Securing Networks in the Broadband Age

SPRING 2017

INFORMED™
INSIGHTS

CableLabs®

CableLabs

Founded in 1988, CableLabs is the Innovation and R&D Lab for the global cable industry. With a strong focus on innovation, CableLabs develops technologies and specifications for the secure delivery of broadband internet access, video, voice and next generation services. It also provides testing, certification facilities and technical leadership for the industry.

CableLabs' mission is to enable cable operators to be the providers of choice to their customers. CableLabs currently has 55 members across four continents.

Inform[ED] Insights

With this report, CableLabs is launching its Inform[ED] Insights series, which will periodically address major technology developments that have the potential to transform the cable business and society at large.

The cable industry connects and entertains people across the globe, contributing significantly to economic growth and enabling rich discourse in our countries of operation. Inform[ED] Insights will provide leaders across sectors and disciplines with communications technology facts and insights on which to base decisions of significance.

The cable industry is a leader in the development of security technologies for the delivery of video and broadband Internet access services.[1]

From its earliest days providing video service, cable operators have faced attackers seeking to steal service, customer data, and video content. As cable operators expanded their offerings to include broadband Internet access and other services, the attacks have only grown in breadth, volume, and sophistication. This paper provides a high-level, technical overview of the technologies and other cable industry efforts to ensure the secure delivery of video and broadband services. These efforts include:

- Protecting the delivery of high-value video content for over 30 years through the implementation and continual improvement of a Conditional Access System (CAS) that has never been breached in a successful, scalable manner.
- Setting fundamental broadband security features through cable Internet access standards for over 20 years to ensure the confidentiality, integrity, and availability of cable broadband services, globally.
- Operating one of the largest public key infrastructure (PKI) systems in the world, enabling trust and authentication for devices connected to the cable network, with over 500 million security certificates issued to date.
- Widely deploying systems that are designed to detect compromised customer-owned devices controlled by botnets.
- Protecting against widespread broadband service outages through the deployment of distributed denial of service (DDoS) mitigation systems to protect cable networks.
- Advancing security standards in the Internet of Things (IoT), including chairing the Security Work Group of the Open Connectivity Foundation (OCF), an umbrella industry body dedicated to IoT.
- Enabling cable-based security technologies to be leveraged in the wider Internet ecosystem, including in Wi-Fi hotspots, smart grid devices, and medical communications, through CableLabs' subsidiary, Kyrio.
- Providing broad-based technology thought leadership on security through substantial contributions to the Internet Engineering Task Force (IETF), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), Wi-Fi Alliance, and the Broadband Internet Technical Advisory Group (BITAG), among other leading technical bodies.

[1] This paper focuses on the technologies and efforts of the cable industry to secure the delivery of video and broadband Internet access services. Although outside the scope of this paper, the cable industry has also invested substantially in securing its other service offerings, including voice (VoIP) services.

Broadband service continues to become more integral to economic activity and social connectivity. The number of connected people and devices continues to grow, as does broadband network capacity and performance.[2] Security provides the fundamental trust that enables these trends, and as the Internet ecosystem grows, all actors must make it a priority. The cable industry's security expertise and investment positions it to play a constructive role in this rapidly evolving, global challenge.

[2] See CableLabs Inform[ED] Insights, ***Cable Broadband Technology: Gigabit Evolution***, Fall 2016. http://www.cablelabs.com/cable-broadband-technology-gigabit-evolution/.

Contents

1. Security Evolving

Cable operators have long incorporated security to protect the delivery of cable services. From the earliest days, cable operators have faced attackers seeking to steal video service, customer data, and video content. With broadband Internet access service, cable operators faced new attacks based on a very different threat landscape and attack vectors. The details and motivations of attacks continue to evolve as does the security incorporated by cable operators. Without sufficient security, a cable operator would be unable to license or deliver video content, or provide a reliable Internet connection.

Globally, the cable industry provides video service to over 394 million subscribers and connects over 173 million subscribers to the Internet.[3] In the United States, cable operators provide video service to approximately 53 million subscribers and broadband Internet access service to approximately 63 million subscribers.[4]

Public concern over cybersecurity continues to grow with the ever-increasing attacks on Internet users and the Internet infrastructure itself.[5] Although attacks on Internet users and infrastructure are not new,[6] these increasing attacks are being driven in part by the rapid increase in the number of Internet-connected devices (e.g., “Internet of Things” or “IoT”) and the general lack of security incorporated into these connected devices.[7] Insecure IoT not only creates risk for individual end-users, but also for the basic functioning of the Internet more broadly, as compromised devices can be used by hackers to launch DDoS attacks that can take down networks and major online services by sending deluges of superfluous traffic.

