Vulnerabilidades de Seguridad en el Servicio de Internet de Banda Ancha en Redes HFC: Impacto y Posibles Soluciones

Daniel Alfonso Borbor Cedeño, Gerald Emilio Jiménez Farfán, Rebeca Estrada(3)
Facultad de Ingeniería en Electricidad y Computación
Escuela Superior Politécnica del Litoral
Prosperina Km. 30.5 Vía Perimetral 100, contiguo a la Cdla. Sta. Cecilia, Teléfono: 2269269, 09-01-5863, Guayaquil-Ecuador
dborbor@gmail.com; geraldjimenezfarfan@hotmail.com

Resumen

El servicio de Internet de banda ancha de las redes hibridas fibra-coaxial es vulnerable en la actualidad en nuestro país debido a diferentes métodos de acceso no autorizado al servicio; con este trabajo se analizarán los problemas de seguridad de estas redes. Se realizara una revisión de los métodos de acceso no autorizado al servicio y proporcionaremos diversas soluciones para prevenir y evitar estos problemas de seguridad, mejorando el control sobre el servicio prestado al cliente, incrementando la disponibilidad de ancho de banda al usuario que paga por dicho servicio, y permitiendo al proveedor ofrecer el servicio a más clientes así como una mejoría en su calidad del servicio

En la actualidad está muy difundido en todo el mundo el acceso a Internet de banda ancha por medio de redes HFC siendo las vulnerabilidades de seguridad de este sistema por tanto un problema global. Por lo tanto la aplicación de las recomendaciones dada en esta investigación será de una magnifica ayuda para combatir el acceso no autorizado al servicio así como del uso indebido del mismo y su crecimiento.

Palabras Claves: *BPI, Cable-Módem, CMTS, DOCSIS, Hackear, Sigma.*

Abstract

The high bandwidth Internet access service of the hybrid fibre-coaxial networks is vulnerable our country's actuality due to different methods of unauthorized access to the service; with this paper we will analyze the security problems in these networks. We will realize a revision of the unauthorized access methods to the service y we will provide several solutions to prevent and avoid these security problems, improving the control over the service given to the client, increasing the availability of band bandwidth to the client that pays for that service, and allowing the provider to offer the service to more clients as well as an improvement in its quality of service.

Nowadays it is very spread around the world the high bandwidth Internet access by means of the HFC networks being, therefore, the security vulnerabilities of this system a global problem. Ergo, the application of the recommendations given in this investigation will be a magnificent aid to address the unauthorized access to the service as well as its improper use and increase.

Keywords: *BPI, Cable modem, CMTS, DOCSIS, Hacking, Sigma.*

1. Antecedentes y Marco Teórico.

En la actualidad las compañías que ofrecen el servicio de Internet de banda ancha a través de las redes HFC DOCSIS se ven afectadas por diferentes métodos de acceso no autorizado al servicio que ellos ofrecen. Debido a la posibilidad de la alteración de los cable-módems (CM) y la existencia de diferentes nodos dentro de la arquitectura de red del proveedor, el acceso no autorizado es una realidad tangible que muchos usuarios tratan explotar a su conveniencia.

1.1. Importancia y Justificación.

El proyecto tiene como fin identificar todas las vulnerabilidades de seguridad en el servicio de Internet de banda ancha de redes HFC, además de brindar posibles soluciones y métodos de prevención para proteger estas redes y evitar futuros ataques.

1.2. Delimitación del Proyecto.

El desarrollo de este trabajo está enmarcado en los siguientes objetivos:

- Análisis del funcionamiento de las redes HFC.
- Análisis de las vulnerabilidades en diferentes sectores de la ciudad del servicio CM de Suratel.
- Implementación de métodos de acceso no autorizado al sistema y análisis de sus limitaciones utilizando un CM Motorola SB5100.
- Análisis de los sistemas de seguridad dentro de los estándares DOCSIS en sus versiones 1.0, 1.1 y 2.0.
- Análisis del posible incremento no autorizado de ancho de banda, tanto para los clientes legales como para los que no los son.
- Análisis de las posibles soluciones de los problemas de acceso no autorizado en los sistemas de seguridad de las compañías que ofrecen servicios de Internet por banda ancha.

1.4. Redes HFC y el Estándar DOCSIS.

Las redes HFC nacieron como una evolución de las antiguas redes CATV. Estas redes nacieron para resolver problemas de recepción en zonas de mala. Eran redes unidireccionales (información sólo iba desde la antena hacia los usuarios). Debido a los avances de tecnología, el incremento de usuarios y mayor oferta de servicios se comenzaron a desarrollar las redes HFC. Entre las ventajas de estas redes se encontraban la reducción en el número de amplificadores, la simplificación y abaratamiento del mantenimiento y la mejora en la calidad de la señal; cada zona podía tener canales independientes y también permitía a la red ser bidireccional. La mayoría de las redes CATV actuales son HFC. En los últimos años, la estandarización de las redes HFC se ha hecho a través del estándar DOCSIS.

