Universidad Técnica Federico Santa Maria
Departamento de Electronica
Valparaiso, Chile

Redes HFC (Hibrid Fiber-Coaxial) y sus vulnerabilidades

Nombre: Juan Cartagena
Rol: 2530020-3

Introducción

En esta investigación se muestran los aspectos más importantes de las redes HFC, sus estándares, topología, funcionamiento y sus vulnerabilidades, pasando por sus principales defectos y las soluciones para cada una de estas fallas para poder así incrementar la seguridad en este tipo de redes.

También se hablara con detalle de las formas existentes de vulnerar y modificar los dispositivos usados para las redes HFC y hacer un uso ilegal de estas o uso adicional del servicio contratado, adicionalmente de las contramedidas para evitar estos tipos de modificaciones y/o ataques a las redes.

La idea no es enseñar el procedimiento para el uso ilegal de estas redes, mas bien es mostrar a cabalidad las vulnerabilidades que estas tienen y a su vez las posibles soluciones que se deberían implementar.

Resumen

Las redes HFC nacen para mejorar los viejos sistemas CATV y optimizar las redes existentes para este servicio implementando el uso de Internet ancho de banda en estas. Estas funcionan en base a un estándar llamado DOCSIS que regula todo los patrones de las redes, desde los cable modem de los usuarios hasta las centrales de monitoreo o CMTS. Basadas en nodos interconectados por fibra óptica a una central y conectados internamente por cable coaxial, estas redes tienes ciertos tipos de vulnerabilidades k son posibles de explotar por el usuario como es la clonación de MACs para el acceso no autorizado al sistema o el aumento de las velocidades de subida y bajada configuradas para el usuario. Pero así como tiene un sinfín de fallas el sistema, también hay muchas medidas para contrarrestar estas fallas y así evitar accesos no autorizados a la red, claro esta que ninguna tecnología es 100% segura pero se pueden tomar las medidas respectivas para tratar de hacer que esta sea lo mas segura posible o simplemente hacerles mas difícil a los hackers conectarse de forma ilegal en sus sistemas.

Red HFC (Hibrid fiber-coaxial)

Red HFC o hibrida fibra-coaxial es denomina de esta forma claramente por que esa compuesta tanto de enlaces de Fibra Óptica como también de cable coaxial. Estas nacen en evolución a las antiguas redes CATV o televisión de antena comunitaria. Esta consta de dividir las zonas de servicios en grupos de entre 500 a 2000 viviendas llamados nodos, la señal llega a cada nodo por cables de fibra y esta es repartida dentro de los nodos por cable coaxial.

La estandarización de las redes HFC se ha hecho mediante el estándar DOCSIS. DOCSIS son las siglas de Especificación de Interfaz de Servicios de Datos Por Cable (Data Over Cable Service Interface Specification), 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, lo cual permite añadir transferencias de datos de alta velocidad a un sistema CATV sobre una infraestructura Híbrida-Fibra-Coaxial (HFC) existente. Este comienza a ser desarrollado por la empresa CableLabs en el año 1997 con la colaboración de otras compañías. DOCSIS es el principal estándar usado por los cable-módem en la actualidad.

El estándar DOCSIS cubre todo elemento de la infraestructura de un cable-módem, desde el equipo local del cliente (CPE por sus siglas en inglés) hasta el equipo terminal (head-end) del operador. Esta especificación detalla muchas de las funciones básicas del cable-módem de un cliente, incluyendo cómo las frecuencias son moduladas en el cable coaxial, cómo el protocolo SNMP se aplica a los cable-módems, cómo los datos son interrumpidos (tanto los enviados como los recibidos), cómo el módem debe conectarse en la red con el CMTS, y como la encriptación es iniciada. Muchas funciones adicionales son definidas, pero por lo general no son usadas a menos que el CMTS lo requiera.