Although IoT creates a new dimension of risk, cable operators continue to build on their security experience to ensure the availability of broadband Internet access service. This paper provides a high-level overview of the history of security in the cable network and the technologies and techniques incorporated today to ensure the secure delivery of

[3] Industry Data, NCTA (Sept. 2016), https://www.ncta.com/industry-data.

[4] Global Multichannel, SNL KAGAN, https://www.snl.com/web/client?auth=inherit#industry/globalMultichannelComp (last visted Apr. 5, 2017).

[5] ***See, e.g., Kim S. Nash & Sara Castellanos, WikiLeaks Spotlights IoT Vulnerability***, THE WALL STREET JOURNAL (MAR. 8, 2017 5:02 PM ET), http://blogs.wsj.com/cio/2017/03/08/wikileaks-spotlights-iot-vulnerability/; David E. Sanger & Nicole Perlroth, ***A New Era of Internet Attacks Powered by Everyday Devices***, THE NEW YORK TIMES (Oct. 22, 2016), https://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-Internet-attacks-powered-by-everyday-devices.html?_r=0; Andrea Peterson, ***Can Anyone Keep Us Safe From a Weaponized ‘Internet of Things’?***, THE WASHINGTON POST (Oct. 25, 2016), http://wapo.st/2dGeRu9?tid=ss_tw; Consumer Reports to Consider Cyber Security in Product Reviews, REUTERS (Mar. 6, 2017), http://www.reuters.com/article/us-cyber-consumerreports-idUSKBN16D0DN.

[6] ***See, e.g.***, Center for Strategic and International Studies, ***Significant Cyber Incidents Since 2006*** (last visited Apr. 11, 2017), https://www.csis.org/programs/technology-policy-program/cybersecurity/significant-cyber-incidents.

[7] ***See, e.g.***, 2016 Internet Security Threat Report, SYMANTEC 16 (Apr. 2016), https://www.symantec.com/security-center/threat-report; Technology, Media and Telecommunications Predictions, DELOITTE 6-8 (2017), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf.

video and broadband services. The paper also highlights the cable industry's efforts to drive increased security in the broader Internet ecosystem. The discussion is generally representative of cable operators, but each cable network operates independently and adopts its own security practices.[8]

2. Cable Networks & Security

A cable operator runs a single physical network with multiple distinct and separate logical networks.[9] This paper focuses on two of those logical networks: One is the network for traditional cable video delivery (e.g., digital broadcast television, that is, video delivered over the cable network, but not over the broadband Internet access connection). The other network is for the provision of broadband Internet access service. The cable network does not, of course, encompass the entire network for video and Internet delivery and, therefore, does not allow a cable operator to secure the end-to-end delivery of video service and Internet access. As seen in Figure 1 below, although the traditional video delivery and Internet delivery are two separate logical networks, they are operated over the same physical (coaxial cable and optical fiber) medium.[10] Even though a cable operator provides video and broadband services over the same medium, video and

[8] Moreover, the paper provides only an illustrative review of the technologies, techniques, and efforts of cable operators in securing the delivery of video and broadband services and the cable industry's security efforts in the broader Internet ecosystem, rather than comprehensive or exhaustive review.

[9] This paper focuses on the logical networks that cable operators use to deliver traditional video and broadband Internet access services. A cable operator may also have additional logical networks for the delivery of analog video, video on demand, and voice (VoIP) services.

[10] Cable networks are often composed of both portions of coaxial and fiber optic cable, together known as hybrid fiber coaxial (HFC) network.

