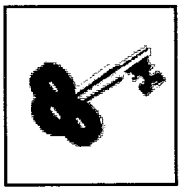

SEGURIDAD A NIVEL DE IP: IPSEC

Pedro Antonio Mur Siles
Estudiante de la ETSETB, UPC y socio colaborador de BJT.
pedro@bjt.upc.es

INTRODUCCIÓN

La utilización de Internet, cada vez más amplia y entre usuarios más diversos, ha provocado la necesidad de proteger todo tipo de información que viaja por la red. Existen diversas propuestas y alternativas para garantizar la seguridad y autentificación de todos los paquetes que vayan por la red. La ampliación del mundo de Internet, junto con los mecanismos de cifrado disponibles, animará, sin duda, al desarrollo de nuevas aplicaciones como comercio electrónico o cualquier actividad desde casa que necesite seguridad como por ejemplo acceso a datos bancarios, etc.

En este artículo se pretende analizar una serie de mecanismos de seguridad que son aplicables a la capa IP y que se han denominado IPSec: la cabecera de autentificación (AH: Authentication Header), el encapsulado de seguridad de carga útil (ESP: Encapsulating Security Payload) así como su combinación, además de los protocolos, la negociación y el intercambio de claves para ambos mecanismos de seguridad (asociaciones de seguridad e intercambio de claves)

También es cierto que existen otros mecanismos de seguridad que se pueden aplicar en otros niveles que no sean el IP, pero no serán motivo del presente documento.

IPSEC

IPSec proporciona servicios de seguridad en la capa IP mediante un sistema para seleccionar los protocolos de seguridad requeridos, determinar los algoritmos usados para los servicios, y determinar unas claves criptográficas necesarias para proporcionar los servicios pedidos. IPSec puede ser utilizado para proteger uno o más "caminos" entre dos hosts, entre dos pasarelas o entre pasarela segura (p.e. encaminador o cortafuegos con IPSec) y host.

El conjunto de servicios de seguridad que puede proporcionar IPSec incluye control de acceso, integridad, autentificación del origen, reenvío de paquetes, confidencialidad (encriptación) y confidencialidad de flujo de tráfico limitado. Debido a que estos servicios son proporcionados por la capa IP, también pueden ser utilizados por las capas superiores (TCP, UDP, ICMP, BGP, etc.)

IPSec utiliza dos protocolos para proporcionar seguridad: la cabecera de autentificación (AH) y el encapsulado de carga útil (ESP). El primero proporciona integridad, autentificación y un servicio opcional de no-repudio. Mientras que el segundo puede proporcionar confidencialidad (encriptación) y confidencialidad de flujo de tráfico limitado. También puede proporcionar integridad, autentificación y un servicio opcional de no-repudio. Ambos (AH y ESP) son vehículos de control de acceso basados en la distribución de claves criptográficas y la administración de flujos de tráfico relativos a este tipo de protocolos de seguridad. Estos protocolos pueden ser aplicados solos o uno en combinación con el otro y tanto en IPv4 como en IPv6. Ambos protocolos soportan dos modos de uso: el modo transporte y el modo túnel. En modo de transporte tendremos confidencialidad en los datos pero las cabeceras IP estarán al descubierto, es decir que si alguien quiere puede obtener el flujo de información y así saber con quien nos comunicamos, en cambio el modo túnel encripta la cabecera IP y crea una nueva cabecera con la dirección del encaminador con lo cual sabríamos a que Intranet va la información pero no a que usuario. La elección entre modo transporte y modo túnel depende de si la comunicación es entre hosts o pasarelas.

IPSec permite al usuario (o administrador) controlar el tipo de seguridad ofrecido. Es decir, en cada paquete se puede especificar: qué servicios de seguridad usar y con qué combinaciones, en qué tipo de comunicaciones usar una protección determinada y por último los algoritmos de seguridad utilizados. Otro punto importante es que debido a que estos servicios de seguridad son valores secretos compartidos (claves), IPSec confía en una serie de mecanismos para concretar este tipo de claves (IKE, SA) que se explicarán a continuación.

