Desarrollo

Antes de hablar acerca de openssl, resulta necesario realizar una explicación acerca de que es SSL.

- SSL:

  La capa de sockets seguro (Secure Sockets Layer, SSL) establece un canal seguro en el nivel de transporte entre dos partes. SSL ofrece privacidad en las comunicaciones al utilizar una encriptación con llave simétrica, y asegura la integridad de los datos mediante códigos de autenticación de mensajes (Messages Authentication Codes, MACs).

  Netscape Communications Corporation desarrolló originalmente el SSL, a mediados de la década de los '90. La versión 2 de SSL fue la primera en ser utilizada ampliamente y la versión 3 otorgaba mayor eficiencia, flexibilidad y un mayor conjunto de características.

  El SSL es un protocolo de dos capas, que opera sobre un protocolo de transporte confiable, usualmente TCP. Existen 2 tipos de uso del protocolo SSL, el primero es conocido como "SSL del Servidor" y el segundo "SSL del cliente", el primero se utiliza para autentificar que una dirección web corresponde a quien dice pertenecer, y la segunda autentifica que la persona que está al otro lado de la conexión es quien dice ser, la primera resulta ser la más utilizada debido a eso se la explicará a continuación:

  Al utilizar SSL del servidor, el navegador web autentifica al servidor web con el cual se quiere establecer una conexión, y se desarrolla un canal cifrado entre ambos puntos, pero por otro lado, el servidor web no autentifica al navegador. Por ejemplo, si un alumno del departamento de electrónica se conecta al webmail del departamento, el alumno quiere asegurarse que se está conectando con este servidor y no con otro que intenta suplantarlo, sin embargo el servidor web no necesita autentificar el navegador del alumno pues

éste se está identificando a través de su login y password. A continuación se explicará el proceso en sí:

En primer lugar el servidor web debe entregar la llave pública de su certificado digital al navegador web, se debe señalar que toda la información contenida en este certificado digital es pública, por lo cual no existe mayor problema en que viaje libremente por la Internet desde el servidor al navegador. Antes que el navegador pueda confiar en la llave pública debe revisar que el certificado digital haya sido firmado por una fuente contenida en la lista de autoridades de confianza del navegador. Una vez pasada esta comprobación, el navegador calcula el hash del certificado y lo compara con el hash que viene incluido en el certificado (descifrado utilizando la llave pública entregada por la autoridad de confianza), si ambos hash corresponden, entonces el navegador tiene la certeza que el certificado no ha sido alterado. Luego se verifica que el certificado se encuentre válido (su fecha de vencimiento aún no ocurra), y después se hace una revisión más profunda del certificado. Entre la información contenida en el certificado, viene la URL del servidor, el navegador comprobará que el nodo que envía la información tenga la misma URL que se encuentra codificada en el certificado. Si todo esto ocurre, el navegador extrae la llave pública del certificado mismo, entonces se genera una clave simétrica la cual se utilizará para cifrar la conversación entre el servidor y el navegador; el motivo de utilizar cifrado simétrico es que éste es rápido y no expande los datos durante la operación de cifrado. La clave simétrica es cifrada con la clave pública del servidor, extraída del certificado de éste y luego la envía, ya que está cifrada con la clave pública del servidor, solo el servidor que es quien posee la clave privada puede descifrar y obtener la clave simétrica que se utilizará en la conversación, ahora ambas partes pueden utilizar esta clave simétrica generada aleatoriamente en el navegador para cifrar y descifrar datos de cada uno.

La autenticación ocurrió, a modo de resumen de la siguiente forma:

El navegador generó una clave simétrica aleatoria y luego la cifró utilizando la llave pública del servidor, el hecho que el servidor web pueda descifrar la

clave simétrica y por ende participar en la conversación, le dice al navegador que él es el servidor real, pues es el único nodo en todo el universo que posee la llave privada capaz de descifrar los datos encriptados con la llave pública, necesaria para desempaquetar la clave simétrica