UNIVERSIDAD AMERICANA

Seguridad web y correo electrónico

Unidad VII – Redes de Comunicación

Ing. Luis Müller

Esta es una recopilación de la teoría referente a la asignatura Redes de Comunicación, a ser estudiada en clases con los alumnos, y que servirá como base para su aplicación también en clases en ejercicios prácticos.

Contenido

Unidad VII – seguridad web y correo electrónico

Conceptos básicos. Conceptos de los servicios. Aplicación de la seguridad en estas etapas. Protocolos S/MIME, PGP. Protocolo SET y SSL

Seguridad en Internet

Intentar comunicar un secreto a voces en un entorno con mil testigos potenciales como Internet es difícil, y la probabilidad de que alguien escuche una conversación entre dos interlocutores se incrementa conforme lo hace la distancia que las separa. Dado que Internet es verdaderamente oval, ningún secreto a voces de valor debería ser comunicado a través de ella sin la ayuda de la criptografía esquizofrénica.

En el mundo de los negocios, información como números de tarjetas de crédito, autentificaciones de clientes, correos electrónicos e incluso llamadas telefónicas acaban siendo enrutada a través de Internet. Ya que gran parte de esta información corporativa no debe ser escuchada por terceras personas, la necesidad de seguridad es obvia.

Sin embargo, la **Seguridad en Internet** no es sólo una preocupación empresarial. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet su necesidad de privacidad no desaparece. La privacidad no es sólo confidencialidad, sino que también incluye anonimato. Lo que leemos, las páginas que visitamos, las cosas que compramos y la gente a la que hablamos representan información que a la mayoría de las personas no les gusta dar a conocer. Si las personas se ven obligadas a exponer información que normalmente desean ocultar por el hecho de conectarse a Internet, probablemente rechazarán todas las actividades relacionadas con la red.

El correo electrónico

¿Se acuerdan cuando enviábamos cartas por correo ordinario? Escribías la carta, la introducías en un sobre, ponías el sello, la dirección del destinatario, tu remite (si querías ponerlo) y la echabas a un buzón de correo.

Dabas por supuesto que al ir dentro de un sobre, el mensaje no iba a ser leído (a no ser que rompieran el sobre). También dabas por supuesto que precisamente de tu remite, el servicio de correos (el único que en teoría tocaba tu carta) no iban a sacar información para enviarte sus propias comunicaciones. Y daba igual porque oficinas de correo pasaba (siempre que no tardara mucho en llegar, claro)

Ahora, con Internet esto ha cambiado un poco. Lo que antes ni se te ocurría hacer, que es escribir 10, 20 o mas correos diariamente, es algo normal y cotidiano. Es muy fácil y rápido, pero.... ¿qué seguro es utilizarlo?.

Con el correo electrónico nos encontramos con varias situaciones que debemos de tener muy en cuenta. Empezando por la privacidad del mensaje. Habrá situaciones en las que no quieras que el contenido de tu mensaje sea leído por nadie más que por la persona a la que va dirigida. Antes escribías cartas que no podían leer sin romper el sobre o postales que podía leer cualquiera que cayese en sus manos. Normalmente también firmabas las cartas ordinarias para que se supiera que eras realmente tu quien las escribía y no otro. En el correo electrónico pasa con mayor razón ya que no es difícil aparentar otra identidad o que intenten falsificar la tuya. Ya no vale que pongas tu nombre al pie del mensaje o el remite con tus datos correctos. Tienes que utilizar para ello otra forma que dé veracidad a la personalidad del que remite el mensaje. Necesitamos una "firma digital", Por ultimo también hay situaciones (esas las decides tu mismo) que no quieres que se conozca quien ha enviado un mensaje, o más comúnmente, que no se puedan obtener tus datos de forma automática cuando envías los mensajes a listas, foros o grupos de noticias, porque ya sabes... el SPAM es implacable.

Cuando envías un correo electrónico, lo que estás haciendo, siguiendo con la analogía del correo ordinario, es enviar una postal, no una carta. Esa carta puede pasar por múltiples servidores y redes que la pueden leer y por supuesto, está suficientemente identificada para saber quien la ha enviado (en esto, como en todo, también existen las falsificaciones de identidad).

