The Evolution of Cable Network Security

Matt Tooley, NCTA

Matt Carothers, Cox Communications

Michael Glenn, CableLabs

Michael O’Reirdan, Comcast

Chris Roosenraad, Time-Warner Cable

Bill Sweeney, Comcast

Abstract

The challenges of protecting networks from cyber threats have evolved from computer viruses and spam plaguing desktop computers to advanced persistent threats and cloud-based multi-gigabit distributed denial of service attacks. This paper examines the evolution of the attack vectors to the DOCSIS™ networks and their associated attack surfaces. It then surveys the tools that are in the DOCSIS standards today that can be used to mitigate the threat vectors. Further it examines the evolution of cable networks technologies such as software defined networking and big data. Finally it then proposes methods to integrate software-defined networks and big data to improve the overall robustness and security of the cable networks.

CABLE NETWORK ATTACK SURFACES

We define an attack surface as the exposed, exploitable vulnerabilities that an adversary can leverage to help them accomplish their objectives. In other words, every point that a system may interact with the outside world is part of its attack surface, and each presents some amount of risk. Intuitively, the “smaller” the attack surface, the less likely a vulnerability will exist on a system that an adversary can exploit. Examples of the attack surface in the real world include (Northcutt n.d.):

- Open ports on servers with software accepting and processing packets on those ports
- Services available inside a firewall
- Software that processes incoming data, email, XML, files, and industry-specific custom data exchange formats (EDI)
- Interfaces, SQL, web forms
- Employee access to sensitive information that may be socially engineered

The attack surfaces can be further broken down into:

- Software Attack Surface – vulnerabilities exposed through applications, databases, and operating systems.
- Human Attack Surface – human vulnerabilities exploited through social engineering, human error, violation of trust by an insider, and/or employee attrition.
- Hardware attack surface – vulnerabilities existing in hardware architectures,

microcode, firmware and BIOS code specific to hardware.

- Network Attack Surface – combining vulnerabilities in a coordinated way through the network to achieve greater results than leveraging the vulnerabilities in isolation.

Software Attack Surface

We define an attack surface as the exposed vulnerabilities that an adversary can exploit to assist them in meeting their objectives. Their objections can include confidential data theft, data destruction, system or hardware destruction using software, denial of service, data or service corruption (including mis-information, inaccurate data and propaganda) and others. An important point is that vulnerabilities must be exposed to the threat actor to be used in their attack. Insecure default system configurations can create a large attack surface for adversaries.

The software attack surface includes software in consumer products that attach to the network, the customer premise equipment (CPE) such as the cable modem, the home gateways and all the other equipment in the home that connects to the network –computers, printers, smartphones, tablets, thermostats, garage door openers, and web cams. Within the operators network the software attack surface encompasses all the networking equipment such as the cable modem termination system (CMTS), and servers on the network such as the DNS and NTP servers.

Human Attack Surface

Humans are a fundamental part of the attack surface. Any device that a human interacts with can be considered part of the attack surface (Dark Reading 2012). The wide spread adoption of an always-on Internet - via its integration into a broad range of devices - has only increased the human attack surfaces as humans interact with the Internet in ever increasing ways. Humans by nature are going to continue to provide a vulnerable attack surface. Education and training can reduce the vulnerability, but at the same time attackers have improved their social engineering techniques.

Hardware Attack Surface

There seems to be an emerging form of attack which relates to the compromise / attack of hardware either at the point of manufacture or prior to delivery to the customer. These are likely to be a part of the cable infrastructure since these are pervasively deployed technologies. The best recent example of this is the Equation Group recently called out by Kaspersky and also the activities of the Tailored Access Operations (TAO) group at the NSA, which was highlighted in various documents released by Snowden.

Network Attack Surface

The network itself provides an attack surface. The sheer scale of the network infrastructure of Internet Service Providers (ISP) and their massive customer base present an incredibly attractive attack surface (Mistry 2014). Large-scale deployments of homogeneous systems create a multiplication effect when a vulnerability is discovered in those homogeneous systems. The significant available aggregate bandwidth in an ISP's network when combined with a common, widespread vulnerability, make ISPs targets for a form of attack known as a distributed denial of service (DDoS) attack that will be discussed later in this paper.

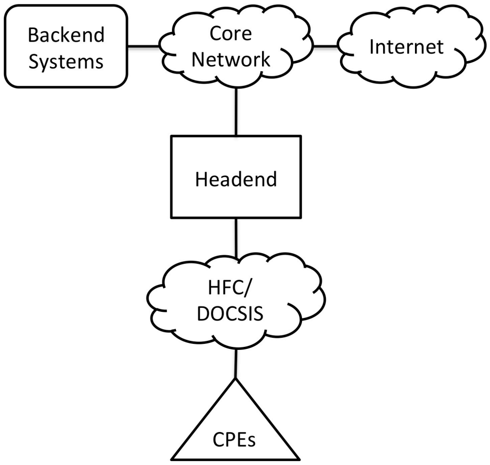

Figure 1 Cable Network

The cable network is no exception. Cable networks have a range of entry points. In addition to the home, businesses and hosting environments, the operators network infrastructure itself provides a number of entry points that include the routers and switches along with the backend processing systems.

ATTACK VECTORS AND COUNTERMEASURES

The term attack surface is used to describe the potential surface areas for the attack vectors. For this paper we define an attack vector as the method a threat actor uses to accomplish their objectives. Over the years we have seen an increase in the number of attack vectors in use with the widespread adoption of the Internet as shown by the total volume of abuse tickets logged by one operator.

