La seguridad en la familia de protocolos SNMP

J.C. Fernández, J.A. Corrales y A. Otero

1.- Introducción

Un sistema de gestión de red basado en el protocolo SNMP (*Simple Network Management Protocol*) está compuesto por los siguientes elementos: varios agentes, o nodos gestionados, al menos una estación de gestión (*manager*), un cierto volumen de información relativa a los dispositivos gestionados y un protocolo para la transmisión de dicha información entre los agentes y las estaciones de gestión.

Los mecanismos utilizados para definir la información relativa a los dispositivos gestionados apenas han sufrido modificaciones desde su aparición a finales de los años 80. Uno de los objetivos principales de su diseño fue la flexibilidad, de modo que la información definida pudiese seguir siendo utilizada posteriormente por protocolos diferentes, o incluso por distintas versiones del mismo protocolo.

Por el contrario el requisito fundamental del diseño del protocolo fue la sencillez, lo que si bien facilitó su expansión en perjuicio de protocolos más complejos, como por ejemplo CMIP (*Common Management Information Protocol*), ha hecho necesarias varias revisiones para adaptar el protocolo a las necesidades actuales, entre las que cabe destacar las exigencias en cuanto a la seguridad del sistema.

2.- Amenazas a la seguridad

El protocolo SNMP proporciona mecanismos para el acceso a un almacén de información jerárquica compuesta por un conjunto de variables. Se distinguen dos tipos distintos de acceso a dicha información: un acceso para lectura que permite consultar los valores asociados a cada una de las variables y un acceso para escritura que permite modificar dichos valores.

Los mensajes de la primera versión del protocolo incluyen una cadena de caracteres denominada nombre de comunidad que se utiliza como un sencillo mecanismo de control de acceso a la información. Los agentes que implementan dicha versión del protocolo disponen generalmente de dos comunidades, o conjuntos de variables (no necesariamente disjuntos), identificadas por un nombre de comunidad configurable por el administrador

del sistema. Una de dichas comunidades recibe el nombre de comunidad pública, y sus variables pueden ser accedidas sólo para lectura. Por el contrario los valores asociados a las variables que componen la otra comunidad, denominada comunidad privada, pueden ser modificados.

Toda la seguridad proporcionada por el sistema se basa en el hecho de que es necesario conocer el nombre asignado a una comunidad para conseguir el acceso a la información proporcionada por sus variables. El nivel de protección ofrecido por la versión original del protocolo es, por tanto, muy débil. Más aún si se tiene en cuenta que los nombres de comunidad incluidos en los mensajes del protocolo SNMP viajan por la red en texto plano y por consiguiente pueden ser obtenidos como resultado de ataques pasivos (escuchas malintencionadas).

Además, y sobre todo en el caso de la comunidad pública, está muy extendido el uso del nombre de comunidad configurado por defecto (*public*) por lo que un usuario ajeno al sistema puede obtener gran cantidad de información acerca del mismo utilizando el protocolo SNMP.

Con el fin de aumentar la seguridad del protocolo es necesario realizar cambios en su modelo administrativo para introducir los conceptos de autentificación, integridad y privacidad así como para mejorar el control de acceso a la información.

En primer lugar se identifican las posibles amenazas a las que dicho protocolo se encuentra sometido. Las más importantes son las siguientes: modificación de los mensajes en tránsito o de su orden, suplantación y ataques pasivos (escuchas). En el caso concreto del protocolo SNMP no se consideran relevantes las amenazas de los tipos negación de servicio y análisis de tráfico.

Una versión segura del protocolo debería impedir en la medida de lo posible ataques de los tipos mencionados. El apartado siguiente describe la evolución que ha sufrido el protocolo a través de sus distintas versiones así como las principales mejoras aportadas por cada una de dichas versiones en relación a la seguridad.

3.- Evolución de la seguridad proporcionada por el protocolo

Cronológicamente hablando, el primer intento serio de dotar al protocolo SNMP de un cierto grado de seguridad se corresponde con la versión denominada SNMPsec, cuyos fundamentos se definen en los RFC 1351 y 1352. Los elementos introducidos en dicha versión para mejorar la seguridad del protocolo forman la base de todas las versiones posteriores y se siguen utilizando en la actualidad.

Las principales innovaciones propuestas en la versión SNMPsec son la identificación unívoca de las entidades que participan en las comunicaciones SNMP, lo que permitirá grandes mejoras y mayor flexibilidad en cuanto al control de acceso, así como la utilización de mecanismos criptográficos para conseguir autentificación, integridad de los mensajes y privacidad.

Dicha versión introduce los siguientes conceptos:

- *Party* SNMP. Es un contexto virtual de ejecución cuyas operaciones se pueden encontrar restringidas a un subconjunto del conjunto total de operaciones permitidas por el protocolo. Un *party* involucra un identificador, una localización en la red utilizando un protocolo de transporte determinado, una vista MIB sobre la que opera, un protocolo de autentificación y un protocolo de privacidad.

- Vista sub-árbol y vista MIB. Una vista sub-árbol es un conjunto de variables de un MIB (*Management Information Base*) que tienen como prefijo un identificador de objeto común. Una vista MIB no es más que un conjunto de vistas sub-árbol.

