tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

040

AUTENTICACIÓN Y CIFRADO DE TRÁFICO SMTP ENTRE SERVIDORES DE CORREO DE LAS ADMINISTRACIÓNES

Jesús Sanz de las Heras
Responsable de seguridad en el correo electrónico
RedIRIS/RED.ES

Pedro R. Benito da Rocha
Servicio de Informática
Universidad de Burgos

Jesús Sanz de las Heras
Pedro R. Benito da Rocha

Palabras clave

Cifrado, autenticación, correo electrónico, seguridad, email SSL, confianza

Resumen de su Comunicación

SSL es conocido por ser usado en las transacciones http en las aplicaciones Web para intercambiar información de forma segura, siendo muy utilizado en aplicaciones en las que los datos son muy sensibles, como por ejemplo la banca electrónica, la telemedicina o determinadas transacciones entre los ciudadanos/empresa y la administración electrónica.

Existen otros protocolos llamados TLS que son una extrapolación de SSL y que se utilizan para otras aplicaciones como por ejemplo la del correo electrónico. Actualmente este protocolo es utilizado por los clientes de correo al recoger (POP e IMAP) los mensajes del buzón a través de un canal seguro y cifrado. Actualmente el tráfico entre servidores de correo electrónico (MTAs) es trasportado en texto claro por la Red.

El objetivo de esta iniciativa es utilizar los protocolos SSL/TLS para crear canales seguros en el intercambio de tráfico SMTP entre Estafetas.. Estos canales son trasparentes al usuario y permitirán crear una Red Segura y de Confianza entre servidores de la Administración que además sirviera de embrión para poder ampliarla a empresas, universidades etc creando un entorno seguro extremo a extremo para el correo electrónico. Para el despliegue de esta red se requiere la emisión de certificados de servidor para generar la cadena de confianza entre los servidores de esta red.

Las ventajas que nos ofrecería esta red de confianza son: Confidencialidad, Verificación, Transparencia, Inalterabilidad y ahorro de recursos

Jesús Sanz de las Heras
Pedro R. Benito da Rocha

AUTENTICACIÓN Y CIFRADO DE TRÁFICO SMTP ENTRE SERVIDORES DE CORREO DE LAS ADMINISTRACIÓNES

1. Introducción

El correo electrónico actualmente es una aplicación de uso masivo y completamente indispensable en Internet. Aunque el Web es la aplicación más conocida y utilizada de la Red pero ninguna institución, empresa o usuario podrá decir que es posible tener presencia en la Red sin correo electrónico. El correo electrónico es una aplicación insegura y vulnerable que requiere introducir todas las medidas necesarias para garantizar su uso para nuestros usuarios y en el caso de la Administración de los ciudadanos, más allá de software antivirus y antispam. También es una aplicación extremo a extremo que permite una amplia interconexión mundial a través de intercambio de correo electrónico lo que por otro lado impide cualquier tipo de actuaciones unilaterales sin interrumpir el Servicio. Es por eso que siempre se buscan soluciones transparentes a los usuarios que son los más sensibles y afectados por cualquier tipo de intervención.

Los mensajes de correo electrónico son como una postal – cualquier "cartero" los puede leer. Los antiguos protocolos en los que se sustentan el correo electrónico fueron tan confiados que concibieron la transmisión de todo tipo de datos a través de la red de forma transparente.

Cifrar mensajes de correo electrónico con PGP o S/MIME sería el equivalente electrónico de un sobre cerrado en mundo del correo postal. Los mensajes de correo cifrados por los emisores viajarán seguros por la red hasta llegar a los destinatarios que serán los únicos que podrá acceder al contenido. Sin embargo, estos métodos individuales, si bien, son útiles han venido planteando varios tipos de problemas que han ralentizado su utilización de forma habitual. Un problema es el legal, ya que algunos países niegan a sus ciudadanos el acceso a métodos de cifrado en aras de la lucha contra el crimen. El segundo problema es de aprendizaje por parte del usuario ya estos métodos de cifrado no son transparentes al usuario que requiere conocimientos informáticos e intervención. Un tercer problema que se plantea en una institución o empresa que implante una política de cifrado personal es ¿Qué ocurre si una tercera persona necesita acceder al correo posteriormente? ¿Qué ocurre con las claves utilizadas por una persona de la empresa que deja de trabajar en ella, o con su correspondencia cifrada? Como el cifrado normalmente sólo se utiliza para prevenir que datos sensibles crucen la red al descubierto, un sistema de encriptación que funcione en el servidor y que sea transparente para los usuarios, como SMTP/TLS (Transport Layer Security – Seguridad de la Capa de Transporte) podría se una buena solución. TLS nos permite crear túneles de cifrado entre servidores cuando la información viaja por las líneas de comunicaciones. Hagamos una breve introducción de TLS.

