

# Inseguridad en Redes de Cable

Hoy en día la tendencia de los usuarios a la hora de decidir sobre su conexión a Internet se decanta por la alta velocidad, bien sea por ADSL o por redes de cable. Sabiendo que cada tecnología tiene sus aspectos positivos y negativos, no se puede decir que una es mejor que otra. En el caso de las redes de cable podemos afirmar que adolecen principalmente de ciertas carencias de seguridad. Existen ataques documentados realizables en estas redes, pero esta información está muy dispersa, lo que ha impedido hasta ahora un análisis global de la situación.



Leonardo Nve

## Funcionamiento de una red de cable

El par fibra óptica/ coaxial permite un amplio conjunto de servicios: pago por visión, vídeo bajo demanda, televisión digital y analógica, telemetría, telefonía e Internet 24 horas a altas velocidades, etc. En este último servicio es en el que se han centrado las investigaciones de ESA Security que se evidencian en este trabajo.

La especificación *Data Over Cable Services Interface Specification* (DOCSIS) es la encargada de asegurar la interoperabilidad del hardware. Además, facilita la instalación y abarca campos como la seguridad en estas redes. Cablemodems (CM), cablerouters (CMR) y cablemodems terminales del sistema (CMTS) son los principales dispositivos que se tendrán en cuenta en este artículo.

Simplificando, el proceso de conexión de los CM (o CMR) sigue los siguientes pasos:

- Cuando encendemos el CM, por el protocolo BOOTP pide IP al CMTS y la configuración que ha de tener.

- El CMTS asigna una IP interna al CM y le dice qué configuración en forma de fichero debe coger y de qué servidor TFTP.

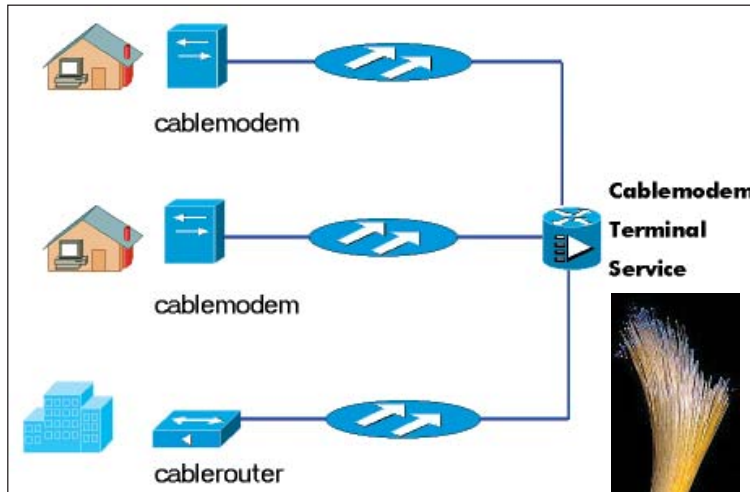
- El CM coge el fichero y se autoconfigura, pudiendo ya proveer de servicio.

Fijándonos para este artículo únicamente en lo relevante de este fichero de configuración, se observa que en él se especifican IPs permitidas para la gestión del CM, comunidades SNMP, número de equipos con permiso para acceder a la red y la velocidad de subida y bajada (ya que es este dispositivo el que regula la velocidad con la que cada cliente accederá a Internet).

Debido a que varios CMs pueden estar conectados a un mismo CMTS, (lo que denominamos segmento), y cada uno puede tener diferentes configuraciones, a la hora de darle de alta el proveedor registra su MAC (la del interfaz coaxial) y le asigna un fichero de configuración. De esta forma, el CMTS para asignar una configuración primero consulta la base de

datos MAC - fichero de configuración.

Por lo que se refiere al tráfico de red, el CM recibe tramas ATM (pueden ser otras diferentes, pero éstas son las más habituales) desde el CMTS, que transforma en tramas ethernet. Éstas son enviadas por su interfaz interna, por la que está conectado a uno o varios equipos a través de red ethernet, o bien a través de un conector USB que la emula. Igualmente el CM transforma el tráfico



co ethernet que mandan los equipos internos a tramas ATM.

Para los usuarios todo lo que hay es simplemente tráfico ethernet. El proceso de conexión del usuario es muy simple: los equipos piden por DHCP una IP y el CMTS les asigna una IP, que puede ser interna o directamente de Internet, con su correspondiente gateway.

## VULNERABILIDADES:

### 1. Captura de tráfico ajeno

Bajo la consideración de que las redes de cable funcionan como una red ethernet, lo primero que se podría deducir es que las mismas vulnerabilidades que son aplicables a este tipo de redes son aplicables a las redes de cable. En realidad, esto es sólo una verdad a medias.

En una red de cable existen dos canales, uno de subida, único para cada CM, y otro de bajada, que es el mismo para todos los usuarios de un segmento. Es decir, los datos de

bajada de todos los usuarios llegan a todos los CM.

