

Criptografía y Seguridad de Datos

Seguridad sobre la Capa de Transporte

Profs. Rodolfo Sumoza/Carlos Figueira

Universidad Simón Bolívar

figueira@ldc.usb.ve

Basado en una presentación de Henric Johnson

Blekinge Institute of Technology, Sweden

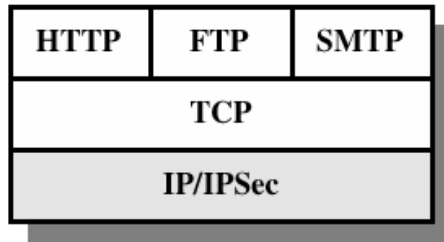
Contenido

- Consideraciones previas
- Secure Socket Layer (SSL)
- Transport Layer Security (TLS)

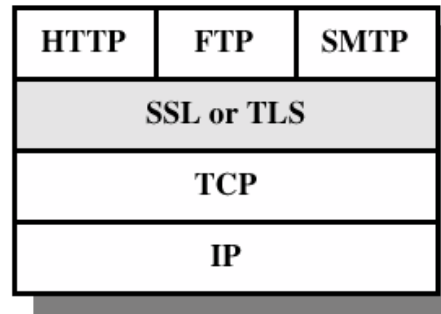
Consideraciones previas

- La WEB es de índole pública.
- La plataforma Web es compleja, esconde muchos defectos de seguridad.
- Los servidores Web son fáciles de configurar y manejar.
- Los usuarios no están al tanto de los riesgos.

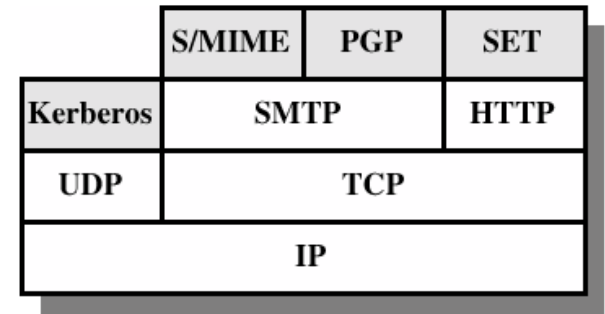
Facilidades de Seguridad en la pila de protocolos TCP/IP



(a) Network Level



(b) Transport Level



(c) Application Level

SSL y TLS

- SSL fue creado por Netscape
- El grupo de trabajo TLS fue formado en la IETF
- La primera versión de TLS puede ser vista como SSLv3.1