SSL es un protocolo desarrollado por Netscape en 1994. El desarrollo de SSL y su aceptación como estándar para cifrado fue uno de los más importantes hitos en el crecimiento de Internet y del comercio electrónico. Lo mas novedoso y exitoso de SSL es que es completamente transparente al usuario proporcionando cifrado y protección de datos.

SSL es conocido por ser usado en el protocolo HTTP para transferir información de forma segura, siendo muy utilizado en aplicaciones en las que los datos son muy sensibles, como por ejemplo la banca electrónica o el mundo de la telemedicina. Con la versión 3.1 de SSL nació TLS, el cual es aplicable a otros protocolos que no sean HTTP, pudiendo así ampliar su uso a otras aplicaciones entre las que está el correo electrónico (SMTP). El uso de ambas tecnologías aplicadas al correo electrónico se conoce como SMTP/TLS. También existe POP/TLS e IMAP/TLS que permitirán cifrar las trasmisiones POP e IMAP entre el cliente y el servidor de correo.

SMTP/TLS por tanto nos permitirá únicamente cifrar las transacciones electrónicas entre máquinas, es decir, entre servidores de correo electrónico. La información trasmitida entre máquinas sólo es cifrada cuando viaja por la red, se cifra en el servidor emisor y se descifra en el receptor. Es decir los mensajes de correo electrónico cuando están almacenados o procesados por los servidores no están cifrados lo que, entre otras cosas, nos evita los problemas arriba mencionados para los sistema de cifrado personal.

En resumen la tecnología TLS aplicada a los protocolos de correo (SMTP,POP, IMAP) nos permite crear un "túnel seguro" para la transmisión de mensajes desde un servidor seguro a otro protegiendo los mensajes en el tránsito por la Red. Entre MTAs (pasarelas o relays de correo), TLS nos proporciona ventajas básicas como:

- El emisor y receptor se autentican mutuamente, evitando problemas de seguridad tipo DNS spoofing o "man-in-the middle"
- TLS evita que se pueda ver el contenido del mensaje durante su transmisión.
- El contenido de un mensaje de no puede ser modificado en el tránsito

De esta forma el mensaje que crea el usuario puede viajar de forma cifrada, no sólo hasta el MTA, si no entre este y el buzón del destinatario. Este túnel asegura un grado de protección muy alto en su tránsito por una red abierta y por lo tanto expuesta a ataques como es Internet.

A grandes rasgos TLS aplicado a los MTA de correo electrónico es un medio seguro para el envío de mensajes de correo electrónico en un medio inseguro como es Internet, proporcionando privacidad, confidencialidad, inalterabilidad y verificación del servidor de origen de una forma transparente para el usuario.

En la Figura 1. Se muestra un gráfico del mecanismo TLS y el túnel de cifrado.