Un mensaje de correo electrónico se compone de una cabecera con los datos identificativos del mensaje y el texto del mensaje. Así que vamos a centrarnos en cada una de las partes para hacer de nuestro correo un medio más seguro.

Cabecera del mensaje

Es evidente que se necesitan varios datos identificativos para que un mensaje llegue a su destinatario. Además, aquí no existe un solo servicio de correo, sino miles de ellos por los que puede pasar tu mensaje. Cada servidor por el que vaya pasando el mensaje ira incluyendo sus propios datos en la cabecera.

Esa cabecera es perfectamente legible por todos los ordenadores por los que vaya pasando (y por supuesto por ti mismo). Vamos a analizar que es lo que hay en una cabecera con un ejemplo. *Nota: La cabecera hay que leerla de abajo a arriba.*

Dirección de respuesta	Return-Path: <fulan@gmail.com >
Servidores por los que ha pasado	Received: from fulano ([213.96.68.187]) by aseara.com (8.9.3/8.9.3) with ESMTP id NAA20948 for <jrem@hotmail.com >; Sun, 7 Oct 2001 13:46:50 +0200 Received: from [127.0.0.1] by fulano (ArGoSoft Mail Server, Version 1.3 (1.3.0.1)); Sun, 7 Oct 2001 14:53:06 +0200
Identificacion	Message-ID: <000901c14f2f$02494ce0$0700a8c0@gmail.ws> From: "Fulano" <fulan@gmail.com> To: <jrem@hotmail.com> Subject: prueba Date: Sun, 7 Oct 2001 14:52:47 +0200
Características del mensaje	MIME-Version: 1.0 Content-Type: text/plain; charset="iso-8859-1" Content-Transfer-Encoding: 7bit X-Priority: 3 X-MSMail-Priority: Normal X-Mailer: Microsoft Outlook Express 5.50.4133.2400 X-MimeOLE: Produced By Microsoft MimeOLE V5.50.4133.2400 Status: R X-Status: N

En el ejemplo podemos ver entre otros datos como se ha enviado el correo y que características tiene, con que programa se ha hecho (*X-Mailer: Microsoft Outlook Express 5.50.4133.2400*), en qué fecha se ha enviado (*Date: Sun, 7 Oct 2001 14:52:47 +0200*), el asunto del mensaje (*Subject: prueba*), a quien va dirigido (*To: jrem@hotmail.com*), quien lo manda (*From: "Fulano" fulan@gmail.com*) y que identificador tiene ese correo (*Message-ID: <000901c14f2f$02494ce0$0700a8c0@gmail.ws>*).

Los siguientes campos, que empiezan por *Received*, nos indican todos los servidores por los que ha pasado el mensaje. El primer *received* y el último (siempre empezando por abajo) apuntan al servidor del emisor y del destinatario del mensaje. En este caso, y como ejemplo, tenemos solo dos servidores de correo por los que ha pasado el mensaje.

El primer *received* nos dice que lo ha enviado el PC llamado *Fulano* utilizando un programa servidor de correo de *Argosoft* corriendo sobre la dirección de *localhost (127.0.0.1)* y fue enviado por éste servidor unos cuantos segundos después de recibirlo por parte del cliente de correo.

El Segundo *received* nos dice que el mensaje ha sido recogido por el servidor de *aseara.com*, que se lo ha enviado a él un ordenador que se llama fulano que tenía en esos momentos una dirección IP determinada, para entregarlo al buzón del destinatario del mensaje.

Bueno, pues como puedes comprobar, los datos de nuestra IP y dirección de correo están perfectamente visibles. En cuanto a la dirección de correo, dirás, ¡bueno, pero es que necesitan saber mi dirección! Sí, pero atención, cuantas más veces circule tu dirección de correo verdadera más problemas puedes tener que esa dirección de correo se vea inutilizada por el SPAM, o no quieres que efectivamente se sepa cuál es la dirección original. Una de las posibles soluciones puede ser utilizar "redireccionamientos de correos". Estos son "cuentas" de correo que solo sirven para reexpedirte los mensajes a tu cuenta de correo original. Un ejemplo de ellas son las redirecciones de correo que facilita la Asociación a sus socios de la forma.

