Seguridad en SNMPv3.

Por Alejandro Corletti (acorletti@hotmail.com)

1. Introducción:

En el mes de enero del año 1998 IETF propone un conjunto de RFC desde la 2271 a la 2275 las cuales definen un conjunto de medidas para implementar las tres grandes falencias que poseía el protocolo SNMP, estas son:

- Autenticación.
- Seguridad.
- Control de acceso.

Estos nuevos estándares propuestos son los que definen la nueva versión de este protocolo denominada versión 3. El propósito es definir una arquitectura modular que de flexibilidad hacia futuras expansiones.

Luego de un tiempo, en el mes de abril de 1999 aparecen ya como borrador estándar los mismos conceptos con algunas mejoras, dejando obsoletos los anteriores. Estas son las recomendaciones 2571 a la 2575, las cuales sientan definitivamente el funcionamiento de SNMPv3. Estas son:

2571 An Architecture for Describing SNMP Management Frameworks. B. Wijnen, D. Harrington, R. Presuhn. April 1999. (Format: TXT=139260 bytes) (Obsoletes RFC2271) (Status: DRAFT STANDARD)

2572 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP). J. Case, D. Harrington, R. Presuhn, B. Wijnen. April 1999. (Format: TXT=96035 bytes) (Obsoletes RFC2272) (Status: DRAFT STANDARD)

2573 SNMP Applications. D. Levi, P. Meyer, B. Stewart. April 1999. (Format: TXT=150427 bytes) (Obsoletes RFC2273) (Status: DRAFT STANDARD)

2574 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). U. Blumenthal, B. Wijnen. April 1999. (Format: TXT=190755 bytes) (Obsoletes RFC2274) (Status: DRAFT STANDARD)

2575 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP). B. Wijnen, R. Presuhn, K. McCloghrie. April 1999. (Format: TXT=79642 bytes) (Obsoletes RFC2275) (Status: DRAFT STANDARD)

A lo largo de este texto se desarrollará un resumen de las principales características de estas RFC, centrando la atención en los aspectos referidos a seguridad.

2. Entidades:

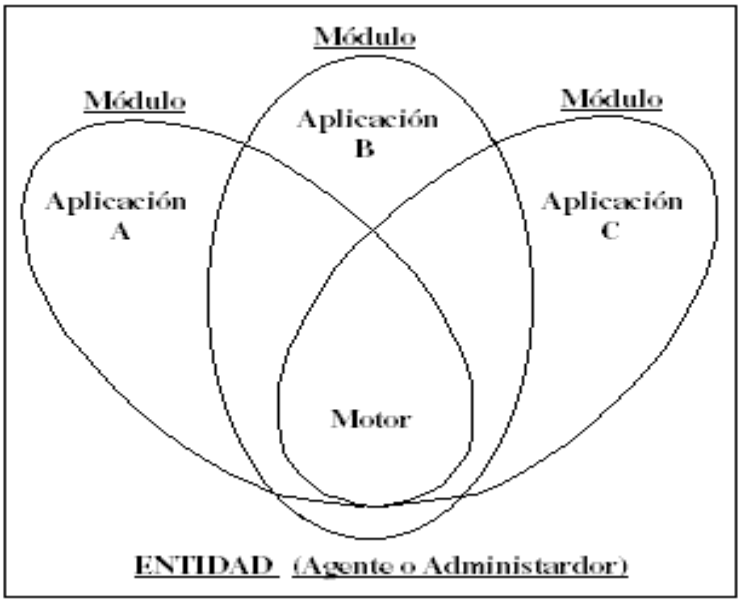
El concepto de entidad es una conjunto de módulos que interactúan entre sí, cada entidad implementa una porción de SNMP y puede actuar como los tradicionales nodo AGENTE, nodo GESTOR, o combinación de ambos.

Cada entidad incluye un MOTOR SNMP, siendo éste el encargado de implementar las funciones de:

- Envío de mensajes.
- Recepción de mensajes.
- Autenticación.
- Encriptado y desencriptado de mensajes.
- Control de acceso a los objetos administrados.