- Política de control de acceso. Es el conjunto de clases de comunicación autorizadas entre dos *parties* SNMP o lo que es lo mismo el conjunto de mensajes del protocolo SNMP cuyo uso se permite entre dos elementos participantes en una comunicación de gestión.

- Protocolo de autentificación. Sirve al mismo tiempo para autentificar los mensajes y para poder comprobar su integridad. Se suele utilizar un mecanismo de firmas digitales, como por ejemplo el algoritmo MD5 que calcula un *digest* del mensaje. El valor obtenido se incluye entre los datos transmitidos a la hora de llevar a cabo una comunicación.

- Protocolo de privacidad. Sirve para proteger las comunicaciones contra escuchas malintencionadas. Se utiliza, por ejemplo, el algoritmo simétrico de encriptación DES (*Data Encryption Standard*).

La versión SNMPsec se adopta inicialmente con la introducción de la versión 2 del protocolo SNMP y pasa a denominarse SNMPv2p (*Party-based* SNMPv2).

Posteriormente el marco de trabajo SNMPv2, cuya definición no contiene ningún estándar en cuanto a seguridad, se asocia con otros modelos administrativos referentes a seguridad, y aparecen tres nuevas versiones del protocolo: SNMPv2c, SNMPv2u y SNMPv2*.

La versión SNMPv2c (*Community-based SNMPv2*) utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y como tal no incluye mecanismos de seguridad. Las únicas mejoras introducidas en la nueva versión consisten en una mayor flexibilidad de los mecanismos de control de acceso, ya que se permite la definición de políticas de acceso consistentes en asociar un nombre de comunidad con un perfil de comunidad formado por una vista MIB y unos derechos de acceso a dicha vista (*read-only* o *read-write*).

La versión SNMPv2* proporciona niveles de seguridad adecuados, pero no alcanzó el necesario nivel de estandarización y aceptación por el IETF (*Internet Engineering Task Force*).

Por último, la versión denominada SNMPv2u (*User-based SNMPv2*) reutiliza los conceptos introducidos en la versión SNMPsec, introduciendo la noción de usuario. En este caso, las comunicaciones se llevan a cabo bajo la identidad de usuarios en lugar de utilizar el concepto de *party* existente en las versiones precedentes. Un mismo usuario puede estar definido en varias entidades SNMP diferentes.

4.- La seguridad en la versión 3 del protocolo

La principal novedad introducida en la versión 3 del protocolo SNMP es la modularidad. En dicha versión una entidad SNMP se considera compuesta por un motor y unas aplicaciones. A su vez el motor se divide en cuatro módulos: *dispatcher*, subsistema de proceso de mensajes, subsistema de seguridad y subsistema de control de acceso.

Se observa, por tanto, que en la versión SNMPv3 se independizan los mecanismos utilizados para la seguridad (autentificación y privacidad) y para el control de acceso. De este modo, una misma entidad puede utilizar diferentes modelos de seguridad y control de acceso simultáneamente, lo que incrementa notablemente la flexibilidad y la interoperabilidad.

Se define un modelo estándar para seguridad basada en usuarios, USM (*User Security Model*) y otro para control de acceso basado en vistas, VACM (*View-based Access Control Model*). Se aprovechan los conceptos definidos en las versiones previas y al mismo tiempo la modularidad del protocolo permite la introducción de futuros modelos independientes de los actuales.

5.- Conclusiones

El nivel de seguridad proporcionado por la versión original del protocolo SNMP no es adecuado para las necesidades actuales. En caso de utilizar una gestión basada en dicha versión es imprescindible estar informado de los riesgos involucrados, debido a la sensibilidad de la información accesible a través de dicho protocolo. Además, se debe intentar en la medida de lo posible disminuir la influencia de dichos riesgos utilizando, por ejemplo, nombres de comunidad complejos. Incluso se puede restringir el acceso utilizando mecanismos externos al protocolo, como por ejemplo listas de control de acceso implementadas sobre *firewalls*.

Versiones posteriores del protocolo han hecho uso de mecanismos criptográficos y de listas de control de acceso para proporcionar mayor seguridad en las comunicaciones. La utilización de dichas versiones trae consigo una mayor dificultad en la configuración del sistema pero el nivel de seguridad obtenido es mucho mayor.

Bibliografía

Para mayor información sobre el tema se refiere al lector a los documentos oficiales, es decir a los RFCs relacionados con las diferentes versiones del protocolo SNMP. A continuación se indica el número correspondiente a los documentos asociados a cada una de dichas versiones:

SNMP	RFC 1155-1157, 1212-1213
SNMPsec	RFC 1351-1353
SNMPv2p	RFC 1441-1452
SNMPv2c	RFC 1901
SNMPv2u	RFC 1910
SNMPv3	RFC 2271-2275

Otra valiosa fuente de información sobre temas relacionados con la familia de protocolos SNMP es la publicación periódica Simple Times, a la que puede accederse en http://www.simple-times.org.

José Carlos Fernández Rodríguez,
zz96f022 [at] etsiig [dot] uniovi.es
José Antonio Corrales González,
ja [at] lsi [dot] uniovi.es
Adolfo Otero Rodríguez
otero [at] lsi [dot] uniovi.es
Área de Lenguajes y Sistemas Informáticos,
Universidad de Oviedo

Actualizado el 17/10/2003
RedIRIS © 1994-2005