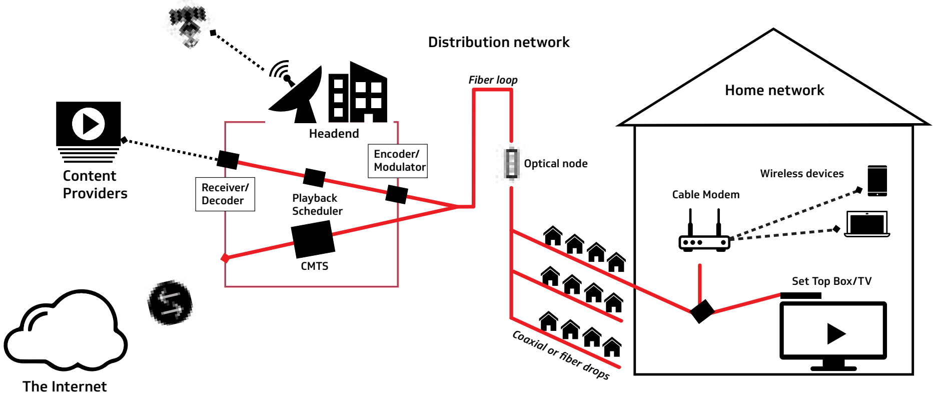

Figure 1: The Cable Network for Video and internet Service
Red Lines Show the Cable Video and internet Networks

broadband data are transmitted over separate channels (or frequencies) and the encoding of the video and broadband are different and not interchangeable, inherently adding a layer of protection to each service from intrusion by the other.
Traditional video delivery has changed dramatically since the late 1940's when cable got its start in delivering television signals to homes that, due to mountains and other geographical features, could not receive over-the-air broadcast television. As show in Figure 1, video is delivered via satellite, fiber or microwave to the cable operator's headend for placement on the cable network. At the cable headend, the video signal is processed and encrypted for delivery over the cable plant, which includes delivery to the optical node and, ultimately, to the home.

Cable operators are part of a larger ecosystem of security, with a primary focus on protecting the services as they are delivered over the cable network. Much as a cable operator can only begin securing video when the video enters the cable operator's network, a cable operator can only protect Internet access traffic while it's on the cable operator's network. As illustrated in Figure 1, cable broadband service generally consists of the connectivity from a subscriber's cable modem, in a subscriber's home or business, to the cable modem termination system (CMTS), which is typically located in a cable operator's headend, and over the cable operator's core network, connecting to the broader Internet.

While the cable operator's focus is primarily on protecting its network to ensure the availability of broadband service, cable operators recognize that cybersecurity is a shared responsibility across the entire Internet ecosystem. To this end, the cable industry actively participates in standards bodies to drive security-by-design into technologies both upstream and downstream from cable's provision of broadband Internet access service. For instance, CableLabs has had a positive impact in these standards bodies, taking security leadership roles in a number of standards bodies, such as the Open Connectivity Foundation, which provides standards for the Internet of Things, and in the Wi-Fi Alliance, which sets standards for Wi-Fi technology.[11]

[11] See discussion ***Driving Security in the Broader Internet Ecosystem***, supra p.11.

3. Securing Cable Video & Broadband Services

The cable industry has always faced adversaries that sought to attack and compromise the networks and services offered by cable operators. This was true during the early years of the cable industry in the delivery of linear video and the attacks have only increased as cable operators have added additional services, most notably broadband Internet access. To continue to provide the quality of service that consumers expect, the cable industry has continued to innovate to address each new security threat.

A. Securing the Delivery of Cable Video Service

The cable industry has a long history in securing its video delivery to minimize theft of service or pirating of content.[12] Since cable's adoption of digital video delivery in the mid-1990's there has been no successful, scalable attack on cable's video security. As described below, Cable operators use a layered, end-to-end approach to security to ensure video content is delivered as intended while minimizing the risk of piracy.

Since cable's adoption of digital video delivery in the mid-1990's there has been no successful, scalable attack on cable's video security.

Security for the Delivery of Traditional Cable Video Service – from Headend to Television. Cable operators use a conditional access system (CAS) to provide security for the delivery of video content from the headend to the set top box. In the U.S., the Advanced Television Systems Committee (ATSC) standards are the basis of cable operator CAS. In comparison, European cable operators use a system based on the Digital Video Broadcasting (DVB) standards, SimulCrypt and MultiCrpyt. While ATSC and DVB CAS are not interchangeable, they both contain three essential physical elements: (i) broadcast equipment at the headend that encrypts (scrambles) and transmits video to the set top box, (ii) set-top boxes that receive signals and transmit them to a security module (typically dedicated hardware) within the box, and (iii) the security module that determines if the set top box is authorized to receive the video and decrypts accordingly.

