THEFT OF SERVICE IN HIGH SPEED DATA SERVICES: A WAY TO DEAL WITH THIS DIFFICULT PROBLEM

Jonathan Schmidt
PerfTech Bulletin Services

Abstract

The residential HSD/Internet services environment is experiencing rapid technology changes. The providers' management tools have not kept pace. That has exacerbated the vulnerability and extent of service theft. Consequently, the tools must change. Some have, as in the newer set-top boxes; DOCSIS 1.1 CMTS/modems use strong certificate-based authentication to prevent service theft through modem cloning and spoofing. At the same time, home networking equipment has become very inexpensive, is common even in MSO offerings, and has filled computer store shelves. With this equipment, the home network devices become anonymous and can exist in large numbers behind a single modem. Similar to the downstream portion of the analog video cable plant, high quality Internet access can be replicated in a tree-and-branch architecture behind that modem and serve many users. WiFi products enable this architecture to be implemented with invisible, wireless links that are also open to opportunistic taps. These links are not susceptible to on-site inspection to check for redistribution.

This paper presents an in-band communication channel that can target all workstations on suspected accounts with unblockable screen alerts, which will utilize these invisible links to become an essential tool in combating such theft.

BACKGROUND

A lot of effort has been devoted to the control of HSD network components to eliminate service theft from modem cloning and spoofing. That has left one remaining service leak — the connection behind the cable modem.

Stopping Modem Spoofing and Cloning

Control of the subscriber modem has been achieved through certificate-based authentication in both configuration and data transfer in DOCSIS 1.1.

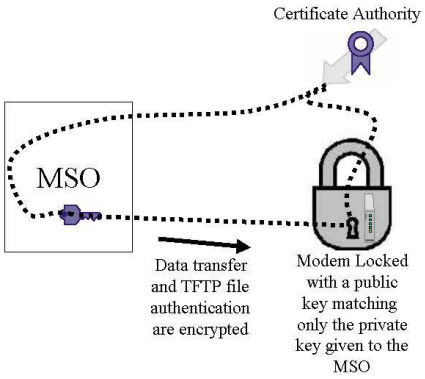

Figure 1: Certificate-based security in modem data transfer and BIN file authentication

Stopping Address Theft and Disruptive CPE Address Configurations

Control of the subscriber CPE network address configuration has also been implemented. With Cable Source-Verify, the DOCSIS MAC domain is protected against rogue CPE configurations for unassigned IP addresses or duplicate IP/MAC addresses.

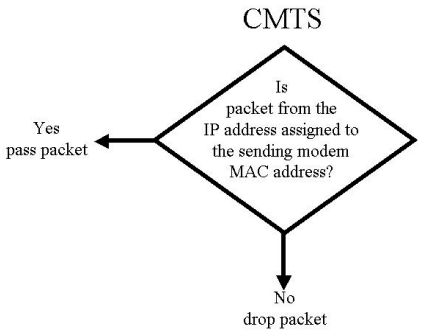

Figure 2: Cable Source-Verify control of Address assignment on DOCSIS network domain

Theft of Service Behind the Modem

A single home networking NAT gateway can be inserted between a network of PCs and the HSD modem and can appear to the network management as a properly configured, single user. However, it can serve high quality Internet access anonymously to many users both inside and outside the account residence through a tree of wired and wireless links. Those users who are outside the primary residence are engaging in theft-of-service according to the Terms of Use clauses in most MSO service agreements.

THE RAPID GROWTH OF HOME NETWORKS BEHIND THE MODEM

The home gateways provide security, anonymity, and the support of multiple workstations through many-to-one address translation, NAT.

Early MSO Rejection Became Acceptance

Early MSO service agreements included wording that would preclude the use of multiple computers through a gateway.

In the first years of HSD Internet provisioning, some attempts were made to detect the number of computers behind a gateway. An example can be found in the paper "A Technique for Counting NATted Hosts," by Steven M. Bellovin of AT&T Labs Research. The paper concludes that the technique is imprecise in the single case, and may only be of use in estimating workstation populations behind home gateways.[1] Indeed, the mechanism doesn't work at all with some gateways, such as Nortel's Instant Internet. It is also easily confused by internal LAN activity such as Windows intra-network activity. The difficulty in definition and detection of the NAT gateways caused very casual, if any, enforcement of anti-gateway provisions.