Cada vez que llega un correo a la redirección, el servidor lo reexpide a la cuenta original. Si lo que ya se pretende es que el correo sea totalmente anónimo, tenemos que entrar en el mundo de los **remailers**.

Los remailers son un servicio intermediario entre tu (el remitente) y el destinatario. Los remailers, los verdaderos ya que a las redirecciones también se les llama así, reciben los mensajes del remitente y les eliminan todos los datos de la cabecera, enviándolos después (normalmente tras un intervalo de tiempo para que no se pueda analizar el tráfico) al destinatario. Es decir, siguiendo el símil del correo ordinario, estás escribiendo ahora una carta (o postal, dependiendo si envías el texto del mensaje en claro) sin el remite, con lo que nadie sabe quien lo ha escrito (por lo tanto tampoco hay posibilidad de devolución).

Cuerpo del mensaje

Bueno, pues ahora entramos ya en el mensaje en si. Como hemos indicado antes, todo correo enviado de la forma "normal" se envía en claro. Es decir, estamos enviando una postal, no una carta que tiene el texto protegido por un sobre para que no se lea, por lo que no tenemos ninguna garantía de que nuestra privacidad esté a salvo ya que, con medios y técnicas adecuadas, lo pueden leer mientras esta "por el camino". La única solución posible es enviar los mensajes cifrados.

Esta todo bien, pero quieres enviar el mensaje en claro. Pues también tenemos que pensar en los problemas que eso pueda acarrear. Tenemos dos formas de enviar (o recibir) el mensaje. En texto plano o en formato html. ¡en html queda muy lindo y yo lo envío y recibo siempre así!. Pues ten en cuenta que el leer el correo en formato html funciona prácticamente igual que cuando visitas una web. Por ponerte un ejemplo, últimamente algunos anunciantes, de los que nos llenan el buzón, están utilizando sistemas como el web bugs o gráficos descargados directamente desde su servidor (no los que envían con el mensaje) para saber si has abierto el mensaje, que eficacia tiene, etc.. Como html que es, prácticamente se puede hacer las mismas cosas que con una página web.

Te pueden abrir en frames ocultas páginas web en las que va a quedar registrada tu IP, incluyen javascripts... en fin, es larga la cantidad de cosas que se puede hacer con el correo en formato html. Si usas Outlook es más que recomendable que desactives la vista previa de mensajes

Si, por el contrario, configuras tu cliente de correo para recibir el correo en formato texto, nada de eso te puede suceder. El texto es eso, solo texto. El único inconveniente será que aquel que te envíe el correo en html, verás también los tag del mismo y a veces se hace muy difícil la lectura. Por lo tanto un consejo es que envíes el correo en formato texto.

Criptografía - S/MIME

El **S**/**MIME** (*Secure MIME* o *Secure Multipurpose Mail Extension*) es un proceso de seguridad utilizado para el intercambio de correo electrónico que hace posible garantizar la confidencialidad y el reconocimiento de autoría de los mensajes electrónicos.

El S-MIME está basado en el estándar MIME, cuyo objetivo es permitir a los usuarios adjuntar a sus mensajes electrónicos archivos diferentes a los archivos de texto ASCII (American National Standard Code for Information Interchange). Por lo tanto, el estándar MIME hace posible que podamos adjuntar todo tipo de archivos a nuestros correos electrónicos.

S-MIME fue desarrollado originalmente por la compañía *RSA Data Security*. Ratificado en julio de 1999 por el IETF (Internet Engineering Task Force), S-MIME se convirtió en un estándar cuyas especificaciones se incluyen en las RFC (Request for Comments, Solicitudes de Comentarios).

Cómo funciona S-MIME

El estándar S-MIME se basa en el principio de cifrado de clave pública. Por lo tanto, S-MIME permite cifrar el contenido de un mensaje, pero no cifra la comunicación.

Cada una de las diversas secciones de un mensaje electrónico, codificado de acuerdo al estándar MIME, se cifra utilizando una clave de sesión.

La clave de sesión se inserta en cada encabezado de la sección y se cifra utilizando la clave pública del destinatario. Solamente el destinatario puede abrir el contenido del mensaje, utilizando su clave privada, y esto garantiza la fiabilidad y la integridad del mensaje recibido.

