UNIVERSIDAD DEL SALVADOR

PROYECTO DE TESIS

MAESTRIA AUDITORIA EN SISTEMAS

OBJETO DE INVESTIGACION

"Seguridad en el Correo Electrónico"

AÑO 2004

Tutor: Lic. Enzo Taibi

Alumno: Ing. Diego N. Pire

INDICE

Planteo del Problema.

Introducción

Vivimos un avance acelerado en materia de tecnología de la información, la cual a generado cambios en una amplia variedad de aspectos que van desde la vida diaria de las personas hasta la reestructuración y reorganización de empresas y gobiernos. Indudablemente el avance logrado en el área de comunicaciones repercutió en forma directa en la calidad y cantidad de información procesada, llegando a niveles impensables tan solo unas décadas atrás; en esta área **el producto más expandido a sido Internet cuyos usuarios habrían sido 5,6 millones a fines de 2003**, un crecimiento de 36,6% con respecto a diciembre de 2002. El número de clientes (persona física o jurídica que recibe una factura por el acceso) habría crecido a fin del año 2003 a 1,6 millones. Este crecimiento es impulsado principalmente por los servicios de banda ancha (broadband), ya que habría llegado a los 240 mil clientes en diciembre de 2003, un aumento de más del 90%. Sobre estos datos, **el correo electrónico es el servicio más utilizado por los internautas en la Argentina, con el 92,5%**. Le siguen la navegación Web (61,8%), el Chat/ICQ (25,7%) y otros (7%). Los primeros dos servicios son usados en forma creciente a medida que se poseen más años de experiencia en la utilización de Internet. Mientras, el Chat/ICQ, en forma inversa, lo utilizan más los principiantes que los usuarios experimentados.

La expansión de Internet y las comunicaciones en general, los avances de la tecnología informática, principalmente el aumento en la capacidad de procesar información y la facilidad de distribuirla, hacen necesario **reformular los conceptos asociados a la seguridad**.

En la actualidad los medios de comunicación vinculados a Internet son de vital importancia para las empresas, llegando a ser, **el correo electrónico, una herramienta indispensable en cualquier oficina**.

Con el aumento en la utilización del correo electrónico como herramienta de distribución de todo tipo de información, tanto los gerentes de sistemas como los responsables de seguridad, necesariamente tendrán que organizar un nuevo esquema de seguridad que contemple este medio masivo de intercambio de información.

Audiencia y enfoque

El enfoque de este trabajo esta destinado a gerentes de sistemas y a responsables de seguridad informática pero igualmente puede ser utilizado como referencia a fines de obtener nuevos conocimientos sobre los componentes involucrados en un proyecto de seguridad de correo electrónico.

Hipótesis

Objeto de la investigación

La utilización de tecnologías de la información cuyos grandes progresos (principalmente en lo referido a las comunicaciones y al aumento en la capacidad de procesamiento) ayudan a las organizaciones a lograr una mejor eficiencia y desempeño, hacen necesario disponer **de nuevos mecanismos que aseguren la privacidad de la información**; Especialmente cuando utilizamos el correo electrónico como herramienta de intercambio de información, sobre un medio de transporte no seguro y masivamente utilizado como es Internet.

Respuesta al problema

El presente trabajo a sido elaborado con la intención de que sirva de referencia a aquellas personas que estén interesadas o necesiten compartir información en forma segura utilizando el correo electrónico, y deseen conocer los mecanismos disponibles para asegurar la privacidad de la información, para lo cual, en el desarrollo del mismo se han ido analizando desde el punto de vista de seguridad cada uno de los componentes que podrían ser involucrados en el funcionamiento del correo electrónico.

Descripción del Entorno

Hoy en día el paradigma de la Aldea Global ya no es una utopía, ni una formulación teórica; la red mundial es cada día más extensa y la oferta de contenidos mayor. Como es de esperar, existen límites en este nuevo campo de acción; la seguridad y la confidencialidad de los datos que viajan por las autopistas de la información peligran si no tomamos cartas en el asunto, y es el temor ante posibles intrusiones lo que está frenando actividades como el comercio electrónico y otras en las que se debe transmitir información confidencial. Pero... ¿Esta limitación es real?, ¿Existe una barrera tecnológica que impide brindar la seguridad necesaria para ejecutar transacciones de diferentes índoles, utilizando Internet como medio de transporte?... o esta sensación de desprotección es simplemente una cuestión de conocimientos y buenas practicas.

Seguridad en el medio de transporte.

Internet

El problema de seguridad de Internet surge porque fue creada para el libre acceso a la información y regida principalmente por las políticas del buen uso de la red.