El estándar DOCSIS es un estándar internacional, no comercial, que define los requerimientos de la interfaz de soporte de comunicaciones y operaciones para los sistemas de datos por cable; cubre todo elemento de la infraestructura de un CM, desde el CPE hasta el equipo terminal del operador. Esta especificación detalla muchas de las funciones básicas del CM de un cliente (modulación de frecuencias en el cable coaxial, aplicación del protocolo SNMP a los CMs, encriptación de datos, etc.); muchas funciones adicionales son definidas, pero por lo general no son usadas a menos que el CMTS lo requiera. El término de equipo Terminal usualmente se refiere al todo el equipo que es usado por un proveedor de servicios para mantener y operar una red de CM.

El estándar DOCSIS fue diseñado para ser completamente compatible con otros servicios que ya existen (y tal vez existan) y se transmiten por el cable coaxial. Los estándares DOCSIS en Europa son conocidos como EuroDOCSIS. El CM y el CMTS no crean una interferencia dañina en la línea coaxial que pueda perturbar otros servicios. Cada canal del espectro está lo suficientemente espaciado para permitir suficiente espacio para que los CMs suban (upload) o bajen (download) datos del CMTS a velocidades muy altas. Tres versiones principales de estándares DOCSIS han sido sacados e implementados: DOCSIS 1.0 (El más popular), DOCSIS 1.1. y DOCSIS 2.0.

1.5. Topología de las redes DOCSIS.

Los equipos se comunican sobre una conexión de red utilizando el protocolo IP a través de una interfaz Ethernet o USB. El CM mismo se conecta a un cable coaxial compartido que usualmente conecta muchos otros módems y termina en un nodo HFC. La figura 1 muestra como funciona esto.

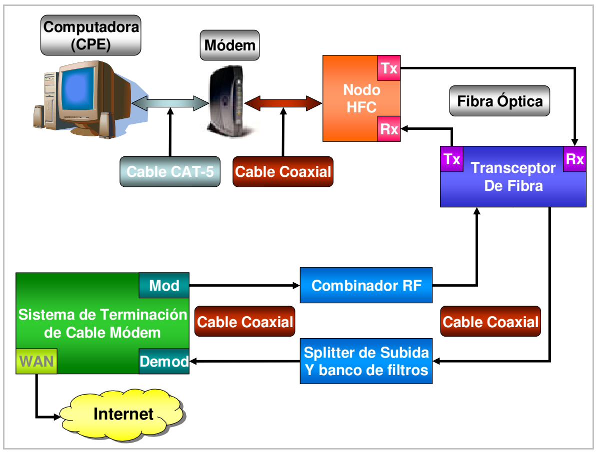

Figura 1. Diagrama detallado de la topología docsis.

Un nodo HFC es un dispositivo de campo de dos vías que toma las frecuencias de radio en un cable coaxial (transmitidas desde el CM), las convierte en señales digitales, y luego transmite los datos a un cable de fibra óptica. Los datos que son recibidos desde el cable de fibra óptica (transmitidos desde el CMTS) son convertidos a una señal analógica y luego son transmitidos a la línea de cobre compartida. Este nodo de fibra (llamado un nodo HFC en la figura 1) convierte las señales analógicas en pulsos digitales de luz que son transferidos a través del cable de fibra óptica. Dos cables de fibra óptica son necesarios. Los nodos HFC ofrecen a los proveedores de servicios muchas ventajas (extender el área de servicio, limitar la ocurrencia de fallas de sistema o una pérdida de servicio a un solo nodo, etc.) Los nodos HFC usualmente son ubicados estratégicamente en vecindarios donde puedan conectar la mayor cantidad de usuarios con la menor distancia promedio total. Estos nodos individuales son conectados a un hub central en el utilizando cables de fibra óptica. El propósito de este concentrador es de que sirva de interfaz entre el cable de fibra óptica desde el campo de servicio y el cable coaxial del CMTS. El hub transceptor de fibra recibe frecuencias de radio de 50 a

860 MHz del dispositivo combinador de RF en la interfaz coaxial. Un combinador de RF es un dispositivo que combina múltiples frecuencias de radio de diferentes fuentes hacia un solo medio compartido; también es usado para añadir al cable coaxial las frecuencias de otros servicios. El hub transmite frecuencias de 5 a 42 MHz a un splitter de subida y banco de filtros. Estos datos son solo los datos que regresan de todos los CMs. Finalmente, tanto las señales de subida como las señales de bajada se conectan al CMTS. Aquí, las frecuencias más bajas del divisor de señales de subida son demoduladas, y las frecuencias más altas de bajada son moduladas al cable coaxial. El dispositivo CMTS procesa todos los paquetes en frecuencia específicas; también tiene un puerto WAN que usualmente está conectado directamente al backbone de Internet o a otra puerta de enlace al Internet.

