UNIVERSIDAD TECNICA
FEDERICO SANTA MARIA

Redes HFC: Vulnerabilidad y Posibles Soluciones

Nombre: Jorge Andrade Catalán

Rol: 2530046-7

Valparaíso, 14 de Julio del 2010

INTRODUCCION

En este informe se muestran los aspectos más importantes de las redes HFC, su topología, funcionamiento, vulnerabilidades y posibles soluciones.

El objetivo es profundizar en las principales vulnerabilidades existentes en este tipo de redes, la modificación de dispositivos y el uso ilegal de este servicio.

Finalmente se explicaran posibles soluciones existentes en la actualidad, su modo de implementación y como todo esto afecto al usuario final.

RESUMEN

En la actualidad está muy difundido en todo el mundo el acceso a internet de banda ancha por medio de redes HFC (Red Hibrida Fibra-Coaxial), estas han sido una evolución de las antiguas redes de CATV (Television por Cable).

Las redes HFC al ser tan masivas actualmente, están expuestas constantemente a posibles violaciones de seguridad, siendo las vulnerabilidades de este sistema un problema global.

El servicio de Internet de banda ancha de las redes hibridas fibra-coaxial cubren gran parte del mercadoactual en nuestro país, en cuanto a conectividad; con este trabajo se analizarán las vulnerabilidades 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.

Por lo tanto la aplicación de las recomendaciones dadas en esta investigación será de una gran ayuda para combatir el acceso no autorizado al servicio así como del uso indebido del mismo.

Red HFC (HibridFiber-Coaxial)

Red HFC es una red de telecomunicaciones por cable que combina la fibra óptica y el cable coaxial como soportes de la transmisión de las señales. Esta tecnología permite el acceso a internet de banda ancha utilizando las redes CATV existentes. Se puede dividir la topología en dos partes. La primera consiste en conectar al abonado por medio de cable coaxial a un nodo zonal y posteriormente interconectar los nodos zonales con fibra óptica. Esta tecnología comienza a implementarse a través de operadores de CATV que además de brindar el servicio de televisión por cable anexaron transportar por el mismo medio la señal de internet de banda ancha.

DOCSIS

Con la creación de redes HFC se ha debido especificar un conjunto de estándares llamado DOCSIS (Data Over Cable Service Interface Specification). DOCSIS fue desarrollado por CableLabs. Se trata de un estándar no comercial que define los requisitos de la interfaz de comunicaciones y operaciones para los datos sobre sistemas de cable, lo que garantiza la interoperabilidad de la tecnología empleada en la transmisión de datos a alta velocidad en una red de cable.

La primera especificación DOCSIS fue la versión 1.0, publicada en marzo de 1997, seguida de la revisión 1.1 en abril de 1999.El estándar DOCSIS se encuentra actualmente en la versión 2.0, publicado en enero de 2002. La versión europea de DOCSIS se denomina EuroDOCSIS. La principal diferencia es que en Europa, los canales de cable tienen un ancho de banda de 8 Mhz (PAL), mientras que en Norte América, es de 6 MHz (NTSC). Esto se traduce en un mayor ancho de banda disponible para el canal de datos de bajada (desde el punto de vista del usuario, el canal de bajada se utiliza para recibir datos, mientras que el de subida se utiliza para enviarlos). También existen otras variantes de DOCSIS que se emplean en Japón.

El 7 de agosto de 2006 salieron las especificaciones finales de DOCSIS 3.0, cuya principal novedad reside en el soporte para IPv6 y el "*channelbonding*", que permite utilizar varios canales simultáneamente, tanto de subida como de bajada, por lo que la velocidad podrá sobrepasar los 100 Mbps en ambos sentidos. Los equipos con el nuevo protocolo llegarán a velocidades de descarga de datos de 160 Mbps y subidas a 120 Mbps. La nueva versión DOCSIS 3.0 ya se encuentra implementada en varios países (Norte América, Europa y Asia principalmente)

Topología de las redes HFC.

El CMTS es un equipo que se encuentra normalmente en la cabecera de la compañía de cable y se utiliza para proporcionar servicios de datos de alta velocidad, como Internet por cable o Voz sobre IP, a los abonados.

Los equipos del cliente o CPE (CostumerPremiseEquipmente), se comunican sobre una conexión de red utilizando elprotocolo IP. Usualmente esto es hecho con una tarjeta de red Ethernet y un cable de categoría-5 (CAT5). El cable-módem se conecta a un cable coaxialcompartido que usualmente conecta muchos otros módems y termina en un nodo HFC.