Estas funciones son provistas como servicios a una o más aplicaciones.

El conjunto de motor y aplicaciones son definidas como los módulos de esta entidad.



3. Gestor tradicional SNMP:

Un Gestor tradicional SNMP interactúa con los agentes SNMP a través del envío de comandos (get,get next y set) y recepción de respuestas. Este incluye 3 categorías de Aplicaciones:

- Aplicaciones Generadoras de Comandos: Monitorean y controlan la administración de datos de un agente remoto.
- Aplicación Generadora de Notificaciones: Inicia mensajes asincrónicos.
- Aplicación Receptora de Notificaciones: Procesa mensajes entrantes asincrónicos.

Estas tres aplicaciones hacen uso de los servicios del motor SNMP.

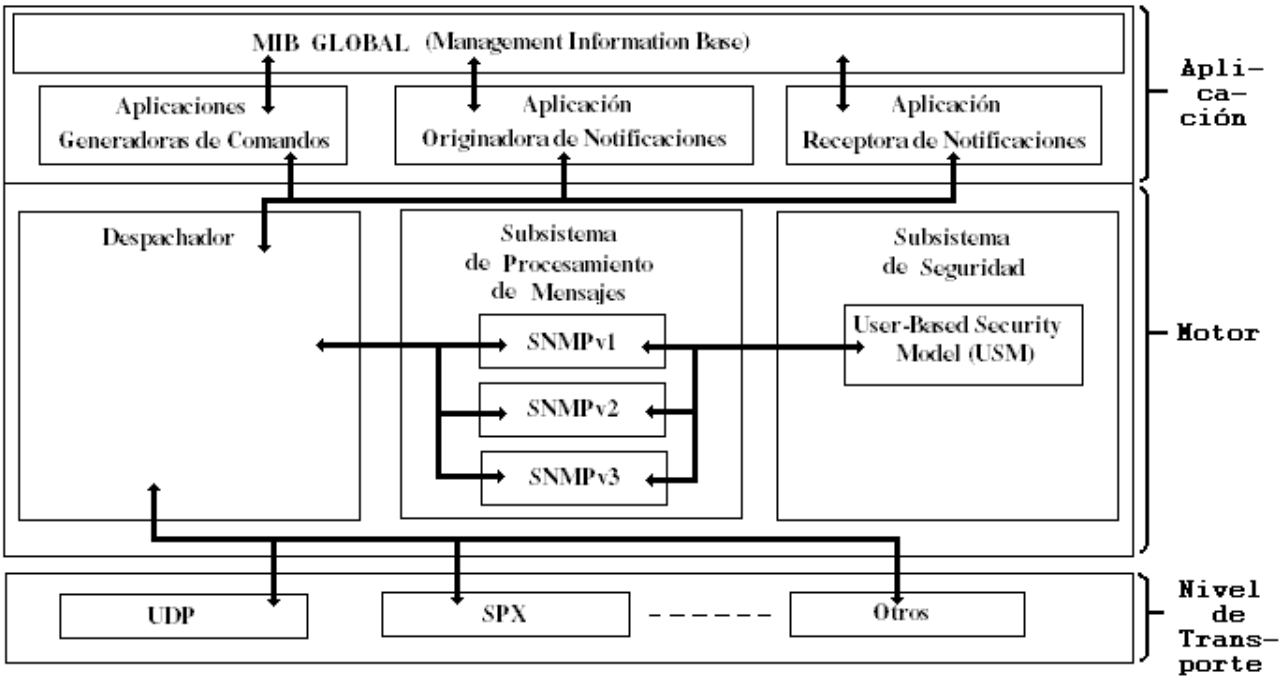
Este motor debe contener:

a. Un Despachador: Encargado de administrar el tráfico. Para mensajes salientes, recibe las PDU (Unidad de datos de Protocolo) de las aplicaciones, determina el tipo de procesamiento requerido (Ej: SNMPv1, SNMPv2 o SNMPv3) y entrega estos datos al módulo de procesamiento de mensajes correspondiente. Para mensajes entrantes, acepta

mensajes del nivel de transporte y lo deriva al módulo de procesamiento de mensajes correspondiente. Consecuentemente al recibir los mensajes procesados desde el módulo, los entregará hacia la aplicación apropiada o hacia el nivel de transporte según corresponda.