1.6. Comunicación de datos en las redes DOCSIS.

El estándar DOCSIS permite dos formatos de modulación, QAM (el más usado) y QPSK. QAM codifica los datos de acuerdo a un mapa de símbolos. El rango de operaciones de la señal (o espectro de la señal) es el área de la frecuencia donde los símbolos y las ondas portadoras coexisten. Al incrementar el nivel QAM, más bits por símbolo pueden ser transmitidos simultáneamente al agregar más puntos en el rango de operaciones de la señal. Los factores que determinan el nivel de QAM máximo son la frecuencia del ancho de banda y el ruido base. Los CMs certificados por DOCSIS utilizan QAM-16 para el canal de subida y los CMTS certificados por DOCSIS utilizan QAM-64 o QAM-256 para el canal de bajada.

2. Vulnerabilidades.

Las fallas o bondades de seguridad que pueden ser encontradas en un sistema de Internet de banda ancha en una red HFC dependerán muchos factores como lo son el estándar DOCSIS utilizado, los CMTS y los CMs utilizados, etc.

2.1. Especificaciones del módem.

El CM 5100 incorpora las tecnologías definidas en DOCSIS 2.0 de A-TDMA y S-CDMA para proveer hasta tres veces mayor capacidad de subida que los sistemas de DOCSIS 1.0/1.1. El SB5100 es interoperable y compatible retroactivamente con DOCSIS 1.0 y 1.1. El Surfboard SB5100 de Motorola cuenta con un integrado BCM3348, un módulo RAM de 8 Mb, una memoria flash (para almacenar su sistema operativo e información necesaria aún si este es desenergizado) y un sintonizador coaxial.

2.2. Funcionamiento de los CMs DOCSIS.

Los procedimientos que un módem debería seguir para registrarse en una red de cable es el proceso de aprovisionamiento que trabaja siguiendo un proceso predefinido. En el proceso de inicialización el CM solicita al CMTS que le envíe los parámetros de configuración necesarios para poder operar en la red de cable. Luego, el CM solicita al servidor TOD la fecha y hora exacta, que se utilizará para almacenar los eventos de acceso del suscriptor. La configuración propia del CM se lleva a cabo después de las solicitudes DHCP y TOD. El CMTS le envía ciertos parámetros de operación vía TFTP, tras lo cual, el CM realiza un proceso de registro y, en el caso de utilizar BPI en la red, deberá adquirir la información necesaria de la central y seguir los procedimientos para inicializar el servicio. Cuando el proceso de inicialización se ha desarrollado satisfactoriamente, el CM está listo para utilizar la red como cualquier otro dispositivo Ethernet sobre los estándares de transmisión admitidos por DOCSIS. Para poder conectarse, el módem busca una frecuencia de bajada utilizando el plan de frecuencia específica para la región para la cual fue construido. El equipo terminal CMTS determina si el nuevo dispositivo esta supuesto a acceder esa frecuencia en particular. Una vez enganchado en el canal de descarga, procede a obtener los parámetros de subida al escuchar paquetes conocidos como UCDs, los cuales contienen los parámetros de transmisión para el canal de subida. Una vez que tanto los canales de subida y de bajada están sincronizados, el módem hace ajustes menores de ranking, que es el proceso de determinar la latencia de la red entre el CM y el CMTS. Para establecer conectividad IP el CM manda un paquete DHCP y escucha por una oferta de paquete DHCP proveniente del equipo terminal. Un servidor DHCP debe ser establecido en el equipo terminal para ofrecer este servicio. El paquete de oferta de DHCP incluye la dirección IP HFC, la dirección IP del servidor TFTP, el nombre del archivo de configuración TFTP, y la dirección IP del servidor de tiempo. El archivo de configuración TFTP contiene parámetros como la configuración SNMP y otras configuraciones de red. Una vez que el módem ha bajado el archivo de configuración, lo procesa. Luego manda una copia exacta de la configuración de vuelta al servidor CMTS, en un proceso conocido como transferencia de parámetros operacionales. Esta parte del proceso de registro es también usada para autenticar al módem. En este punto, el módem ha sido autenticado y le es permitido inicializar BPI. Finalmente, el módem se conecta al backbone de Internet del operador y se le permite acceder a la Web.

2.3. Firmware.

El firmware permite controlar todo aspecto del módem además de cambiar y añadir nuevas características al mismo con sólo actualizarlo. Cuando se hackea un módem, el firmware es la clave; El sistema operativo del CM (parecido a Unix llamado VxWorks) es controlado por el firmware. El firmware está almacenado en la memoria flash; esta a su vez también almacena el bootloader, un archivo de configuración permanente (dirección MAC, serial, etc.), un archivo log y un certificado (firma de identificación DOCSIS). El sistema operativo VxWorks usa código altamente optimizado para tener imágenes del firmware con muy pequeño tamaño (2 o 3 MB cuando es compilado, menor de 1 MB cuando esta comprimido).