Today, for example, Time Warner Cable offers sales, support, and installation of multiple user home gateways and home networking equipment. Home networks are a source of new subscribers and of additional product revenue.

In Comcast's recently acquired AT&T Broadband networks, they promote the sale of multiple IP addresses (up to 4) for extra cost as a solution to the problem of using multiple computers on a single modem. The Terms of Use agreement doesn't appear to forbid the use of NAT gateways. Computers that aren't "directly connected to the modem" are not supported. However, one of their current FAQs provides a configuration for a LinkSys NAT gateway.

Gateways Pass the Knee of the Adoption Curve

The rapid rise in the rate of installation of home gateways has followed the drop in prices ($500 to $50 in 5 years) and the improved simplicity afforded by a synergistic and automatic configuration of

the gateway-HSD and the PC-gateway interfaces.

Microsoft is Focusing on Home Networks

Microsoft now adds protocols to their operating systems and to their hardware gateways to expand the services that can pass through the address translations.

Microsoft intends to incorporate everything from the refrigerator to multi-media components into the home network behind such gateways. This would indicate a continued, increasing population of home networking installations.

WiFi Increases Home Networking Use

Additional demand for gateways has been fueled by the similar reduction in price and greater simplicity of wireless LAN components, mostly the standard called WiFi.

Additional home computers that had been beyond easy reach of wired Ethernet are easily and inexpensively integrated with the home network with these wireless LAN components.

WiFi Is Encountering a Very High Growth Rate

- Shipments of WLAN products increased more than 100 percent in 2002, and will continue growing as the stellar wireless market performer for the next several years.
- Average equipment prices overall dropped by almost 28 percent, while revenues increased by more than 50 percent in 2002 to $2.6 billion[2]
- The WLAN equipment market will continue growing at a 43 percent compound annual growth rate (CAGR) to $10.3 billion in 2006.[3]

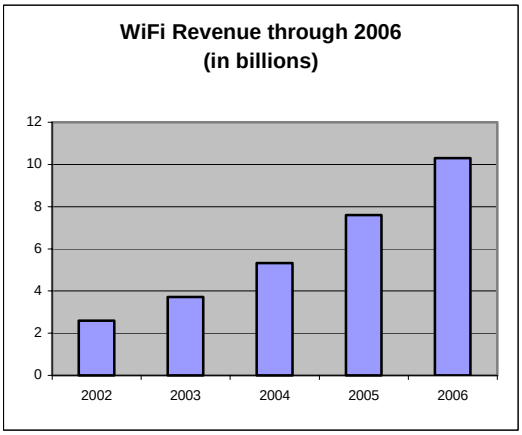

Figure 3: Estimated growth in revenue in WiFi market through 2006

AN ENVIRONMENT INVITING REDISTRIBUTION

Redistribution is Simple to Wire up and with WiFi, Easier than with Analog TV

Home gateways, WiFi components, hubs, switches, cables, and PCs are very simple to configure in a home network to give all PCs access to the Internet. In fact, for the most part, the components configure themselves. An infrastructure required for redistribution within a multi-tenant building, for example, can be constructed entirely with parts and technical assistance from a Radio Shack® store.

Redistribution Can Support Many Users

The high inherent bandwidth of the HSD Internet connection and the bursty data demands of the typical browsing or e-mail user allow these environments to redistribute high quality Internet access to dozens of simultaneous users.

Wireless LANs Offer More Opportunity

WiFi access points can be connected to home gateways entirely within the broadband service agreement. These access points, when connected to a home gateway, can provide anonymous and uncontrolled access to the account's Internet connection over a wide area as large as hundreds of feet around it.

The gateway user's assumed network anonymity combined with a widespread "the Internet is free" attitude adds encouragement to those who are inclined toward service redistribution or an opportunistic wireless tap. Users of WiFi have easy access to programs such as "NetStumbler" and "MiniStumbler" that provide the user with a graphic display of all the locally accessible, unencrypted WiFi networks and the necessary "SSID" to sign on (SSID: ***S****ervice* ***S****et* ***Id****entifier*, a 32-character unique identifier attached to the header of packets sent over a WiFi network). NetStumbler is used with PCs and MiniStumbler is used with pocket computers. These programs are used by ordinary hobbyist computer users and are not restricted to hackers. Open WiFi networks in populated areas don't remain a secret for long.