b. Un Subsistema de Procesamiento de Mensajes: Es el responsable del armado y desarmado de la PDU de este nivel. Recibe y entrega los mensajes del despachador. Si es necesario luego de armar la PDU (mensaje saliente) o antes de desarmarla (mensaje entrante), pasaría la misma al Subsistema de Seguridad

c. Un Subsistema de Seguridad: Es quien ejecuta las funciones de autenticación y encriptado. Recibe y entrega los mensajes al Subsistema de Procesamiento de Mensajes. Este subsistema soporta uno o más modelos distintos de seguridad llamado **User-Based Security Model (USM)** y está definido por la RFC- 2574.



Modelo de referencia de Administrador SNMP

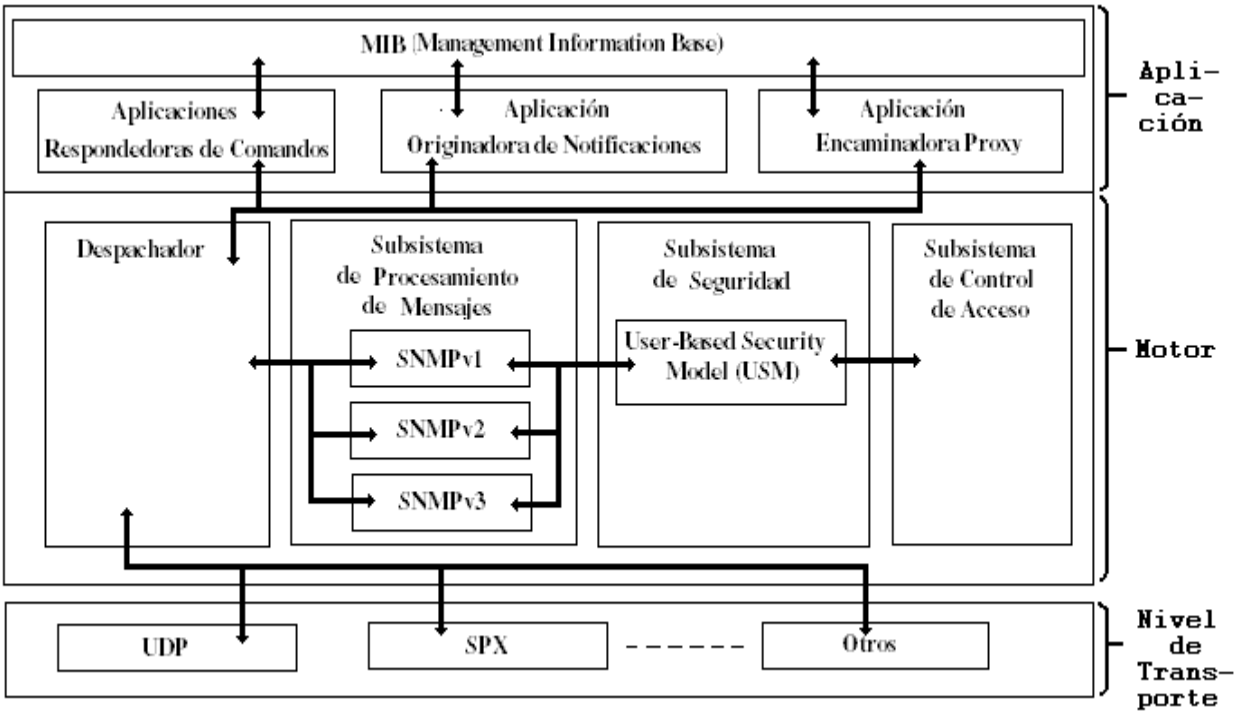
4. Agente Tradicional SNMP:

El agente contiene también 3 tipos de aplicaciones:

- Aplicaciones Respondedoras de Comandos: Provee acceso a los datos administrados.
- Aplicación Generadora de Notificaciones: Inicia mensajes asincrónicos.
- Aplicación Encaminadora Proxy: Encamina mensajes entre entidades.

