SECURING DOCSIS CABLE NETWORKS

Annie Phan
Cisco Systems

Abstract

It is a fact that within all shared networks; there is inherent security risk. Allowing multiple entities access to shared network resources carries with it a number of known vulnerabilities. DOCSIS cable IP networks, because they are based on a shared network architecture are prone to violation of data privacy, theft-of-service attacks, and denial-of-service attacks. However, cable IP networks can be easily protected from these attacks and can supply a level of security roughly equivalent to that of an unshared access medium.

The intended audience for this paper is cable operators who are deploying or wish to deploy data over their networks today.

INTRODUCTION

Network attacks are the result of vulnerable spots within a network subjugated to the advantage of a malicious user. Types of typical network attacks are violation of data privacy, Theft-of-Service, and Denial-of-Service.

All edge and aggregation devices, including IP gateways, billing agents, file servers, and provisioning systems need to be protected accordingly. Standard procedure network protection such as locking down devices, OS hardening, firewalls, and intrusion detection are viewed as best practice security for all shared networks.

This paper will assume that best practice network security has been employed at the cable operator site and will focus primarily on the last mile of the broadband cable data network.

TYPES OF NETWORK ATTACK

Violation of Data Privacy

Violation of data privacy happens when a user gains unauthorized access to data that is sensitive in nature. The data can become at risk for being tampered with, destroyed, or distributed. The information found in a user's email, Internet browser, online banking, or any other personal software application is considered confidential. When a violation of data privacy happens, this confidentiality becomes compromised.

Theft-of-Service

A Theft-of-service attack is when a user illegitimately uses a service, which should be paid for. In a cable network, a Theft-of-Service attack is when a cable modem gains network access and services without a legitimate subscription to the cable operator.

Denial-of-Service

When a network or services supplied by the network partially or entirely fail to function due to malicious activity, it is considered a denial of service. A user or several users are usually unable to access the network or services supplied by the network in this type of attack. A subset of Denial-of-Service attacks is distributed Denial-of-Service attacks. Man-in-the-middle attacks are also known as a type of distributed Denial-of-Service attack. In a distributed Denial-of-Service attack, a host or several hosts are unknowingly

utilized in a schema that prevents the network to function normally.

VULNERABILITIES RELATED TO DATA PRIVACY

Static IP Addressing

Cable modems are frequently provisioned with fixed IP addresses. Once the customer premise device (PC or modem) receives its IP address dynamically, it will keep that IP address persistently. This is a convenience for cable operators which simplifies provisioning and billing

Static IP addresses imply that the layer three identity of a subscriber stays fixed and an individual subscriber is easily identifiable at all times. A "sitting duck" scenario is created for the subscribers. Unlike dial-up Internet services, where the session is ephemeral, broadband cable is always on.

The threat is that once a malicious entity learns the IP address of a host, that host is susceptible to repeated attempts at compromise.

IP addresses of customers can be easily discovered using a port listening device called a "port scanner" connected to the shared network. These devices are commonly used in networks to monitor network traffic types and levels. More commonly known as packet sniffers, they are typically used for legitimate purposes and are readily available to any interested party.

Unauthorized Access Using Netbios

If enabled, NetBios can allow unauthorized access to a host whose IP address was learned from a packet sniffer. The NetBios protocol, a file and print sharing protocol common to Microsoft Windows Operating Systems, is a common mechanism by which user data is compromised. In a trusted network, where all users on the LAN are actively managed,

NetBios can be very useful. However, since cable IP networks are a shared medium with unmanaged hosts, NetBios if not properly enabled, is a relatively easy vulnerability to exploit.

The most frequently identified security holes for subscribers on cable IP networks are NetBios vulnerabilities. Broadband subscribers may unknowingly have ports enabled for file sharing with untrusted users on the same local cable segment. The opportunity exists for any files that contain sensitive information on the customer's hardrive to be exposed to untrusted users. Because many PC vendors install operating systems with file and print sharing enabled by default, many users are unknowing exposed to violation of their data privacy due to vulnerabilities associated with "sharing" services.

Sensitive information such as tax returns, address books, and password files that may exist on a user's PC may be viewed or even tampered. Since the vulnerability exists at the user's PC, a cable operator should encourage their subscribers to disable features such as NetBios when it is not in use for legitimate purposes.