In general, the protection of traditional video service is comprised of three separate cryptographic keys. The first is the secret key, called the "Control Word," that is used to "scramble" the video signal. The security module must be continuously informed of the

[12] Moreover, cable operators have a long history in protecting subscriber privacy, as required by law. ***See, e.g.***, 47 U.S.C.A § 511 (limiting what a cable operator can do with subscriber personally identifiable information, e.g., to provide the cable service and detect unauthorized use of the cable service).

current Control Word so that viewing is uninterrupted. The second part is the Entitlement Control Message (ECM), which is the mechanism used to pass the Control Word from the Headend to the set-top box and, in turn, to the security module. The ECM is encrypted to protect the Control Word during transmission. The third part is the Entitlement Management Message (EMM), which is also encrypted and provides the security module with the authority to decrypt the ECM and use the Control Word to unscramble the video signal. The EMM is typically changed on a monthly basis while the Control Word and ECM are changed much more regularly, typically on the order of seconds.[13]

The video signal is also protected between the set top box and the television, or video display monitor. Since 2003 cable set top boxes have used the High Definition Multimedia Interface (HDMI) output for connecting set top boxes to televisions/video monitors.[14] An HDMI output contains High-bandwidth Digital Content Protection (HDCP). HDCP provides encrypted video between devices, such as set-top boxes and televisions. Manufacturers of devices must receive a license to use HDCP from Digital Content Protection. This license places requirements on the device receiving the HDMI output to meet certain conditions for protecting video content. Manufacturers licensed for HDCP receive a digital key that is used to maintain encryption between devices. HDCP has gone through several versions in response to compromises and to add technical features.[15]

Secure Delivery of Video Service Over the Internet. Cable operators continue to innovate in the delivery of video content, including the delivery of video content over the Internet. As the nature of video service continues to evolve, so have the necessary security features. Video content delivered over the Internet ("Over-the-Top" or "OTT" video) is secured using digital rights management (DRM) systems. DRM systems were originally adopted by Over the Top (OTT) video providers and more recently by cable operators to deliver cable-provided video content to Internet-connected retail devices.[16] Current generation cable set top boxes are designed to receive and render video signals received both from traditional cable video delivery services and from OTT sources delivered over the Internet by third-party providers.

B. Securing Cable Broadband Service

Building on the industry's experience in securing video service delivery, cable operators have long recognized that security of the network would be critical to the provision of

[13] Monitoring Control Access Systems, BRIDGE TECHNOLOGIES (last visited Mar. 29, 2017), http://www.bridgetech.tv/pdf/whitepaper_CAS.pdf.

[14] HDMI was founded by Hitachi, Panasonic, Philips, Silicon Image, Sony, Thomson, RCA and Toshiba and has the support of numerous content providers such as Fox, Universal, Disney, and Warner Brothers. ***Who Supports the HDMI Interface?***, Resources, HDMI (last visited Mar. 29, 2017), http://www.hdmi.org/learningcenter/faq.aspx#2.

[15] ***See*** High-bandwidth Digital Content Protection System, Revision 2.2, DIGITAL CONTENT PROTECTION (Feb. 13, 2013), https://www.digital-cp.com/sites/default/files/specifications/HDCP%20on%20HDMI%20Specification%20Rev2_2_Final1.pdf.

[16] In some instances, OTT providers will also supply a device to support their service.

broadband Internet access service. From the start, the cable industry has incorporated into its broadband service security by design as expressed through the core tenets of information security – confidentiality, integrity, and availability ("CIA triad").[17] The industry's commitment to these core tenets has continued over the past 20 years as evidenced by the continual enhancements to broadband security with each new generation of service. As part of its responsibility for cybersecurity, which is shared by all players in the Internet space, the cable industry also seeks to help drive security enhancements in broadband networks and throughout the ecosystem.

The basic technology that enables the provision of broadband Internet access service over the cable network, including the basic technology for interoperable cable modems and cable modem termination systems (CMTSs), is described in CableLabs' Data Over Cable Interface Specifications (DOCSIS® specifications).[18] The DOCSIS specification includes security protections that ensure the confidentiality, integrity, and availability of broadband service in the access network.

Security was a significant consideration in the very first version of the DOCSIS specifications, the DOCSIS 1.0 specifications issued in 1997. This security focus was driven, in part, because accessing the Internet on a DOCSIS network requires that cable subscribers use a shared network. Each subscriber's Internet traffic is transmitted over a common hybrid-fiber coaxial cable that also carries the Internet traffic of (and is accessible to) a significant group of other subscribers in the same neighborhood. In turn, the initial DOCSIS specification had to include security in its design to prevent hackers from eavesdropping on subscriber Internet traffic from the cable modem to the CMTS.