El Agente tiene los mismos componentes que el Administrador e incluye uno más denominado:

- Subsistema de Control de Acceso: Es el encargado de proveer servicios de autorización para controlar el acceso a las MIBs.Un Agente soporta uno o más modelos de Control de Accesos diferentes llamado **View-Based Access Control Model (VACM)** y se encuentra definido por la RFC-2575.



Modelo de referencia de Agente SNMP

5. Subsistema de procesamiento de mensajes:

Este modelo recibe PDU desde el despachador, tanto salientes como entrantes, las encapsula o desencapsula y acorde a la existencia de mecanismos de seguridad la entrega o no al USM para el tratamiento de los parámetros de seguridad (agregado, criptografiado o decriptografiado) y finalmente las devuelve al despachador para que este las entregue al nivel correspondiente.

Este modelo opera sobre los cinco primeros campos del encabezado SNMP, el cual se detalla a continuación:

Autenticación		Msg Version	Modelo de Procesamiento de Mensajes
		Msg ID	
		Msg Max Size	
		Msg FLAGS	
		Msg Security Model	
		Msg Autoritative Engine ID	Modelo de seguridad de usuario (USM)
		Msg Autoritative Engine Boot	
		Msg Autoritative Engine Time	
		Msg User Name	
		Msg Autentication Parameters	
		Msg Privacy Parameters	
	Encriptado	Context Engine ID	Espacio de PDU
		Context Name	
		PDU (Aplication)	

- *Msg Version:* Corresponde el Nro 3.

- *Msg ID:* Identificador entre las dos entidades para coordinar solicitudes y respuestas
- *Msg Max Size:* Expresa el tamaño máximo en octetos que soporta el emisor.
- *Msg FLAGS:* Están definidos los tres primeros bit y significan lo siguiente:

  Bit 1 (bit de reporte): Si está en 1 entonces el receptor debe especificar bajo qué condiciones este puede causar un reporte. También es empleado en toda solicitud Get o Set.

  Bit 2 (Priv Flag): Indica que se emplea criptografía.

  Bit 3 (Aut Flag): Indica que se emplea autenticación.
- *Msg Security Model:* Indica qué modelo de seguridad se emplea (1 = SNMPv1, 2 = SNMPv2, 3 = SNMPv3).

6. Subsistema de seguridad:

El subsistema de seguridad ejecuta funciones de autenticación y encriptado, para las mismas define uno o más distintos *Modelos de seguridad de Usuario (USM)*. Específicamente la RFC-2574 establece que este modelo protege contra lo siguiente:

- Modificación de Información.
- Falsificación de entidad.
- Modificación de mensaje.
- Difusión de información.

También aclara que no protege contra ataques de negación de servicio ni análisis de tráfico.

Este modelo se emplea para proveer autenticación y privacidad, para esto define dos claves, una clave privada (PrivKey) y otra clave de autenticación (AutKey). El valor de estas claves no es accesible vía SNMP y se emplean de la siguiente forma:

6.1. Autenticación:

Se definen dos alternativas para esta tarea, HMAC-MD5-96 y HMAC-SHA-96.

La mecánica de esta función es que a través de una cadena de bit de entrada de cualquier longitud finita, generará un único resumen de salida de longitud fija. Que en el caso de esta norma es de 20 Byte para SHA o 16 Byte para MD5.

Esta función es llamada “One Way“ pues no es posible a través del resumen de salida obtener el texto de entrada, también resultará computacionalmente imposible obtener un valor de salida igual a través de otro valor de entrada, como así tampoco desde un valor de salida ya calculado, obtener otro valor de entrada diferente al verdadero.

La aplicación aquí propuesta toma los datos y la clave y produce un resumen:

- Resumen = H (clave, datos).

En cualquiera de los dos casos, se toman como válidos los primeros 96 bit, descartando el resto.

Esta especificación soporta el protocolo HMAC [RFC-2104] con la opción SHA1 (Hash Message Autentication-Secure Hash Standard Versión 1) [RFC-2403] y MD5 (Messge Digest Verión 5) [RFC-2403].