2.4. Clonación de CM.

El principal motivo por el cual es posible la clonación de un CM y la respectiva cuenta de usuario asignado al mismo es debido a la infraestructura de las redes HFC; la división por nodos es necesaria ya que debido a que el tamaño y cantidad de usuarios del servicio en una región determinada puede llegar a ser tan grande el sistema se puede saturar obligando a dividirse en secciones teniendo un CMTS por cada nodo. Este hecho es lo que permite a un usuario con un cable-módem conectarse a un nodo el cual se registra con su respectivo CMTS y a su vez al mismo tiempo con la misma dirección MAC o identificación de equipo, conectarse en otro nodo y registrarse con otro CMTS, lo que da a lugar a que la clonación sea efectiva o sea realizable con éxito. Por lo tanto la clonación de un CM se basa en clonar la dirección MAC de un CM en un nodo distinto al cual se piensa conectar permitiendo así el acceso al servicio a un usuario no autorizado.

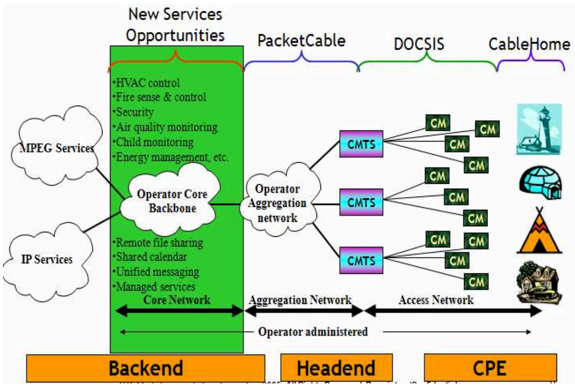

Figura 2. Esquema de la división de secciones teniendo a un CMTS por nodo.

El proceso de modificación de un cable-módem para cambiar la dirección MAC del mismo es diferente dependiendo de la marca y modelo del módem a modificar; por eso, el presente trabajo se ha centrado en cómo se realiza la modificación de un módem marca Motorola modelo SurfBoard 5100.

2.5. Modificación (Hack) del Firmware.

El hackeo de mayor éxito de un CM lo realizo un grupo de personas denominado TCNISO (www.tcniso.net); este firmware lo llaman SIGMA y, es el más utilizado debido a sus funciones y compatibilidades de sus diferentes versiones. El hackeo del firmware original fue posible debido a una falla de seguridad en el mismo y para esto fue utilizado un método conocido como desbordamiento del buffer o pila. Basándose en esta falla y colocando un punto de parada antes del reinicio del módem se tuvo acceso para ingresar datos a la memoria RAM y desde allí ejecutar comandos. SIGMA, desarrollado por TCNISO, es un programa que ejecuta instrucciones en el firmware del módem una vez que este se ha iniciado. Existen distintas versiones de SIGMA. Entre estas están versiones dependiendo del modelo del módem a utilizar y de la especificación DOCSIS utilizada por el ISP tal como SIGMA 1.7 (Motorola sb4100 y sb4200 y DOCSIS 1.0), SIGMA X (Motorola SB5100 y DOCSIS 1.0), o SIGMA X2 (Motorola sb5100 y DOCSIS 1.0, 1.1 y 2.0). Cabe indicar que existen otros firmwares modificados para otras marcas de módems y también existen métodos de hackeo de ciertos parámetros para la mayoría de módems utilizados en el mercado. Para este estudio escogimos revisar el SIGMA X2 en su versión original y la versión con algunos cambio realizada por FERCSA (www.cablemodemhack.tk) el cual se denomina SIGMA X2 Stealth Edition 13.5.

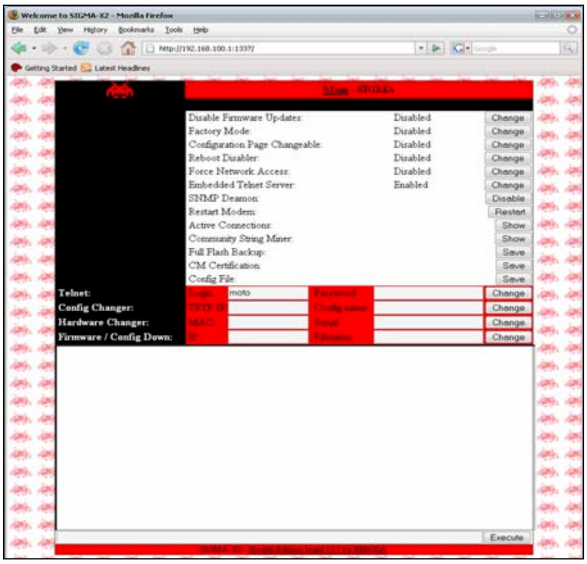

Figura 3. Interfaz gráfica de la página web de configuración de Sigma X2 Stealth Ed. V.13.5