ASOCIACIONES DE SEGURIDAD (SA)

Para suministrar confidencialidad en las comunicaciones es imprescindible el uso de claves (siempre

y cuando el medio por donde viajan no sea seguro). Estas claves deben ser conocidas tanto por el emisor como por el receptor pero por nadie más. También es conveniente no usar siempre las mismas claves para dificultar la faena de posibles criptoanalistas. Por tanto, nos encontramos con el primer problema: el emisor y el receptor deben decirse que clave usaran antes de empezar la comunicación. Pero no basta con eso, también deben acordar que nivel de seguridad quieren y que algoritmos utilizaran. Del hecho de esta necesidad de acuerdos surge la idea de Asociación de seguridad.

Una SA es una relación entre dos o más usuarios que describe como estos usuarios van a utilizar los servicios de seguridad para comunicarse entre ellos. Toda comunicación que requiera IPSec debe establecer una SA (o varias como veremos más adelante) antes de enviar datos. Todos los datos que van por una SA tienen el mismo tipo de seguridad, los mismos algoritmos y la misma clave de sesión, por tanto los problemas antes mencionados se transforman en la creación de la SA. Existen multitud de protocolos que se encargan de realizar lo anteriormente citado aunque el más extendido es el ISAKMP (Internet Security Association and Key Management) que se comentará posteriormente.

Una asociación de seguridad viene unívocamente identificada por una dirección IP y un índice de parámetro de seguridad (SPI), pero en ella son diversos los parámetros que se pueden definir para darle a la comunicación la seguridad que nos convenga:

- Algoritmo de autentificación y modo de utilización del algoritmo con la cabecera de autentificación de IP (requerido para AH).
- Claves utilizadas con el algoritmo de autentificación en uso con la cabecera de autentificación (requerido para AH).
- Algoritmo de encriptado, modo del algoritmo y transformación que se está utilizando con el encapsulado IP de la carga de seguridad útil (requerido para ESP).
- Claves usadas con el algoritmo de encriptado en uso con el encapsulado de seguridad de la carga útil (requerido para ESP).
- Presencia/ausencia y tamaño de la sincronización de criptografía o inicialización del campo vector para el algoritmo de encriptado (requerido para ESP).
- Claves de autentificación usadas con el algoritmo de autentificación que es parte de la transformación ESP, si hay alguna. (requerido para ESP)
- Tiempo de vida de la clave o tiempo en el que se debería cambiar la clave (recomendado para todas las implementaciones)
- Tiempo de vida de la SA (recomendado para todas las implementaciones)
- Dirección origen de la SA, debería ser una dirección comodín, si existe más de un sistema que envía datos que comparten la misma asociación de seguridad con el destino. (recomendado para todas las implementaciones)
- Nivel de seguridad (por ejemplo, secreto o no clasificado) de los datos protegidos.

ISAKMP (INTERNET SECURITY ASSOCIATION AND KEY MANAGEMENT)

En el ISAKMP diferenciamos dos fases. En la primera se definen los parámetros de seguridad que se van a usar durante la negociación y en la segunda fase se definen los parámetros que se usaran durante la comunicación. Es decir, primero se crea una SA llamada ISAKMP SA que será usada exclusivamente para la negociación y cuyos parámetros vienen definidos en la fase 1. Luego, en la fase 2 se negociará la seguridad posterior encriptando por medio de la ISAKMP SA de modo que nadie sabrá como encriptaremos ni que seguridad vamos a usar dando lugar a la creación de la SA definitiva.

A) Fase 1

Se pueden usar dos modos en la fase 1: el modo principal y el modo agresivo. En el modo principal los dos primeros mensajes negocian los parámetros de seguridad (la del ISAKMP SA), los dos siguientes sirven para intercambiarse los valores públicos de Diffie Hellman, y los dos últimos sirven para autentificarse. En el modo agresivo los dos primeros paquetes negocian la seguridad e intercambian los valores públicos de Diffie Hellman, el tercer paquete sirve para identificar al receptor y el cuarto para autentificar al emisor.