6.2. Criptografía:

Para esta actividad USM emplea el algoritmo DES (Data encryptation Standard) [ANSI X3.106] en el modo cifrado encadenado de bloques (CBC). La clave privada (PrivKey) antes mencionada de longitud 16 byte es empleada aquí dividiéndola en dos, los primeros 8 Byte, es decir 64 bit son empleados como clave para DES, el cual solo tendrá en cuenta 56, dejando 8 para control de paridad. Los últimos 8 Byte son empleados como Vector de Inicialización (IV) para comenzar con el cifrado en cadena.

Esta técnica CBC, se basa en tomar el primer bloque de texto plano, y realizar una operación XOR con un Vector de inicialización y luego de esta operación recién se pasará al cifrado de ese bloque. En el segundo bloque se realizará nuevamente la operación XOR, pero esta vez será el texto plano de este bloque con el bloque cifrado anteriormente, y luego se cifrará. Esta mecánica se irá realizando en los sucesivos bloques, es decir XOR con el bloque cifrado anterior y luego cifrado.
El descifrado se realiza en forma inversa.

- cifrado = E (clave, texto).
- D (clave, cifrado) = texto.

6.3. Campos del encabezado de USM:

Antes de tratar los campos de este modelo se debe tener en cuenta al concepto de autoritativo:

- Caso 1: Cuando un mensaje SNMP contiene datos que esperan una respuesta (Get, GetNext, Get Bulk, Set o Informes), entonces el receptor de ese mensaje es Autoritativo.
- Caso 2: Cuando un mensaje SNMP contiene datos que no imponen respuesta (Trap, Respuestas o Reportes), entonces el emisor de ese mensaje es Autoritativo.

Acorde a la gráfica anterior del encabezado SNMPv3, se puede apreciar que USM emplea los seis campos siguientes al Modelo de Procesamiento de Mensajes. Estos campos se detallan a continuación:

- *Msg Autoritative Engine ID:* Identificador de la entidad Autoritativa.
- *Msg Autoritative Engine Boot:* Este valor es un contador monótono creciente que identifica la cantidad de veces que la entidad autoritativa fue inicializada o reinicializada desde su configuración inicial.
- *Msg Autoritative Engine Time:* Este valor es un entero que describe el tiempo transcurrido en segundos desde el momento en que la entidad autoritativa incrementó el *Msg Autoritative Engine Boot* (es decir el tiempo desde la última vez que inició o reinició). Las entidades autoritativas llevan su tiempo exacto en segundos y las no autoritativas llevarán por cada entidad autoritativa con la que se comuniquen una apreciación del mismo, que servirá para compararlos en el momento oportuno (como se verá a continuación). Este valor son 32 bit, en el caso de no reinicializarse una entidad se irá acumulando y al llegar al valor máximo volverá a cero (En realidad como es un

valor de 32 bit, 2^{32} segundos son en el orden de 68 años, por lo tanto el sistema debería ser extremadamente sólido para no detenerse nunca en este lapso)

- *Msg User Name:* Nombre del usuario de este mensaje.
- *Msg Authentication Parameters:* Aquí es donde va el código de autenticación es decir el valor obtenido por HMAC. En el caso de no emplear autenticación es nulo.
- *Msg Privacy Parameters:* El valor aquí expuesto es el que se empleará para obtener el Vector de Inicializaciín (VI) para el algoritmo DES. En el caso de no emplear criptografía es nulo.