2.6. Uncap.

Para realizar el uncap hay que tener cierta información utilizada por el ISP para comunicarse con el módem. Estos datos pueden obtenerse utilizando un sniffer. El método para obtener los archivos de configuración, el cual es compatible con DOCSIS 1.1

y 2.0, consiste en sniffear archivos de configuración en la red. Una vez que se sepa el nombre del cual se desea utilizar, se accede a la interfaz SIGMA y se coloca el nombre del archivo de configuración deseado en el campo correspondiente. Con esto, cada vez que se inicie el módem este automáticamente ira en línea usando el archivo de configuración deseado por el usuario.

2.7. Método de los Bitfiles.

El método de los Bitfiles, es un modo de administración secreta en los cable-módem Motorola serie SurfBoard mediante el cual el usuario puede usar un agente SNMP local para cambiar algunos parámetros de configuración de fábrica del módem a través de un árbol privado MIB. Cambiando los valores de los OIDs en los MIB, se puede cambiar algunos de los parámetros de fábrica del módem sin necesidad de cables ni modificaciones de hardware. También se puede modificar la memoria, permitiendo así cambiar la información o código en el módem; todos los módems son vendidos con la opción deshabilitada, pero para habilitar este modo se debe modificar vía SNMP un valor OID del módem el cual requerirá vía TFTP la transferencia de un archivo denominado bitfile (en el SB5100, el archivo es vxWorks.st)

2.8. Desarrollo del acceso no autorizado al servicio.

Existen algunos métodos para acceder a diferentes secciones del servicio de Internet de banda ancha en una red HFC que son utilizados y aprovechados por medio de los CMs. Algunas de estas técnicas pueden ser utilizadas individualmente o en conjunto para lograr obtener los objetivos deseados. Aquí haremos referencia a algunos de los métodos descritos anteriormente en el capítulo y como de esta manera se podrá acceder al servicio de Internet o a ciertos aspectos del mismo sin autorización para ello. Para empezar el usuario podría modificar el CM. Para realizar esto el usuario debería clonar una MAC o dirección física de un CM conectado a un CMTS diferente del suyo. Para que un usuario consiga una MAC a clonar este debería escanear la red HFC con un sniffer y copiar las MAC pertenecientes a otro nodo; luego de esto el usuario debería modificar la MAC de su módem. Para cambiarle la MAC al módem el usuario deberá escoger si desea utilizar el método de los bitfiles vía SNMP o si desea modificar el firmware para de esta manera tener un método fácil y sencillo para cambiar la MAC cada vez que lo requiera. A continuación, el usuario debería constatar si se encuentra en una red DOCSIS 1.0 o en un CMTS que no esté forzando el uso de BPI+. Luego de cambiar la MAC, el usuario debería configurar la BPI en el módem para trabajar en modo 0; En el caso de que el sistema este forzando el uso de BPI + (DOCSIS 1.1 o 2.0), el usuario además de cambiar la MAC debería de copiar los certificados digitales del módem. Esto se lo logra ya sea por medio del método de los bitfiles o por medio de copiar la nonvol del módem utilizando el cable JTAG y el software SchwarzeKatze. Si se desea modificar el módem, se debería hacerlo copiando la nonvol o los certificados vía SNMP del módem al cual pertenece la MAC a clonar. Luego de esto el usuario debería ingresar a la página de configuración de SIGMA y establecer las debidas configuraciones en la misma. Aquí debería indicar la MAC y el serial a utilizar, deshabilitar actualizaciones de firmware deshabilitar reinicialización del módem por parte del ISP, habilitar el forzar el acceso a la red y deshabilitar el SNMP Daemon cada vez que reinicie el módem ya que de esta manera evitaría que el módem sea monitoreado por el ISP. Luego de esto el usuario debería conectar el módem a la red coaxial y verificar los valores de intensidad de señal en la página web de diagnóstico del módem. Una vez que el módem se haya sincronizado, la señal de receive, send y llegue a estar online, el usuario debería tener acceso a Internet. Si por algún motivo no sucediera que el módem llegue a estar online, lo más común es que sea necesario cambiar la MAC. Un usuario clandestino podría además asignarse una IP fija al módem basándose en los datos de IP obtenidas por DHCP de un módem legal.