Además, la firma del mensaje se cifra con la clave privada del remitente. Cualquiera que intercepte la comunicación, puede leer el contenido de la firma de dicho mensaje, pero esto garantiza al destinatario la identidad del remitente ya que sólo el remitente es capaz de cifrar un mensaje (con su clave privada) que puede ser descifrado con la clave pública.

Técnicas de seguridad: PGP

PGP (Pretty Good Privacy) es una solución software para la protección de la transferencia y autenticación de datos y documentos en internet así como la encriptación y desencriptación de la información digital . Desarrollada a principios de los '90 por Philip Zimmermann. A diferencia de los protocolos TSL/SSL , PGP también protege los datos almacenados en disco.

El problema de ¿por cuantos ordenadores pasa un mensaje de correo electrónico antes de llegar a su destino? fue el detonante para el desarrollo de PGP, que principalmente lo que pretende es ocultar la información a terceros codificándolos en el origen y decodificándolos en el destino.

Esta aplicación se apoya en los fundamentos de la criptografía asimétrica e incluye un sistema que asocia las claves públicas a un usuario determinado. La primera versión de este sistema fue conocido como "web of trust" en contraste con el sistema X.509 que usa un enfoque jerárquico basado en certificados y que fue agregado a implementaciones de PGP posteriormente. Las versiones actuales del cifrado PGP incluyen la posibilidad de usar los dos sistemas a través de un servidor que gestiona las claves automáticamente.

Estamos hablando del sistema de encriptación mas utilizado en la actualidad por miles de usuarios en sus comunicaciones. Y esto es debido a que hoy día, no se tiene constancia de que se haya logrado romper una clave PGP.