The Billing Method Doesn't Discourage Redistribution

The billing method for most HSD Internet access accounts is a fixed rate for a fixed bandwidth high-speed connection. There is no limit on consumption and, therefore, no extra cost to the account holder for extra use. This method is unlike that for water and electricity, for example, but is similar to the downstream portion of an analog TV cable plant and can be expected to similarly encourage theft. Redistribution subjects the account holder to no additional billing if not caught.

MSO are expected to offer tiered services based on consumption and that may reduce the illegal practice both because of the potential for extra charges to the tiered services account holder as well as the conversion of some participants to being subscribers of the more attractive, less expensive, low consumption service.

However, collecting additional revenues from high-bandwidth users accustomed to "free" access could be problematic unless addressed before tiered services are introduced.

DETECTING REDISTRIBUTION

Redistribution is, indeed, a problem since each instance represents one or more potential subscriptions that are lost.

It does not appear that there is a method to attack the problem by prevention either in configuration or warnings in the terms of service. Therefore detection and response to detection represent the remaining option.

Detection with Network Equipment

Detection of likely incidents of service theft should be much easier than with analog cable TV theft since the multiple users behind the gateway create a protocol stream that has a variety of signatures that indicate the number of individual users.

Although, as shown in the Bellovin AT&T Labs paper, identification of individual accounts with multiple users is imprecise with standard network devices that observe at L3, specialized devices could be used to identify such accounts when

inspecting other layers. For example, data passing through a device similar to a firewall could identify accounts exhibiting many simultaneous connections or the use of many versions of browsers, or the checking of many different e-mail accounts. Although it is possible within the character of the protocol, equipment to perform such checks has not been brought into such service.

Detection of likely redistribution situations is not necessarily an indication of a definite redistribution event. It is only a violation if users outside the account residence are accessing the Internet through it.

Drive-by Detection of Open WiFi Points

The default installation of most WiFi components establishes the network without encryption. These networks can often be detected with simple PC equipment and freely available software such as NetStumbler. When detected in this way, the drive-by inspection PC can also detect if the network has an Internet connection through the HSD network of the MSO.

Interestingly, unsecured WiFi equipment is not in violation of the Terms of Use agreement in force with the subscriber and, therefore, is not an indication of a definite event of redistribution. It is only a violation if users access the Internet through the network from points outside the account residence.

Other External Indicators

There are also other external flags to indicate potential redistribution activity such as:

- Blatant advertising of wireless "WiFi hotspots" at the location of a residential broadband subscriber
- Mass service cancellations at a multi-tenant location.
- Alert service representatives who spots trends of returned modems in a concentrated area.
- A serendipitous tipster

REAL SERVICE THEFT, VAGUE INDICATIONS, INVISIBLE LINKS

The Vulnerable Revenue is Real

"Comcast has found that the Internet business has become even more profitable than providing basic cable service. The capital costs are lower: a cable modem costs $50 compared with a television set-top box at $225. And churn - the rate at which customers cancel their service - is far lower for Internet service than for video."[4] The HSD service and subscriber base is a major asset. Vulnerabilities can chisel away at the revenue and do it well before the loss is measurable with current tools.

The Service Theft Problem is Real

The NCTA "2000 Report on Cable Industry Lost Revenue" indicates theft of video services is 10% throughout all service levels from basic to premium.[5] These figures occur despite the fact that it is illegal to possess cable descramblers in 32 states.

HSD networks face corner-store availability of the complete set of equipment, legal to sell and own, required to implement an extensive wired or wireless re-distribution system.

The Indications are Frustratingly Vague

The network indicators of service re-distribution, although potentially more varied than that for cable TV, can be difficult to extract and would often flag a benign situation.

Ambiguous evidence for potential service redistribution requires a more controlled response than the traditional service disconnection and personal confrontation.

Invisible Links are Difficult to Spot

On-site inspection, the major tool of cable TV service theft control, is clearly ineffective in the case of HSD propagation through wireless links.

REAL TIME MESSAGING TO ALL SCREENS BEHIND A TARGET MODEM

This paper describes the utility of an in-band communication channel that can target all workstations on suspected accounts with unblockable screen alerts. It can utilize these invisible links to reach all hidden workstations. It is an effective new tool for this new problem.