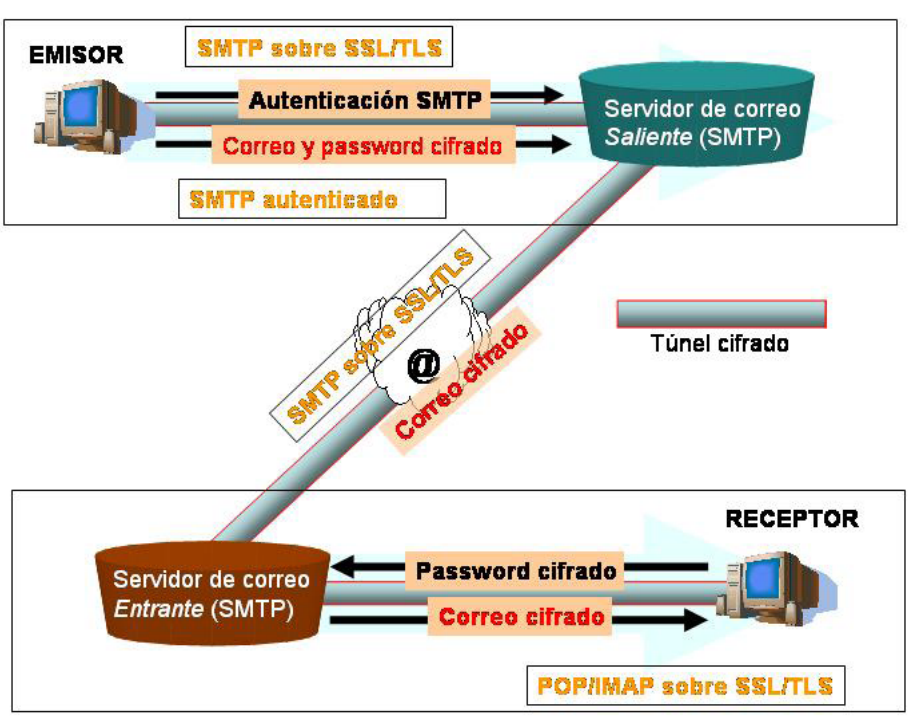

Figura1. Tránsito de información cifrada entre emisor y receptor a través de la Red

2. ¿Cómo funciona?

Una Estafeta cliente (A) desea establecer una sesión SMTP segura con una Estafeta B para el intercambio de correo. Para saber si la Estafeta B soporta STARTTLS enviará la orden EHLO. Si la Estafeta B lo soporta, responderá con un listado de características que soporta. Si el cliente B está de acuerdo responderá con la orden STARTTLS y la negociación está preparada

Ahora llega la parte mas complicada: la estafeta cliente A deberá presentar un certificado SSL. El servidor B comparará la autoridad de certificación del certificado con las autoridades que el reconoce. Si el certificado es aceptado (verify=OK) y se confía en él se iniciará la transacción cifrada. En el caso que la verificación no sea correcta (verify=FAIL" o "verify=NO) y no confíe en el certificado la transacción del mensaje se realizara en texto plano de forma habitual. En la mayor parte de los casos la verificación fallará y la transacción SMTP será en texto claro. Sólo serán cifradas las transacciones con estafetas de la Red Segura.

Implementación

El objetivo de esta implementación es crear un Red segura de Estafetas de correo electrónico. Para ello será necesario crear:

- Protocolo. Configurar los servidores para que dialoguen el protocolo SMTP/TLS.
- Confianza. Las estafetas de esta Red sólo dialogarán de forma segura con otros servidores en los que confían. Es decir sólo confiarán en interlocutores que dispongan de un certificado raíz de confianza

Los servidores que estén preparados con TLS hablarán y negociarán un intercambio seguro sin necesidad de intervención. El servidor que reciba la petición comprobará la raíz del certificado con las que el tiene. Si es correcto y confía en ella se establecerá el canal cifrado para la transacción SMTP de correo electrónico entre ambos servidores.

Debemos aclarar que las estafetas de coreo de esta Red segura llevarán a cabo sus actividades habituales de encaminamiento de correo, pero sólo será con los miembros de la Red Segura con los que se establecerán las transacciones SMP/TLS.

No podrán establecer un intercambio de correo seguro con la Red segura aquellos usuarios cuyo proveedor de correo no dispusiera del certificado raíz de los servidores de la Red Segura de la Administración. Estos proveedores deberán solicitar un certificado para que los usuarios puedan hacerlo. Si no lo solicitan el intercambio de correo es el habitual en texto plano y sin cifrar. Siempre será un valor añadido que los proveedores de Servicio ofrezcan este servicio con lo que de forma colateral se consigue

Por tanto esta Red Segura de la Administración estaría formada por servidores de correo de de las administraciones públicas españolas que desearán participar pudiéndose adherir a la iniciativa otros operadores, instituciones, empresas o universidades. Para la puesta en marcha de esta iniciativa será necesario:

- Disponer de un mapa del estado del correo en las diferentes administraciones.
- Crear configuraciones TLS para los diferentes sistemas existentes
- Definir unos criterios de asignación de certificados
- Crear una infraestructura de PKI o reutilizar las existentes para disponer de certificados para servidores de correo