Arquitectura SSL

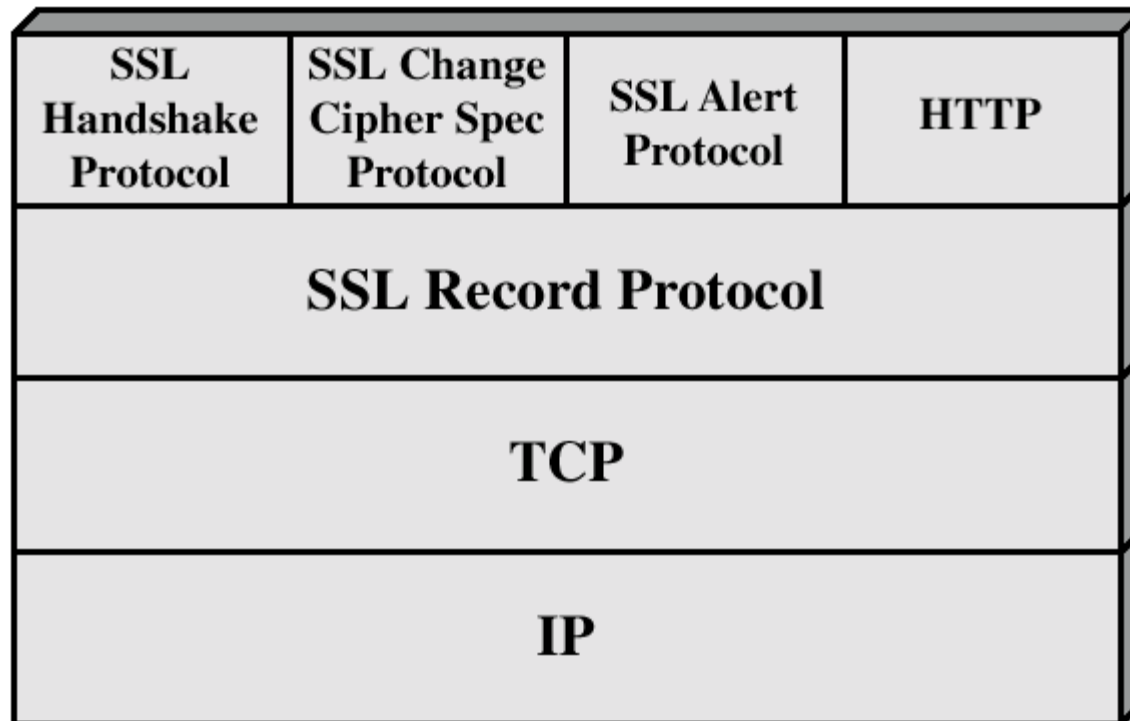
