Proyecto de cifrado de tráfico SMTP entre MTAs RedIRIS

Autor: Jesús Sanz de las Heras (RedIRIS)
Fecha: Enero 2006

Introducción

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

SSL proporciona cifrado para el tráfico Web (http) pero no es muy utilizado para el correo electrónico. La versión SSL v3.1 se creó una buena solución para cifrar tráfico SMTP. Oficialmente se conoce como TLS (Transport Layer Security) que proporciona el mismo sencillo uso de SSL pero para protocolos SMTP usados en el correo electrónico. La combinación de ambas tecnologías se conoce vulgarmente como SSL/TLS.

La tecnología TLS crea 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 (relays de correo) TLS nos proporciona ventajas básicas como:

- Emisor y receptor están se autentican mutuamente, evitando problemas de seguridad tipo DNS spoofing o "man-in-the middle"
- TLS protege el contenido de posibles interceptaciones.
- El contenido de un mensaje de no puede ser modificado en el tránsito

Por tanto un usuario crea un mensaje el cual es enviado en texto plano (también podría ser cifrado) a su servidor de correo, MTA., habilitado como TLS. Este MTA crea un túnel seguro con el servidor remoto para asegurar que el mensaje está protegido en su viaje por una Red abierta como es Internet.

Básicamente TLS nos proporciona: privacidad y confidencialidad (cifrado), verificación del servidor origen e inalterabilidad del mensaje, ventajas suficientes para evaluar su viabilidad.

Justificación

Si este protocolo SSL/TLS nos proporciona tantas ventajas. Si los criterios de seguridad son importantes en los servicios y aplicaciones. Si RedIRIS tiene que intentar desarrollar servicios novedosos y útiles. ¿Porque no utilizarlo en las transacciones SMTP entre MTAs de la Comunidad Académica y crear una **Red segura y de confianza de correo electrónico**? Las ventajas que nos ofrecería esta red de confianza serían:

- **Confidencialidad** para transmitir información sensible: resultados de investigaciones, calificaciones, datos personales, contraseñas etc.
- **Verificación** del MTA origen. Al reconocer al MTA origen como seguro se pueden evitar: virus, spam, servidor mal configurados y poco deseables 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 (RACE). Seguridad extremo a extremo
- **Inalterabilidad** de los mensajes en el tránsito.

Además y no menos importante, la comunidad científica sería pionera y definiría un nuevo entorno en la seguridad y fiabilidad del correo electrónico en Internet que permitiría que otros proveedores o empresas se unieran a la iniciativa (**transferencia tecnológica**) para crear un marco seguro de correo electrónico en Internet. También sería ampliable a otras instituciones académicas Latinoamericanas (RedClara) a través del proyecto HERMES (Hacia un Entorno de Red de Mensajería Electrónica Segura) reflejado en http://hermes.reuna.cl

Nota aclaratoria: Es necesario remarcar que con esta red de confianza y cifrado de tráfico SMTP **no se rechazarán** transacciones SMTP ni mensajes de correo que **no estén en esta red**. El objetivo es confiar en las transacciones seguras entre instituciones de esta red además de disfrutar de las ventajas arriba descritas.

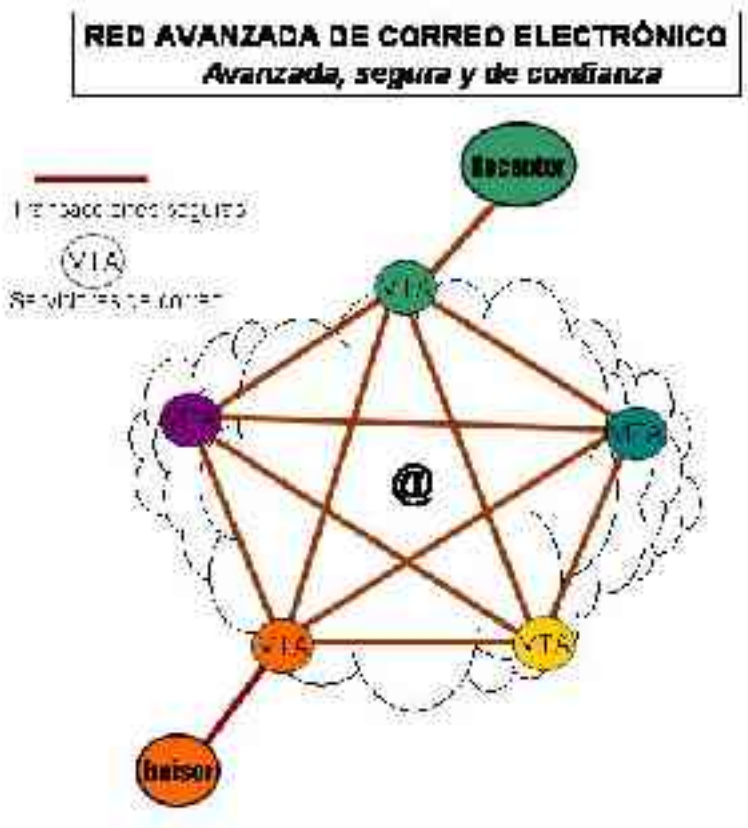

***Figura1**. Modelo propuesto de Red de segura y de confianza de correo en la Comunidad RedIRIS*

Objetivos y desarrollo

El objetivo principal de este proyecto es esplegar una **Red de Confianza y Segura de intercambio de correo electrónico** (figura 1.). Para ello será necesario:

- Documentar requerimientos mínimos y las correspondientes configuraciones e TLS en los diferentes tipos de paquetes del MTA.
- Evaluar qué infraestructura de CA se podrá utilizar para este proyecto entre las PKIs disponibles de RedIRIS:
    - PKI Comunidad RedIRIS http://www.rediris.es/pki/
    - pkIRISGrid CA http://irisgrid.es
- Definir una infraestructura de CA (Autoridad de Certificación) en función de la PKI seleccionada.
- Definir una maqueta de pruebas con las instituciones interesadas.
- Definir una política de funcionamiento de la Red de confianza.