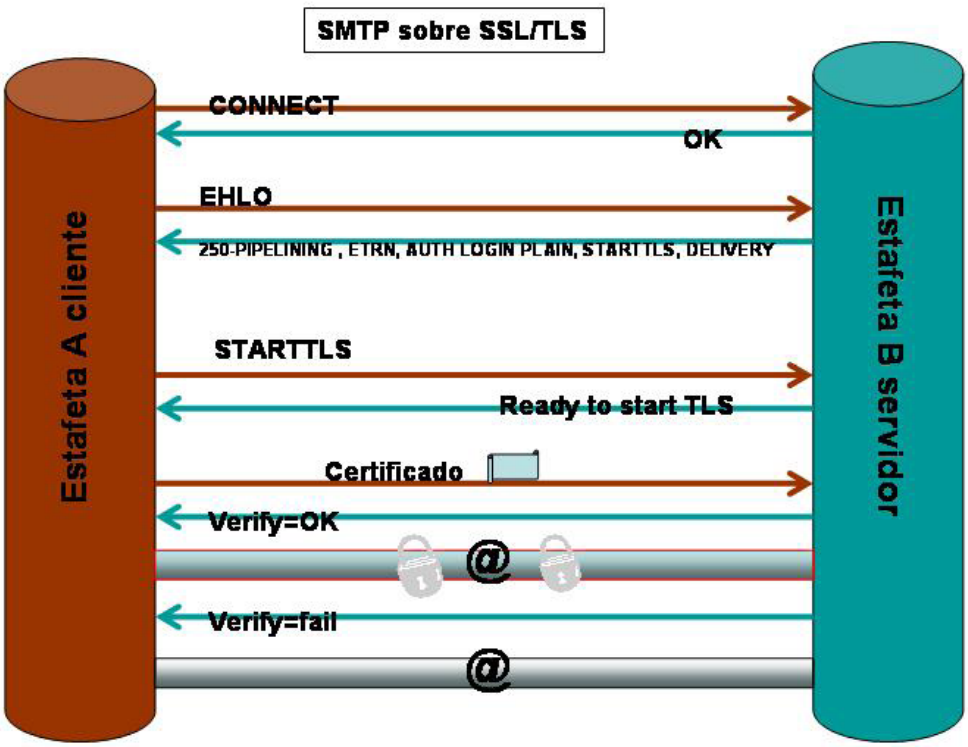

Figura 2. Protocolo para crear canal seguro para el intercambio de tráfico SMTP

El modelo propuesto en este artículo ofrece adicionalmente la ventaja de ser de fácil de mantenimiento tras la configuración inicial del servidor. Los protocolos utilizados son abiertos, estandarizados y los programas informáticos utilizados son estables, abiertos y ampliamente utilizados. No requiere inversión adicional.

Conclusiones

La tecnología TLS aplicada a los protocolos de correo (SMTP,POP, IMAP) nos permite crear un "túnel seguro" para la transmisión de mensajes desde un servidor seguro a otro, protegiendo los mensajes en el tránsito por la Red. Proporcionándonos ventajas tales como:

- Confidencialidad para transmitir información sensible: documentos, contratos, calificaciones, datos personales, contraseñas etc.
- Verificación del origen. Al reconocer al servidor (MTA) origen como seguro se pueden evitar: virus, spam (correo publicitario no deseado), tráfico de servidores mal configurados, etc.
- Transparencia de cara al usuario ya que no deben configurar nada en sus clientes de correo. Completaría la idea que tienen los usuarios del servicio cuando accede a su buzón por medios seguros. El uso combinado de esta red y los criterios RACE redundarían en una seguridad extremo a extremo.
- Inalterabilidad de los mensajes en el tránsito.
- Ahorro de recursos puesto que los mensajes provenientes de la red de confianza no deben pasar por costos filtros antivirus / antispam que ralentizan la entrega de mensajes.

De esta forma el mensaje que envía el usuario puede ser trasmitido por la red de forma cifrada, no sólo hasta el MTA destino si no entre éste y el buzón del destinatario. Este túnel asegura un grado de protección muy alto en su tránsito por una red abierta y por lo tanto expuesta a ataques como es Internet.

El despliegue de este sistema de cifrado en la Administración podría tener diferentes potenciales beneficiarios:

- Creación de una Red Segura de intercambio de correo electrónico entre servidores de las diferentes administraciones del Estado español independientemente del proveedor al que estuvieran conectadas.
- Trabajadores de las administraciones públicas.
- Usuarios que intercambien correo con las diferentes ventanillas de la Administración. El ciudadano no percibirá nada directamente, es un valor añadido de calidad por parte de la Administración y que el ciudadano sabrá apreciar.
- Como efecto colateral fomentará que los servicios de correo electrónico de otros proveedores comerciales y empresas implemente esta tecnología mejorando la seguridad y calidad de Internet.