SECURING DATA PRIVACY

Baseline Privacy Interface 1.0

Securing the subscriber's identity and sensitive data should begin at the cable modem. The Data-Over-Cable Service Interfaces Specification (DOCSIS) version 1.0 features a Baseline Privacy Interface (BPI) Specification to improve the security of data privacy over cable networks. The purpose of BPI is to provide a fundamental level of protection for all devices that

attach to the cable modem network. When BPI is enabled, it helps prevent a user from passively listening on the cable network to learn sensitive information that was passed in the clear from neighboring modems.

The primary goal of BPI is to secure data privacy. BPI encrypts all traffic flows between the cable modem and cable modem termination system (CMTS).[1] This is helpful for protecting sensitive data that is exchanged across the RF portion of the cable network.

BPI uses 56-bit DES encryption to encrypt traffic in both the upstream and downstream directions. This affords cable modems roughly the same security found at the last mile in point-to-point circuit based networks. The Baseline Privacy Key Management (BPKM) protocol outlines the encryption algorithm used to exchange public-key information for the traffic exchanges between cable modems and CMTS.

Baseline Privacy is not enabled by default on cable modems, but it can be easily enabled through the DOCSIS configuration file. Once BPI is enabled, minimal utilization of the cable modem's CPU is used because BPI encryption and decryption occurs within cable modem chipsets. In other words, there is negligible change in performance when BPI is enabled on all devices of the cable modem network.

VULNERABILITIES RELATED TO THEFT-OF-SERVICE ATTACKS

Theft-of-Service attacks are typically committed through device cloning or device spoofing. These methods can be used in Denial-of-Service attacks as well. This section of the paper will discuss MAC address, IP address, and software spoofing in relation to Theft-of-Service attacks.

Weak User Authentication In BPI 1.0

In a DOCSIS 1.0 network, BPI mainly protects against unauthorized access to personal data using strong data encryption. BPI 1.0 does not have any type of authentication distribution protocol between the cable modem and CMTS; hence it does not provide strong protection from theft of service. MAC address spoofing can bypass BPI in this case, despite the encryption between the CMTS and cable modem, since there lacks authentication between them. In a "best practice" security model, strong protection is constructed upon not only strong encryption, but also strong authentication. Authenticating users in a cable environment becomes critical to protection against cloned devices.

IP Address Cloning and Spoofing

In networks where BPI is not enabled, a user could easily have the ability to learn the IP addresses that are in use. Using a packet sniffer, a user can learn the entire network structure, if all the relevant IP address information is left unencrypted. The threat is that a user can clone an IP address or spoof an unused IP address in the fixed range of addresses provisioned by the cable operator and then commit a theft of service.

Even with BPI enabled, a poor IP addressing scheme can still fall at risk to theft of service. Suppose the cable operator took a simple approach to IP address provisioning, where all cable modems reside in a single class of addresses. The entire cable modem network would become a flat structure with a single autonomous class of IP addresses, with no classification between different groups of users. As a feature, all DOCSIS cable modems have their IP addresses provisioned via DHCP. Essentially, DOCSIS cable modems are self provisioning, similar to "plug and play".

The threat is that a user who is not a current broadband subscriber will have the ability to place their modem anywhere on the network, automatically be provisioned with an IP address via DHCP, and thus gain network access illegitimately. It is for this reason it is advisable to configure multiple scopes within the DHCP provisioning server.

Multiple scopes allow the flexibility to differentiate between new (untrusted) cable modems and existing subscriber (trusted) cable modems. A default scope can be created such that it will have limited or no public Internet access for devices that have not yet been subscribed. Additional configuration in the network on routing or switching gateways will be needed to accommodate the different scopes and limit access control.

Once a subscriber contacts their cable operator to properly register their cable modem, the MAC address of the device is manually put into the provisioning system. From there the subscriber's cable modem will be tracked for billing and placed in a new IP address scope. The new subscriber will have to reset their cable modem so that it will request a new address from the new scope during initialization. Then the cable modem will be granted complete network access with the new IP address.

Again, this method does not include strong authentication for cable modem users. If a user had the ability to learn a legitimate subscriber IP address, bypassed the DHCP server and spoofed the address; there would be nothing to prevent network access to this user. This is despite if the network was configured within a hierarchal IP address scheme. There still remains the threat of theft of service or even denial of service once a malicious user clones or spoofs an IP address.

Software Spoofing

In a DOCSIS cable network, a cable modem will download via TFTP a binary configuration file after it has completed DHCP negotiation[2]. This is one of the final steps before the modem can become completely registered. Pertinent provisioning information about the cable modem including IP gateway, upstream bandwidth, downstream bandwidth, quality of service, software image and privacy can be specified by the DOCSIS configuration file.