BPI – Encrypted Communications. The first DOCSIS specifications addressed security through the Baseline Privacy Interface (BPI). BPI provides a fundamental level of protection for all devices that attach to the cable modem network. BPI prevents a user from passively listening on the cable network to learn sensitive information that is transmitted to or from a household that was passed in the clear from or to neighboring cable modems. In short, BPI encrypts all traffic flows between each cable modem and the CMTS to ensure those transmissions remain confidential.[19] With DOCSIS 3.1 (the most recent release of the DOCSIS specification), a cable operator can now encrypt communications using 2048 RSA encryption, a very

BPI encrypts all traffic flows between each cable modem and the CMTS to ensure those transmissions remain confidential.

[17] *See, e.g.*, Chad Perrin, The CIA Triad, TECHREPUBLIC (Jun. 30, 2008), http://www.techrepublic.com/blog/it-security/the-cia-triad/.

[18] Specifications, CABLELABS (last visited Mar. 29, 2017), http://www.cablelabs.com/specs/.

[19] Baseline Privacy Interface Specification SP-BPI-I03-010829, CableLabs (Nov. 19, 2001), https://apps.cablelabs.com/specification/baseline-privacy-interface-specification/.

strong security standard that is further detailed below.

Secure Device Authentication through PKI. DOCSIS network security has improved over time using ever-stronger digital keys. In 2000, a Public Key Infrastructure (PKI) was adopted in the DOCSIS 1.1 specification.[20] Cable's PKI, which is managed by CableLabs' subsidiary, Kyrio, provides the same type of device authentication (protecting against rogue devices) and data encryption that is used by banks and the military.[21] Cable's PKI security allows a cable operator to authenticate cable modems on their network, permit a cable modem to access the CMTS, thereby allowing access to the cable operator's network and the Internet, and disallowing a modem to access the network in the event of a security breach. The cable PKI provides a unique, immutable, and attestable digital identity to every cable modem and CMTS on the cable plant at the time of manufacture. These digital identities, known as digital certificates, bind to the device and serve to authenticate its identity in a manner that is extremely difficult to spoof. CableLabs, through Kyrio, has issued over 500 million digital certificates combined, making cable's PKI one of the largest PKIs in the world.

Secure PKI Implementation. A PKI is only as secure as its implementation and that is in part a function of the care taken to only provide certificates to trusted organizations.[22] The digital certificate identifies the modem, the manufacturer, the certificate version and issuer, and key validity dates. Cable modem and CMTS manufacturers only receive digital certificates to insert into their cable devices after authentication of the manufacturer, such as through a DUNS number,[23] and the manufacturer has contractually agreed that it will safeguard the digital certificates and only use them in cable modems and CMTSs that are built in compliance with CableLabs specifications. This ensures that the digital certificates are not put into insecure network devices or devices designed to harm the Internet and/or those who rely upon the Internet. The manufacturer receives the digital certificates through a secure delivery mechanism. Digital certificates that are lost, stolen or otherwise compromised are revoked so as not to allow the affected device(s) access to the cable network.

Secure Software Updates. The digital certificates also ensure that only software updates

[20] Specifications, CABLELABS (last visited Mar. 29, 2017), http://www.cablelabs.com/specs/.

[21] Like banks and the military, Cable's PKI uses X.509 certificates. ***See, e.g.***, Margaret Rouse, ***Definition: X.509 Certificate***, TECHTARGET (last visited Mar. 31, 2017), http://searchsecurity.techtarget.com/definition/X509-certificate; X.509 Public Key Certificates, Windows Dev Center, MICROSOFT (last visited Mar. 31, 2017), https://msdn.microsoft.com/en-us/library/windows/desktop/bb540819(v=vs.85).aspx.

> Public key cryptography relies on a public and private key pair to encrypt and decrypt content. The keys are mathematically related, and content encrypted by using one of the keys can only be decrypted by using the other. The private key is kept secret. The public key is typically embedded in a binary certificate, and the certificate is published to a database that can be reached by all authorized users.

[22] ***See, e.g.***, Roger A. Grimes, ***Free public certificate authorities: Nice idea, big flaw***, INFOWORLD (Mar. 28, 2017), http://www.infoworld.com/article/3185484/security/free-public-certificate-authorities-nice-idea-big-flaw.html.