Como ya se ha mencionado, en el fichero de configuración de un CM viene el número de equipos que pueden acceder a la red. El CM registra las MACs de los equipos que piden IP por DHCP. Sólo puede almacenar tantas MACs como equipos permitidos y esta lista la refresca cada vez que es reiniciado. Además de para restringir el número de equipos a los que dar servicio, el filtro por MAC también sirve para que el CM no permita que el tráfico de bajada de otros usuarios llegue a nosotros.

Aquí es cuando saltan las alarmas por primera vez. El que escribe estas líneas se preguntó, "¿y si cambio la MAC de mi tarjeta de red por la de otro usuario?". Haciendo esta prueba en un laboratorio diseñado para estas investigaciones, pudo comprobarse que me llegaba el tráfico de bajada de mi otro equipo, el cual estaba conectado al mismo CMTS pero con otro CM. Igualmente, al otro usuario le llegaba mi tráfico de bajada. Esto es, sistemas MS Windows levanta una alerta de duplicidad de MACs en la red (el sistema ve que recibe paquetes pero que esa IP no es la suya). Esta alerta se puede eludir sencillamente no generando tráfico de red.

A la hora de llevar este ataque a la realidad, para conseguir la MAC de un cliente, sólo habría que ejecutar nuestro *sniffer* preferido, hacer pings a IPs colindantes y al recibir la respuesta ver la MAC de la tarjeta de red origen.

La gravedad del asunto es muy alta, ya que, aun a pesar de no tener el tráfico de subida, un usuario malicioso podría analizar el tráfico que recibimos, qué webs visitamos, puede leer

nuestro correo si captura el tráfico mientras nosotros nos bajamos el correo, e incluso, si tenemos algún servicio que requiera una autenticación sin codificar (por ejemplo un servidor FTP), podría ver el *login/password* que usan usuarios externos para entrar en nuestros servicios.

Pero puede ser incluso más grave. Como parte del compendio de herramientas internas para auditorías, en ESA Security hemos desarrollado una herramienta capaz de secuestrar la conexión, pudiendo, por ejemplo, tomar el control cuando el usuario ya se ha autenticado contra un servicio (piénsese por ejemplo en una conexión Telnet).

Al analizar la forma de resolver este problema, se pensó en enrutar todos los paquetes a través del CMTS (generalmente un Cisco UBR7200). De esta manera, la MAC de origen entre comunicaciones locales siempre será la del enrutador y al no existir tráfico de bajada para el router no es susceptible de ser interceptado.

A esta solución se le encontraron varios problemas. Uno es que se presupone el desconocimiento de la MAC del usuario "objetivo". Otro problema es que, mediante consultas a través de Netbios, MS Windows dice la MAC de la tarjeta de red.

## 2. Tráfico Broadcast de Netbios

Me voy a centrar poco en este punto ya que me consta que esta vulnerabilidad ha sido rápidamente solucionada por los Operadores de Cable. En los primeros tiempos del cable, primero en EEUU y después en España, y ante mi asombro e incredulidad, los paquetes *broadcast* del protocolo Netbios actuaban como tales dentro de un mismo segmento de red, pudiendo cualquier usuario ver en "toda la red" de MS Windows los usuarios que tienen Netbios activado. Esto, sumado a que la mayoría de estos usuarios no son ni administradores ni siquiera informáticos, compartían alegremente sus discos duros a merced de virus, *hackers* y curiosos.

La solución que tomaron los Operadores fue filtrar por un lado los paquetes broadcast y por otro los puertos 139 y 445. En todo caso, desde mi punto de vista la supresión de servicios legítimos no es la solución a los problemas. La solución debería de ser la información a los usuarios sobre cómo mantener una mínima seguridad.

## 3. Desvío de tráfico mediante paquetes ARP

Aun solucionando los ataques anteriormente explicados, aunque sea imposible o muy difícil conseguir la MAC de un usuario a quien queremos "sniffar" el tráfico, aún nos quedan los ataques de ARP spoofing. Al igual que en una red ethernet con un switch, el ataque consiste en hacer que un equipo crea que la MAC de una IP local es la de otro equipo de la misma red. Así, le enviará a este mismo el tráfico que originalmente no era para él.

Este ataque en las redes de cable consiste en hacer que el CMTS crea que la MAC de cierto usuario es la de otro y al enrutar hacia la red de cable lo hará con una MAC errónea que será reconocida por el CM del usuario malicioso y no por el del usuario original.

Este ataque permite desviar un paquete TCP por cada conexión que tuviera el usuario legítimo. La conexión no continuaría, ya que no sigue la negociación, pero con ese paquete se pueden averiguar los sitios por los que navega ese usuario, partes de correos-e y muchas cosas más. Peor aún, con este simple paquete se puede hacer el anteriormente mencionado secuestro de conexión, con las consecuencias ya expuestas.

## 4. Seguridad del hardware

Existen otros peligros que conciernen a los Operadores: el hardware que controla la velocidad de conexión, que mide el tráfico individualmente y hace otras funciones im-

portantes, está en los hogares u oficinas de los usuarios.