The threat is that a user could access the DOCSIS configuration files by either compromising the existing TFTP server on the network or copying an existing file traveling across the wire, and tamper with the existing parameters of the file. Users can even compile their own DOCSIS configuration files for their own modems.

A user could commit a theft of service by using the DOCSIS configuration file to provision more upstream or downstream bandwidth for their cable modem. A user could also illegitimately trigger a new software image update through the DOCSIS configuration file and gain access to later feature sets in later software image updates if available on the TFTP server. The threat is that a user could upgrade the software image of their cable modem to an image meant for a higher-class user (i.e. business class with commercial services) without having to pay for that upgrade.

PROTECTION AGAINST THEFT-OF-SERVICE ATTACKS

Baseline Privacy Plus Interface

Authentication of cable modems on a DOCSIS network was addressed in DOCSIS version 1.1[3]. In DOCSIS 1.1 the new and improved BPI was created. It is called the

Baseline Privacy Plus Interface (BPI+). BPI+ uses RSA encrypted digital certificates to authenticate cable modems on the network. [4] It is substantially more difficult for a user to fake an embedded digital certificate than it is to spoof or clone MAC addresses. In the BPI+ specification, each cable modem uses a unique X.509 digital certificate that is issued by the cable modem manufacturer. This gives the CMTS the ability to strongly authenticate cable modems before they can successfully register online.

BPI+ inherited all the strengths that came with BPI. BPI+ protects data privacy using the same 56-bit DES encryption. Like BPI, all BPI+ encryption and decryption occurs at the hardware level, which means the performance impact is negligible when enabled across all devices in the cable network. BPI+ is not enabled by default, but it can be easily enabled through the DOCSIS 1.1 configuration file in the same fashion BPI was. It is advisable to always have BPI+ enabled to protect against theft of service. The authentication found in BPI+ helps protect against violation of data privacy, MAC address spoofing/cloning, and IP address spoofing/cloning.

IP Address Provisioning

To fend against users that are sophisticated enough to spoof an IP address by bypassing the cable operator's DHCP server, some CMTS manufacturers have decided to leverage the DHCP process for an additional level of cable modem monitoring. For example, Cisco Systems' CMTS line has the ability to verify MAC address and IP address pairs by reading the option 82 relay-agent option of DHCP.

Cisco Systems' CMTS will compare the IP address that the MAC address is trying to register with against what the DHCP server has already recorded within its scope(s). If for any reason, a cable modem and IP address pair exists that does not match against the pair found on the DHCP server, the CMTS can deny access to the mismatched MAC address. This provides authentication between the cable modems and CMTS at a layer 3 level. This prevents a user from registering online with a modem that has a cloned or spoofed IP address.

Although all DOCSIS 1.0 and DOCSIS 1.1 certified cable modems are required to receive their IP address via DHCP[5], not all DOCSIS certified CMTS's leverage the option 82 relay-agent information in DHCP. Cable operators should make themselves familiar with the IP security features that are available on their CMTS by checking with the manufacturer.

DOCSIS 1.1 Named Service Class

Quality-of-Service (QoS) profiles, that include upstream and downstream bandwidth specifications, can be created on DOCSIS 1.1 CMTS's. QoS profiles combined with named service classes eliminate the need to distribute QoS information in the DOCSIS configs files via TFTP. Cable operators with DOCSIS 1.1 CMTS's can provision cable modems with a named service class and then associate those modems with the QoS parameters configured on the CMTS. This moves sensitive information off of the TFTP server.

This provides a level of security mainly because it alleviates the need to protect a targeted TFTP server, also the parameters that a malicious user would typically tamper with, such as allocated bandwidth, no longer have to remain on the TFTP server. The added benefit of having the QoS parameters specified by the CMTS is that all interaction between the CMTS and the cable modem can be additionally secured with BPI enabled.

Common Open Policy Server (COPS)

In the DOCSIS 1.1 specification, cable modems authenticate with a Common Open Policy Server (COPS). This affords the cable operator greater authentication that extends beyond BPI+. This protocol uses a client/server model that maintains message integrity and reliability.[6] COPS is a stateful protocol in that it allows the server to push configuration information to the client, and then allows the server to remove that information from the client when it is no longer applicable. This helps prevent modems from unauthorized access on the network, thus curtailing theft of service.