[23] A DUNS number is a unique nine-digit identifier used to establish a business credit file. D&B D-U-N-S Number, DUN & BRADSTREET (last visited Apr. 8, 2017), http://www.dnb.com/duns-number.html.

that come from either the cable modem manufacturer or from the cable operator can be downloaded into the cable modem. This extra level of security is achieved through special digital certificates, called "code verification certificates" or "CVCs," which are provided to the manufacturer and the cable operator. A CVC digitally signs a software update so that the software update is both encrypted and identified with its source. A cable modem will only accept software updates that are signed with the appropriate CVC. Use of a CVC to secure software updates minimizes the risk that a cable modem will be infected with malware or other malicious code as part of the software update process.

Increasing Cryptographic Strength. Cable has continued to strengthen the implementation of its PKI. As of the date of this paper, the DOCSIS specifications are at version 3.1. Cable modems and CMTSs built to the DOCSIS 3.1 specifications follow the guidelines of the National Institute of Standards and Technology (NIST) and use a 2048 RSA key for encryption.[24] It is estimated that that it would take a current standard desktop computer more than 6 quadrillion years to crack a 2048 RSA encryption key.[25]

It is estimated that that it would take a current standard desktop computer more than 6 quadrillion years to crack a 2048 RSA encryption key.

Prevention of IP Address Spoofing. Cable operators have incorporated technology to prevent the use of spoofed Internet Protocol (IP) addresses. Every device on the Internet that routes traffic or directly terminates traffic receives a public IP address and serves such purposes as allowing the end-user to reach a web page and receive email. The cable operator assigns a public IP address to each device attached directly to its network (e.g., logical router in a cable modem). Each packet sent from the device includes this unique source IP address. IP address spoofing occurs when someone creates a false IP address to conceal the identity of the device, to have a device impersonate another device, or pretend to be on a different ISP's network. While IP address spoofing has some legitimate uses, such as testing a website's performance, IP address spoofing is also used to conceal someone's identity when they are committing illegal acts and in DDoS attacks.

Cable operators are able to block outbound Internet traffic sent with a spoofed IP address at the CMTS. The CMTS checks IP packets sent from the customer premise equipment to ensure that the source IP address on the packets matches the source IP address assigned by the CMTS. If the addresses do not match, then the CMTS discards the packet. The incorporated anti-spoofing measures are very similar in substance and method to

[24] DOCIS 3.1 Security Specification, Version 107, CABLELABS (Jan. 11, 2017), https://apps.cablelabs.com/specification/CM-SP-SECv3.1.

[25] *See, e.g.*, Check Our Numbers: The Math Behind Estimations to Break a 2048-bit Certification, DIGICERT (last visited Mar. 31, 2017), https://www.digicert.com/TimeTravel/math.htm.

the Internet Engineering Task Force (IETF) standards for anti-spoofing.[26]

Protections Against Cloned Cable Modems. The cable industry continues to deploy increased security features to combat the issue of cloned modems. A cloned modem is used to steal broadband service and is also used to hide criminal activity on the Internet.[27] Cloned modems occur when one modem presents itself on the cable network interface card (NIC) which assists in connecting the device to a network such as the Internet. It is the NIC that turns the data from your device into the electronic signals that pass over the cable network and become packets on the Internet. The NIC has a media access control (MAC) address that is hardcoded into the NIC during the manufacturing process. While an IP address is used to locate a device on a network, much like a building has a street address, the MAC address identifies the NIC. Each NIC's MAC address is a unique 48-bit hexadecimal address. This unique 48-bit address translates into 281 quadrillion unique possible addresses; therefore, the likelihood of two modems with the same MAC address on the same network segment is extremely low.[28]

Cable modem cloning occurs when the MAC address and other pertinent information are taken from one modem and used in another modem. The cloned modem would then be allowed on the cable network and receive broadband service like the original modem. These attacks involve copying all or pertinent parts of one modem's firmware onto a different modem, requiring physical access to the modem as well as a high level of technical expertise, which limits the scale and scope of this risk.

The DOCSIS network has continued to evolve to provide increased security measures to thwart cable modem cloning. For example, these measures include preventing a cloned cable modem from downloading old files to further its impersonation, IP address verification, message integrity checks between the CMTS and the modem to ensure the

integrity of files downloaded from the CMTS to the modem, and using digital certificates uniquely assigned to each modem.

