

# Seguridad en Redes de Banda Ancha.

Jordi Forné, Miguel Soriano, Francisco Recacha, J. L. Melús  
Departamento de Matemática Aplicada y Telemática (U.P.C.)

**ABSTRACT.-** La presencia de un gran número de servicios de muy diversa índole es uno de los factores que más influyen en el desarrollo de la futura red Digital de Servicios Integrados de Banda Ancha (RDSI-BA) [CCITT I.321]. Sin embargo, todos estos servicios presentan un denominador común: la necesidad de proteger los datos ante un uso no autorizado. Por lo tanto, parece necesario la implantación de sistemas de seguridad adecuados a las necesidades de los distintos servicios.

En este artículo se presentan las características generales que deben satisfacer estos servicios de seguridad, teniendo en cuenta las restricciones impuestas por las características intrínsecas de las redes de banda ancha. Se analizará la arquitectura y ubicación de los servicios de seguridad, y se apuntarán algunas características que deben satisfacer los protocolos de gestión de claves, teniendo en cuenta su coste y comportamiento ante posibles amenazas.

## 1. INTRODUCCIÓN

En los últimos años se está realizando un gran esfuerzo en el desarrollo de una red de alta velocidad que integre servicios de voz, datos e imagen. El CCITT (denominado UIT a partir de 1992) adoptó la Red Digital de Servicios Integrados de Banda Ancha [CCITT I.121] y el modo de transferencia asíncrono (MTA, o ATM en inglés) como modo de transferencia universal para dicha red.

MTA es una técnica orientada a conexión, basada en la segmentación del flujo de información en unidades de longitud fija denominadas celdas, constituidas por una cabecera de 5 bytes y un campo de datos de 48 bytes. Durante el establecimiento de conexión se establecen todas las características del servicio, así como el circuito virtual utilizado durante toda la comunicación. El enrutamiento se realiza mediante los identificadores de camino virtual (VPI) y de canal virtual (VCI) presentes en la cabecera de todas las celdas.

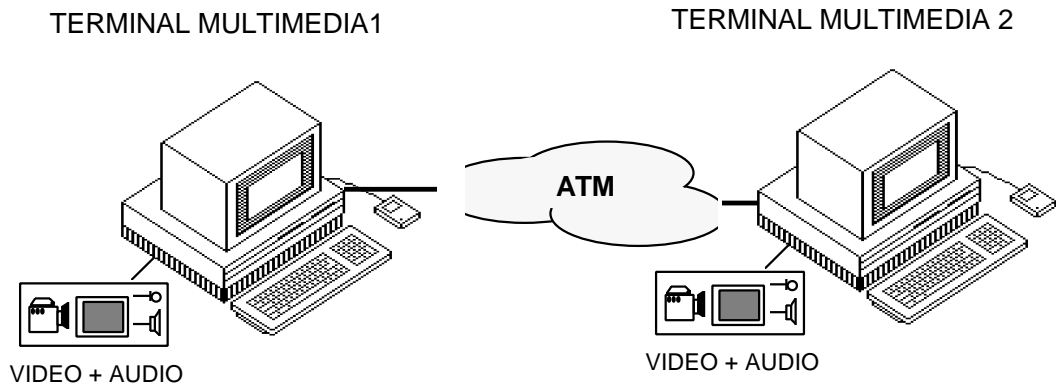


Figura 1

Aunque seguirán existiendo terminales únicamente de datos y de voz (teléfonos), los terminales multimedia constituirán el soporte de acceso a la red RDSI-BA para la integración de todos los servicios en una única plataforma. Cada terminal deberá tener un interface adecuado para las aplicaciones de vídeo, audio y datos que soporta. La figura 1 muestra dos terminales multimedia que se comunican a través de una red MTA.

La necesidad de mecanismos para proporcionar comunicaciones seguras en la futura red pública de banda ancha es evidente, y es deseable una solución global estándar con el objetivo de reducir el coste y permitir la operación entre usuarios. Un mecanismo necesario para alcanzar un nivel de seguridad aceptable (ya sea para servicios de confidencialidad, integridad o autenticación) es el cifrado de la información. Por ello es necesario la elección de un algoritmo criptográfico para llevar a cabo este cifrado, que exigirá un soporte hardware debido a la alta velocidad de las aplicaciones multimedia. Bajo un punto de vista de eficiencia económica es recomendable que este hardware pueda ser utilizado para todas las aplicaciones que manipulan información crítica.

En caso de una nueva red en la que todos los nodos deben ser instalados se pueden adoptar mecanismos de seguridad extremo a extremo [FORD94], dotando a los terminales multimedia de los dispositivos hardware requeridos para dar seguridad a la información. En caso de trabajar con nodos instalados previamente, un aspecto a considerar es la compatibilidad entre todos los dispositivos. También debe tenerse en cuenta que las necesidades de seguridad no son las mismas para los distintos servicios,

por ejemplo, la gestión de claves será distinta en comunicaciones punto a punto, o comunicaciones multipunto.