2.9. Análisis de las Vulnerabilidades en el servicio Cable-Módem de TVCable.

En el caso del servicio ofrecido por Satnet del grupo TV Cable en la ciudad de Guayaquil – Ecuador el servicio tiene muchas vulnerabilidades siendo estas diferentes de acuerdo al sector. Este ISP utiliza diferentes CMTS siendo estos 4; dos de los CMTS utilizados son de la marca Motorola del modelo BSR1K (trabajando con DOCSIS 1.1), uno es el Motorola BSR64K (trabajando con DOCSIS 1.1) y el último es uno marca ARRIS modelo C4 (de estos CMTS este es el más seguro ya que trabaja con DOCSIS 2.0). En los CMTS Motorola se pueden realizar el Uncap y se puede utilizar cualquier programa para sniffear la red en el protocolo SNMP. Por ende, es en estos CMTS donde se realiza en su mayoría la clonación. La nomenclatura de los archivos de este ISP es muy insegura ya que para la misma se utiliza la misma dirección MAC a la cual se encuentra asignada, siendo de esta manera: cm-dirección_MAC. De esta manera, un usuario sniffeando la red por direcciones MAC o conociendo la dirección MAC de otro usuario con mayor velocidad, podrá saber fácilmente cual es el nombre de archivo de configuración correspondiente y utilizarlo para hacer uncap a su módem. A pesar de que este CMTS está configurado para forzar la utilización de BPI+ en los módems y con esto evitar la fácil clonación de MAC, aún es posible clonar módems en este CMTS por medio de la copia de los certificados de otro módem conectado a otro CMTS.

3. Medidas de seguridad básicas.

No existen garantías de que se puede tener un dispositivo o red completamente seguro o que se pueda crear un mecanismo de seguridad que nunca necesitara de una actualización de mejora en un futuro. Los métodos de seguridad son modificados de forma rutinaria para hacerlos más difíciles de romper. Hay que tomar precauciones para prevenir que vulnerabilidades recientemente publicadas afecten de manera negativa una red de banda ancha activa y en crecimiento.

3.1. Mínima Interacción con el Usuario.

El cable-módem físico está diseñado para ser un dispositivo que trabaje solo y tenga casi ninguna interacción con el usuario; algunos módems permiten interactuar con información de diagnóstico, pero estas páginas están diseñadas para que el usuario sólo pueda revisar los datos.

3.2. Revisión de Integridad de Mensaje.

Para prevenir que el cable-módem baje y procese un archivo parcial o corrupto, un chequeo de redundancia de error es realizado utilizando un valor de checksum; esto también es conocido como integridad de datos (CmMic) Este es sólo usado para integridad de datos y no ofrece protección posibles cambios de los contenidos del archivo de configuración; para esto un segundo checksum de 16 bits es usado: El CmtsMic protege la autenticidad del archivo de configuración al incorporar un mecanismo de seguridad criptográfico conocido como HMAC.

3.4. Encriptación de Datos.

BPI es un subconjunto de características de seguridad diseñado para proteger la privacidad de datos en una red DOCSIS. La encriptación del flujo de datos es inicializada en el paso de privacidad base del proceso de aprovisionamiento. Los paquetes de datos sobre la intranet del proveedor son encriptados usando el algoritmo DES y un sistema de claves criptográficas privadas/públicas conocidas como el esquema de KEK.

3.5. Certificaciones Digitales.

El uso de certificados digitalmente firmados es para la autenticación del dispositivo, actualizaciones seguras de firmware, y privacidad de datos (en la forma de encriptación) Cada cable-módem que sigue las especificaciones de DOCSIS 1.1 contiene un certificado digitalmente firmado de su manufacturero que es utilizado en el chip flash del módem. Esta certificación contiene muchos rasgos únicos acerca del módem, tal como su dirección MAC y su número de serie de fábrica, y es conocido como el Certificado de Verificación de Código (CVC). Al instalar un certificado en un cable-módem, un operador de servicios puede asegurarse que el módem solo bajará e instalará el firmware que al cual está autorizado por el CMTS.

3.6. Configuración Dinámica.

A través de extensiones adicionales de QoS, un operador de cable puede implementar características tales como configuración dinámica. La configuración Dinámica es un módulo que permite al servidor de aprovisionamiento generar los archivos de configuración en la marcha cuando un cable-módem está tratando de registrarse en la red. Este tipo de configuración de host permite que el equipo de cada cliente sea configurado individualmente cuando sea necesario, en lugar de usar archivos de configuración predefinidos.

3.7. Otras medidas de seguridad.

Otras características pueden ser implementadas que no son especificadas en el estándar DOCSIS. Por ejemplo, scripts del lado del servidor también pueden ser instalados en los equipos terminales; estos involucran cambios o adiciones a la activación o aprovisionamiento actual del un equipo por un administrador de servicio autorizado.

Un tipo medida de seguridad más nueva y común es llamado el modo de bloqueo. Esta característica implementada en el CMTS asigna perfiles restringidos de QoS a los cable-módems que fallan la Revisión de Integridad de Mensaje (MIC).