En la fase 1 el punto clave es al autentificación, de nada nos sirve encriptar un mensaje si no estamos seguros de que la persona a la que le llega no es un impostor. Hay diversos métodos de autentificación pero todos ellos se basan en el uso de claves asimétricas, por ello es primordial conocer la clave pública de la persona con quien nos vamos a comunicar. Para evitar que un impostor nos diera su clave pública diciendo que es la de otra persona (con lo cual le enviaríamos información creyéndonos que es otro), existen las Autoridades de certificación (CA). Estas nos garantizan que una clave pública es de un usuario concreto. La figura 1 nos ilustra como se realiza este intercambio.

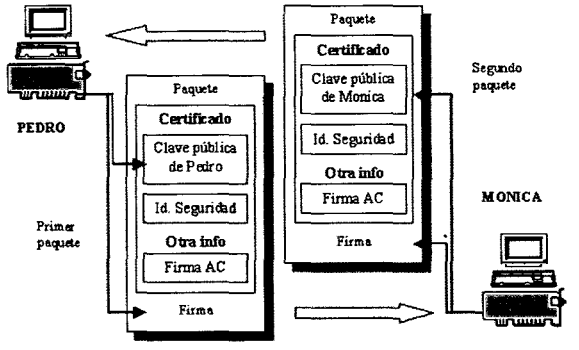

Figura 1: Intercambio de claves públicas

Una vez los usuarios se han autentificado entonces ya pueden generar una clave de sesión mediante los valores públicos requeridos por Diffie Hellman. Esto acontece tal como se ilustra en la figura 2.

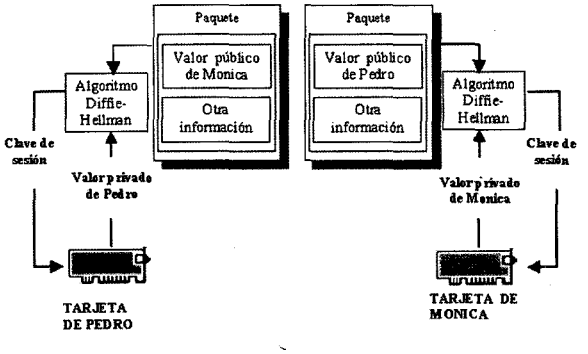

Figura 2: Generación de clave de sesión

B) Fase 2

Ahora que ya disponemos de una comunicación segura (el ISAKMP SA) ya podemos empezar a negociar los parámetros de la SA, esto sucede en la fase 2. En esta fase se usa el "modo rápido" que consiste en que un usuario presenta una serie de alternativas al otro quien o bien elige una de ellas o presenta otra serie de alternativas, y así hasta llegar a un acuerdo. También se debe especificar el SPI (Índice de parámetros de seguridad) que se le asignará a la SA pues será su identificador.

Después de unos campos de control, se propone el tipo de seguridad (AH por ejemplo) y a continuación se presentan diversas alternativas (transforms) al otro usuario, quien debería responder con el mismo mensaje pero con una sola transform, la que haya elegido.

Resumiendo, hay dos fases de negociación. La primera es llevada a cabo por las tarjetas de red de los usuarios o por las pasarelas (cortafuegos) si se diera el caso, y es cuando se decide como proteger el tráfico de la negociación estableciendo un ISAKMP SA La segunda fase se usa para crear la SA que servirá para crear los parámetros de seguridad para el intercambio posterior de datos; aquí son los usuarios (la aplicación) quienes fijan las características de la SA. El hecho de tener dos fases es ventajoso pues varios SA pueden ser definidos por una misma ISAKMP SA además así proporcionamos confidencialidad a las características de las SA creadas en la fase dos, es decir que nadie sabe con que algoritmo ciframos la información

C) Funcionamiento

Cuando requerimos de una comunicación segura con IPSec (AH, ESP) entonces necesitamos tener una SA. Lo primero que debemos hacer es elegir el tipo de seguridad que queremos y fijar los algoritmos. Una SA puede tener o AH o ESP pero no ambos, si queremos tener ambas protecciones deberemos usar una combinación de SAs llamada "SA bundle". Otro parámetro que debemos elegir es si queremos modo transporte o modo túnel.