## 2. UBICACIÓN DE LOS SERVICIOS DE SEGURIDAD.

La arquitectura del terminal juega un papel fundamental en el diseño de un sistema de seguridad entre terminales conectados a una red RDSI-BA. A continuación presentaremos algunas opciones para integrar seguridad, comentando las ventajas y desventajas de las distintas opciones. La elección de una opción u otra dependerá de la arquitectura particular del terminal multimedia.

En este apartado presentamos las principales opciones para ubicar el cifrado de la información, la gestión de claves y la autenticación según la arquitectura MTA.

### 2.1. Cifrado de la información

La ubicación del cifrado dentro del modelo de referencia MTA es compleja y a menudo sujeta a controversia. La figura 2 presenta las tres posibilidades que serán consideradas.

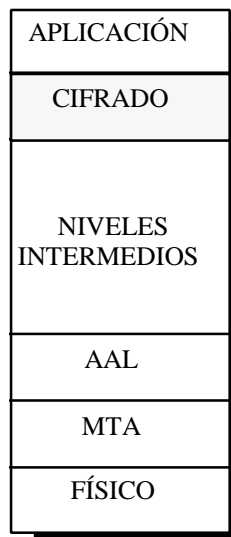


Figura 2a

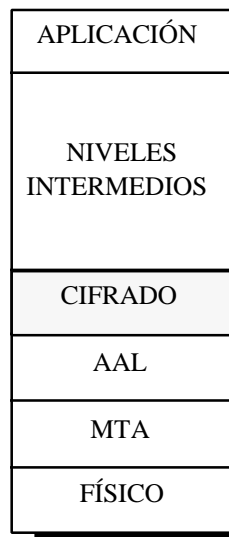


Figura 2b



Figura 2c

La primera posibilidad es ubicar el cifrado inmediatamente debajo del nivel de aplicación, tal como se observa en la figura 2a. En esta situación, los datos procedentes de aplicaciones críticas se cifran en el terminal origen antes de ser transmitidos a los niveles intermedios, a continuación son encapsulados con los protocolos de

comunicaciones correspondientes y finalmente son transmitidos a través de la red. En el extremo destinatario se realiza el proceso inverso, de modo que los datos son descifrados justo antes de ser entregados al nivel de aplicación. Esta solución presenta las siguientes ventajas:

- La cantidad de datos a cifrar es menor, ya que las cabeceras introducidas por los niveles por debajo del nivel de aplicación no son procesadas.
- La gestión de claves se simplifica, ya que se asocia una clave con cada aplicación.

El inconveniente que presenta esta opción es que no siempre puede adoptarse. En algunos casos, la arquitectura del terminal multimedia impone que aplicaciones de audio y video accedan directamente a los niveles inferiores, impidiendo esta solución. Lógicamente podría ubicarse la seguridad a este nivel para aplicaciones de datos que lo requieran, y dotar de mecanismos alternativos de seguridad para el resto de aplicaciones de audio y video. Sin embargo, creemos interesante estudiar mecanismos globales de seguridad para toda la información multimedia, independientemente de su naturaleza, por lo que deben considerarse las opciones presentadas en las figuras 2b y 2c.

La segunda opción es ubicar el proceso de cifrado inmediatamente debajo de la capa de adaptación (AAL: ATM Adaptation Layer), tal como se indica en la figura 2b. Esta opción sólo debe aplicarse cuando es viable y no se puede adoptar la solución anterior. Sus ventajas frente a la opción 2c son las siguientes:

- Los bloques de información son de mayor tamaño, mejorando la eficiencia del proceso de cifrado (el número de veces que la información es procesada y se selecciona la clave criptográfica adecuada disminuye).
- Trabajando a este nivel se asegura el orden y no duplicidad de las tramas correspondientes a un mismo canal virtual.

Si la arquitectura del terminal no posibilita las soluciones anteriores, debe ubicarse el proceso de cifrado entre los niveles AAL y MTA, tal como indica la Figura 2c. En tal caso, las celdas MTA (unidades de información pequeñas) procedentes de distintas aplicaciones deben alcanzar el dispositivo de cifrado, y posiblemente se deberá modificar la clave. Dado que es posible que dos celdas consecutivas correspondan a distintos servicios, se precisa un conmutador de claves muy rápido, o varios cifradores actuando en paralelo, uno para cada aplicación o canal. Además, debe tenerse en cuenta que trabajando a este nivel puede haber pérdidas de tramas, lo cual obligaría a trabajar

con cifradores robustos a estas pérdidas. En caso de utilizarse cifradores en flujo (ver sección 3.1), estos deberían funcionar en modo autosincronizante.

