cnrf.htm

Cisco Systems. "Configuring DHCP, ToD, TFTP services on Cisco's CMTS". 2001.
http://www.cisco.com/warp/public/109/all_in_one_config.shtml

Cisco Systems. "Cable Monitor Command for the Cisco Cable Modem Termination System". January 3, 2002.
http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_cmon.htm

Gingold, Davide. "Integrated Digital Services for Cable Networks". September 1996.
http://rpcp.mit.edu/~gingold/thesis/gingold-thesis.pdf

Cable Television Laboratories, Inc.. "Cable Data Modem Performance Evaluation". November 15, 1996.
http://www.cablelabs.com/about_cl/pubs/ModemPerf.pdf

Cable Television Laboratories, Inc.. "CableLabs Concludes Milestone Certification Wave". December 2000.
http://www.cablelabs.com/about_cl/SPECS/December2000/SpecsNewsIndex.html

Cable Datacom News published by Kinetic Strategies, Inc.. "Accessing The DOCSIS Migration Path". December 1, 2001.
http://www.cabledatacomnews.com/dec01/dec01-5.html

Cable Datacom News published by Kinetic Strategies, Inc.. "Cable Data Network Architecture - Distribution Hub". 2001.
http://www.cabledatacomnews.com/cmic/hub.html

Cable Datacom News published by Kinetic Strategies, Inc.. "Cable Data Network Architecture – Home Environment". 2001.
http://www.cabledatacomnews.com/cmic/home.html

Anonymous. "DocsDiag – DOCSIS Cable Modem Diagnostics".
http://homepage.ntlworld.com/robin.d.h.walker/docsdiag

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Sunkad, Venkatesh and Cable Television Laboratories, Inc.. "Quality-of-Service: A DOCSIS/PacketCable Perspective – Part I". June 2000.
http://www.cablelabs.com/about_cl/SPECS/MayJune2000/news.pgs/story5.html

Gillespie, Greg. "Down the Pipe". September 1996.
http://caffeine.ieee.org/INST/sep96/thepipe.html

Vuksan, Vladmir. "Cable Modem Providers HOWTO". June 13, 2001.
http://www.linuxdoc.org/HOWTO/Cable-Modem/index.html

PC World Magazine. "Cable Modem: A Good Second Choice". August 2000.
http://www.pcworld.com/resource/article/0,aid,17150,pg,7,00.asp

Cable Television Laboratories, Inc.. "Data-Over-Cable Service Interface Specification DOCSIS 1.0 Baseline Privacy Interface Specification". November 19, 2001.
http://www.scte.org/standards/pdf/webdocs/SP-BPI-C01-011119.pdf

Cable Television Laboratories, Inc.. "Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface Specification". November 19, 2001.
http://www.scte.org/standards/pdf/webdocs/SP-RFI-C01-011119.pdf

Cable Television Laboratories, Inc.. "Data-Over-Cable Service Interface Specification DOCSIS 1.0 Operations Support System Interface Specification Radio Frequency Specification". November 19, 2001.
http://www.scte.org/standards/pdf/webdocs/SP-OSSI-RFI-C01-011119.pdf

Cable Television Laboratories, Inc.. "Data-Over-Cable Service Interface Specification DOCSIS 1.1 Radio Frequency Interface Specification". March 1, 2002.
http://www.cablemodem.com/Specs/SP-RFIv1.1-I08-020301.pdf

Cable Television Laboratories, Inc.. "Data Over Cable Interface Specifications Cable Modem Termination System-Network Side Interface Specification". July 2, 1996.
http://www.cablemodem.com/Specs/SP_CMTS_NSII01-960702.pdf

Gao, Junming and Siripunkaw, Pak. "Event Notification Management Information Base for DOCSIS 1.1 Compliant Cable Modems and Cable Modem Termination Systems". 2000.
http://www.ietf.org/internet-drafts/draft-ietf-ipcdn-docsisevent-mib-01.txt

Woundy, Richard. "RFC 3083 Baseline Privacy Interface Management Information Base for DOCSIS Compliant Cable Modems and Cable Modem Termination Systems". March 2001.
http://www.faqs.org/rfcs/rfc3083.html

Thornhill, Chris. "Securing DOCSIS Networks". November 2001.
http://www.cabledatacomnews.com/nov01/nov01-6.html