Una vez negociados y aceptados los parámetros, todos los paquetes IP que viajen entre el primer usuario y el segundo (recordar la unidireccionalidad de las SA) irán con dicha seguridad hasta que, o bien acabe la comunicación, o bien finalice el tiempo de vida de la SA. Si ocurre esto último habrá que hacer el proceso desde el principio de nuevo pasando exactamente por los mismos pasos que antes.

D) Algoritmos disponibles

Los algoritmos que podemos usar son varios aunque en la figura 3 se presentan los más utilizados.

Algoritmos para Encriptación	Algoritmos de Hash	Métodos de autentificación
DES-CBC	MD5	Clave pre-compartida
IDEA-CBC	SHA	Firmas DSS
BLOWFISH-CBC	Tiger	Firmas RSA
CAST-CBC		Encriptación con RSA
3DES-CBC		Encriptación revisada con RSA
RC5-R16-B64-CBC		

Figura 3: Algoritmos disponibles actualmente

E) SAD Y SPD

Para elegir entre todas estas posibilidades a la hora de dar seguridad a un mensaje debemos ir a consultar al SPD (Security Policy Database). Allí tene-

mos todas las posibles combinaciones que nos son permitidas. Una vez hayamos escogido una el sistema verificará el SAD (Security Associations Database). Allí se indican todos las SA que hay abiertas. Si hay alguna SA abierta que se corresponde con nuestras necesidades (igual seguridad, algoritmos y destino) nos será asignada y sino se abrirá una nueva SA con tales especificaciones. El resultado es que se nos devolverá un valor que será el SPI (Índice de parámetros de seguridad) de la SA que nos ha sido asignada. A partir de entonces en todos los paquetes IP destinados a esta comunicación deberemos ponerles el SPI y también decir si se trata de una seguridad AH o ESP. Esto debemos indicarlo porque en realidad hay dos SAD, uno para las comunicaciones con AH y otro para las que usan ESP, es también por esta razón que AH y ESP no pueden estar combinados en una única SA

A partir de aquí la gestión del flujo de información es muy sencilla. Para el flujo saliente en cada paquete IP se siguen los siguientes pasos:

- Se comprueba si va a usar AH o ESP o ambos, y se mira el SPI.
- Se busca en la adecuada SAD (la de AH o la de ESP) la SA que corresponda con el SPI
- Una vez encontrado se codifica la información tal como indique la SA y se envía el paquete.

Para el flujo entrante el método es muy similar:

- Se mira la dirección IP destino del paquete y si no coincide con la nuestra se descarta
- Se comprueba si el paquete esta codificado con AH o ESP y se anota el SPI
- Se busca en la adecuada SAD (la de AH o la de ESP) la SA que corresponda con el SPI.
- Se decodifica el paquete según se indica en la SA.

Si usamos modo túnel los 2 primeros pasos son los mismos que los anteriores pero además la pasarela (que es quien se encarga de la gestión de la seguridad en este caso) deberá, para flujo saliente codificar la cabecera IP (además de la parte de datos) y construir una nueva cabecera IP con la dirección de la pasarela destino (no con la del host) y enviar el paquete. Y para el flujo entrante decodificar el paquete de datos y la cabecera IP encriptada y enviar el paquete al destinatario final.