Resumiendo, la opción 2a es la más conveniente si la arquitectura del terminal permite su adopción, y a nivel general podríamos decir, que mientras más bajo se ubique el proceso de cifrado mayor es la cantidad de información a proteger y aumentan los requisitos del cifrador (velocidad, conmutación de claves y capacidad de trabajar con posibilidad de pérdidas de celdas).

## **2.2. *Gestión de claves.***

La gestión de claves es el mecanismo mediante el cual terminales multimedia negocian una clave para cifrar una comunicación (ver sección 3.2, para mayor detalle). Debe tenerse en cuenta que sólo es conveniente dar seguridad a aquellas aplicaciones que manipulan información crítica. En consecuencia, la gestión de claves debería ubicarse a nivel de aplicación para obtener un interface adecuado con los usuarios y las aplicaciones.

## **2.3 *Autenticación.***

Un problema fundamental para la seguridad de un sistema es la autenticación o verificación de la entidad que genera ciertos datos, así como su integridad. Deben considerarse tres tipos de autenticación

- Autenticación entre usuarios.
- Autenticación del usuario frente al terminal (identificación) y del terminal frente al usuario.
- Autenticación mútua entre terminales.

La primera opción (autenticación entre usuarios extremos) implica que cada usuario debe verificar su identidad ante todos los otros que participan en la comunicación (uno para comunicaciones punto a punto, o varios para comunicaciones multipunto). Cada usuario autorizado debe poseer material asociado a su clave, almacenado en un dispositivo como una tarjeta inteligente. Bajo un punto de vista de seguridad esta opción puede considerarse muy válida, aunque el coste en gestión de claves es muy elevado si hay muchos usuarios.

Otro aspecto a considerar es el control de acceso de usuarios a terminales, basado en la verificación de su identidad. Si el usuario no tiene porqué creer en la

autenticidad del terminal es preciso que se establezca un proceso de autenticación mutua. En algunos casos la autenticación entre usuarios remotos se puede conseguir a partir de técnicas de autenticación entre terminales y autenticación mutua entre usuario y terminal reduciendo complejidad y coste del sistema, aunque el nivel de seguridad ofrecido puede ser menor.

Los procesos de autenticación y control de acceso, así como la gestión de claves deberían ubicarse a nivel de aplicación para tener un interface adecuados con usuarios y aplicaciones.

### **3. SERVICIOS Y MECANISMOS DE SEGURIDAD**

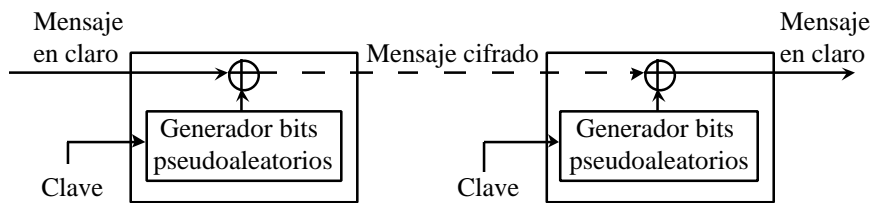
En esta sección se presentarán los problemas asociados a los servicios de confidencialidad de la información, integridad, autenticación y al mecanismo de gestión de claves.

#### ***3.1. Confidencialidad e Integridad de la Información***

La velocidad a la que circulan los datos en una red de banda ancha es muy elevada, lo cual supone que el proceso de cifrado de datos deba ser muy rápido; de otra forma constituiría un cuello de botella y se perderían tramas. En consecuencia, parece evidente que se precisa un cifrador que trabaje a velocidades muy elevadas.

Actualmente, los cifradores en flujo [RUEP86] parecen ser la mejor opción para conseguir implementaciones rápidas de los servicios que deben aplicarse sobre la información sensible (confidencialidad, integridad, autenticidad, ...). Las técnicas de cifrado en flujo consisten en generar una secuencia pseudoaleatoria (PN) que se suma al mensaje (módulo 2), y así se obtiene el texto cifrado. La misma secuencia pseudoaleatoria se genera en el receptor, y al sumarle el texto cifrado se obtiene el mensaje en claro. Como se ha dicho anteriormente, determinadas aplicaciones como audio y vídeo pueden ser no fiables (no incorporar mecanismos de corrección de errores durante la transmisión), de modo que no se garantiza el orden ni la llegada de todas las tramas. En tales circunstancias, si se selecciona un cifrador en flujo, debería ser capaz de trabajar en modo autosincronizante. La figura 3 muestra el esquema de un cifrador en flujo síncrono y un cifrador autosincronizante.