Tres versiones principales de estándares DOCSIS han sido sacados e implementados. El más popular, el cual la mayoría de los cable-módems y equipos terminales soportan, es DOCSIS 1.0. DOCSIS 1.0 es el estándar original implementado en 1998. La principal meta de este estándar fue crear interoperabilidad entre cable-módems y proveedores de servicios. DOCSIS 1.0 incluye muchas especificaciones que son opcionales y que no son requeridas para la certificación, y esto resultó en muchos problemas de seguridad. Por ejemplo, los clientes fueron capaces de cambiar el

firmware de su módem ya que el servidor SNMP del módem no estaba configurado para deshabilitar la administración local Ethernet.

Topología de las redes HFC.

Los equipos del cliente o CPE (Costumer Premise Equipmente) por sus siglas en inglés, tales como una PC casera, se comunican sobre una conexión de red utilizando el protocolo IP. Usualmente esto es hecho con una tarjeta de interfaz de red Ethernet y un cable de categoría-5 (CAT5); sin embargo, nuevos modelo de módems proporcionan una interfaz USB en su lugar. El cable-módem mismo se conecta a un cable coaxial compartido que usualmente conecta muchos otros módems y termina en un nodo HFC. La figura 1.1. Muestra como funciona esto.

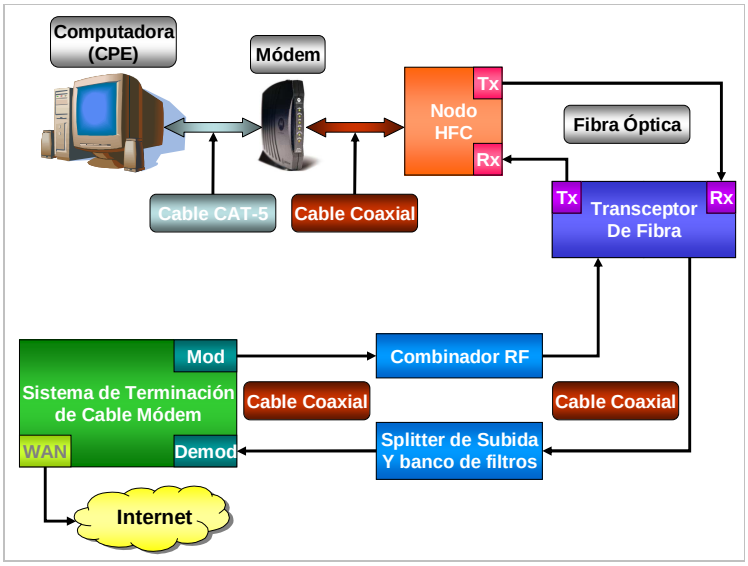

Figura 1.1. Diagrama Detallado de la Topología DOCSIS

Un nodo híbrido de fibra y coaxial (HFC) es un dispositivo de campo de dos vías que convierte las frecuencias analógicas a señales digitales y viceversa. El nodo de fibra toma las frecuencias de radio en un cable coaxial (transmitidas desde el cable-módem), 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 1.1) 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: Uno para la

transmisión de datos (Tx) y el otro para la recepción de datos (Rx). Los nodos HFC ofrecen a los proveedores de servicios muchas ventajas.

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 nodo concentrador o repetidor multipuesto (hub) central en el equipo terminal del proveedor (llamado transceptor de fibra en la figura 1.1.) 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 (entradas) hacia un solo medio compartido (salida). El combinador de RF también es usado para añadir al cable coaxial xlas frecuencias de otros servicios, tales como los canales de televisión digital o análoga. El hub transmite frecuencias de 5 a 42 MHz a un divisor de señal (splitter) de subida y banco de filtros. Estos datos son solo los datos que regresan (subida) de todos los cable-módems.

Finalmente, tanto las señales de subida como las señales de bajada se conectan al Sistema de Terminación de Cable-módems o CMTS (Cable Modem Terminal System). 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, el cual usualmente está montado sobre un bastidor (rack), procesa todos los paquetes en frecuencia específicas; también tiene un puerto de Red de Área Amplia (WAN) que usualmente está conectado directamente al backbone de Internet o a otra puerta de enlace al Internet.