En el caso de que usáramos AH más ESP tendríamos un SA bundle que no es mas que la concatenación de dos SA En este caso el paquete antes de ser enviado pasaría por dos SAs una de ESP y otra de AH, y a la hora de recibirlo sucedería lo mismo.

AH (Authentication header)

Como se ha dicho anteriormente, proporciona integridad, autentificación y protección anti-repudio. Este último parámetro es opcional y puede ser escogido cuando se establece la asociación de seguridad. AH proporciona autentificación a tanta información como sea posible de la cabecera, además de los datos de capas superiores. Sin embargo, algunos campos de la cabecera IP pueden cambiar en tránsito y el valor de estos campos, cuando llegan a destino no pueden ser predichos por el que los envía. Estos valores no pueden

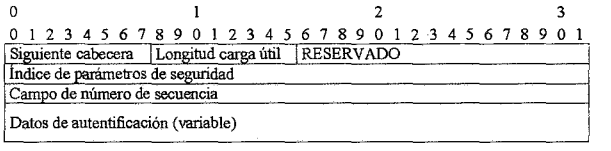

Figura 4: Formato del paquete AH

ser protegidos por la AH. Se puede utilizar en modo transporte o en modo túnel.

Todos los campos descritos en la figura 4 son obligatorios, es decir, que siempre están presentes en el formato AH y están incluidos en el cálculo del valor de comprobación de integridad (ICV). La cabecera AH tiene que ser múltiple de 64 bits.

El índice de parámetros de seguridad es un número arbitrario de 32 bits que, en combinación con la dirección IP destino y el protocolo AH, únicamente identifica la asociación de seguridad para este paquete. En el caso de que el SPI tome el valor 0 significará que no existe ninguna SA. El número de secuencia contiene un número creciente de contador. Es obligatorio y siempre está presente incluso si el receptor no elige habilitar el servicio anti-repudio. Los contadores de emisor y receptor se inicializan a 0 cuando se establece la SA. El emisor lo incrementa para esa SA e inserta el nuevo valor en este campo. Por tanto, el primer paquete enviado usando una determinado SA tiene como número de secuencia el 1. Si está activado el anti-repudio (por defecto), el emisor comprueba para asegurarse que el contador no ha pasado un ciclo antes de insertar el nuevo valor en el campo. En otras palabras, el emisor no enviará otro paquete en la SA si haciéndolo causa que el número de secuencia pase un ciclo.

El ICV está dentro del los datos de autentificación. El algoritmo de autentificación empleado para el cálculo del ICV se especifica en la asociación de seguridad establecida anteriormente. En comunica-

ción punto a punto, algoritmos apropiados son los denominados MACs (Keyed Message Authentication Codes) basados en algoritmos de encriptación simétrica (p.e. DES) o en funciones hash (p.e. MD5 o SHA-1). Para comunicaciones multicast son apropiados los algoritmos de hash combinados con algoritmos de firma asimétrica. De todas formas se pueden utilizar otros algoritmos.

Para finalizar, el ICV del AH se calcula sobre los campos de la cabecera IP que son o constantes en tránsito o son un valor predecible en destino, la cabecera AH (todos los campos, aunque los datos de autentificación, donde se encuentra este valor, se suponen 0) y los datos de niveles superiores, que se asumen como constantes durante el trayecto.

Una vez recibido el paquete, el receptor calcula el ICV sobre los campos apropiados del paquete, usando el algoritmo de autentificación especificado y verifica que es el mismo que el ICV incluido en el campo de datos de autentificación. Si coinciden, entonces el paquete es válido y se acepta. Si el test falla, el receptor debe descartar el paquete recibido.

En las figuras 5 y 6 se pueden observar los paquetes IPv6 en modo transporte y túnel después de aplicar AH.

