



Seguridad en Redes

Protocolos Seguros

junio de 2009



Índice

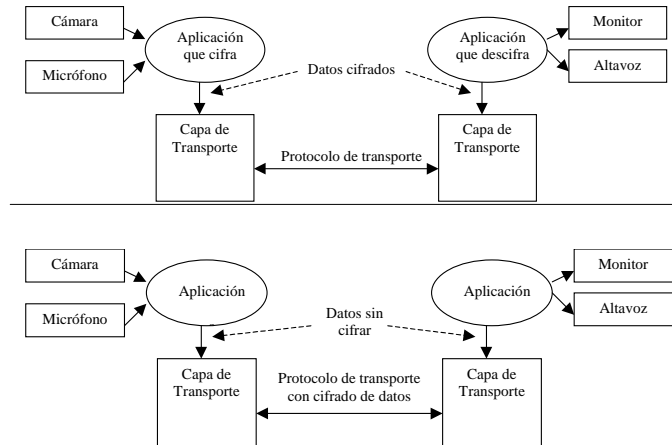
- ¿Dónde situar la seguridad? Podría ser en varias capas...
Lo veremos con algunos ejemplos.
 - En la capa de Enlace: Seguridad inalámbrica. WEP y WPA
 - En la capa de Red: IPSec
 - En la capa de Transporte: SSL (TLS)
 - En la capa de Aplicación: PGP
- Resumen.

junio de 2009

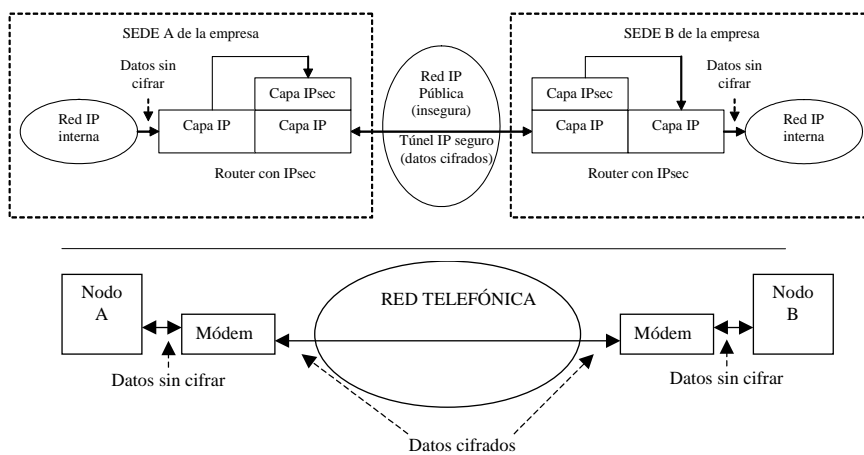
2



Seguridad: ¿Dónde?(I)



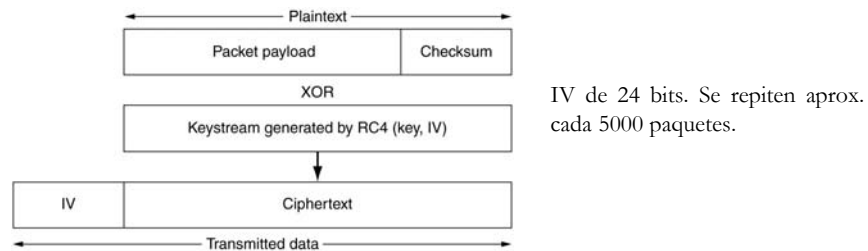
Seguridad: ¿Dónde? (y II)





Seguridad inalámbrica

- **Problema:** La seguridad perimétrica no protege aquello que no está dentro del perímetro. Si existen nodos inalámbricos el aparcamiento no está protegido.
- 802.11 definió WEP (*Wired Equivalent Privacy*) para proporcionar seguridad a nivel de enlace. Desafortunadamente es **muy** inseguro.



Wi-Fi Protected Access (WPA)

- Puede funcionar con un servidor de autenticación (RADIUS, generalmente) que distribuye claves diferentes a cada usuario o en modo de clave pre-compartida: PSK (*pre-shared key*). Utiliza RC-4, al igual que WEP.
- Implementa un protocolo de Integridad de Clave Temporal (TKIP – *Temporal Key Integrity Protocol*) que cambia las claves de 128 bits dinámicamente.
- Aumenta el tamaño del IV a 48 bits. Mejora el mecanismo de CRC y contador de tramas para evitar ataques de repetición.
- WPA2 se basa en 802.11i e incluye el algoritmo AES (Rijndael) para cifrado.



IPsec (RFCs 2401, 2402 y 2406 entre otros).