TFTP Server/ DHCP Server Hardening

The DHCP server and TFTP server portion of the cable operator network is critical. To prevent compromise of these servers, best practice network security measures need to be employed. Firewalls should be implemented to keep all unwanted or unexpected traffic out. For security that extends beyond packet filtering, Intrusion Detection Systems (IDS) can be used. An IDS can listen to all traffic and monitor for any inconsistencies in the traffic. An IDS has the ability to flag interesting traffic and in some cases police against attack. These measures are not only used to ward against Theft-of-Service attacks but also against Denial-of-Service attacks as well.

VULNERABILITIES RELATED TO DENIAL-OF-SERVICE ATTACKS

Denial-of-Service (DoS) attacks are generally initiated by the exploitation of vulnerabilities within the cable operator site and not within the last mile of the cable network. This is mostly because critical devices whose failure would cripple the network and services supplied by the network reside at the cable operator headend. Distributed DoS attacks do usually utilize the last mile of the cable network in order to gain anonymity during attack as well as to launch attacks from many more hosts in order to overwhelm the network or network services.

IP Redirects

The IP address information of default gateways, time servers, TFTP servers, and name servers supplied by the DHCP policy for DOCSIS cable modems. . If a user were able to compromise the DHCP server they could redirect all IP traffic to a bogus IP address or their own server. This could create a large-scale Denial-of-Service attack, since all connected cable modems would be unable to register properly or be denied network service.

Man-in-the-Middle (MitM)

A Man in the Middle is an exploit that targets the victims TCP based applications like Telnet, rlogin, ftp, mail application, web browser, etc. Without BPI enabled across the cable network, any connected user could become prone to having their system compromised. A malicious user could sniff packets from the network, modify them, and then insert them back into the network. An attacker can grab unencrypted confidential information from a victim's network based TCP application. The authenticity and integrity of the data would then be compromised, at which point the victim could be denied service.

Distributed Denial-of-Service

If a malicious user were able to compromise multiple systems, they could attack the network on a wide scale. Assuming control of multiple customer premise devices throughout the cable modem network, a distributed DoS attack is possible. Broadcast storms could be initiated

throughout the network, overloading CPU utilization of critical gateway routers and switches. The result would be large numbers of subscribers unable to reach the network.

PROTECTION AGAINST DENIAL-OF-SERVICE ATTACKS

Perimeter Security Measures

As stated earlier when protecting critical devices from Theft of Service, the cable operator site should employ perimeter security measures such as firewalls and intrusion detection systems to decrease the incidence of attack. Best practice security measures can defend against IP redirects, broadcast storms, and other types of DoS attacks. The main idea is to have strong access control to all critical gateway systems.

Firewalls are stateful packet filters, which can police access to and from a host. Firewalls have the ability to filter by source, destination, and message type. Access control lists (ACLs) have the ability to limit telnet access, web browsing, and FTP usage. Firewalls can be employed to control access to critical gateway systems.

As mentioned earlier Intrusion detection systems (IDS) listen to all traffic and monitor for any suspicious activity. The IDS has the ability to identify specific signatures that indicate a host may intend to initiate a broadcast storm or transmit a packet with tampered headers. When suspicious activity is identified, the IDS will send an alarm. If configured properly, it can also react against particular types of attack. The IDS can block offending traffic with dynamic Access Control Lists (ACLs) or reset the offending connection.

Securing Data Privacy

Enabling BPI or BPI+ will lessen the likelihood of a user taking control of its neighboring modems, since the 56-bit DES encryption discourages compromise. With the additional authentication found with BPI+, users will be discouraged from unauthorized access on the cable network as well.

CONCLUSION

Broadband cable subscribers need to trust the cable operator. However, due to security risks, cable operators must always be wary of subscriber behavior. Security is an ongoing process as opposed to a one-time event. The threats on any given network are not necessarily representative of all the vulnerabilities within the network, as much as it is the human factor, which exists there. In the future, stronger encryption for user authentication and data privacy should be expected.

---

[1] Baseline Privacy Interface Specification SP-BPI-I03-010829

[2] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification (Released v1.0 SP-RFIC01-011119

[3] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification (Interim v1.1 SP-RFIv1.1-I07-010829)

[4] Baseline Privacy Interface Plus Specification SP-BPI+-I07-010829

[5] Data-Over-Cable Service Interface Specifications, Radio Frequency Interface Specification (Released v1.0 SP-RFIC01-011119) (Interim v1.1 SP-RFIv1.1-I07-010829)

[6] Common Open Policy Server Specification RFC2748