Vulnerabilidades

Las fallas o bondades de seguridad que pueden ser encontradas en un sistema de Internet de banda ancha en una red HFC de cualquier operador en todo el mundo dependerán de los siguientes factores utilizados por el proveedor de servicios, los cuales son:

- El estándar DOCSIS utilizado.
- La marca del CMTS utilizado en la cabecera junto con sus respectivas opciones de seguridad y utilización de aplicaciones.

- Scripts, plugins, herramientas de monitoreo o soluciones específicos para los ruteadores o CMTS utilizados que puedan ser implementados en los mismos.
- Parámetros especificados y utilizados en los archivos de configuración a enviar a los módems.
- El módem utilizado el cual no debería permitir que el usuario lo modifique a su conveniencia.

La especificación DOCSIS detalla los procedimientos que un módem deberían seguir para registrarse en una red de cable; esto es llamado el proceso de aprovisionamiento (provisioning).En el proceso de inicialización, en primera instancia, el cable-módem solicita al CMTS que le envíe los parámetros de configuración necesarios para poder operar en la red de cable, Inmediatamente después, el cable-módem solicita al servidor de hora del día, la fecha y hora exacta, que se utilizará para almacenar los eventos de acceso del suscriptor. Luego de esto comienza el proceso de registro haciendo efecto la privacidad de línea base(BPl) o BPI+ según sea la versión de DOCSIS, estos son certificados de seguridad usados en DOCSIS. Una ves hecho el registro el Cable-modem comienza a escanear frecuencias de bajada desde una lista que viene incorporada en el cable-modem, una ves que encuentra una frecuencia de bajada este se engancha a ella previa comprobación de la MAC del cable-modem. Una ves enganchado al canal de bajada este escucha paquetes conocidos como Descriptores de Canal de Subida que contienen los parámetros de transmisión para el canal de subida, una ves que el canal de subida y el de bajada están sincronizados, el MODEM hace ajustes menores con la ubicación de rango. Luego el cable-modem debe de establecer conexión IP con el CMTP, luego este recibe la dirección IP del servidor TFTP y el nombre del archivo de configuración TFTP. Ahora el módem debe conectarse con el servidor TFTP y pedir el archivo de configuración TFTP. Este archivo contiene parámetros importantes, tales 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. Si el módem está enlistado en la base de datos del CMTS como válido, el módem recibe un mensaje del CMTS que este ha pasado el registro. En este punto, el módem ha sido autenticado y le es permitido inicializar su privacidad base, un paso adicional que le permite al módem inicializar características de privacidad que le permiten encriptar y desencriptar su propio tráfico

de red desde y hacia el CMTS. La encriptación está basada en un certificado privado digital (estándar X.509) que es instalado en el módem antes de su registro. Finalmente, el módem se conecta al backbone de Internet del operador y se le permite acceder a la Web. En este punto el cable-módem está en estado operacional

- Clonación De Cable-Modems:

El cable-módem es el equipo fisco al cual el usuario tiene acceso y es mediante el que se conecta a la red HFC privada del proveedor de servicios de Internet. Para funcionar necesita de un sistema operativo llamado Vxworks el cual realiza las funciones necesarias para permitir el acceso al módem a la red

El principal motivo por el cual es posible la clonación de un cable-módem y la respectiva cuenta de usuario asignado al mismo es debido a la infraestructura de las redes HFC, estas se dividen en nodos o secciones lo cual tiene la ventaja de que si un nodo cae o sale de línea, sólo se verán afectados los usuarios conectados a ese nodo y el resto de usuarios conectados a los otros nodos no se verán afectados, además esto es necesario ya que debido al tamaño y cantidad de usuarios del servicio en una región determinada puede llegar a ser tan grande que el sistema se satura obligando a dividirse en secciones teniendo un CMTS por cada nodo.

Por lo tanto este factor es inevitable ya que en grandes ciudades la cantidad de usuarios llega a ser tan grande que se llega a necesitar hasta más de una decena de nodos dependiendo de la capacidad de los CMTS utilizados.

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 cable-módem se basa en clonar la dirección MAC de un cable-módem en un nodo distinto al cual se piensa conectar permitiendo así el acceso al servicio a un usuario no autorizado.