- **Problema:** Hubo años de batallas dentro de la IETF para determinar dónde colocar la seguridad de canal. La solución de compromiso fue incorporarla en la capa de red *opcionalmente* ya que podía aliviar el problema sin estorbar demasiado.
- El resultado fue llamado **IPsec**, conjunto de protocolos para **establecimiento de claves autenticación** y **encriptación** de los paquetes IP en un flujo de datos.
- Opera en la capa de Red del modelo OSI y se utiliza también en IPv6. Es independiente de los algoritmos utilizados.
- La arquitectura IPsec utiliza el concepto de **asociación de seguridad (SA)** que identifica los algoritmos y parámetros utilizados.

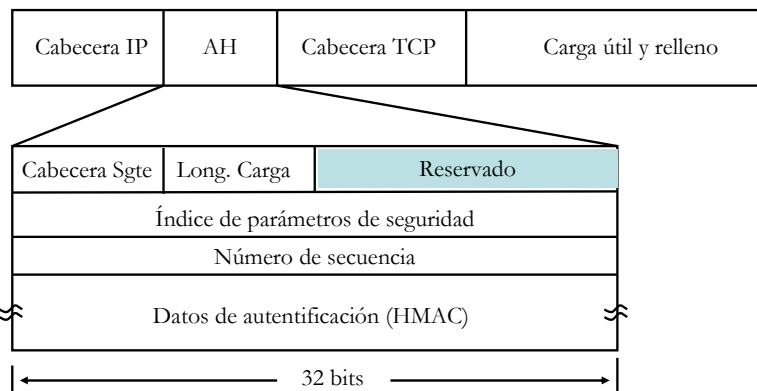


IPsec: Detalles Técnicos

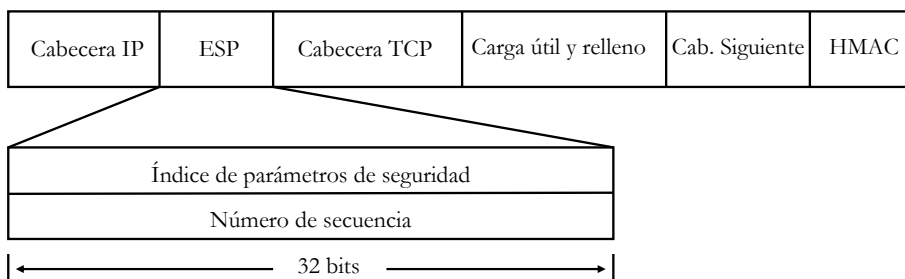
- **Intercambio de claves: ISAKMP/IKE (RFC 2408/2409)**, *Internet Security Association and Key Management Protocol/Internet Key Exchange*, basado en Diffie-Hellman. Utiliza UDP en el puerto 500 para establecer la SA negociando opciones e intercambiar una clave de sesión. Comprometido recientemente, se trabaja en la versión 2 (RFC 4306).
- **Encabezado de Autenticación (AH)**
 - Proporciona **integridad de los datos** y **autenticación** pero no confidencialidad.
- **Carga Útil de Encabezamiento de Seguridad (ESP)**
 - Proporciona **integridad, autenticación y confidencialidad**. Acabará por sustituir totalmente a AH, ya que puede funcionar sin cifrado.



Authentication Header (AH)



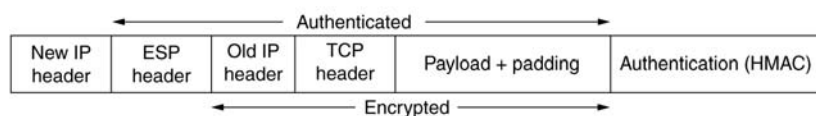
Encapsulating Security Payload (ESP)





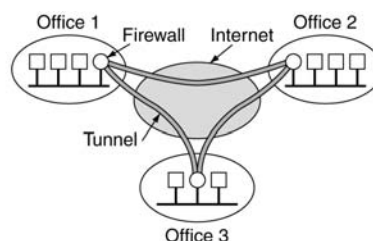
Modo túnel

- Lo visto anteriormente es el **Modo de Transporte**, pero IPsec también puede utilizarse en **Modo Túnel**, donde todo el paquete IP es encriptado y encapsulado sobre un datagrama IP nuevo.
- Se utiliza generalmente para establecer **túneles seguros** entre encaminadores, o máquinas sobre Internet.



Redes Privadas Virtuales

- **Idea:** Construir una red privada (cuyo tráfico no puede ser husmeado ni modificado) sobre una red pública. Se establecen túneles seguros entre los *firewalls* de las redes locales.