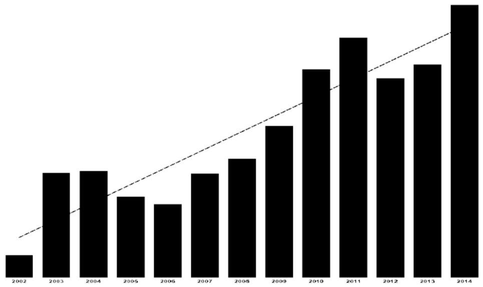

Figure 2 Total Abuse Ticket Volume 2002-2014

The abuse attack vectors can be categorized into two broad categories – penetration attacks and denial of service (DoS) attacks. Penetration attacks are those attacks that use a delivery mechanism to transport a malicious payload to the target host or system to gain unauthorized control (IT Law Wiki n.d.). According to US-CERT “a denial-of-service or distributed denial-of-service attack is an attempt to prevent legitimate users from accessing information or services.” (United States Computer Emergency Readiness Team 2013). The most common types of DoS attacks rely on flooding a network with network traffic and overwhelming the victim’s system. In addition, malicious software that prevents a legitimate user from using the intended device or service falls into this category.

Penetration Attacks

As an attack vector, the two primary forms of penetration attacks are unauthorized malicious software and unauthorized access.

Viruses & Spyware

The malicious software includes spyware, viruses, and Trojan horses, with the US-CERT team describing spyware as a type of malicious software that collects information from a computing system without the users consent (United States

Computer Emergency Readiness Team 2013).

The first computer virus is believed to be the Creeper Virus (Chen and Robert 2004) that was first detected in the early 1970s and was used to infect DEC PDP-10 computers. Until the mainstream adoption of Internet, most malware was limited to impacting only the host computer system and the user's ability to interact with the system. In some cases, once the malicious software was successfully loaded on the system, it denied the user interaction with the system.

The mainstream adoption of the Internet and the resulting expanded attack surface area, led to an increase in the malware infecting computer systems as shown in Figure 3. Note the data was not normalized for factors such as subscriber growth and improved detection capabilities. Therefore, the overall growth may not be as pronounced as shown in figure, but even without normalizing the data we can discern a continued upward trend in malware detected.

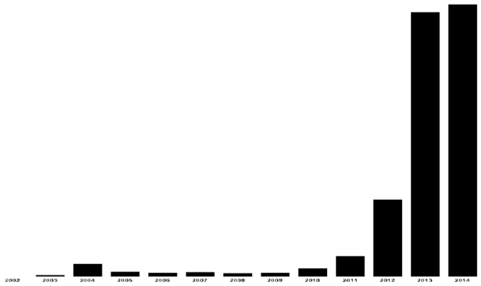

Figure 3 Malware Detected Trouble Tickets 2002-2014

One of the primary countermeasures used against viruses and spyware has been antivirus and malware detection programs.

Phishing

Attacks using the human attack surface leveraging email are known as phishing. Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity or by installing backdoors such as keystroke loggers. Phishing tries to fool the target into unknowingly revealing sensitive information to the threat actor or handing over the information by using social engineering, convincing the target to install malicious software, unknowingly download malicious software from website, go to a malicious website using their browser, or to call a number.

Phishing countermeasures include (United States Computer Emergency Readiness Team n.d.):

- Consumer awareness and training
- Shutting down phishing host sites
- Web browser toolbars
- Strong Authentication and Authorization
- Anti-virus software

Botnets

As malware evolved, additional features were added that allowed malware to go from operating in an isolated instance to multiple instances working together through coordinated command and control (C2) systems. A collective of malware infected devices operating under a unified C2 system through the Internet is commonly referred to as a botnet (robot + network). The botnet itself became a new attack vector, since the botnet could be used to send spam or participate in forms of attacks such as a distributed denial of service attacks at greater scale and with larger impact than infected machines working in isolation. The individually infected bots in the botnet communicate with a command and control center for instructions to allow them to work in coordinated fashion.

In addition to the countermeasures used against viruses and spyware, as noted in the Anti-bot Code of Conduct for ISPs (ABCs for ISPs) (Communications Security, Reliability and Interoperability Council (CSRIC) 2012), botnets can be detected by monitoring the network for communications with known botnet command and control centers and then taking action to block the communication to the command and control and/or notifying infected end-users so that they can take the necessary actions to remediate the infected machine.

In the early days of botnet mitigation, some ISPs would identify C2 servers and concentrate on blocking communications to or taking down C2 servers. This approach was far easier for ISPs than trying to notify customers and assisting them in mitigating and remediating large numbers of infected subscriber devices. Threat actors recognized this weakness in their architectures and designed redundant, multiple layers of C2 servers; increased the sophistication of C2 protocols; and designed peer to peer C2 protocols to obfuscate C2 communication paths and to make the C2 architecture more resilient.

It should be pointed out that ISPs are not the only Internet ecosystem player that can effectively notify users and assist in mitigating and remediating infected devices. Banks, search engines, and e-commerce providers all have the ability to identify, notify, mitigate and remediate their customers and devices with malware infections. As demonstrated in coordinated law enforcement botnet takedowns, these ecosystem players can be more effective in remediating botnet infections with their customers than ISPs.

Denial of Service Attacks

The second category of attacks is the denial of service attack. As the name implies, a DoS attack is an attack that prevents a legitimate user from accessing information or service. DoS attacks come in many forms – email spam, network flood, server overload, resource exhaustion and others. Attacks sources can be concentrated or distributed, leveraging amplification techniques to maximize their effects.