Modificar el sistema operativo del módem o firmware es el paso que mayores posibilidades da a un usuario para realizar un sinnúmero de actividades no permitidas normalmente con el firmware original del módem. Para que esto sea posible, primero es necesario encontrar una falla de seguridad en el mismo y explotarla, permitiendo al usuario utilizarla para acceder al sistema del módem y desde ahí tener acceso al sistema del módem ejecutando funciones y comandos para realizar cambios en el

funcionamiento del mismo, como en este caso, cambiar su MAC. Para poder hacer este cambio es necesario conectarse por un puerto JTAG que el modem trae en su interior.

- UNCAP:

Otro método para alterar el modem es el uncap, uncap es el proceso de bajar un archivo de configuración vía TFTP, que no corresponde a la cuenta designada del módem, y cuya finalidad es tener un archivo de configuración que tenga mayores límites de velocidades de transferencia de bajada y subida de información a través del módem. Puede que la MAC que se esté utilizando tenga asignado un archivo de configuración no deseado por el usuario debido a su velocidad asignada; en este caso el usuario podría uncapear el módem, es decir, incrementar su velocidad de transferencia bajando un archivo de configuración que le corresponde a otra MAC.

Este método funciona sólo en sistemas DOCSIS 1.0 y no en las en las especificaciones DOCSIS superiores. Esto se debe a que, en primer lugar, la medidas de seguridad no permiten bajar estos archivos del servidor TFTP, segundo no permiten al módem ir al estado de online si este se bajo el archivo de configuración de otro medio que no sea el cable coaxial, y tercero los archivos de configuración de especificaciones DOCSIS superiores al 1.0 vienen con una verificación MD5 y encriptación con una clave dada por el ISP que impiden que registrar al módem en la red si su archivo de configuración fue editado por un usuario al no realizar satisfactoriamente la comprobación MD5.

Medidas de prevención.

En lo que respecta a medidas preventivas, hay que recordar que los ingenieros de redes HFC son los responsables de asegurar y mantener la red (de banda ancha) cable-módem. Para este efecto, los ingenieros cuentan con dos herramientas indispensables a su disposición. Estas herramientas son el hardware de enrutamiento de banda ancha (CMTS) y los softwares de administración de red. Un ingeniero de red puede trabajar con estas herramientas sin necesidad de abandonar el equipo Terminal. Si un ingeniero debe salir a hacer trabajo de campo (en el área del subscriptor), herramientas adicionales, como módems de diagnóstico seguros, también podrían usarse. Cuando se asegura una red, el ingeniero de red debe resolver adecuadamente todos los aspectos de la seguridad de banda ancha. Este proceso de asegurar una red HFC es muy consumidora de tiempo, además de ser caro, especialmente cuando un nuevo hardware es requerido, como cuando se migra de DOCSIS 1.0 a DOCSIS 1.1/2.0;

y 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.

Entre algunas de las opciones que los administradores de red tienen para asegurar una red se encuentran las siguientes:

- Evitar colisiones de MAC
- Actualización de Plataformas a DOCSIS 1.1/2.0
- Deshabilitar la compatibilidad retroactiva
- Habilitar la Privacía Base (BPI/BPI+)
- Considerar utilizar firmware hecho para las necesidades de la empresa.
- Utilizar firmware firmado
- Asegurar el Protocolo de Administración Simple de Red (SNMP)
- Usar monitoreo activo
- Mantenerse actualizado

Conclusiones

Se puede concluir de este trabajo que por mas que se creen nuevas tecnologías o nuevos medios de seguridad, siempre habrán personas que podrán quebrar estas seguridad ya sea para hacer daño o para hacer abuso de estas, podemos hacer mas difícil que se quiebre la seguridad de estas pero igual se hará, solo nos queda el método mas eficiente para controlar los accesos ilegales que es el constante monitoreo de el estado de las conexiones y estar al tanto de los procedimientos que usan los hacker para explotar estas fallas.

Referencias

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL
Facultad de Ingeniería en Electricidad y Computación
“Vulnerabilidades de Seguridad en el Servicio de Internet de Banda Ancha en Redes HFC: Impacto y Posibles Soluciones”
TESIS DE GRADO
Año: 2007