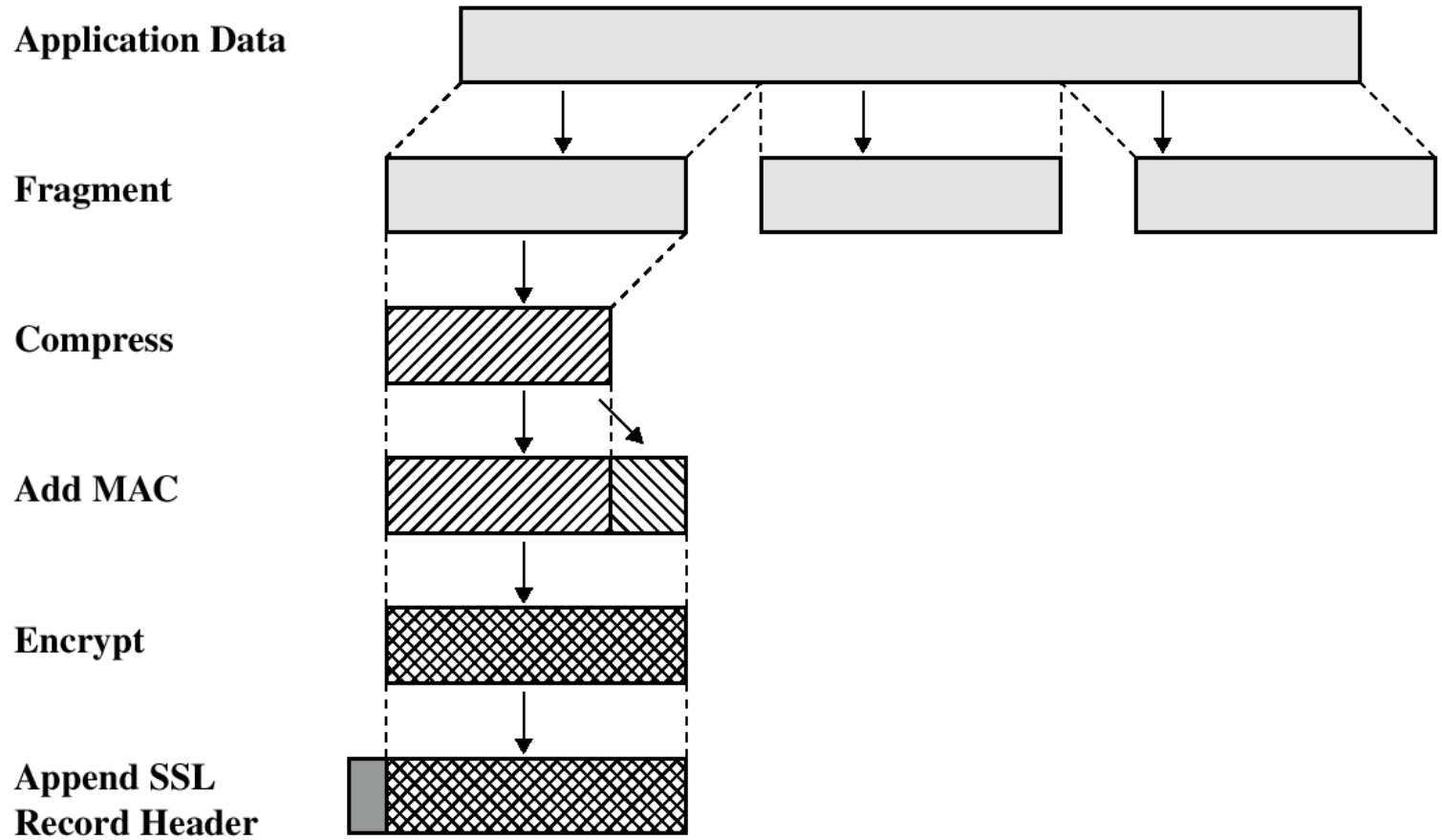
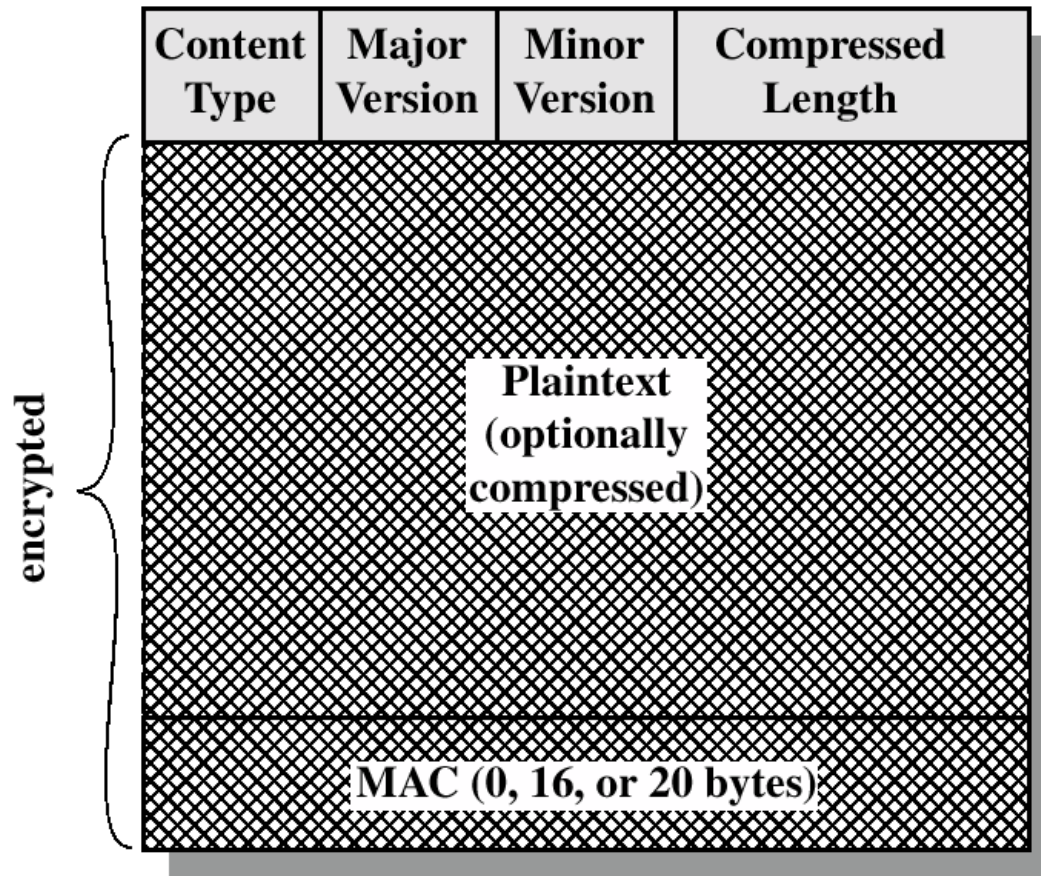