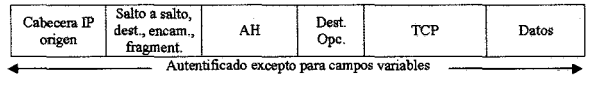

Figura 5: Paquete IPv6 después de aplicar AH en modo transporte

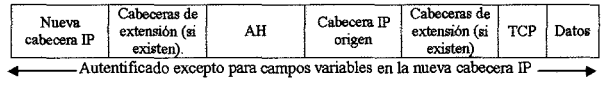

Figura 6: Paquete IPv6 después de aplicar AH en modo túnel

ESP (ENCAPSULATING SECURITY PAYLOAD)

Los servicios de seguridad que nos puede ofrecer ESP son confidencialidad, autentificación, anti-repudio, integridad y confidencialidad parcial en el flujo de tráfico. Hay que tener en cuenta que: la confidencialidad y/o autentificación deben estar activos; no puede haber anti-repudio ni integridad sin autentificación y que para que haya confidencialidad en el flujo de tráfico debe seleccionarse el modo túnel.

El formato del paquete ESP variará según la seguridad elegida así como también variara su localización dentro del paquete IP conforme al modo seleccionado (modo transporte o túnel). Pero en general el formato del paquete ESP se puede definir como la figura 7.

En el campo de datos de carga útil es donde se encuentra la información propiamente dicha. Consiste

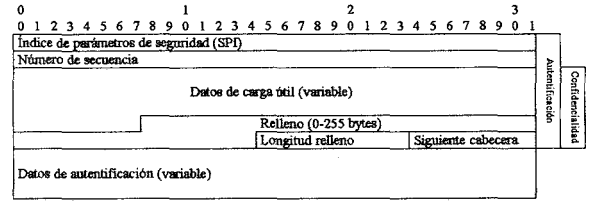

Figura 7: Formato del paquete ESP

en un número indefinido de bytes (mucho mayor que el mostrado en la figura 7) que contienen la información encriptada que queremos transmitir. Muchos algoritmos de encriptación necesitan un vector de inicialización que les sirve de sincronización. Cuando este vector es requerido va incluido en los datos de carga útil. En este caso es importante que el algoritmo especifique la exacta localización y el tipo de estructura del vector en cuestión. En el caso de que hayamos escogido autentificación en este campo tendremos un ICV, muy similar al que utiliza el AH que nos servirá para cerciorarnos de si alguien a modificado el paquete después de haber sido enviado. Hay que darse cuenta que esta autentificación es sobre la información encriptada es decir que para comprobar que la información que nos llega es auténtica deberemos codificarla, lo cual puede no sernos útil dependiendo del sistema que se utilice.

En las figuras 8 y 9 se pueden observar los paquetes IPv6 en modo transporte y túnel después de aplicar ESP.

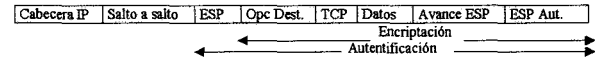

Figura 8: Paquete IPv6 después de aplicar ESP en modo transporte

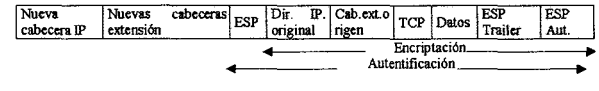

Figura 9: Paquete IPv6 después de aplicar ESP en modo túnel

COMBINACIÓN: AUTENTIFICACIÓN MÁS PRIVACIDAD

Los dos mecanismos de seguridad de IP se pueden combinar para transmitir un paquete IP que tenga autentificación y privacidad. Existen dos técnicas que

se puedan utilizar, diferenciadas por el orden en que se apliquen los dos servicios.