- Evaluar posibles servicios adicionales: whitelist, servicios web etc

Los objetivos de esta iniciativa se complementan con el Servicio operativo de calidad **RACE** (Red Académica de Correo Electrónico http://www.rediris.es/mail/race) cuyo objetivo es crear una infraestructura de calidad y segura dentro del servicio interno de correo electrónico las instituciones. Ambas iniciativas por tanto permitirían el intercambio de correo de forma segura (autenticado/cifrado) entre usuarios de las diferentes instituciones de la comunidad RedIRIS a través de la infraestructura de red de RedIRIS (Figura 2.) en tres pasos:

1. **Emisor de correo**. Zona institucional. Protocolo SMTP y extensiones SSL. El emisor envía el correo al "servidor de correo saliente" autenticándose en el servidor por un canal cifrado.
2. **Transmisión de correo** por la Red. Protocolo SMTP y extensiones SSL. El servidor Saliente inicia una sesión SMTP/TLS con el Servidor Entrante, verificándose y validandose claves y cadena del certificado.
3. **Recepción de correo**. Zona institucional. Protocolo POP/IMAP y extensiones SSL. El receptor se autentica y recibe en su buzón el correo de forma cifrada.

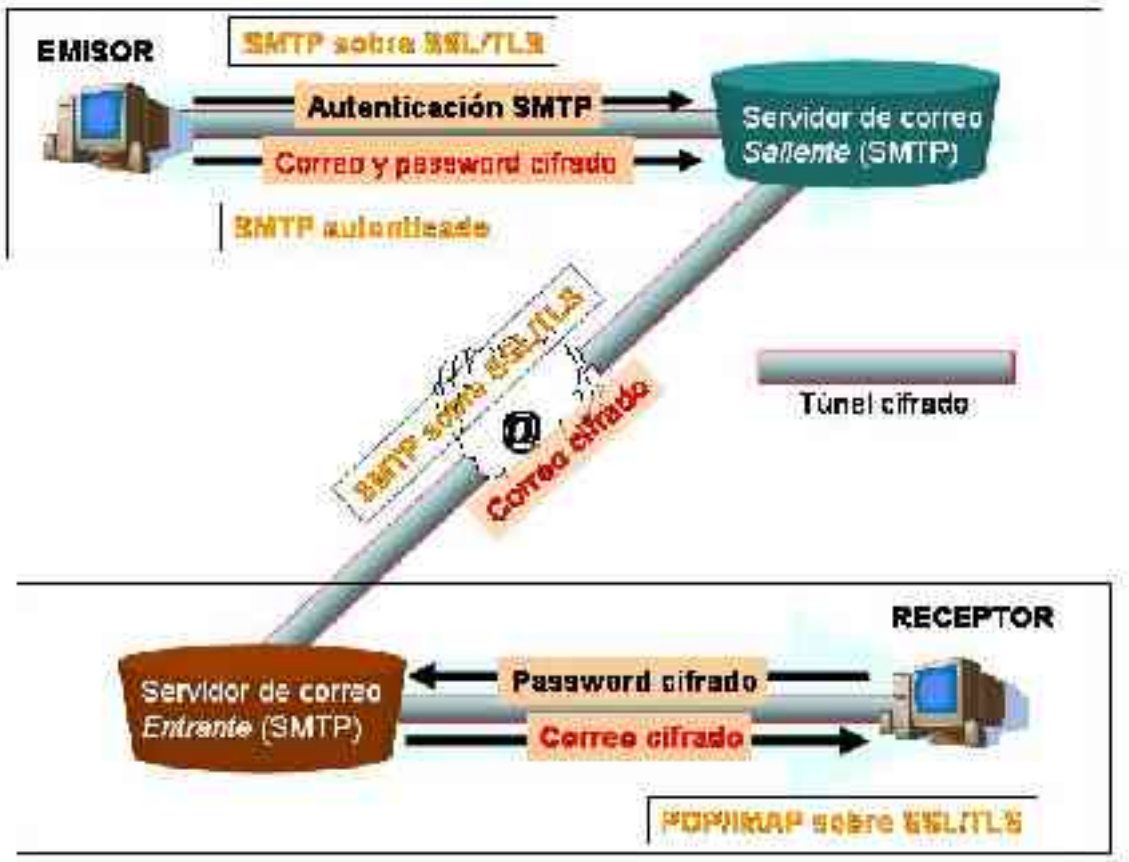

***Figura2**. Tránsito de información cifrada entre emisor y receptor a través de la Red*

El aspecto más importante para el despliegue de esta iniciativa es la creación de una infraestructura que permita la emisión y validación de chequeos de **certificados en la transmisión de correo por la Red** que podrán convivir con los certificados (PKI) propios de cada institución**.** Habrá que evaluar cual de las dos actuales PKI de las que dispone RedIRIS (pkIRISGrid o pkiRedIRIS) se ajustan mas a las necesidades de este Proyecto.

Fase de pruebas:

- Se creará un sistema de gestión de CAs basado en TinyCa para la emisión de certificados firmados.
- Se definirá un protocolo para la emisión de certificados a las instituciones participantes
    - Mecanismos
    - Criterios
- Se evaluará la posibilidad de crear una whitelist accesible vía DNS

Plazos

Recursos