La secuencia de pasos a seguir con estos campos para la transmisión de un mensaje en este modelo es:

a. Como primera actividad se criptografían los datos en caso de implementar esta función.

b. Si se realizó el paso a. entonces se coloca en el campo *Msg Privacy Parameters* el valor correspondiente para generar el IV.

c. Si se emplea autenticación, la totalidad del mensaje se ingresa para obtener el resumen HMAC y su resultado es ubicado en el campo *Msg Authentication Parameters.*

En el caso de la recepción sería:

a. Realiza el cálculo de HMAC.

b. Compara el valor calculado con el correspondiente al campo campo *Msg Authentication Parameters*.

c. Si ambos valores son iguales, entonces toma el mensaje como auténtico y no ha sido alterado.

d. Verifica si el mismo está en un tiempo de ventana válido. Esta actividad se realiza de la siguiente forma:

1) Toda entidad no autoritativa guarda tres parámetros en forma local de cada entidad autoritativa con la que se comunica, estos son:

- El valor más reciente de *Msg Autoritative Engine Boot* recibido en la última comunicación.
- El valor de tiempo estimado que debería tener la entidad autoritativa.
- El último valor de tiempo recibido de la entidad autoritativa en el campo *Msg Autoritative Engine Time.*

2) Al recibir un mensaje compara los campos del mensaje recibido con estos parámetros almacenados localmente.

3) Las condiciones para que un mensaje sea considerado no auténtico son:

- Diferencia de *Msg Autoritative Engine Boot.*
- Diferencia en ± 150 segundos entre el valor calculado de *Msg Autoritative Engine Time* y el recibido en el mensaje.

4) Si un mensaje es considerado no auténtico, una indicación de error es enviada al módulo respectivo.

e. Finalmente si está criptografiado, descifra el mismo.

6.4. Localización de claves:

Una clave localizada es un secreto compartido entre un usuario y un motor SNMP autoritativo.

El problema del empleo de una sola clave por parte del usuario con todos los agentes es que si se descubriera la misma, sería vulnerable todo el sistema. Si el caso fuera lo contrario es decir que se deseara emplear una clave distinta para cada agente, entonces el usuario debería recordar todas las contraseñas lo cual en la práctica no es viable.

Para dar solución a estos problemas la RFC 2574 propone este proceso por el cual una clave única de usuario (o pueden ser dos: una para privacidad y otra para autenticación) es convertida a múltiples claves únicas también, una para cada motor SNMP, este proceso es lo que se denomina **Localización de claves**. Las características fundamentales que propone este proceso son:

- Cada agente SNMP tiene su propia clave única para cada usuario autorizado a administrarlo, por lo tanto si la clave de uno de ellos es comprometida, no lo serán las del resto.
- La clave de un usuario es diferente en cada agente SSSNMP, por lo tanto si se compromete la clave de un agente, no comprometerá al resto ni a la clave del usuario.
- La administración de la red, puede realizarse en forma segura remotamente desde cualquier punto de la red.

Este proceso se genera a partir de una contraseña de usuario (Passw) que puede tener cualquier longitud. La RFC 2574 no hace referencia sobre la misma, pero las políticas de seguridad deberían determinar las pautas para que no sea trivial. Los pasos a seguir en este proceso son:

a. El usuario introduce una contraseña ***(Passw)*.**

b. El primer algoritmo repite la misma tantas veces como fuera necesario para producir una cadena de caracteres de longitud 2^{20}, es decir 1.048.576 octetos.

c. Se aplica el algoritmo hash con MD5 o SHA1 (explicados en 6.1.), y se obtiene la clave de usuario ***(Ku)*** de longitud 16 o 20 octetos, acorde a la función empleada.

d. Se concatena la clave de usuario (Ku) con el identificador de cada motor SNMP (SNMP engine ID) y nuevamente se aplica el algoritmo hash con MD5 o SHA1 y se obtiene la clave de usuario Localizada ***(Kul)*** de longitud 16 o 20 octetos, acorde a la función empleada.