Email spam

The widespread adoption and use of the Internet resulted in a corresponding widespread adoption and use of e-mail. With the widespread adoption of email came the introduction of a new threat vector – spam. Spam is not limited to email, as spam refers to the use of an electronic messaging system such as email or Instant Messaging (IM) to send unsolicited messages. Email became the vehicle of choice for those who send spam (i.e. spammers), because of the ability to reach a large target audience for very low cost. Spam is reported to compose some 80 to 90 percent of all the email. (M3AAWG 2014). Spam without effective filtering tools results in a denial of service attack, as email inboxes become filled with junk mail and the network transit links similarly become filled to capacity with junk mail. For network operators with limited Internet transit, email spam can consume large portions of network capacity and effectively impact the bandwidth available on their network for other purposes.

As shown in Figure 4, the amount of deliberate spam sent by legitimate businesses via e-mail has decreased over time while the amount sent by malware-infected PCs has risen.

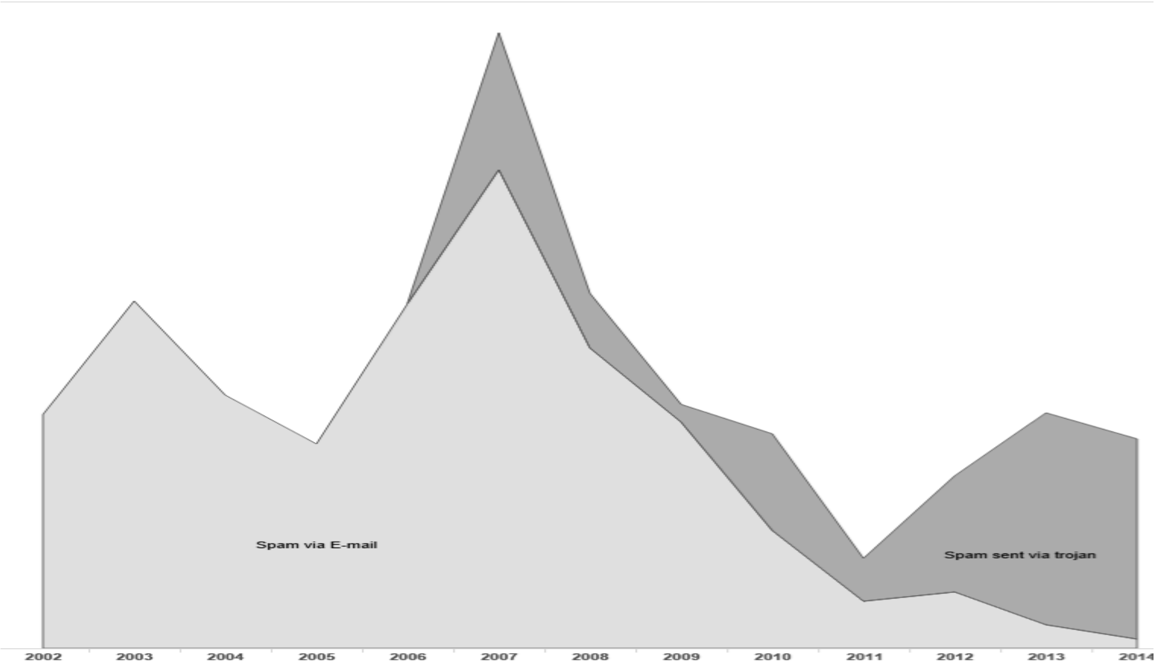

Figure 4 Spam via Email vs. Spam via Bot

The Messaging Malware Mobile Anti-Abuse Working Group (M^{3}AAWG) has published a series of best practices and countermeasures for mitigating spam. Included in the best practices is the blocking or management of the well-known SMTP port, port 25 (M3AAWG 2005), to prevent unauthorized use of the SMTP relay function in the email servers.

Network DoS Attacks

One of the earliest forms of a DoS attack using the network attack surface is the ping flood attack, in which the attacker overwhelms the victim with Internet Control Message Protocol (ICMP) echo request (ping) packets. Attackers developed the Distributed Denial of Service (DDoS) attack as a way around the countermeasures for DoS flood attacks (ping, TCP SYN, UDP, and MAC address).

Distributed Denial of Service Attacks

One of the earliest noted forms of a DDoS attack is the Smurf attack (Wikipedia contributors 2015). A Smurf attack is where a large number of ICMP packets with the intended victim's spoofed source IP address are broadcast to a computer network, resulting in a large number of ICMP responses getting sent to the victim (Wikipedia 2015).

As noted in Akamai's 2014 State of the Internet Report (Akamai 2014), both the volume of DDoS attacks and the average bandwidth per attack continued to increase. Akamai also reported that attackers continued to favor force over technique aided by mass exploitation of web vulnerabilities, millions of Internet Of Things (IOT) devices, and successful botnet building.

The growth in botnets provided a platform for more sophisticated DDoS attacks leveraging an installed base of bots. The botnets created an attack vector that has the potential to harness a large number of computers working together in a coordinated fashion. By harnessing the aggregate bandwidth of the network using infected hosts, attackers dramatically increase the scale and magnitude of the attacks. DDoS attacks occur at all seven layers of the OSI stack (National Cybersecurity and Communications Integration Center 2014). The FCC CSRIC IV Working Group 5 on Remediation of Server Based DDoS Attacks created a complete taxonomy of different types of DDoS attacks and mitigation or remediation best practices (Communications Security, Reliability and Interoperatbility Council 2014). There are four major categories of DDoS attacks:

- Direct and reflective volumetric attacks
- Application layer attacks
- State exhaustion attacks, and
- Control plane attacks

The US-CERT team lists a number of countermeasures for mitigating large scale DoS/DDoS attacks (United States Computer Emergency Readiness Team 2013) that include:

- Layer 3 & 4 line-rate access control lists (ACLs) and rate limits
- Layer 4-7 Packet Screens, session limits, and SYN cookies

Distribute Reflective Denial of Service Attack

The magnitude of the DDoS attack vector can be further increased using a reflection amplification technique resulting in a Distributed Reflective Denial of Service (DRDoS) attack (United States Computer Emergency Readiness Team 2014). The reflection amplification is achieved by first sending a set of requests that get reflected. The attacker sends forged requests of some type; typically the source address in the IP headers is forged or spoofed, to a very large number of computers that will reply to the requests. The amplification in the attack is achieved by sending a request that results in a response much larger than the request. A good example of this is a DNS request. The DNS request is a small number of bytes (e.g. ~60 bytes), but can result in a response that is much larger (e.g. >1000 bytes).

The DNS Amplification attack (United States Computer Emergency Readiness Team 2013) is a popular form of a DRDoS attack, in which attackers use publically accessible open DNS servers (aka open resolvers) to flood a target system with DNS response traffic. The attacker sends a DNS lookup request to an open DNS server with the source address spoofed to be the target's address. The DNS server then sends the DNS record response it is sent instead to the target. The attacker's DNS request is typically submitted to request as much zone information as possible to maximize the amplification effect.

The US-CERT team has identified 11 different potential attack vectors for UDP protocols that include DNS, NTP, and SNMPv2 (Rossow 2014) that can be used for DDoS/DRDoS attacks.

DDoS attacks require a different set of countermeasures than simply blocking the traffic on an abused TCP or UDP port because some implementations of protocols may send the response using same IP port on which it was received. Instead of blocking the port, a widely used countermeasure will check for the spoofed IP addresses as described in IETF BCP 38 (Senie and Ferguson 2000) and BCP 84 (Baker and Savola 2004).

Man-in-the-Middle

Yet another attack vector is the Man-In-The-Middle attack (MITM). In a MITM attack the adversary secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. MITM the middle attacks can be performed using a number of techniques:

- Network taps that mirror to offline analysis system
- Re-routing the traffic
- Masquerading as the intended destination for an open WiFi or cellular access point

Over the last couple of years there have been widespread reports of persistent Internet surveillance by governments by using a network tap (optical or electrical tap) to mirror/copy all the traffic to an offline storage and analysis system. (Gorman and Valentino-Devries 2013) These taps were upstream from cable companies and performed on the Internet backbone.

These widespread reports have prompted a response by the Internet community to recommend encrypting all Internet communications. In 2014, the Internet Architecture Board (IAB) released a statement recommending that encryption should be deployed throughout the Internet protocol stack (Internet Architecture Board 2014). Earlier in the year, in May 2014, the IETF did a technical assessment and declared pervasive monitoring is an attack on privacy with the release of BCP-188/RFC 7258, Pervasive Monitoring Is an Attack, (Farrell and Tschofenig 2014). To mitigate the attack on privacy, RFC 7258 recommends that encryption should be authenticated where possible and that all newly designed protocols should prefer encryption. A second IETF RFC was released that advocates for the use of "Opportunistic Security" (Dukhonvi 2014). Opportunistic Security recommends upgrading from cleartext to unauthentic session encryption when authenticated encryption is not available. The concept here is that some encryption, even if unauthenticated, is better than no encryption.

It should be noted that adding encryption and authentication techniques can cause system availability to decrease and creates a larger attack surface for denial of service attacks. Disrupting the authentication or encryption mechanisms and the larger packets sizes and CPU/memory requirements to implement these technologies increase the ability of threat actors to disrupt the underlying protocol or service.

MITM attacks can be performed in a number of ways. One method is to use a technique known as "route hijacking" where the attacker intentionally announces an illegitimate route advertisement using the Border Gateway Protocol (BGP) to other networks. The rogue route can result in the traffic getting diverted away from its intended route. Once diverted, the traffic can either result in the destination being unreachable and creating a DoS attack, or it can be diverted through additional networks resulting in MITM attack. There are a number of counter-measures described in the NIST publication SP-800-54 (Kuhn, Sriram and Montgomery 2007) with prefix filtering being the most basic mechanism for protecting BGP routers from routing disruptions (Kuhn, Sriram and Montgomery 2007, 42).

A third form of MITM attacks can occur as a result of masquerading or spoofing. Attackers masquerade as open public WiFi access points by spoofing the WiFi SSID and as destination websites by spoofing the hostname using a technique known as DNS spoofing. A DNS spoofing attack uses forged DNS information to supply the victim with an illegitimate IP address that takes them to the attack site instead of the intended site. As a countermeasure to DNS spoofing, the IETF developed a suite of specifications, Domain Name System Security Extensions (DNSSEC) (Wikipedia contributors 2015) to enable DNS clients to authenticate the DNS data.

Countermeasures Summary

Attack Surface	**Attack Vector**	**Countermeasures**
Software	Virus/Spyware	Detection
Human, Software	Phishing	Consumer awareness, Site shutdowns, Browser toolbars, Authentication & Authorization, and Anti-virus software
Software, Network	Spam	Port Blocking Access Control Filtering
Software, Network	Bots	Network monitoring Anti-virus software
Network	DoS/DDoS	Filtering, Access Control Network Ingress Filtering
Network	Man-in-the-Middle	BGP Prefix filtering, DNSSec, Encryption, secure WiFi access points

CABLE STANDARDS

The DOCSIS™ standards employ a number of features that can be used as part of deploying countermeasures for the threat vectors discussed in this paper.

Cable Modem Protocol Filters

DOCSIS supports two IP protocol-filtering methods. The initial method specified in DOCSIS 1.0 is specified in RFC 4639 (Woundy and Marez 2006) and supports filtering at the IP layer and the logical link control (LLC) layer and only supports IPv4. With the release of DOCSIS 1.1, as part of adding support for IPv6, the concept of the Upstream Drop Classifier (UDC) was introduced. UDCs enhanced the filtering capabilities by adding support for IPv6 and rules that were mutually exclusive of whether it was TCP or UDP. The inclusion of UDC further reflects that upstream filtering is best done as close as possible to source in the cable modem (CM) itself, while downstream filtering is best done in the cable modem termination system (CMTS) or further up in the network.

The filters can be statically configured as part of the cable modem provisioning process or they can be dynamically configured. They can filter on any combination of:

- IP Protocol – TCP, UDP
- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Type of Service (TOS)
- Direction

Source Address Verification

The DOCSIS specification (CableLabs 2014) includes a feature known as Source Address Verification (SAV). The SAV feature per the specification defaults to "enabled" on the CMTS and ensures that the customer premise equipment (CPE) located behind a cable modem cannot spoof addresses in order to obtain access to services or disrupt the services to others. When the SAV feature is enabled, the CMTS drops any upstream packets whose IP source address has not been assigned by the operator, including those whose source IP address has already been assigned to another device.

The feature provides an implementation of network ingress filtering of upstream traffic as described in the IETF's BCP-38 (RFC 2827). In addition to preventing DDoS traffic using spoofed source IP addresses, the feature also prevents theft of service by users statically assigning an IP address not assigned to the cable modem.

Baseline Privacy Plus (BPI+)

Baseline Privacy Plus (BPI+) is one of the DOCSIS security specifications. BPI+ provides two key security features – data privacy over the cable network and unauthorized access to the network's RF media access control (MAC) layer services. BPI+ provides data privacy by encrypting the packet or user data in the DOCSIS frames. Cable modems ship with an X.509 certificate installed in them. During the modem registration process, the CM must send its X.509 certificate to the CMTS for authentication. The authentication process prevents forged and cloned modems from gaining access to the network services.

PacketCable™ Multimedia

The PacketCable Multimedia Specification (PCMM) (CableLabs 2011), provides a dynamic quality-of-service (QoS) framework for dynamically changing the provisioned bandwidth on a per IP-flow basis. The framework supports dynamically creating a "gate" that has attributes that describe the packet filter similar to those of the static cable modem filters as well as QoS attributes such as bandwidth allocated for the IP-flow.

PCMM can be used as a countermeasure for blocking or rate limiting of threat vector traffic such as e-mail spam or DDoS traffic that is originating from a CPE behind a cable modem.

IETF

In addition to security elements in the DOCSIS and PacketCable specifications, the IETF specifications include many security elements. Two key areas for securing the network reside with securing the BGP and DNS. Both of these protocols are considered critical for the operation of the Internet. If either service is disrupted, it can have regional or global effects on Internet traffic.

Border Gateway Protocol

BGP is the routing protocol for border routers to exchange routing information between autonomous systems (AS) on the Internet (IETF 2006). As a countermeasure for a DDoS attack, the routers can be configured to null route (aka black hole) the attack traffic. The effect of the null routing is to drop all the packets of the attack traffic. A variation of a black hole is to sink hole the traffic. When sink holing the traffic, instead of null routing and dropping the attack traffic, the attack traffic is sent to a capture device where the data can be used for further analysis.

BGP Flowspec is another technique operators use to distribute granular router ACLs to a large number of routers using BGP. BGP Flowspec can be used to automate distribution of blocking or rate limiting ACLs to mitigate DoS/DDoS attacks in minutes instead of manually configuring ACL on routers that can take hours or days.

DNSSEC

The IETF enhanced the DNS protocol with a set of security extensions, DNSSEC. DNSSEC was designed to protect application from using forged or manipulated DNS data as the result of a MITM attack. To validate DNS queries, all the responses are signed with a digital certificate. By checking the digital certificate, the DNS resolver can check that the information is the same as what the domain owner published. These extensions have been adopted by a number of major ISPs but there is considerable resistance to further adoption.

APPLICATIONS OF EMERGING TECHNOLOGIES FOR CYBER COUNTERMEASURES

A number of technologies are emerging that may prove to be valuable, as they mature, in providing new, effective countermeasures. Included in this list of emerging technologies is:

- BGP Security (BGPSec)
- Big Data
- Software Defined Networking
- Network Virtualization Function

BGPSec

The IETF is developing an extension, BGPSec, to secure the BGP protocol. Currently the BGP protocol is vulnerable to what is known as "route hijacking" that can lead to a MITM attack. Route hijacking occurs when a network or AS advertises that it can route to select destinations that it is not authorized to advertise. However the adoption of this set of extensions is likely to be a very long process and is not guaranteed.

BGP security involves several important aspects of verification:

- Route origin verification – ensuring that the route announcement was made by the authorized party
- Path verification – ensuring that the route the data traversed was not maliciously manipulated or affected by human error

BGP security involves several aspects for successful deployment and wide spread implementation:

- An accurate database of authorized routes
- A secure method for publishing authorized routes globally
- A scalable and secure method to verify route origin
- A scalable and secure method to verify the path the data took to the end user and that the path was the best or most appropriate path

Not all of the above requirements must be met at once. For example, route origin verification alone would be a big step forward for securing the BGP protocol.

Several methods for securely publishing route information have been proposed with the most prominent method being Resource Public Key Infrastructure (RPKI) (American Registry for Internet Numbers n.d.). Route Origin VERification (ROVER) (Gersch 2012) is an alternative method that may be more scalable.

Big Data

As a result of the previously discussed reports of the pervasive monitoring and the Internet community's response to work to secure all Internet communications by encrypting all traffic, this will have an impact on security operations and network management (Moriarty and Morton 2015). Some current security techniques will need to evolve and adapt to effects of encryption, while others will cease to work effectively.

The term "Big Data" has been described to mean data sets so large or complex that processing and storage applications are inadequate. The large data sets create challenges in the analysis, storage, and visualization across the data set. Big Data is one technology that can be leveraged to improve the passive monitoring capabilities as part of adapting and evolving to the realities of trend towards ubiquitous encryption for Internet traffic.

Operators often have multiple sources of threat feeds. The threat feeds typically includes DNS data, multiple C2 feeds, multiple black/white lists, and indicators of compromise (IOC) feeds. The threat feed information may or may not be stored in dedicated repositories as the feed information is often specific for the supporting network appliances. The data feeds result in large data sets and therefore are often not retained for long periods of time due to the limits of the conventional data storage technology. Big data technology can be applied to the multiple threat feeds to create a single repository with the aggregated data. The data in the single repository can then be analyzed and correlated to identify trends and other threat patterns for the application of an appropriate counter-measure.

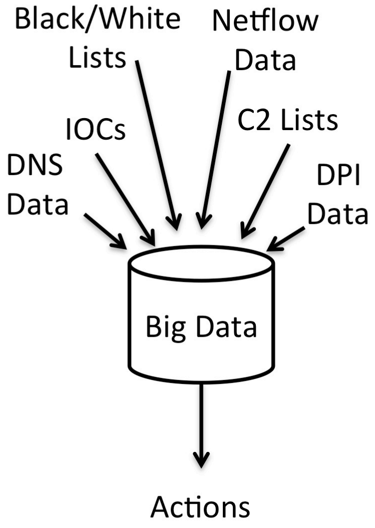

Figure 5 Big Data - Threat Aggregation

SDN

Software-Defined Networking (SDNs) is an approach to networks that decouples the networks data or forwarding plane from its control plane to provide a centralized view of the overall network. SDNs enable the automation of network services through a policy-based decision framework such as PacketCable Multimedia and 3GPP's Policy-Charge Rules Function (PCRF) to orchestrate which network traffic goes where. Figure 6 illustrates the SDN logical architecture.

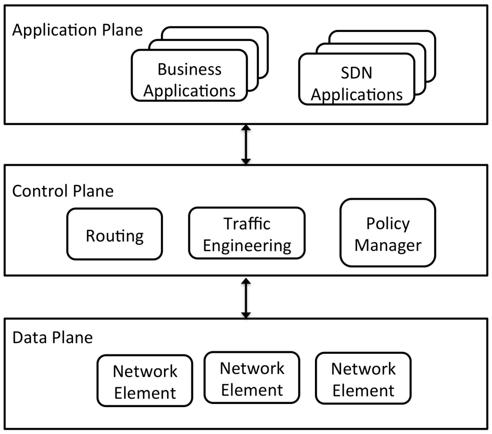

Figure 6 SDN Logical Architecture

Network function Virtualization (NfV) decouples network functions from proprietary hardware appliances to virtualize network services. NfV delivers the virtualized infrastructure upon which an SDN's control plane software, L2/L3 data plane software, and network services can run.

The NfV technology can be extended to the CPE device(s) in the home to create a virtual CPE where most of the CPE functions are pulled into the operator's network. The CPE device then acts as a simple layer-2 device for providing network connectivity and all the network services functions such as NAT, firewall, routing, VPN, filtering, etc. being delivered by the virtual CPE in the headend or service provider's cloud.

The combination of NfV with SDN (NfV/SDN) provides two key features for cybersecurity countermeasures:

- Elastic scaling of the network functions
- Ability to dynamically re-allocate packet processing across the SDN

SDN + NETWORK SECURITY

The NfV/SDN architecture can be enhanced with Big Data to provide a means for operators to automate network countermeasures. This architecture can be used to build and deploy a suite of network security SDN applications. In addition to the two previously mentioned key features of the NfV/SDN architecture, it also helps operators to mitigate the impacts the threat vectors discussed earlier by leveraging the inherent pseudo-wire techniques (e.g. L2VPN, DOCSIS service flows, PCMM Gates) to filter, block, isolate or reroute suspect traffic.

The virtual CPE as part of this architecture will allow for better security and operational control for the operator. Better control is provide due to the fact that the operator has better visibility and control of the various state information in the virtual CPE such as the NAT tables, local routing and VPN, and packet filters. This will enable the operator to more quickly address and mitigate network issues.

A key element in SDN architecture is the SDN controller. Conceptually the SDN controller communicates to various access networks elements in the cable networks headend (e.g. CMTS, CCAP) and provides a platform for developing technology-agnostic network applications (e.g. L2VPN application connecting end-points across the underlying networks). SDN improves the process for dynamically binding an IP-flow to pseudo-wire (e.g. DOCSIS service flow or PCMM gate in the DOCSIS network and VLAN in the core) to isolate the suspect traffic from other traffic.

As shown in Figure 7, we are proposing two new SDN applications – 1) Security and 2) a BGPSec cryptographic processor.

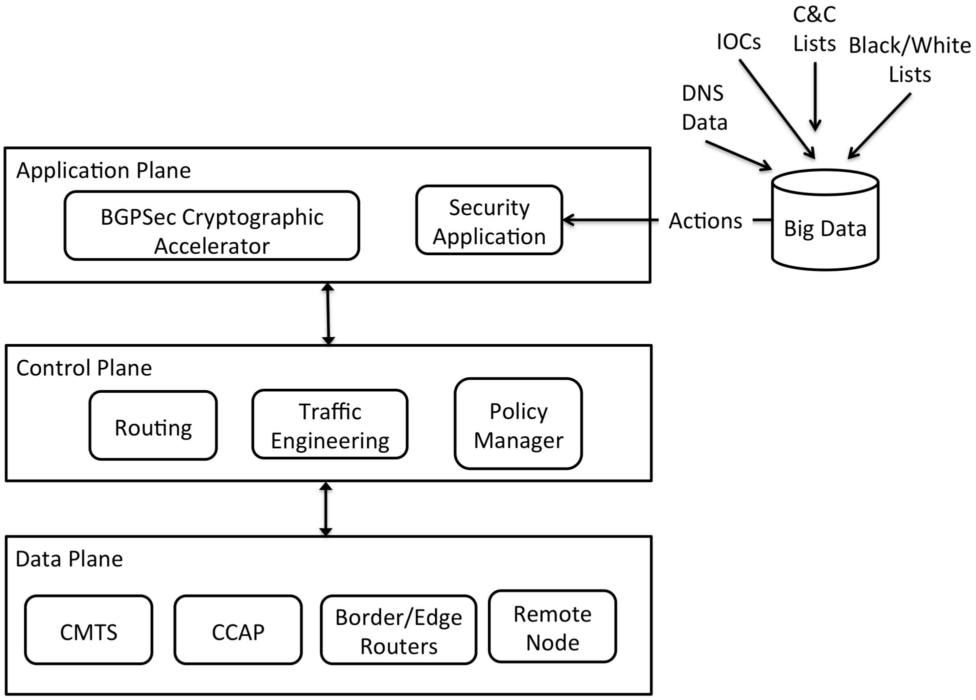

Figure 7 Security Apps in Cable SDN Architecture

This security application would ingest the analyzed and correlated threat feed actions from the Big Data system along with traffic flow information occurring on the network and orchestrate a set of network counter-measures that include:

- Blocking or rate limiting malicious traffic as close to the source as possible
- Routing suspect traffic to a sinkhole or black hole
- Routing the traffic to the data scrubbing system
- Dynamically adding bandwidth
- Add CPU and memory resources in the controller plane to mitigate resource attacks
- Dynamically adding a pseudo-wire for the suspect traffic to provide a level of isolation
- Dynamically isolating and routing critical device traffic (such as medical device traffic) to authorized locations to minimize the expose of the data and device attack surface

The second SDN application is a dedicated BGPSec cryptographic processing application. BGPSec is a cryptographically intense protocol (Small Business Innovation Research n.d.). BGPSec requiring two levels of cryptography. First, each of the RPKI objects must be verified and second, it requires the router to sign and verify each BGP message that it sends (Goldberg 2014). The volume of cryptographic processing can fluctuate due to network conditions. The capability to dynamically add additional cryptographic processing (e.g. CPU) can reduce the network convergence time when there is a network change. In addition, the use of the NfV/SDN architecture allows standard off-the-shelf CPUs to be used instead of custom cryptographic processors.

The addition of the BGPSec cryptographic SDN application can help to reduce the cost of deploying BGPSec by eliminating the need for dedicated cryptographic processors in the routers. The broad adoption of BGPSec and the ability to authenticate advertised routes will greatly reduce or eliminate accidental and malicious route hijacks and BGP MITM attacks.

SUMMARY

In this paper we have surveyed the current network threat landscape in terms of both the network attack surfaces and the associated network attack vectors. We further illustrated how the NfV/SDN architecture can be integrated with Big Data to allow operators to address real-time threats in an automated fashion. An enhanced NfV/SDN architecture was proposed that can be enhanced with Big Data to provide a means for operators to automate network countermeasures.

BIBLIOGRAPHY

Akamai. "[state of the internet] / security - Q4/2014 Report." 2014.

American Registry for Internet Numbers. *RESOURCE PUBLIC KEY INFRASTRUCTURE (RPKI).* https://www.arin.net/resources/rpki/ (accessed March 31, 2015).

Baker, Fred, and P. Savola. "Ingress Filtering for Multihomed Networks." March 2004. http://www.rfc-editor.org/bcp/bcp84.txt (accessed April 2, 2015).

CableLabs. *Data-Over-Cable Servicee Interface Specification DOCSIS 3.1 - Security Specification.* Specification, CableLabs, 2014.

CableLabs. *PacketCable(TM) Specification Multimedia Specification.* specification, CableLabs, 2011.

Chen, Thomas, and Jean-Marc Robert. *The Evolution of Viruses and Worms.* 2004. http://vxheaven.org/lib/atc01.html (accessed 3 9, 2015).

Communications Security, Reliability and Interoperability Council (CSRIC). *Final Report: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) (A Voluntary Code).* Federal Communications Commission, 2012.

Communications Security, Reliability and Interoperatbility Council. *Working Group 5 Remediation of Server-Based DDoS Attacks Final Report.* Federal Communications Commission, 2014.

Dark Reading. *Minimizing the Attack Surface Area: A Key to Security.* 03 23, 2012. http://www.darkreading.com/analytics/security-monitoring/minimizing-the-attack-surface-area-a-key-to-security/d/d-id/1137387 (accessed 03 16, 2015).

Dukhonvi, V. "Opportunistic Security: Some Protection Most of the Time." *IETF.org.* December 2014. http://www.ietf.org/rfc/rfc7435.txt.pdf (accessed March 30, 2015).

Farrell, S., and H. Tschofenig. *Pervasive Monitoring is an Attack.* May 2014. http://www.rfc-editor.org/rfc/rfc7258.txt (accessed March 27, 2015).

Gersch, Joseph. *ROVER- BGP Route Origin Verification via DNS.* April 2012. https://ripe64.ripe.net/presentations/57-ROVER_RIPE_Apr_2012.pdf (accessed March 31, 2015).

Goldberg, Sharon. *Why Is It Taking So Long to Secure Internet Routing.* Vers. Volume 12. acmqueue. September 11, 2014.

http://queue.acm.org/detail.cfm?id=2668966 (accessed March 24, 2015).

Gorman, Siobhan, and Jennifer Valentino-Devries. "New Details Show Broader NSA Surveillance Reach." *The Wall Street Journal*, August 21, 2013.

IETF. *RFC 4271 - A Border Gateay Protocol 4 (BGP-4).* January 2006. http://www.ietf.org/rfc/rfc4271.txt (accessed March 20, 2015).

Internet Architecture Board. *IAB Statement on Internet Confidentiality.* November 14, 2014. https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/#more-7754 (accessed March 27, 2015).

IT Law Wiki. *Penetration Attack.* http://itlaw.wikia.com/wiki/Penetration_attack (accessed 03 17, 2015).

Kuhn, Rick, Kotikalapudi Sriram, and Doug Montgomery. *Border Gateway Protocol Security.* National Institute of Standards and Technology, NIST, 2007.

M3AAWG. *M3AAWG Email Metrics Program: The Network Operators' Perspective - Report #16 - 1st Quarter 2012 through 2nd Quarter 2014.* M3AAWG, 2014.

M3AAWG. *Managing Port 25 for Residential or Dynamic IP Space Benefits of Adoption and Risks of Inaction.* M3AAWG, 2005.

Manadhata, Partyusa K. "An Attack Surface Metric." PhD Thesis, School of Computer Science, Carnegie Mellon University, Pittsburgh, 2008.

Manadhata, Pratyusa K, and Jeannette M Wing. *Attack Surface Measurement.* IEEE Transactions on Software Engineering, 2010.

Mistry, Bipin. *DDoS Attack left "Sweden not Working".* 12 2014, 2014. http://www.securitybistro.com/?p=9047&utm_content=infosecurity&utm_source=twitterfeed&utm_medium=twitter (accessed 03 16, 2015).

Moriarty, K., and A. Morton. "Effect of Ubiquitous Encryption." Vers. 1. *IETF Network Working Group.* March 2015. http://www.ietf.org/id/draft-mm-wg-effect-encrypt-01.txt (accessed March 30, 2015).

National Cybersecurity and Communications Integration Center. *DDoS Quick Guide.* January 29, 2014. https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf (accessed March 17, 2015).

Northcutt, Stephen. *Security Laboratory: Defense in Depth Series.* http://www.sans.edu/research/security-laboratory/article/did-attack-surface (accessed 03 16, 2015).

Open Web Application Security Project (OWASP). *Attack Surface Analysis Cheat Sheet.* 7 18, 2014. https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet (accessed 3 11, 2015).

Rossow, Christian. "Amplification Hell: Revisiting Network Protocols for DDoS Abus." *Internet Society.* February 23, 2014. http://www.internetsociety.org/sites/default/files/01_05.pdf (accessed August 11, 2014).

Senie, D., and P. Ferguson. *RFC 2827 - Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing.* May 2000. http://tools.ietf.org/html/rfc2827 (accessed March 18, 2015).

Small Business Innovation Research. *Cryptographic Acceleration for Border Gateway Protocol Security (BGPSE...* http://www.sbir.gov/content/cryptographic-acceleration-border-gateway-protocol-security-bgpsec-1 (accessed March 24, 2015).

United States Computer Emergency Readiness Team. *Alert (TA13-088A) - DNS Amplification Attacks.* July 22, 2013. https://www.us-cert.gov/ncas/alerts/TA13-088A (accessed March 18, 2015).

—. *Alert (TA13-088A) DNS Amplification Attacks.* March 29, 2013. https://www.us-cert.gov/ncas/alerts/TA13-088A (accessed March 17, 2015).

—. *Alert (TA14-017A) UDP-based Amplification Attacks.* March 07, 2014. https://www.us-cert.gov/ncas/alerts/TA14-017A (accessed March 17, 2015).

—. *Security Tip (ST04-015) Understanding Denial of Service Attacks.* 02 16, 2013. https://www.us-cert.gov/ncas/tips/ST04-015 (accessed 03 17, 2015).

—. *Spyware.* 02 06, 2013. https://www.us-cert.gov/security-publications/spyware (accessed 03 17, 2015).

—. *Technical Trends in Phishing Attacks.* https://www.us-cert.gov/sites/default/files/publications/phishing_trends0511.pdf (accessed Mach 18, 2015).

Wikipedia contributors. *Domain Name System Security Extensions.* Vers. 650332715. March 7, 2015. http://en.wikipedia.org/w/index.php?title=Domain_Name_System_Security_Extensions&oldid=650332715 (accessed March 24, 2015).

—. *Smurf Attack.* Wikipedia, The Free Encyclopedia. January 26, 2015. http://en.wikipedia.org/w/index.php?title=Smurf_attack&oldid=644239924 (accessed March 24, 2015).

Wikipedia. *Smurf Attack.* The Free Encyclpedia Wikipedia. 01 26, 2015. http://en.wikipedia.org/w/index.php?title=Smurf_attack&oldid=644239924 (accessed 03 16, 2015).

Woundy, R., and K. Marez. "RFC 4639 - Cable Device Management Information Base for Data-Over-Cable Service Interface Specification (DOCSIS) Compliant Cable Modems and Cable Modem Termination Systems." *IETF.org.* December 2006. http://www.ietf.org/rfc/rfc4639.txt (accessed March 24, 2015).