[26] ***Compare*** DOCSIS 3.1 Security Specification, Version 107, CABLELABS (Jan. 11, 2017), https://apps.cablelabs.com/specification/CM-SP-SECv3.1 ***with*** Ferguson, P. and D. Senie, ***Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing***, BCP 38, RFC 2827, DOI 10.17487/RFC 2827, May 2000, http://www.rfc-editor.org/info/rfc2827 ***and*** Baker, F. and P. Savola, ***Ingress Filtering for Multihomed Networks***, BCP 84, RFC 3704, DOI 10.17487/RFC 3704, March 2004, http://www.rfc-editor.org/info/rfc3704.

[27] By using a cloned modem, the criminal's activities are not associated with his or her account but rather with the account of the subscriber whose modem has been cloned. When law enforcement seeks information about the user, the cable operator is only able to provide information about the subscriber (e.g., physical address), rather than the criminal who is using the cloned modem for nefarious purposes. Owen Parsons, ***DOCSIS Theft and Cloning***, CED MAGAZINE (Mar. 5, 2013 8:52PM), https://www.cedmagazine.com/article/2013/03/docsis-theft-and-cloning.

[28] *Id.*

Customer Notification and Remediation Systems. Major cable operators have developed and deployed systems that seek to detect and identify consumer devices that have been infected by malware and are participating in a botnet.[29] Once detected and identified, cable operators notify the affected subscribers and provide information on how to address the issue. These systems use data from reputable Internet research groups that specialize in botnet identification, including a list of Internet Protocol (IP) addresses that are infected and those that belong to bot command and control channels. Cable operators then look for malicious behavior exhibited by bots such as spam, sources of DDoS attacks, and repeated connections requests to known command and control channels. This information is aggregated to confirm whether one or more of a subscriber's connected devices has been infected.[30]

DDoS Mitigation. Major cable operators have invested heavily in DDoS monitoring and mitigation systems to ensure the availability of their broadband Internet access services. A DDoS attack seeks to make a device, service, or network resource unavailable to its intended users by flooding the target with superfluous network traffic in an attempt to overload systems and prevent some or all legitimate traffic from getting through to the target of the attack. These attacks originate from more than one IP address and often from many thousands or hundreds of thousands of IP addresses. Both the frequency and magnitude of DDoS attacks continue to grow, fueled in large part by the widespread deployment of insecure IoT devices.[31]
The largest vendor of DDoS mitigation systems for ISPs, Arbor Networks, reported that their systems alone defended against more than 135,000 DDoS attacks per week as of December 2016 across all targets, including customers and network and service infrastructure.[32]

The largest vendor of DDoS mitigation systems for ISPs, Arbor Networks, reported that their systems alone defended against more than 135,000 DDoS attacks per week as of December 2016 across all targets, including customers and network and service infrastructure.

[29] *See, e.g.*, Comments of the National Cable & Telecommunications Association, In the Matter of Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware, U.S. Dept. of Commerce, Dkt. 110829543-1541-01 (Nov. 14, 2011), https://www.nist.gov/sites/default/files/documents/itl/NCTA-Comments-to-BotNet-FRN-11-14-11.pdf.

[30] Notably, given that cable operators have limited visibility into a subscriber's home network, these systems often are unable to identify the specific offending device, particularly as the number of devices in the home increases. In addition, hackers continuously adapt their techniques to avoid detection; as a result, these systems cannot provide complete protection.

[31] *See, e.g.*, Technology, Media and Telecommunications Predictions, DELOITTE 6-8 (2017), https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions.pdf.

[32] Worldwide Infrastructure Security Report, Arbor Networks Special Report Vol. XII, ARBOR NETWORKS 23, 25 (2017), https://www.arbornetworks.com/insight-into-the-global-threat-landscape.

Cisco estimates an increase of DDoS attacks over the next 5 years will be on a similar trajectory to IoT growth in general: 20%+ CAGR.[33] Currently, DDoS attacks can comprise over 10% of a country's Internet traffic while they are active, with the largest DDoS attacks now approaching a terabit per second of malicious traffic.[34] Cable operators have implemented DDoS mitigation technologies that protect their networks and guard against widespread service disruptions and outages. The most prominent network DDoS mitigation techniques involve specialized equipment that learns and identifies normal Internet traffic sources, destinations and volumes. When Internet traffic anomalies are detected, the abnormal traffic can be separated from the normal traffic so that the DDoS attack does not negatively impact Internet access broadly. However, since hackers are continuously evolving their techniques, these systems cannot provide complete protection.

Driving Security in the Broader Internet Ecosystem. CableLabs and cable operators continue to take an active role in many broader industry efforts to help drive a more secure Internet ecosystem.