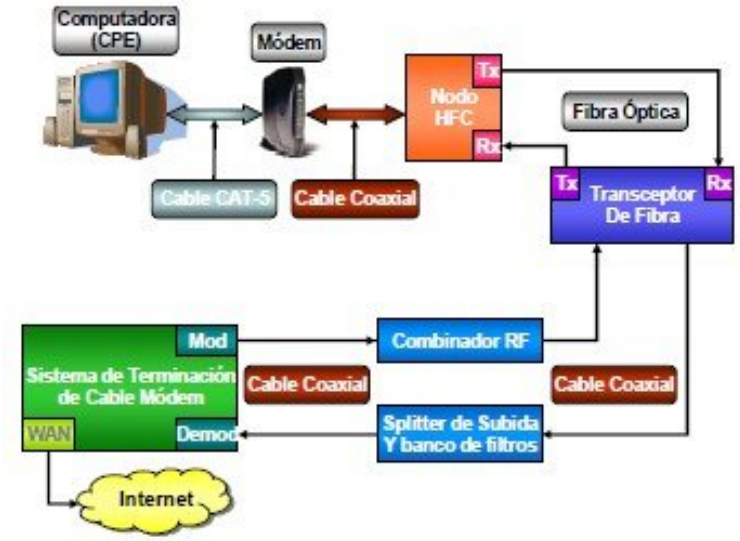
Un nodo HFC es un dispositivo de campo de dos vías que convierte las frecuencias analógicas a señales digitales y viceversa. El nodo defibra toma las frecuencias de radio en un cable coaxial transmitidas desde el CM, las convierte en señales digitales, y luego transmite los datos a un cable de fibra 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 HFC 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, estos usualmente son ubicados estratégicamente en sectores 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 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. El combinador de RF también es usado para añadir al cable coaxial las 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 de todos los CM. 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, el cual usualmente está montado sobre un bastidor, 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.

Topología Red HFC



Seguridad y Vulnerabilidad en Redes HFC

La seguridad o vulnerabilidad de la red HFC está determinada por varios factores.

- Estándar DOCSIS (1.x, 2.0 o 3.0)
- CMTS utilizado en cabecera con sus opciones de seguridad y aplicaciones.
- Herramientas de monitoreo Implementadas por los cable-operadores.
- Parámetros de conexión en archivo de configuración que es enviado al CM.

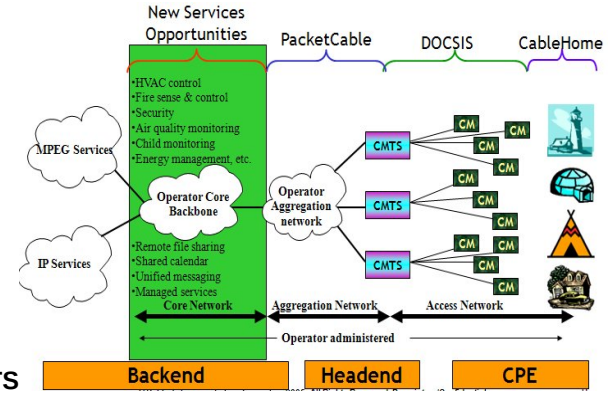
La especificación DOCSIS detalla los procedimientos que un módem deberían seguir para registrarse en una red de cable; esto es llamado el proceso de aprovisionamiento (provisioning).

Registro e inicialización del CM con el CMTS

1. Configuración en canal de bajada a utilizar (DownstreamChannel)
2. Obtención de parámetros de subida (UpstreamParameters)
3. Rango de frecuencia en el canal de subida a utilizar (UpstreamRanging)
4. Establece conexión IP a través de DHCP
5. Establece Hora y Fecha para efectos de monitoreo
6. Transferencia de parámetros de operación a través de TFTP
7. Registra Conexión con CMTS
8. Inicia Privacidad de Línea Base (BPI o BPI+)

Clonación de Cable Modem (CM)

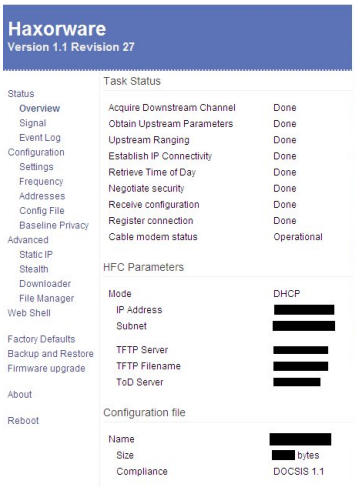
El CM es el equipo fisco al cual el usuario tiene acceso y es mediante el que se conecta a la red HFC del proveedor de servicios de Internet.Este método es posible gracias a la arquitectura de la red HFC. En caso que un CMTS se caiga de la red, no todos los usuario se verán afectados, solo aquellos conectados a dicho CTMS, esta es una vulnerabilidad bastante explotada.Esto permite a un CM conectarse a un nodo y establecer conexión con su respectivo CMTS. Al mismo tiempo con la misma MAC clonada en otro CM puede conectarse a otro nodo y establece conexión con un CMTS distinto.