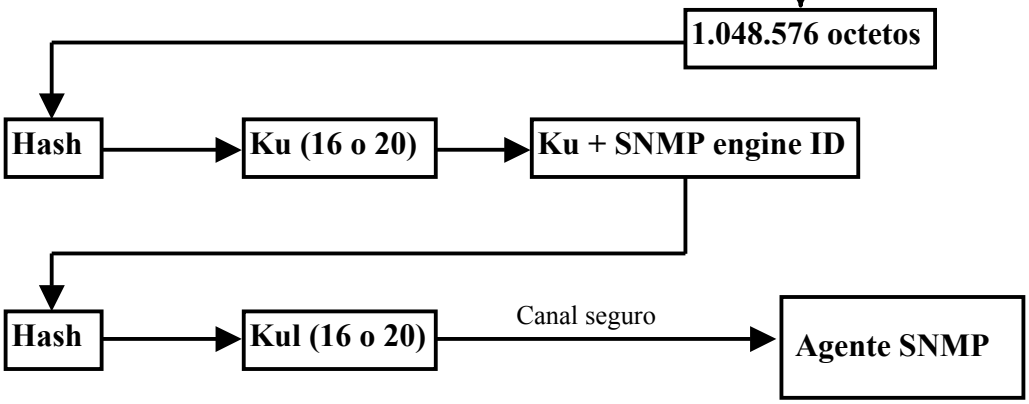
e. Esta clave debe ser configurada en los agentes SNMP del sistema en forma segura.

f. Queda almacenada en cada agente SNMP esta última Kul por cada usuario, la cual se debe tener en cuenta que no es una contraseña sino la función "One Way" de ciertas concatenaciones de esa contraseña, es decir que desde esta no se puede reconstruir la contraseña del usuario, y como la misma no está disponible vía SNMP, no se podría tener acceso a ella.

RESUMEN:

User → Passw → Algoritmo:

```
while (count < 1048576) {
    cp = password_buf;
    for (i = 0; i < 64; i++) {....
```



7. Subsistema de Control de Accesos:

Este subsistema se ejecuta en los agentes tradicionales, permitiendo determinar quien está autorizado a acceder a la MIB de los mismos. El único modelo definido para esta actividad se denomina *Modelo de Control de Accesos basado en Vistas* (VACM: View-Based Access Control Model) y está definido en la RFC-2575.

VACM tiene dos características fundamentales:

- Determina si un acceso a la MIB local está permitido.
- Posee su propia MIB en la cual se definen las políticas de acceso y habilita la configuración remota.

Se definen cinco elementos que constituyen la VACM:

a. Grupos: Es un conjunto de cero o más duplas {Modelo de Seguridad, Nombre de seguridad} que definen los Objetos que pueden ser administrados por ese Nombre.

b. Nivel de seguridad: Define qué tareas serán permitidas (lectura, escritura o notificación) para cada grupo.

c. Contexto: Es un subconjunto de instancias de objetos en la MIB local. Permite agrupar objetos con distintas políticas de acceso.

d. Vistas de la MIB: Define conjuntos específicos de objetos administrados, los cuales se pueden agrupar en jerarquías de árboles y familias de manera tal que se pueda, por ejemplo, restringir su acceso a determinados grupos.

e. Política de acceso: VACM permite a un motor SNMP ser configurado para asegurar un conjunto de accesos correctos, los cuales dependen de los siguientes factores:
   - Los distintos usuarios pueden tener distintos privilegios de acceso.
   - El nivel de seguridad para una determinada solicitud.
   - El modelo de seguridad empleado para procesar las solicitudes de mensajes.

- El contexto de la MIB.
- La instancia al objeto para el cual fue solicitado el acceso.
- El tipo de acceso solicitado (lectura, escritura o notificación).

8. Bibliografía consultada:

- Stallings, W. (1998). *"SNMP, SNMPv2 SNMPv3 and RMON 1 and 2",* Third Edition. Addison-Wesley,.
- Blumenthal, U., Hien N. Y Wijnen, B. (1997). *"Key Derivation for Network Management Applications"*. IEEE Network, May/Jun.
- RFC-2571 *"An Architecture for Describing SNMP Management Frameworks"*. B. Wijnen, D. Harrington, R. Presuhn. April 1999.
- RFC-2572 *"Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)"*. J. Case, D. Harrington, R. Presuhn, B. Wijnen. April 1999.
- RFC-2573 *"SNMP Applications"*. D. Levi, P. Meyer, B. Stewart. April 1999.
- RFC-2574 *"User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)"*. U. Blumenthal, B. Wijnen. April 1999.
- RFC-2575 *"View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)"*. B. Wijnen, R. Presuhn, K. McCloghrie. April 1999.