Otras formas de seguridad incluyen funciones o comandos de terceros como lo son los comandos de Cisco: cable privacy bpi-plus-enforce, el comando cable qos permission, el comando cable source-verify, el comando dhcp leasequery y el comando cable tftp-enforce. Hay que tomar en cuenta que los hackers siempre están creando soluciones que den la vuelta a las medidas de seguridad. Es por eso que los administradores de red tienen que estar al tanto con la comunidad hackeadora de cable-módems.

4. Medidas de Prevención.

Durante los últimos 5 años, los sistemas de cable de banda ancha que se manejan por especificaciones DOCSIS han sido vulnerables a una variedad de métodos de hackeo. Esto ha sido posible parcialmente porque los administradores de red no han invertido el tiempo suficiente en investigar los métodos de hackeo y aprender cómo deshabilitarlos. En lo que respecta a medidas preventivas, cuando se asegura una red, el ingeniero de red de resolver adecuadamente todos los aspectos de la seguridad de banda ancha. El esperar que un parche de firmware o de software arregle una vulnerabilidad específica no es un buen método para asegurar una red de banda ancha. Los ingenieros de banda ancha necesitan estar constantemente actualizados en lo a tecnología de hackeo concierne, ya que si existiese un hueco abierto, un hacker potencial podría tomar ventaja de este. El permitir que formas de hackeo operen sin ninguna restricción es una receta para el desastre.

4.1. Evitar las colisiones de MAC

Cuando dos cable-módems intentan ponerse en línea ocurre una colisión MAC. Cuando este problema ocurre, el primer cable-módem que se registró con el CMTS es puesto fuera de línea, y al segundo cable-módem se le permite registrarse. Sin embargo, una anomalía aparece cuando una colisión MAC ocurre en una red HFC. Cuando un cable-módem intenta registrarse, su flujo de datos es encapsulado por el nodo local y luego es puenteado directamente al CMTS correspondiente. Si este intenta registrar una dirección MAC que ya esta registrada a través de un nodo una segunda vez a través de otro nodo. Este problema se lo puede solucionar por medio de comandos como cable mac access control list de Cisco.

4.2. Actualización de Plataformas a DOCSIS 1.1/2.0

El realizar una actualización de mejora de DOCSIS 1.0 a 1.1 o 2.0 es tanto caro como consumidor de tiempo. Uno de los mayores gastos será el comprar nuevos equipos CMTS que estén de acuerdo a las especificaciones DOCSIS 1.1/2.0 que cuestan $5000 (por unidad) o más. Sin embargo, la mejora valdrá la pena: Hay muchas vulnerabilidades en una red con especificaciones DOCSIS 1.0, y una mejora a DOCSIS 1.1/2.0 (y en un futuro, DOCSIS 3.0) es una manera segura de arreglarlas.

4.3. Deshabilitar la compatibilidad retroactiva.

La mayoría de las redes de cable trabajan utilizando un modo híbrido DOCSIS. Una de las razones para este soporte de tecnología antigua es que aún existen clientes que utilizan DOCSIS 1.0 y cuyos cable-módems no pueden recibir una actualización a DOCSIS 1.1/2.0, además de ser un proceso muy costoso y consumidor de tiempo. Aún a pesar de esto, los proveedores de servicios que aún soportan DOCSIS 1.0 son sólo vulnerable a la mayoría de ataques de hackers conocidos.

4.4. Habilitar la Privacía Base (BPI/BPI+)

Para habilitar BPI, tanto el cable-módem como el CMTS deben estar funcionando con firmware capaz de funcionar en modo BPI; este soporta características como ACLs. La especificación DOCSIS 1.1 se centra en BPI para proveer a los administradores de red con un mayor nivel de seguridad. BPI+ mejora mucho más la fuerza de encriptación de una débil codificación DES simple de 56 bits a una codificación DES triple de 56 bits que es usado para encriptar tanto el tráfico de subida como el de baja desde y hacia el CMTS.

4.5. Utilizar firmware firmado.

Una imagen de firmware puede ser firmada por hasta tres certificados conocidos CVCs. El firmware es firmado digitalmente con el CVC del fabricante y opcionalmente puede ser co-firmado (aunque es altamente recomendado) con el CVC del operador o el de DOCSIS. Los módems que han sido mejorados para usar el firmware con firmas digitales son mucho más seguros ya que ellos sólo aceptaran actualizaciones de firmware cuando los CVCs bajados por el módem a través del proceso de aprovisionamiento son iguales a los CVCs que protegen al firmware.

4.6. Asegurar el Protocolo de Administración Simple de Red (SNMP)

Es importante restringir el acceso al servidor SNMP del módem para asegurarse de que sólo el personal y los dispositivos autorizados puedan administrar el cable-módem. La manera correcta para hacer esto en DOCSIS es configurando un conjunto de objetos SNMP en el grupo docsDevNmAccess y codificar los valores de configuración en el archivo de configuración de inicialización del CM. En la tabla 1 se muestran los principales objetos SNMP docDevNmAccess que hay que asegurar.