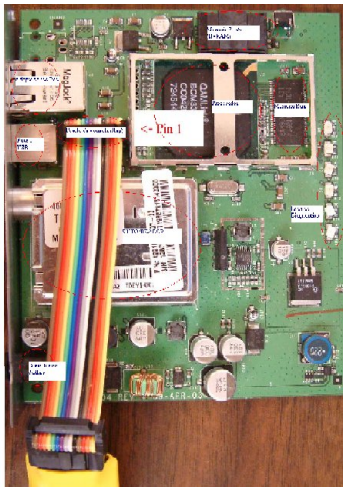


CM conectado en distintos CMTS

Por lo tanto la clonación de un CM se basa en clonar la MAC de CM en un nodo distinto al cual se piensa conectar permitiendo así el acceso alservicio a un usuario no autorizado.Para poder clonar la MAC es necesario modificar el firmware del CM o bien activar el Factory Mode para tener acceso a los parámetros de configuración del CM. Para que esto sea posible, primero es hay que conectarse al puerto JTAG del modem que se encuentra en sus interior. Con las herramientas necesarias tanto de hardware (USBJTAG o BLACKCAT), como de software (USBJATG SCRIPT, HAXORWARE, SIGMA) es posible ingresar al firmware del CM y modificarlo.

Firmware modificado Haxorware cargado por el puerto JTAG





UNCAPPING

Otra vulnerabilidad en la red HFC es en el proceso de obtención de parámetros del archivo de configuración a través de TFTP. Este archivo de configuración contiene los parámetros necesarios para realizar la conexión, además de los parámetros de bajada y subida a la cual se conectara el CM.

Al tener el firmware modificado, una de las tantas opciones es la de descarga del archivo de configuración (Config File), el cual puede ser editado con cualquier editor Hexadecimal. Con esto modificamos los parámetros de bajada y subida. Luego creamos un servidor TFTP propio para subir el archivo de configuración, así el CMTS no se entera de la modificación del config file servido por él.

Este tipo de falla en la seguridad es muy explotada debido a que es posible alcanzar altas velocidades de conexión dependiendo del DOCSIS.

Config File modificado a una tasa de 80 Mbps/10 Mbps

	1	2	3	4	5
01 Class ID	2				
02 Maximum DS Rate	81920000				
03 Maximum US Rate	10240000				
04 US Channel Priority	1				
05 Minimum US Data Rate	0				
06 Maximum US Xmit Burst	1600				
07 Privacy Enable	1				
Skip This Flow	☐	☐	☐	☐	☐

Medidas de Seguridad Implementadas

Los cable-módems pueden implementar cinco diferentes formas de seguridad. Estas son:

- Restricciones en la habilidad para mejorar el firmware
- Control de dispositivos asegurados por el proveedor de servicios.
- Un checksum criptográfico (algoritmos HMAC-MD5) que aseguren la integridad del archivo de configuración.
- Certificación digitalmente firmada (usada para la autenticación de los módems)
- Claves públicas y privadas usadas para encriptar datos y comunicaciones.

Adicional a estos métodos básicos, softwares de terceros, tal como la función TFTP Enforce de Cisco, pueden añadir más opciones de seguridad al proceso de registro, tal como autenticación adicional. Estos métodos son primeramente diseñados para autenticar el equipo del usuario final y la información de registro.

Conclusión

Por más que se creen nuevas tecnologías o nuevos medios de seguridad, siempre habrán personas que podrán vulnerar estas fallas de seguridad ya sea para hacer daño o para hacer abuso de estas, podemos hacer más difícilque se quiebre la seguridad de la red, solo nos queda el método maseficiente para controlar los accesos ilegales que es el constante monitoreo del estadode las conexiones y estar al tanto de los procedimientos que usan los hacker paraexplotar estas fallas.

DOCSIS 3.0 parece ser un avance bastante significativo en el tema de seguridad HFC, pero así como se pueden solucionar algunas brechas de seguridad, se puede producir otras. Lo importante es que las ISP se preocupen de asegurar sus redes invirtiendo en hardware de alta tecnología y del software correspondiente para el constante monitoreo.

Fuentes de Referencia:

- http://es.wikipedia.org/wiki/DOCSIS
- http://www.forocable.com/foro/ (foro de debate)
- http://majorthreat.net/ (firmware alternativo)

Presentaciones Adicionales

- *"Transferencia de Datos Mediante Cablemodems"*

Ingeniero Juan GarciaBish

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

Escuela Superior Politécnica Del Litoral