Cable Datacom News published by Kinetic Strategies, Inc.. "Verisign Moves Into Cable Modem Security". August 1, 2000.
http://www.cabledatacomnews.com/aug00/aug00-7.html

Cable Datacom News published by Kinetic Strategies, Inc.. "CableLabs Selects VeriSign For Security". February 1, 2001.
http://www.cabledatacomnews.com/feb01/feb01-6.html

Cable Datacom News published by Kinetic Strategies, Inc.. "DOCSIS Cable Modem Security Plan Receives Mixed Reviews". April 1998.
http://www.cabledatacomnews.com/apr98/april98-2.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Cable Television Laboratories, Inc.. "DOCSIS Digital Certificate Instructions".
http://www.cablemodem.com/downloads/DOCSIS_Digital_Cert_Instructions_011205.pdf

Cable Television Laboratories, Inc.. "DOCSIS Digital Certificate FAQ".
http://www.cablemodem.com/downloads/DigitalCertiFAQ050801.pdf

Cable Television Laboratories, Inc.. "Security in DOCSIS-based Cable Modem Systems".
http://www.cablelabs.com/about_cl/SPECS/September_SPECSTECH/tech.pgs/leadstory.html

Graham, Robert. "Sniffing FAQ". April 15, 2000.
http://secinf.net/info/misc/sniffingfaq.html

Anonymous and Macmillan Computer Publishing. "A Hacker's Guide to Protecting Your Internet Site and Nework; Chapter 12 Sniffers".
http://secinf.net/info/misc/maxsec/ch12/ch12.htm

Sipes, Steven. "Why your switched network isn't secure". September 10, 2001.
http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm

Denkinger, Troy. "Sniffing gives admins a look inside a network". April 6, 2000.
http://chicagotribune.com/templates/misc/printstory.jsp?slug=chi%2D000406finaldebug

Polchinksky, Matt. "How I turned my cable modem into a sniffer". May 2, 2001.
http://cert.uni-stuttgart.de/archive/vuln-dev/2001/05/msg00024.html

McWilliams, Brian. "How To Punch A Network Sniffer In The Nose". December 6, 2001.
http://www.info-sec.com/internet/01/internet_120601b_j.shtml

Brass Cannon Consulting. "Hubs, Switches, and Routers – A Hands-on How-To". January 10, 2002.
http://handsonhowto.com/lan102.html

Romanski, James. "Using SNMP for Reconnaissance". August 12, 2000.
http://www.sans.org/newlook/resources/IDFAQ/SNMP.htm

Cicirelli, Stephen. "Securing SNMP in Windows". August 28, 2000.
http://rr.sans.org/incident/SNMP.php

Carnegie Mellon University. "Home Network Security". December 5, 2001.
http://www.cert.org/tech_tips/home_networks.html

Walker, Andy. "Hackers on your home PC? Expect it and protect yourself". February 18, 2000.
http://www.cyberwalker.net/features/hackers-at-home.html

Ehrlich, Scott. "Obtaining Ethernet Addresses". November 6, 2000.
http://www.blu.org/pipermail/discuss/2000-November/018532.html

Glass, Brett. "Got Broadband? You're Under Attack". June 12, 2001.
http://www.extremetech.com/print_article/0,3428,a=1620,00.asp

Meinel, Carolyn. "Guide To (mostly) Harmless Hacking". September 31, 1998.
http://www.infowar.com/hacker/hack_090398g_j.shtml

MCSE Magazine. "The Home Guard"
http://www.mcsemag.eu.org/basics/sec04.htm

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Adams, Michael. Open Cable Architecture. Cisco Press November 22, 1999. Pages 124-160.

Farmer, James and Large, David and Ciciora, Walter S.. Modern Cable Television Technology: Video, Voice, & Data Communications. Morgan Kaufmann Publishers January 15, 1999). Pages 231-246.

Internet Newsgroups (Several of these newsgroups are accessible on free NNTP servers. I accessed them through AT&T's NNTP server - nntp://netnews.attbi.com.)

alt.cable-ip
athome.discussion-homenetworking
attbi.discussion-homenetworking
attbi.users-cablemodem
cableinent.cable_modems
comp.dcom.modems.cable

© SANS Institute 2002, Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced