SCTE·ISBE CABLE-TEC EXPO 2017
DENVER, CO
OCTOBER 17-20

2017 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS

Service Theft in DOCSIS Networks

Identifying the Hidden Leaks in Your System

A Technical Paper prepared for SCTE/ISBE by

Egbert Westervelt
Sr. Security Engineer
Irdeto
Eindhoven, NL
EWesterveld@irdeto.com

Edward Florendo
Service Delivery Manager
Irdeto
Hoofddorp, NL
edward.florendo@irdeto.com

Dave Belt
Technology Evangelist
Irdeto
Conifer, CO US
(303) 653-7647
dave.belt@irdeto.com

Table of Contents

Introduction

The following describes a technical proof of concept (POC), developed by the authors, and performed for a major U.S. cable operator. This effort looks at the prevalence of service theft on broadband networks, focusing initially on Data-over-Cable Service Interface Specifications (DOCSIS), but the technologies applied herein can extend to other networks including digital subscriber line (DSL), fiber and Wi-Fi.

The effort incorporated a two-tiered approach. The first component consisted of extensive forensic research via the Internet, using open sourced intelligence (OSINT) techniques, identifying known attack vectors directly from the hackers themselves. This qualitative intelligence was then used to develop a service monitor appliance designed to actively monitor for service theft.

The results of this comprehensive theft assessment are quite significant with regards to the level of theft involved. When one looks at the lost revenue, as well as the increased overbuild costs, it quickly becomes impractical to not address this hidden issue.

The Problem

The high-level concepts and technologies implemented within this effort are applicable to many different broadband technologies. For the sake of keeping the topic focused, we will focus solely on DOCSIS network technologies herein.

Theft of service has been a well-known problem within DOCSIS networks and there have been some significant efforts by the industry to address the issue. The release of the DOCSIS 3.0 security specification (Cable Television Laboratories) is one case in point. By introducing the use of public key infrastructure (PKI) device authentication, each device can now uniquely pair to a cable modem termination system (CMTS). This specification had a significant impact on system security, so much so that it has spawned a black market for pre-DOCSIS 3.0 modems on the Internet. Many operators have pushed forward to move their entire networks to DOCSIS 3.0 technology, which would provide a higher level of scrutiny and security, however this effort involves the elimination of all older devices from the network, a significant consumer premise equipment (CPE) expense.

Assuming that DOCSIS 2.x devices have flawed security, the efforts described herein are focused primary on DOCSIS 3.x devices. While the DOCSIS 3.0 specification outlines the use of PKI certificates for device authentication, it says little about the implementation on the devices themselves. As a result, the protection of the credentials, as well as the overall protection of the device platform varies greatly and leaves significant gaps for theft to occur.

Project Initiative

The POC described herein was performed for a major North American operator with the intent of quantifying the theft described. A general gap was identified between the CMTS and actual reconciliation with the operator's billing systems. A major portion of the POC was intended to bridge this gap. Simultaneously, the vendor's cybersecurity team performed a comprehensive search of the "dark web" to identify known attack vectors against the operator's network. This information was then fed back into the reconciliation system to identify these attacks occurring and mitigate in real time.

Approach

1. System Assessment

The initial effort consists of inventory and assessment of the operator's system. CMTS as well as CPE hardware are inventoried and current configurations noted. These are compared to the manufacturer recommended security configurations and changes are suggested where necessary.

2. Online OSINT Research

For the up-front research, the solution vendor performs an online deep dive using the inventory information obtained during system assessment. Research into the Internet is performed looking specifically for attacks against the CPE utilized by the operator, as well as targeted attacks against the operator's network itself. This information yields specific attack vectors that are then implemented into the service monitor appliance utilized for modem reconciliation, continually improving its accuracy of detection and removing rogue devices.

3. Modem Reconciliation

Modem Reconciliation consists of the integration of a service monitor appliance into the operator's data center. This appliance consists of a Hadoop database that identifies all devices connected to the network via CMTS and reconciles these devices with a valid billing address. Failure to reconcile indicates one of two issues: either the device was not registered properly via the operator's processes, or a case of real theft is occurring. In the former case, it is in the operator's interest to reconcile these processes so that an accurate measurement of theft can be made in the latter.

Once the initial reconciliation is complete, the system continues monitoring the usage patterns of the connected devices based on the attack vectors identified in the system assessment. Once a positively identified rogue device is identified, it can be mitigated per the operator's policies. It is important here to err on the conservative side as removal of valid devices clearly creates a poor customer experience.

Ultimately it is the continuous feedback loop of the online research coupled with the service monitor appliance that makes this solution a success. As new mitigations are implemented, the cybersecurity research team can monitor the hackers' reactions online, staying in sync with them as the continual cat and mouse game plays out.

Findings

The following provides a summary of the findings from the POC.

1. Online OSINT Research

Multiple exploits were identified through online research, providing a very distinct picture of the avenues used by hackers into an operator's system.

1.1. Hacking Exploits

A significant body of knowledge has been dedicated to the direct hacking of DOCSIS modems on an operator's network. Access to the DOCSIS endpoint enables free access to service as well as potential access to the operator's backend systems on more sophisticated gateway appliances. Some of the more significant forums and discussions identified were as follows.

- Discussions on how to directly hack into CPE – Step by step instructions on how to hack directly into DOCSIS devices are prevalent, not only on dark web sites, but also on regular web sites. Exploits are usually on a specific vendor and device basis and frequently utilize the Joint Test Action Group (JTAG) interface and/or soldering of leads and interfaces directly onto the circuit boards. Instructions include detailed circuit board diagrams indicating access points for a "noob" hacker.
- Discussions and techniques on how to circumvent security measures – Similar to device hacking, these discussions are at more of a system level and focus on how to gain access to the network, primarily through a hacked device.
- Discussions of security measures and countermeasures by multiple system operators (MSO) – Frequently as soon as an operator rolls a new piece of firmware with a new security measure in place, a slew of exploits dependent upon the previous vulnerability become unavailable. To a potential piracy service this is the equivalent of an operator outage and as such the hackers are immediately looking for the next exploit. The cat and mouse game of measures and countermeasures are well documented within these hacker forums.
- Trade of modem device files – Frequently an exploit is enabled, or supplemented by the modification, ingestion or spoofing of modem data. Sharing of these memory images enables a fellow hacker to recreate a particular exploit.
- Trade of medium access control (MAC) addresses and PKI certificates –The DOCSIS standard ties the device authentication to the MAC address so these are frequently traded together. MAC address cloning is a well-known attack vector on DOCSIS networks. So long as two devices with the same MAC address don't reside on the same CMTS, these devices can coexist peacefully on an operator's network.
- Trading of modem configuration and boot files – Modification of device configuration and boot files enables a potentially lower tired subscriber to obtain a higher level of service. Once a modification is made, the files along with upgrade instructions are shared openly.

1.2. Sale of Theft Related Products

Designed for the lazy hacker or non-technical person who merely wants cheap service, pay services provide a number of exploits packaged into an easy to use product. Examples are as follows.

- Sale of hacked modems – There has been since the turn of DOCSIS 3.0 a black market for DOCSIS 2.0 modems due to their inherent lack of security features. As operator's cut off these devices from their networks, the market is now turning to pre-hacked DOCSIS 3.x devices. The exploits described above are applied in a production manner to a block of devices and sold at a premium enabling free or upgraded service.
- Sale of activation services – A cable customer with a specific piece of CPE can send this to an activation service to have the exploits described above applied to their device for a fee. Alternatively, an exploit package and instructions are sometimes offered in order to gain free or upgraded service.
- Sale of hacking and modification services – For the customer with a device without a pre-defined hack, custom services are offered to open the device. The device is sent to the hacker and a general tool box of exploits is applied to find entry into the device. Once a known exploit is defined, it may be resold as one of the other services above.

1.3. Internal Theft

Internal theft is as described, theft from within the organization itself with the goal of external monetization.

- Bad contractors – These are self-identified internal contractors to a particular operator who sell enablement services. A customer with a cable modem provides its MAC address and for a fee the modem is registered within the operator's backend service.

1.4. Social Engineering

In addition to the dark web and sheer persistence, information is also obtained through social engineering techniques, also shared on the dark web. Examples include the following.

- "Play Dumb" Techniques – Methods for convincing a customer service agent (CSA) to reauthorize a device or remove a device from a blacklist.
- "Pumping" for Information– Hackers will often try to engage a CSA or a higher level service technician in conversation so they may extract additional information regarding an operator's security measures
- Names of Internal Systems –internal system names are indentified and published to support hackers in their conversations with technicians when they attempt to extract security information

Based on this research it is clear that the attack vectors as well as markets created around them are numerous. Much of the information gleaned from this online search was then used to develop the service monitor appliance discussed below. This appliance allows the operator to quantify the theft occurring on a particular network.

2. Service Monitor Appliance

The service monitor appliance performs the modem reconciliation described in the Approach section. By reconciling every modem with a billing account, a consistent accounting of these devices on the network is obtained. Additionally, cross checking of firmware versions and configurations ensures that all devices on the network are authorized to be there. Rogue devices are removed based on the trust level of the detection. The following outlines some of the major theft identified on the operator's network analyzed for the POC.

2.1. No Billing Account

Devices on the network with no billing account can have multiple reasons for being unregistered. These can be via stolen credentials, internal registration or simply slipping through the operator's provisioning processes. A full 2% of the devices on the network per day fell into this category identifying the largest loss within the POC.

2.2. Billing Status Disconnected

These devices have an account associated with them; however, their billing status is set to disconnected. The reasons for this status can include internal registration, modification via social engineering or gaps within the operator's system. Of the devices within the POC, 0.4% per day were identified with a disconnected status.

2.3. Restricted Boot File

Devices with a restricted boot file have an alternate configuration than provisioned or firmware that is not authorized for use on the device. Reasons for this variation indicate some form of firmware tampering. Of the devices within the POC, .2 - .3% per day were identified with rogue firmware.

2.4. Cloned MAC Address

One of the most understood attacks is also apparently one of the most addressed. MAC address cloning on the network accounted for only .06% of theft.

Additional theft cases were monitored, however with diminishing returns moving forward. All told, the level of loss on the network is significant enough to warrant a closer look by the operator. The loss in revenue due to free service, along with the additional operational expenditure and build out costs quickly justify closing this gap.

Conclusions

We have presented the results of a POC researching DOCSIS service theft performed with a major U.S. operator. The first phase of the effort searched the dark web as well as regular web sites for information on hacking of the operator's CPE and network. This search identified numerous attacks against both, providing qualitative intelligence for the development of second phase.

The second phase consists of the deployment of a service monitor appliance to reconcile modems on the network with registered billing accounts. This implementation provided a definite accounting of rogue, unaccounted and otherwise lost devices. This appliance identified a consistent network loss of an accumulated 2.5%. This type of loss amounts to real numbers when looking at lost revenue as well as additional operational expenditure and build out costs.

DOCSIS networks have provided us with increasing levels of security with each version of the DOCSIS specification that is published. Even so, there are still gaps remaining in the implementations creating significant opportunities for theft of access.

Abbreviations

CSA	customer service agent
CMTS	cable modem termination system
CPE	consumer premise equipment
DOCSIS	Data-over-Cable System Interface Specifications
DSL	digital subscriber line
JTAG	Joint Test Action Group
OEM	original equipment manufacturer
OSINT	open sourced intelligence
MAC	medium access control
MSO	multiple system operator
PKI	public key infrastructure
POC	proof of concept
SCTE	Society of Cable Telecommunications Engineers
STB	set-top box

Bibliography & References

Cable Television Laboratories, Inc. (2016, June). CM-SP-SEC3.0-I16-160602, data-over-cable service interface specifications, DOCSIS 3.0 security specification. Louisville, CO: Author.