Figure 7.2 SSL Protocol Stack

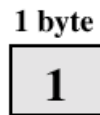
Operación del Protocolo SSL Record



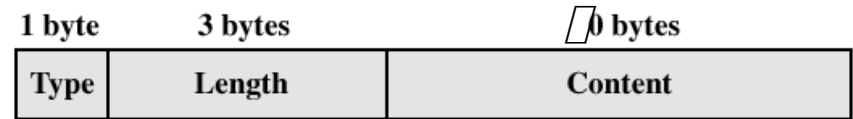
Formato del Prot. Record



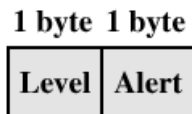
Formato de los protocolos SSL



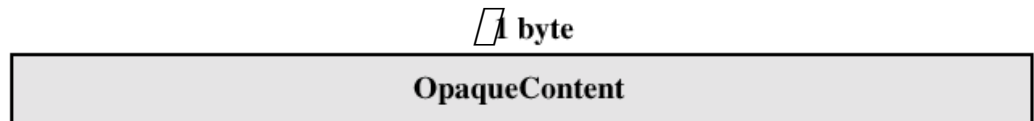
(a) Change Cipher Spec Protocol



(c) Handshake Protocol



(b) Alert Protocol

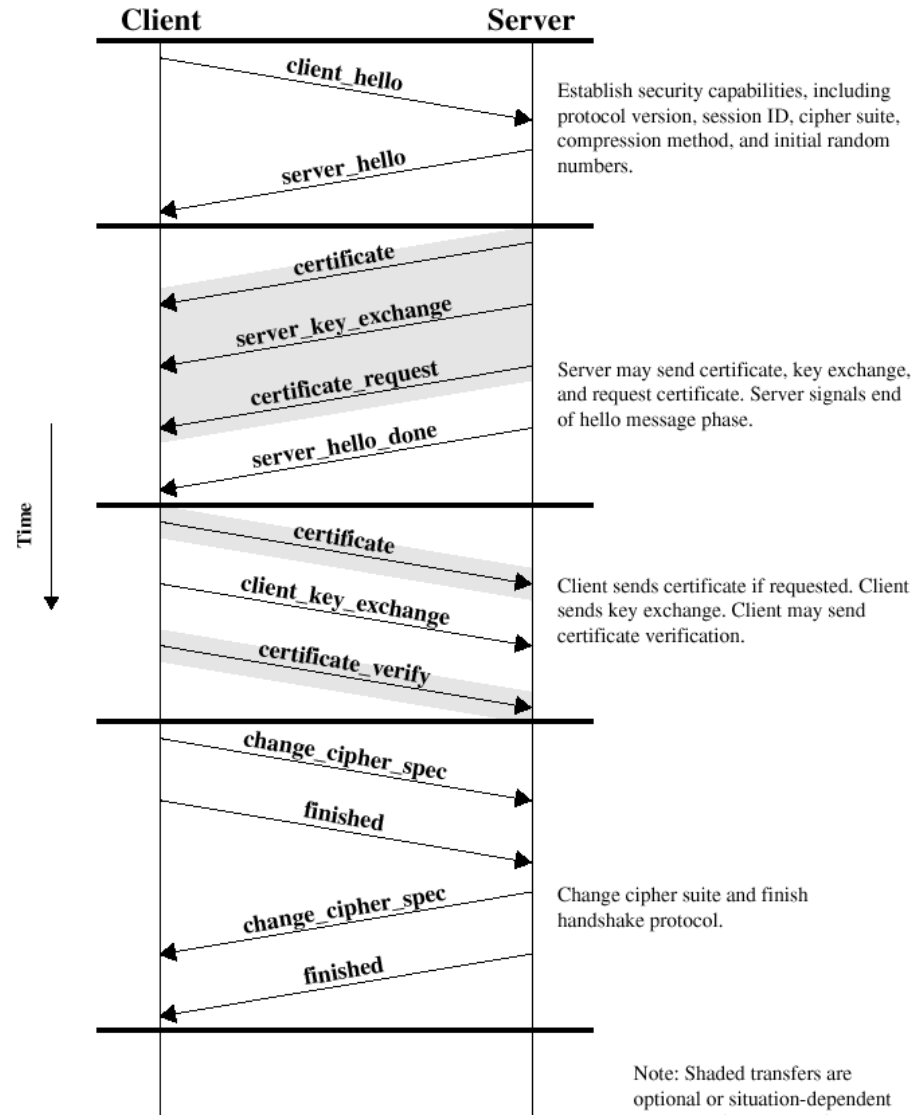


(d) Other Upper-Layer Protocol (e.g., HTTP)

Protocolo de Negociación inicial (*Handshake*)

- La parte más compleja de SSL.
- Permite al servidor y al cliente autenticarse mutuamente.
- Negocia el cifrado, el algoritmo MAC y las claves criptográficas.
- Se usa antes de transmitir datos de aplicaciones.

Secuencia de *Handshake*



Transport Layer Security TLS

- Protocolo record: mismo formato que SSL.
- Definido en RFC 2246, muy similar al SSLv3.
- Diferencias:
 - Número de versión
 - MAC, PRF (pseudorandom function)
 - Códigos de Alerta, Esquemas de cifrado
 - Tipos de certificados del cliente
 - Mensajes certificate_verify y finished
 - Cómputo de la criptografía, Relleno

OpenVPN

- Alternativa a IPSec para redes privadas virtuales
- Basada en TLS/SSL
- Sencilla (¡IPSec es complejo!)
- Flexible (espacio usuario), implementaciones libres robustas