### Cifrador síncrono



### Cifrador autosincronizante

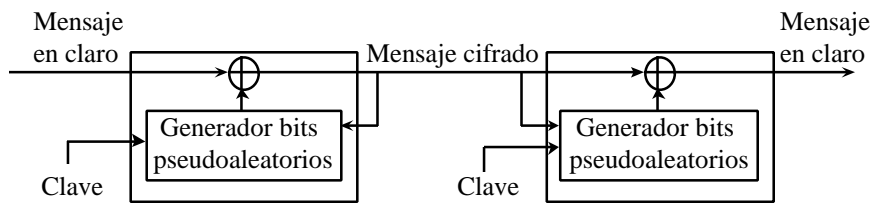


Figura 3.

Una de las características de los cifradores síncronos es que si se pierde un bit en el texto cifrado, el mensaje restante a partir de dicho bit se recibirá incorrectamente. Sin embargo, en los cifradores autosincronizantes la secuencia pseudoaleatoria depende del texto cifrado, permitiendo que cuando hay pérdidas el sistema sea capaz de recuperarse al cabo de  $n$  bits, siendo  $n$  la memoria del cifrador.

### 3.2. *Gestión de claves*

Las técnicas de cifrado en flujo requieren claves para proteger los datos. Estas claves denominadas de sesión, deben ser negociadas entre los dos terminales antes de establecer una comunicación segura. Además, estas claves deben ser renovadas cada cierto tiempo para dar mayor robustez al sistema, siguiendo una política de seguridad.

En consecuencia, es preciso un protocolo de gestión de claves para establecer comunicaciones seguras. Las principales consideraciones que debe satisfacer dicho protocolo son las posibles amenazas que puede sufrir el sistema de seguridad en cuestión, y la arquitectura del sistema. Entre los distintos requisitos podríamos citar los siguientes:

- **Confidencialidad de claves:** Las claves deben mantenerse secretas durante su transmisión.

- Detección de modificaciones : Cualquier modificación realizada por un usuario no autorizado debe ser detectada.
- Detección de repeticiones. Un posible ataque consiste en la réplica de tramas, con el objetivo de conseguir la ejecución de un mismo proceso más de una vez. Cualquier repetición ilícita de tramas debe ser detectada por el protocolo. Básicamente existen tres mecanismos para detectar réplicas: contadores, marcas temporales, y retos, siendo esta última técnica la más aconsejable [BIRD93, FUMY93] especialmente en entornos de área extendida, donde la presencia de contadores o la necesidad de sincronismo de reloj es poco práctica.
- Autenticidad de origen: La identidad del emisor del mensaje debe ser verificada.

La velocidad del proceso de gestión de claves no es tan importante como la del proceso de cifrado de información, ya que la clave de sesión se negocia off-line. Esta característica permite la opción de criptosistemas de clave pública facilitando la gestión y reduciendo el número de claves del sistema.

Las comunicaciones punto a punto pueden ser protegidas usando protocolos de gestión de claves en los que intervienen las dos entidades que gestionan la clave. Obviamente en entornos con muchos usuarios es necesario la presencia de entidades verificadoras como centros de certificación. Parecen recomendables protocolos basados en modificaciones del protocolo de autenticación NS (Needham - Schroeder) [NEED78], puesto que a la vez garantizan autenticación mutua. En estos casos, las dos entidades juegan un papel similar en la comunicación y la clave de sesión puede ser generada por una de las dos entidades, o conjuntamente por las dos .

En caso de comunicaciones multipunto, es preciso otro conjunto de protocolos ya que un número considerable de clientes puede abrir una sesión con un servidor ( distribución de TV, ...) La clave de sesión debe ser generada por el servidor y distribuida de forma segura a los clientes cuando se conectan al servidor.

## BIBLIOGRAFÍA

- [BIRD93] R. Bird et al., "Systematic Design of a Family of Attack-Resistant Authentication Protocols". IEEE Journal on Selected Areas in Communications. Volume 11. Number 5. June 1993

- [CCITT I.121] CCITT Recommendation I.121. "Broadband Aspects of ISDN". Geneva, 1991
- [CCITT I.321] CCITT Recommendation I.321. "B-ISDN Protocol Reference Model and its Applications". Geneva, 1991
- [FORD94] W. Ford. Computer Communications Security. Ed. Prentice Hall. 1994
- [FUMY93] W. Fumy and P. Landrock, "Principles of Key Management". IEEE Journal on Selected Areas in Communications. Volume 11. Number 5. June 1993
- [NEED78] Needham, R. M. and Schroeder, M. D., "Using encryption for authentication in large networks of computers", Communication of the ACM, Vol. 21. No. 12, December 1978, pp. 993-999.
- [RUEP86] Rueppel, R. A., *Analysis and Design of Stream Ciphers*. Springer-Verlag (1986).