Lección 9: Introducción al protocolo SSL

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Dr. Alfonso Muñoz
amunoz@diatel.upm.es
Universidad Politécnica de Madrid
R&D Security Researcher. T>SIC Group – UPM

SSL (Secure Sockets Layer)

- La empresa Netscape Communication crea en la década de los 90 el protocolo estándar SSL, un procedimiento para proporcionar comunicaciones seguras en una red.

- Es un protocolo criptográfico que proporciona confidencialidad, autenticidad e integridad en una comunicación cliente/servidor.

¿Cómo establecer una comunicación segura con SSL?

- SSL Handshake protocol

  Facilita la negociación de parámetros de seguridad para facilitar la confidencialidad, integridad y autenticidad en una comunicación entre cliente y servidor.

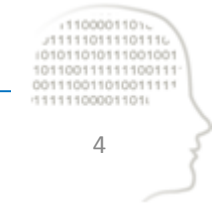
- SSL Record protocol

  Especifica la forma de encapsular los datos transmitidos y recibidos, incluidos los de negociación.

Ejemplo negociación básica autenticación servidor. SSL handshake protocol (I)

1. El cliente envía un mensaje “ClientHello” especificando la versión más alta del protocolo TLS soportada, un número aleatorio y una lista de algoritmos de autenticación, cifrado y MAC (Message Authentication Code), así como algoritmos de compresión.

2. El servidor responde con un mensaje “ServerHello”, indicando la versión del protocolo seleccionado (la más alta que soporten cliente y servidor), un número aleatorio, los algoritmos que selecciona de los enviados por el cliente y su certificado digital (mediante un mensaje Certificate) para autenticarle.



SSL handshake protocol (II)

3. El cliente verifica el certificado del servidor, típicamente mediante una autoridad de confianza o PKI. A continuación el cliente responde con un mensaje ***ClientKeyExchange***, el cual contiene una *PreMasterSecret (un número secreto)*, con información para generar la clave de sesión. Si se utiliza el algoritmo RSA este mensaje irá cifrado con la clave pública del servidor y este número aleatorio generado por el cliente será de 48 bytes.

SSL handshake protocol (III)

4. El cliente y el servidor usan los números aleatorios intercambiados y la PreMasterSecret (el servidor necesita utilizar su clave privada para recuperarla). Con estos datos calculan un secreto común, denominado “master secret”. Todas las subclaves de la conexión serán derivadas de ésta mediante la función pseudoaleatoria establecida.

5. El cliente ahora envía un registro **ChangeCipherSpec** e indica al servidor que a partir de ese momento toda la información intercambiada será autenticada y, si así lo estableció el servidor, cifrada.

SSL handshake protocol (IV)

6. Finalmente el cliente envía un mensaje **Finished** firmado y cifrado, conteniendo un hash y MAC de los mensajes negociados anteriormente.

7. El servidor intentará descifrar el mensaje Finished enviado por el cliente y verifica el hash y el MAC. Si el descifrado o la verificación falla, la conexión no tiene lugar.

SSL handshake protocol (V)

8. Si todo va bien, el servidor envía un ChangeCipherSpec indicando al cliente que a partir de ese momento todo lo que le envíe estará firmado y, si fue negociado, también cifrado. El servidor envía su mensaje Finished firmado y cifrado, validándolo el cliente, conteniendo un hash y MAC de los mensajes negociados anteriormente.

9. Finaliza la fase de negociación, pudiendo intercambiar mensajes cliente y servidor autenticados y cifrados (si así fue establecido).

Aplicaciones del protocolo TLS/SSL

TLS: Mejora SSL en la protección frente a nuevos ataques (nuevos algoritmos criptográficos, evita downgrade, etc.).

USOS:

- Comercio electrónico y banca online
- Securizar redes privadas virtuales (OpenVPN)
- Autenticación y cifrado de datos VoIP

Seguridad del protocolo TLS/SSL

- La versión más moderna del protocolo TLS con las extensiones recomendadas, puede considerarse segura frente a los ataques conocidos.
- Los ataques que vulneran su seguridad se centran especialmente en engañar al usuario con la dirección a la que se conecta o con el certificado digital que autentifica al servidor.

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contacto: info@intypedia.com