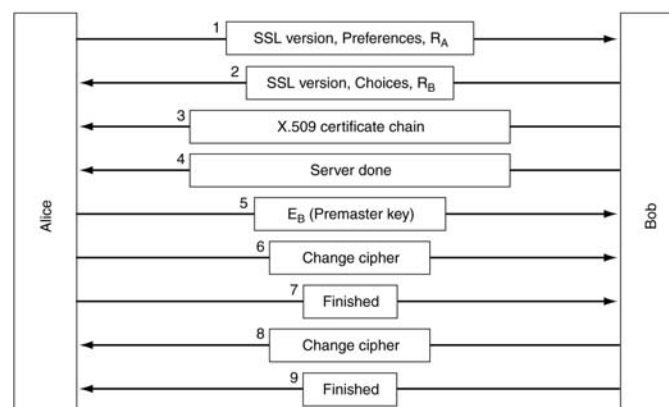


Secure Sockets Layer: SSL

- Diseñado por Netscape Comm. Corp en 1995
- **Esencia:** SSL es una capa de seguridad que se sitúa sobre la capa de transporte. Se usa, generalmente, en combinación con HTTP (HTTPS), pero puede usarse con cualquier otro protocolo.
- Ahora se conoce como *Transport Layer Security* (TLS) y está estandarizado en la RFC 2246
- Consiste en dos fases separadas:
 - Establecimiento de la conexión.
 - Utilización de la conexión segura.
- Soporta múltiples algoritmos criptográficos.

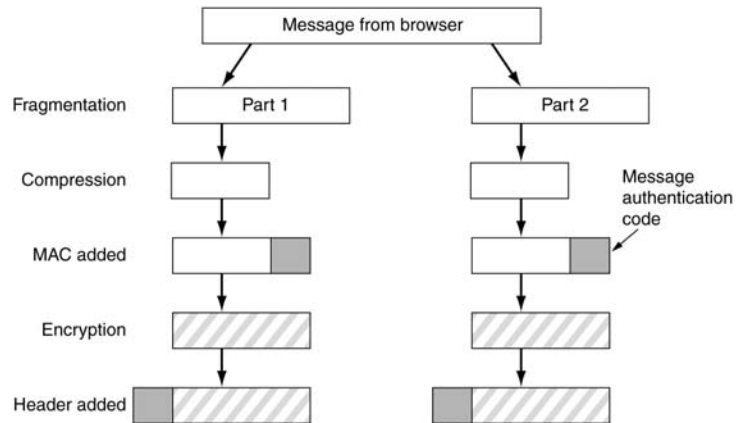


SSL: Protocolo de Establecimiento de Conexión

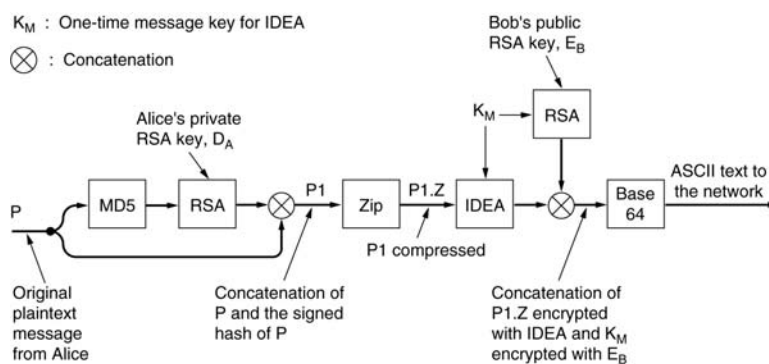




SSL: Protocolo de Transporte de Datos



Pretty Good Privacy (PGP)





Resumen

- Los protocolos seguros (aquellos que proporcionan canales de transmisión seguros) pueden situarse en varias capas diferentes. La discusión hoy en día sigue abierta.
- Como ejemplo de seguridad en la capa de **enlace**, hemos visto **WEP** y **WPA**, que pretenden añadir privacidad en las transmisiones de nodos inalámbricos.
- Cuando el IETF trabajaba en IPv6 y pretendía añadir seguridad, las discusiones fueron encarnizadas. El resultado fue **IPSec** que aporta un método independiente de los algoritmos empleados para proporcionar seguridad a nivel de la **capa de red**.
- Mientras tanto Netscape diseñó un protocolo seguro a nivel de transporte: **SSL**, básicamente para proporcionar accesos seguros a la web (**https**). Hoy en día se conoce como **TLS** y permite emplear cualquier protocolo de aplicación.
- Pero los usuarios de la red generalmente no confían en ningún método de seguridad que no sea empleado directamente en la capa de aplicación. Ronald Rivest diseñó **PGP** para añadir seguridad y autenticación al correo como primera aplicación de las técnicas criptográficas serias.
- La seguridad corporativa emplea generalmente varias de estas técnicas. Veremos ejemplos y casos prácticos próximamente.