Es sabido en el mundo de la seguridad que si terceros pueden manipular a su antojo hardware de propiedad ajena, éste ha de ser considerado no confiable. Esto mismo es lo que sucede en redes de cable. Los CM y CMR que se usan como hardware de acceso poseen sistemas de gestión remota por SNMP o vía WEB. Estos sistemas suelen ser accesibles por defecto (comunidades SNMP public y private). Existen manuales en Internet sobre esta cuestión a disposición de cualquiera.

Aun a sabiendas de que mediante los archivos de configuración que se cargan al arrancar el CM los Operadores pueden cambiar la configuración de este hardware, puede afirmarse que este hardware no es confiable. Usuarios con una "curiosidad extrema"

Vulnerabilidad	Recomendación
Tráfico Broadcast	Filtro a nivel del CMTS.
Captura de tráfico ajeno ARP spoofing	Instalar DOCSIS v1.1 o v2.0 MACs Estáticas. Sistemas IDS.
Seguridad del hardware	Mantenimiento actualizado de los firmwares y versiones de sistemas operativos.

pueden manipular estos equipos para averiguar datos que pueden comprometer el sistema. El problema se agrava si son estos mismos usuarios los propietarios de este hardware y no es posible obligarles a que dejen intactos los equipos. En este caso, se podría discutir la legalidad o no de «ocultar» las contraseñas (o comunidades SNMP) que un Operador le configura a un hardware de propiedad ajena. Además, se podría conseguir que el CMTS le diera al usuario más velocidad de la que tiene contratada.

Por otro lado, si echamos un vistazo a la Bugtraq e investigamos en sitios web relacionados con la seguridad, encontraremos un número de vulnerabilidades reducido pero realmente graves que afectan a estos dispositivos de acceso: comunidades SNMP por defecto que siempre están ocultas, acceso vía web a zonas restringidas, denegaciones de servicio.

Utilizando estos fallos hemos conseguido modificar las tablas de enrutamiento de estos dispositivos. El uso más extendido de esto es modificar la ruta hacia el servidor TFTP donde están los archivos de configuración, poner nosotros uno y engañar al CM con otra configuración. Así, se puede configurar el CM para que acepte todos los equipos que queramos y velocidades más altas de las contratadas.

Es sabido que estos ataques son practicados con asiduidad entre clientes de Operadores de Cable y el fraude ha aumentado de forma alarmante en los últimos tiempos.

### SOLUCIONES: MEDIDAS DE SEGURIDAD

Al analizar las medidas de seguridad debemos diferenciar entre las de los usuarios,

(ya sean individuos con una conexión para su hogar, o empresas que usan este tipo de acceso para su trabajo rutinario), y las propias de los Operadores.

a) **Las de los usuarios.** Como ya se ha expuesto, las comunicaciones por cable han de considerarse inseguras. Por tanto, los usuarios han de procurar codificar sus conexiones más importantes y en la medida de lo posible reducir los servicios que ofrecen al exterior (como el Netbios).

– Por lo que se refiere específicamente a los individuos, contar con cortafuegos personales e incluso desarrollar un manual de "Homesecurity" sería lo recomendable.

– En cuanto a las empresas, deberían contar con el asesoramiento de profesionales expertos en la materia dada la criticidad del uso del cable por parte de éstas para sus comunicaciones.

En cualquier caso, los usuarios deben exigir a sus Operadores las medidas de seguridad necesarias para tener cierto nivel de seguridad, de forma que las vulnerabilidades descritas anteriormente tengan una incidencia mínima.

### b) Las acciones por parte del Operador de Cable.

En primer lugar, mantener actualizados los dispositivos de acceso. Con esto se evita la explotación de las vulnerabilidades descubiertas en estos dispositivos. Otras medidas que se deberían adoptar son: MACs estáticas, sistemas IDS que detecten los ataques de ARP spoofing y equipos con MACs duplicadas. Igualmente, se debe restringir de forma efectiva el acceso al servidor TFTP del cual un usuario podría obtener los ficheros de configuración necesarios para subirse la velocidad y defraudar así al Operador.

Aunque en realidad, los fallos están en el propio DOCSIS v1.0. Posiblemente para cuando se publique este artículo estará ya la v1.1 y en breve la v2.0. Los Operadores han de actualizarse dado que se supone que estas nuevas versiones incorporarán mecanismos para evitar estos fallos. Tan pronto como estén disponibles comprobaremos si esto es realmente así.

La conclusión es que las redes de cable aun no siendo seguras, pueden serlo. Para ello se ha de exigir que así sea al Operador y que éste y todos los usuarios sean perfectamente conscientes de la existencia de estas vulnerabilidades, y de que a raíz de éstas se pueden derivar muchas más. Incluso, en nuestro Departamento tenemos diferentes técnicas de explotar la misma vulnerabilidad, eludiendo así el efecto de parches temporales.

Se trata en definitiva de aprovechar todas las ventajas que nos ofrecen las redes de cable sin asumir riesgos innecesarios por parte de todos los agentes implicados. ■

LEONARDO NVE

Consultor de Seguridad

Departamento Técnico

ESA Security

leonardo@esa-security.com