Unlicensed Users Will Know They Have Been Discovered

Informational, personalized warnings are effective in dissuading service theft without the unpleasant, confrontational contact that normally accompanies service theft situations. By using the providers' own channel, it becomes a way to communicate with both the unlicensed users as well as inadvertent opportunists who grab service through the anonymous Ether of WiFi.

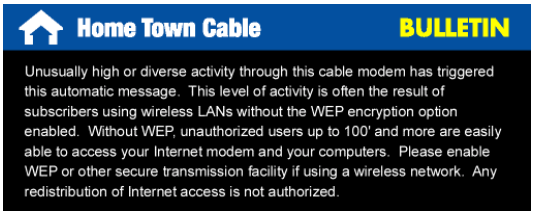

Figure 4: Sample bulletin

Immediate Messaging to Every PC User Is Not Available with Traditional Means

Up to now, there has been no reliable mechanism to reach anyone on a PC with or without a gateway. Most of a provider's subscribers don't have a known e-mail address and of those who use the provider's e-mail address, few of them check it regularly. A recent Forrester report determined that over one-third of all e-mail users change their address over the course of a single year. The variety of incompatible instant messaging systems is not useful, and not just because of the incompatibility.

Many providers are opposed to maintaining a software component on subscriber PCs. Software components rapidly degenerate to nonfunctionality. And, a sizable portion of subscribers will blame any malfunction of their computer on the provider-installed software.

Other Communications Channels are Unreliable and Untimely

Telephone calls go unanswered, door knocks are expensive and have many other problems, and bill stuffers are mostly thrown away, unread.

Creating a Mechanism to Allow the MSO to Use their Own Channel to Communicate with Subscribers

The normal Internet Protocol does not provide for any communications to a browsing subscriber except for the pages

that are requested from the destination site or from pages, in turn, linked from the destination site.

The constraints of the carrier-grade requirement of the MSO limits the opportunities for a solution and defines the requirements:

- Absolutely no software or configuration change required at the subscriber PC
- Operational on any workstation, PC, Macintosh, Linux, or other device with a browser even through wireless links
- Transparent to DOCSIS versions
- Operational in the presence of any gateway or firewall or pop-up blocking software
- Installation in the provider network while the network is operating
- Failsafe operation in that any failure in the delivery system does not affect the normal operation of the network
- Non-disruptive to the network operation and throughput
- Security controls to guarantee access functions from only authorized personnel and locations
- Delivery to individual targeted users or described groups with a characteristic determined by a database or subnet
- Proof-of-delivery receipt
- Delivery of fully interactive screens in order to provide abuse warnings and, in the case of virus contamination alerts, a screen that also includes the remedy

The facility to accomplish this type of communication that meets the above requirements was developed in 2002 and deployed testing has begun by Perftech Bulletin Services and the MSO WideOpenWest.

The installation consists of router-attached devices called Bulletin Directors that are distributed to aggregation routers