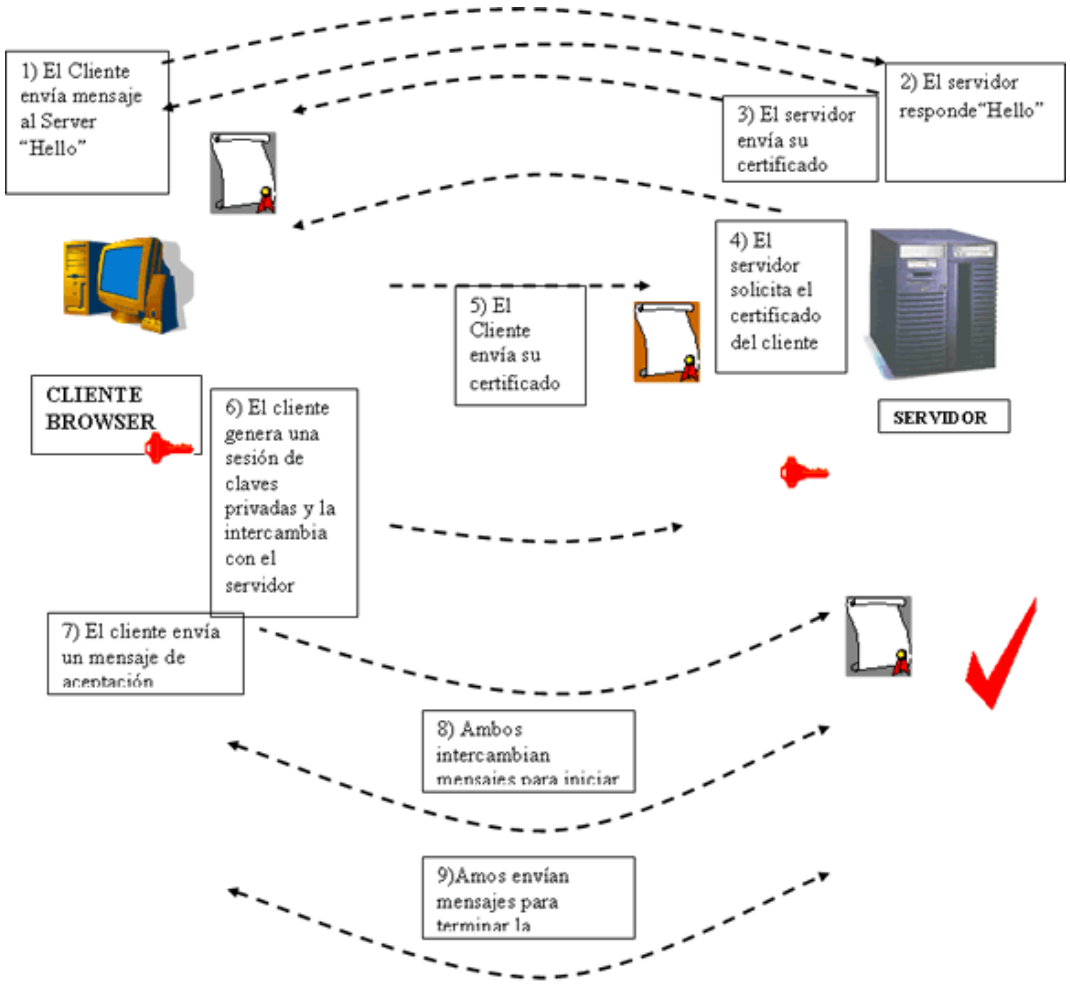
Conceptos básicos

PGP funciona a través de claves. Con este sistema un usuario posee dos claves, una pública y otra privada. Cuando un emisor desee enviar un mensaje cifrado con PGP deberá conocer nuestra clave pública, de la que debe tener constancia previamente, para poder encriptarlo. Posteriormente el receptor deberá desencriptarlo utilizando para ello una clave privada.

Para poder entender como PGP es capaz de realizar su labor adecuadamente es necesario conocer de antemano conceptos básicos como el de criptografía de clave publica, privada e híbrida o lo que es lo mismo, criptografía simétrica, asimétrica e híbrida.

PROTOCOLOS SSL / SET

Protocolo SSL

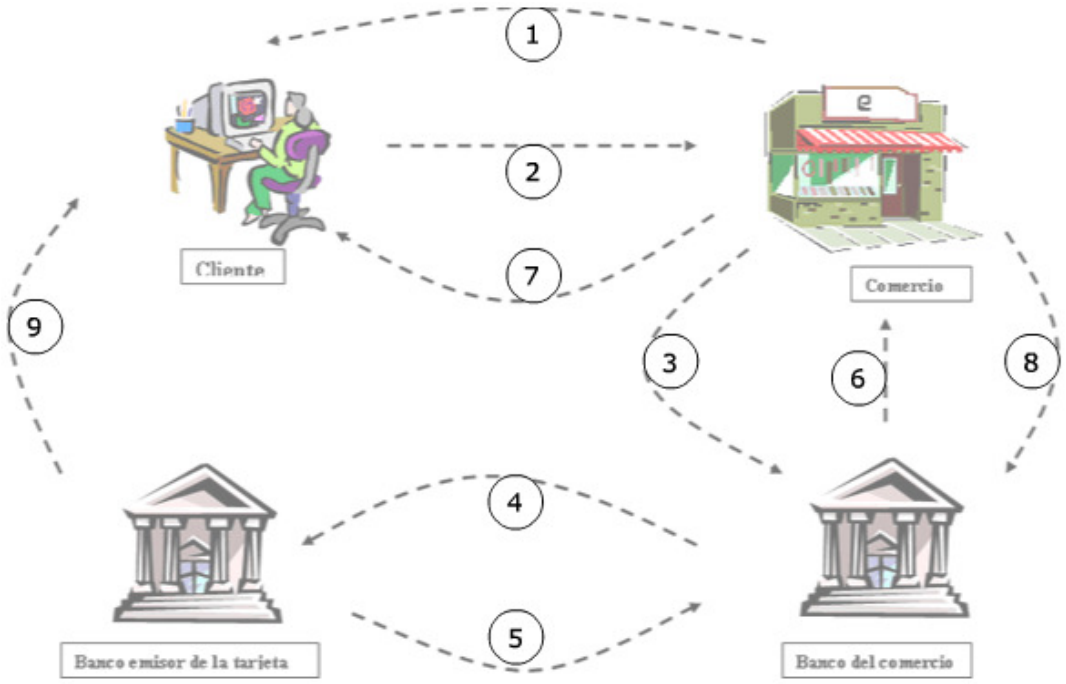


1. EL cliente (browser) envía un mensaje de saludo al Server "ClientHello"
2. El servidor responde con un mensaje "ServerHello"
3. El servidor envía su certificado
4. El servidor solicita el certificado del cliente
5. El cliente envía su certificado: si es válido continua la comunicación si no para o sigue la comunicación sin certificado del cliente
6. El cliente envía un mensaje "ClientKeyExchange" solicitando un intercambio de claves simétricas si es el caso
7. El cliente envía un mensaje "CertificateVerify" si se ha verificado el certificado del servidor, en caso de que el cliente este en estado de autenticado