TABLA 1. Objetos SNMP docsDevNmAccess

Nombre OID	ID del Objeto	Tipo de Dato
docsDevNmAccessIP	1.3.6.1.2.1.69.1.2.1.2.1	Dirección IP
docsDevNmAccessIPMask	1.3.6.1.2.1.69.1.2.1.3.1	Dirección IP
docsDevNmAccessCommunity	1.3.6.1.2.1.69.1.2.1.4.1	Cadena de Octetos
docsDevNmAccessControl	1.3.6.1.2.1.69.1.2.1.5.1	Número Entero
docsDevNmAccessInterfaces	1.3.6.1.2.1.69.1.2.1.6.1	Cadena de Octetos
docsDevNmAccessStatus	1.3.6.1.2.1.69.1.2.1.7.1	Número

		Entero

4.7. Usar monitoreo activo.

El monitoreo activo es la herramienta más importante para detectar a los hackers. El monitoreo activo es cuando el personal contratado activamente sondean los cable-módems de los clientes, revisan los logs de los routers y del sistema, examinan de manera aleatoria los perfiles de los clientes para ver si no hay anomalías, o revisan el ancho de banda actual para asegurarse de que ninguna dirección MAC está bajando más datos de la que está supuesta a bajar.

4.8. Mantenerse actualizado

Como la mayoría de los programas, los firmwares de los cable-módems son actualizados de manera rutinaria por su fabricante para añadir características o arreglar vulnerabilidades. Los fabricantes y vendedores de hardware, tales como Motorota, tienen servidores FTP especiales para los MSOs que contienen actualizaciones de firmware y notas de lanzamiento explicando los cambios en cada archivo de firmware y discutiendo las mejoras de firmware y arreglos de seguridad.

5. Conclusiones y Recomendaciones.

5.1. Conclusiones.

- Los hackers siempre estarán al tanto de cualquier modificación que se haga en el sistema.
- Se concluyó que mientras más sofisticado sea un sistema de comunicación con el cable-módem, más difíciles serán de hackear.
- Los administradores de red necesitan conocer todas las características y configuración de seguridades existentes cuando estén asegurando su red.
- El no restringir el rango IP del servidor SNMP de un cable-módem es un gran error ya que permite que cualquier IP en una subred dada tener acceso SNMP.
- Los administradores deben saber cómo los hackers piensan y las técnicas que ellos podría utilizar para evitar que los detecten.

5.2. Recomendaciones.

- Activar, forzar y deshabilitar la compatibilidad retroactiva de todas las características de seguridad de los sistemas DOCSIS que estén utilizando los cuales han sido mencionados en esta tesis, como por ejemplo en DOCSIS 1.1 o superior forzar la verificación de certificados digitales usando BPI +.
- Se recomienda la contratación de un profesional para que establezca manualmente un software del lado del servidor para que filtre de manera correcta el tráfico de red de tal manera que sólo los clientes verdaderos reciban servicio.
- Utilizar nombres de archivos de configuración codificados, de manera que no sea fácil saber por parte de un usuario el archivo de configuración perteneciente a una MAC de una velocidad conocida, haciendo así mas difícil el uncap.

6. Referencias.

[1] CABLE SECURITY, "Cable Source-Verify and IP Address Security," http://www.cisco.com/en/US/tech/tk86/tk803/technologies_tech_note09186a00800a7828.shtml, Cisco.com, Noviembre 2005.

[2] MILLET MARK, "Theft of Service-Inevitable?," http://www.cable360.net/ct/operations/bestpractices/15302.html, The cable360.net Network, Diciembre 2005.

[3] MONTAÑA ROGELIO, "Acceso Residencial de Banda Ancha," Universidad de Valencia, Departamento de Informática, www.uv.es/montanan/ampliacion/amplif_6-p2.ppt, Enero 2007.

[4] TERGAARD ROLF, "What is Baseline Privacy?," http://www.cable-modems.org/articles/security/, Cable-Modems.org: The Cable-Modem Reference Guide, 2006.

[5] RIDDEL JEFF, "Security in PacketCable Networks," http://www.networkworld.com/community/?q=node/14912, Network World, Julio 2007.

[6] SHAH N. y KOUVATSOS D., "A Tutorial on DOCSIS: Protocol and Performance Models," http://www.comp.brad.ac.uk/het-net/HET-NETs05/ReadCamera05/T08.pdf, Universidad de Bradford, Julio 2005.

[7] DerEngel "Hacking the Cable Modem What Cable Companies Don't Want You to Know". www.nostarch.com/cablemodem.htm No Starch Press, Septiembre 2006.