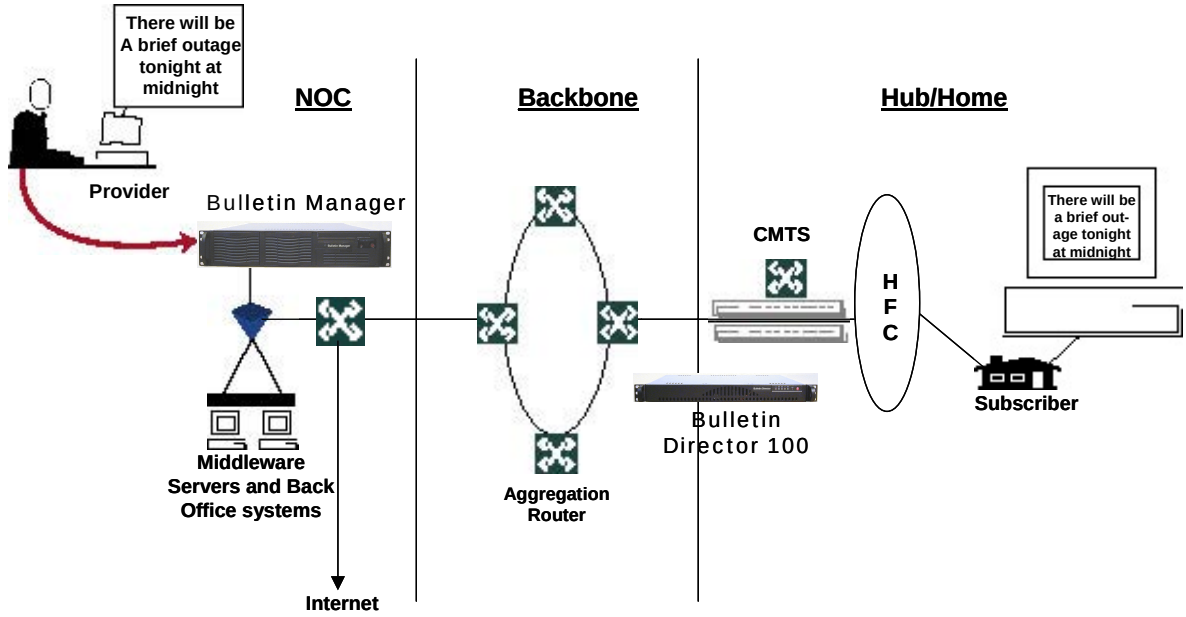

Figure 5: Sample network configuration

and a management device that administers the policies for bulletin delivery.

Installation takes place while the network is up and running using a fail-safe layer 4 redirection only of upstream port-80 traffic. None of the downstream traffic or other upstream traffic passes through the director devices assuring both performance and privacy. There is no measurable impact on network throughput.

As expected in the initial deployment, installation was made into an operating network and the network performance was unaffected. Test bulletins are successfully delivered to the targeted accounts.

How It Will Be Used

The communication can be used to warn and stop likely abusers by dispelling the illusion that "they don't know I'm here." Every unlicensed screen will display a selected alert whether inadvertently or intentionally involved in the theft of service. Warnings can become sufficiently insistent that surfing becomes difficult.

The result can be expected to turn many unlicensed users into paying subscribers. An analysis by Time Warner Cable as presented in "Cable And Broadband Security Case Study: The Broadband & Internet Security Task Force"[6] demonstrated that nearly 1/3 of all discovered unlicensed cable TV connections were turned into paying subscribers. Unauthorized re-distributors can also be turned into commercial accounts when they need to continue the re-distribution.

An Economical Solution

The cost of this solution is a small. Amortized over several years, the cost per subscriber is in cents per year. That is very small when compared to the cost of on-site visits and personal confrontation with the account holder.

A Broadly-Applicable Support Tool

Unlike cable TV or telephone service where the subscriber's premises device is a fixed, passive entity, HSD Internet broadband access is a complex technical partnership between the provider's network and the subscriber's computer and configuration — all of which is required to sustain Internet accessing activities. Immediately available provider-subscriber communication is clearly a requirement for proper support of such a system.

For those subscribers who do not know that their personal WiFi network is being abused and hacked and, therefore, insecure, the revelation is welcome.

Advance-warnings of system outages would be more than welcome by users who have incorporated the Internet access into critical work-at-home activities, stock trading, or auction participation. It would also be welcome at the provider's support call center where the call floods that accompany such outages would be significantly diminished.

Alerts should be issued about temporary outages in subsystems such as e-mail servers. Informed users are not likely to be participants in call floods and are likely to be less agitated and more understandable when kept informed.

Instances of disruptive network operation due to virus contamination in a subscriber's PC can demonstrate the value of immediate, interactive communication to handle this difficult support problem. In this case, the subscriber can be delivered an alert

immediately upon being seated at the PC and browsing. The alert would contain an explanation along with a button that would be a remedial link to decontamination facilities.

CONCLUSION

Theft of service is going to get worse. Support problems are going to get more severe and complex. The subscriber population is going to keep growing at a very high level. The provider's own communications channel is the key tool in the control of all these issues.

CONTACT INFORMATION

Jonathan Schmidt
Vice-President Business Development
210-349-7152
jon@perftech.com

REFERENCES

[1] Steven M. Bellovin, "A Technique for Counting NATted Hosts," from AT&T Labs Research, Nov. 2002.
[2] Forward Concepts, Feb. 2003
[3] InStat/MDR, Feb. 2003
[4] Saul Hansell, "In Broadband, Comcast Lets Users Find Their Own Flourishes, " New York Times, March 17, 2003
[5] "2000 Report on Cable Industry Lost Revenue," NCTA, March 20, 2003
[6] "Cable And Broadband Security Case Study: The Broadband & Internet Security Task Force, Tap Audit," Time Warner Cable, Syracuse, NY Division