- **IPv6 and Domain Name System Security (DNSSEC):** The cable industry has been a leader in the deployment of next generation IP addressing, IPv6, as well as implementation of DNSSEC.
- **National Institute of Standards and Technology (NIST) Cybersecurity Framework and FCC CSRIC:** The cable industry has engaged and provided substantial contributions to NIST's Cybersecurity Framework and the recommendations produced by the FCC's Communications Security, Reliability and Interoperability Council (CSRIC).[35]
- **Open Connectivity Foundation (OCF):** CableLabs and Comcast hold board seats, and CableLabs chairs the Security Work Group of OCF – an industry effort to develop a secure interoperability specification for IoT.[36]
- **Broadband Internet Technical Advisory Group (BITAG):** The cable industry was a driving force behind BITAG's recent report on IoT security and privacy recommendations.[37]
- **Wi-Fi Alliance:** CableLabs and the cable industry were instrumental in driving increased security into the Hotspot 2.0 specification, which is the underlying technology

[33] White paper: Cisco VNI Forecast and Methodology, 2015-2020, CISCO (Jun. 6, 2016), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html.

[34] *Id.*; Nicky Woolf, ***DDoS Attack That Disrupted Internet Was Largest of Its Kind in History, Experts Say***, THE GUARDIAN (Oct. 26, 2016 16:42 EDT), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet.

[35] *See* NIST, Cybersecurity Framework (last visited Apr. 10, 2017), https://www.nist.gov/cyberframework; FCC, Communications Security, Reliability and Interoperability Council (last visited Apr. 10, 2017), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-10.

[36] Membership List, OPEN CONNECTIVITY FOUNDATION (last visited Mar. 31, 2017), https://openconnectivity.org/about/membership-list.

[37] Internet of Things (IoT) Security and Privacy Recommendations; A Broadband Internet Technical Advisory Group Technical Working Group Report, BITAG (Nov. 2016), https://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php.

for the Wi-Fi Alliance "Passpoint" certified hotspots. In addition, CableLabs, through Kyrio, provides a managed PKI service to the Wi-Fi Alliance to secure "Passpoint" certified hotspots.[38]

- **Open Automated Demand Response (OpenADR):** CableLabs has worked with electric utilities to ensure the security of Internet-connected "smart grid" devices. Specifically, CableLabs, through Kyrio, provides electric utilities with a managed PKI service that ensures device security for smart grid and in particular, automated demand response.[39]
- **Center for Medical Interoperability (CMI):** CableLabs provides technology expertise to help ensure device and system security as CMI develops interoperability standards and specifications for the medical and healthcare industries.[40]
- **Other:** CableLabs and the cable industry have also provided technology thought leadership and contributed substantially to other broad industry security efforts, including at the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), the Internet Engineering Task Force (IETF), the Wireless Broadband Alliance, and the European Telecommunications Standards Institute (ETSI).[41]

4. Conclusion

The cable industry has a long history of securing its services from theft, abuse, and hacking. Security has been a core design element of cable services, including both video and broadband. As broadband service continues to grow, encompassing a larger ecosystem of actors and becoming more important to our economies and societies, cable is continuing its focus on security to ensure the availability of broadband service, a key enabler of connectivity. Cable is actively using its security expertise within the broader Internet ecosystem to enable the trust that must be central to an ever-expanding Internet.

[38] *See* Certificate Authority Vendors; THE WIFI ALLIANCE (last visited Mar. 31, 2017), http://www.wi-fi.org/certification/certificate-authority-vendors.

[39] *See* OpenADR and Cybersecuirty, OPENADR ALLIANCE (last visited Mar. 31, 2017), http://www.openadr.org/cyber-security.

[40] About the Center, CENTER FOR MEDICAL INTEROPERABILITY (last visited Mar. 30, 2017), http://medicalinteroperability.org/about-the-center/.

[41] Why M^{3}AAWG? MESSAGING MALWARE MOBILE ANTI-ABUSE WORKING GROUP (last visited Mar. 31 2017), https://www.m3aawg.org/about-m3aawg; About the IETF, THE INTERNET ENGINEERING TASKFORCE (last visited Mar. 31, 2017), https://www.ietf.org/about/; What We Do; WIRELESS BROADBAND ALLIANCE (last visited Mar. 31, 2017), http://www.wballiance.com/what-we-do/at-a-glance/; About ETSI; EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE (last visited Mar. 31, 2017), http://www.etsi.org/about.