A) Encriptado antes de autentificación

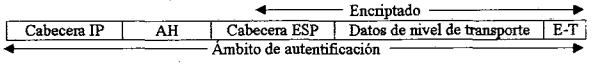

Figura 10: Encriptado antes de autentificación (modo transporte o túnel) en IPv6

En este caso, el paquete IP entero transmitido se autentifica, incluyendo ambas partes, la encriptada y la no encriptada. Primero se aplica ESP a los datos que se van a proteger, después incorpora al principio la cabecera de autentificación y la(s) cabecera(s) IP en texto nativo. De hecho, existen dos casos:

- ESP en modo transporte. La autentificación se aplica al paquete IP entero pero sólo el segmento de la capa de transporte se protege por el mecanismo de privacidad.
- ESP en modo túnel. La autentificación se aplica al paquete IP entero entregado a la dirección IP destino externa y la autentificación se lleva a cabo en el destino. El paquete IP interno se protege por el mecanismo de privacidad para su entrega al destino IP interno.

B) Autentificación antes del encriptado

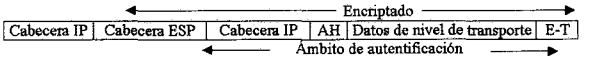

Figura 11: Autentificación antes de encriptado (modo túnel) en IPv6

Esta técnica sólo es apropiada para ESP en modo túnel. En este caso la cabecera de autentificación se sitúa dentro del paquete IP interno. Este paquete interno es autentificado y protegido por el mecanismo de privacidad.

Cabe destacar que este método puede ser preferible por las siguientes razones. Primero, ya que el AH se protege por el ESP, es imposible que cualquiera intercepte el mensaje y altere el AH sin ser detectado. Segundo, puede ser deseable almacenar la información de autentificación con el mensaje y el destino para una referencia posterior. Es más conveniente hacer esto si la información de autentificación se aplica a un mensaje no encriptado; de la otra forma, el mensaje tendría que ser reencriptado para verificar la información de autentificación.

CONCLUSIÓN

Las cabeceras AH y ESP están definidas tanto en IPv4 como IPv6. En el caso de IPv4 las nuevas cabeceras son añadidas al paquete como opciones adicionales. En el caso de IPv6, el protocolo ya está diseñado para incorporar estas cabeceras y se disponen en el orden óptimo para no entorpecer el tráfico de manera ostensible.

Los mecanismos de seguridad que se han citado son, en principio, suficientes para asegurar que toda información que viaje por la red vía protocolo IP será segura, fiable y autentificada. Estamos en el comienzo de una era donde Internet va a jugar un papel muy importante en la sociedad y por consiguiente la seguridad que pueda tener va a ser uno de los principales condicionantes ya que la mayoría de aplicaciones que se van a poder llevar a cabo necesitarán rellenar datos personales, algunos de ellos muy importantes o hacer transacciones bancarias de gran importancia y saber que existe un protocolo que va a proteger este tipo de transmisión de información va a empujar a desarrollar nuevas aplicaciones e impulsar las ahora poco existentes que necesitan una seguridad y fiabilidad del 100%.

IPSec está todavía en fase de desarrollo y por tanto los mecanismos de seguridad pueden ser modificados. El futuro de dichos mecanismos de seguridad es bastante incierto, cabiendo la posibilidad de que nunca sean realmente utilizados ya que se tiende a ofrecer seguridad a nivel de aplicación, donde la seguridad se ofrezca de modo transparente al usuario siendo esta de punto a punto.

BIBLIOGRAFÍA

[1] William Stallings. 1995. Network and Internetwork Security, principles and practice. Ed. Prentice Hall.
[2] Cisco systems: http://www.cisco.com
[3] Softpro: http://www.softpro.com/softpro
[4] SSH: http://www.ipsec.com
[5] http://www.cs.ucl.ac.uk/staff/J.Crowcroft/mmbook/book/node345.html
[6] http://www.web.mit.edu/network/isakmp
[7] http://www.whatis.com/IPSec.htm
[8] Kent, S., and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, Noviembre 1998
[9] Kent, S., and R. Atkinson, "IP Authentication Header", RFC 2402, Noviembre 1998.
[10] Kent, S., and R. Atkinson, "IP Encapsulating Protocol", RFC 2406, Noviembre 1998.
[11] D. Pper, "The Internet IP Security Domain of Interpretation for ISAKMP", RFC 2407, D.