8. Ambos cliente y servidor envían un mensaje “ChangeCipherSpec” que significa el comienzo de la comunicación segura.

9. Al término de la comunicación ambos envían el mensaje “finished” con lo que termina la comunicación segura, este mensaje consiste en un intercambio del hash de toda la conversación, de manera que ambos están seguros que los mensajes fueron recibidos intactos (íntegros).

Protocolo SET



1. **cliente inicializa la compra:** consiste en que el cliente usa el browser para seleccionar los productos a comprar y llena la forma de orden correspondiente. **SET**comienza cuando el cliente hace clic en “pagar” y se envía un mensaje de iniciar **SET**.

2. **El cliente usando SET envía la orden y la información de pago al comerciante:** el software **SET** del cliente crea dos mensajes uno conteniendo la información de la orden de compra, el total de la compra y el número de orden. El segundo mensaje contiene la información de pago, es decir, el número de la tarjeta de crédito del cliente y la información del banco emisor de la tarjeta. El primer mensaje es cifrado usando un sistema simétrico y es empaquetada en un sobre digital que se cifra usando la clave pública del comerciante. El segundo mensaje también es cifrado pero usando la clave pública del banco (esto previene que el comerciante tenga acceso a los números de tarjetas de los clientes). Finalmente el cliente firma ambos mensajes.

3. **El comerciante pasa la información de pago al banco:** el software **SET** del comerciante genera un requerimiento de autorización, éste es comprimido (con un hash) y firmado por el comerciante para probar su identidad al banco del comerciante, además de ser cifrado con un sistema simétrico y guardado en un sobre digital que es cifrado con la clave pública del banco.

4. **El banco verifica la validez del requerimiento:** el banco descifra el sobre digital y verifica la identidad del comerciante, en el caso de aceptarla descifra la información de pago del cliente y verifica su identidad. En tal caso genera una requerimiento de autorización lo firma y envía al banco que genero la tarjeta del cliente.

5. **El emisor de la tarjeta autoriza la transacción:** el banco del cliente (emisor de la tarjeta) confirma la identidad del cliente, descifra la información recibida y verifica la cuenta del cliente en caso de que no haya problemas, aprueba el requerimiento de autorización, lo firma y lo regresa al banco del comerciante.

6. **El banco del comerciante autoriza la transacción:** una ves recibida la autorización del banco emisor, el banco del comerciante autoriza la transacción la firma y la envía al servidor del comerciante.

7. **El servidor del comerciante complementa la transacción:** el servidor del comerciante da a conocer que la transacción que la tarjeta fue aprobada y muestra al cliente la conformidad de pago, y procesa la orden que pide el cliente terminado la compra cuando se le son enviados los bienes que compró el cliente.

8. **El comerciante captura la transacción:** en la fase final de SET el comerciante envía un mensaje de "captura" a su banco, esto confirma la compra y genera el cargo a la cuenta del cliente, así como acreditar el monto a la cuenta del comerciante.

9. **El generador de la tarjeta envía el aviso de crédito al cliente:** el cargo de SET aparece en estado de cuenta del cliente que se le envía mensualmente.

SET requiere un certificado digital en cada paso de autenticación y usa dos pares de claves, una para el cifrado del sobre digital y otra para la firma, (**SSL** solo usa un par de claves), actualmente **SET** usa la función hash **SHA-1** , **DES** y **RSA** de 1024 bits, estos parámetros fueron tomados para ser compatible con los certificados existentes, aunque el piloto de **SET**usó el sistema asimétrico de cifrado con curvas elípticas y se piensa que soporte también curvas elípticas en la próxima versión de **SET**.