ARPANET, la red precursora a Internet, fue un proyecto del departamento de defensa de los EEUU, mas precisamente de United States (US) Defense Advanced Research Proyect Agency (DARPA), el cual intentaba desarrollar un conjunto de protocolos para conectar los recursos de los computadores en forma transparente en varias localizaciones geográficas.

Allá por 1971 cuando Ray Tomlinson, un investigador del departamento de defensa de los EEUU, se envió a si mismo el primer correo electrónico, no podría haber imaginado la magnitud que alcanzarían este tipo de comunicación.

Desde ese momento es que las aplicaciones para enviar y recibir mensajes estuvieron disponibles en los sistemas de ARPANET, sin embargo, ellas solamente podían ser utilizadas para enviar y recibir mensajes en cuentas del sistema local.

Solamente después de que Tomlinson modificara el sistema de mensajería para que los usuarios puedan enviar mensajes a usuarios conectados en otra ARPANET y esta modificación estuvo disponible para otros investigadores; el correo electrónico se convirtió rápidamente en la aplicación de mayor utilización sobre la ARPANET.

Puesto que la ARPANET fue inicialmente concebida para una pequeña y estable comunidad de investigadores, tubo pocas necesidades relacionadas con la seguridad por los que los primeros estándares e implementaciones colocaron poco énfasis sobre este tema.

Y siendo que la ARPANET evolucionó en Internet, el correo electrónico continuó siendo la aplicación mas ampliamente utilizada tanto para uso personal como laboral, pero este crecimiento no estuvo acompañado por el desarrollo de un esquema de seguridad y hoy en día, no podemos darnos el lujo de esperar a que se modifiquen la bases de Internet para disponer de un medio de transporte seguro, aunque ya existan proyectos para hacerlo realidad.

Conceptos básicos del correo electrónico

Previamente a que una persona pueda comprender los conceptos de la seguridad aplicados al correo electrónico debe comprender completamente los elementos básicos que componen el sistema de mensajería electrónica, como es que los mensajes son compuestos, almacenados y enviados. Para mucha gente una vez que el mensaje fue redactado y enviado, este deja su sistema para aparecer mágicamente en la casilla del destinatario; esto podría ser así, aunque la realidad nos indica que el manejo y envío de mensajes puede ser bastante más complejo.

Para comprender como funciona este proceso, es mejor analizar cada una de las partes involucradas. La mayoría de los clientes de correo electrónico requiere que el usuario ingrese, al menos, los siguientes datos: Titulo del mensaje, cuerpo del mensaje y receptor/es. Cuando estos campos son completados y el usuario envía el mensaje, este es transformado en un formato estándar especificado por la RFC 822.

En el contexto de la RFC 822, los mensajes son vistos como cabecera (envoltura) y cuerpo (contenido). En la envoltura se encuentran los datos referentes a la transmisión, recepción y envío del contenido del mensaje. El estándar descrito en la RFC 822 se aplica solamente al contenido, sin embargo el estándar del contenido descrito incluye una serie de campos cabeceras que pueden ser utilizados por el sistema de correo para crear el sobre o envoltura.

Una vez que el mensaje es traducido en el formato definido por la RFC 822, este puede ser transmitido. Usando las conexiones

de red, el cliente de red conocido como “Mail User Agent” (MUA) se conecta al servidor de correo “Mail Transport Agent” (MTA). Luego de inicializada la comunicación, el cliente de correo provee al servidor la identificación del emisor, y usando los comandos del servidor le informa los destinatarios del mensaje. Aunque el mensaje contiene una lista con los receptores, el servidor de correo no examina el mensaje para obtener esta información. Solamente después de completar la lista de receptores se completa el mensaje. A partir de este momento, la entrega del mensaje queda bajo el control del servidor de correo.

Una vez que el servidor de correo esta procesando el mensaje, varios eventos ocurren: identificación del servidor receptor, establecimiento de otra conexión, y transmisión del mensaje. Utilizando el Domain Name Services (DNS), el servidor determina el servidor de los receptores, y establece las conexiones con los servidores receptores y envía el mensaje utilizando el mismo mecanismo que el cliente utilizó inicialmente. En este momento puede ocurrir lo siguiente: si el servidor se encuentra en el mismo sitio que la casilla de correo destino el mensaje es enviado utilizando el “Local Delivery Agent” (LDA) también conocido como “Mail Delivery Agent” (MDA), en este caso todo el procesamiento y entrega del mensaje se encuentra en la misma unidad lógica, el MDA concentra su tarea en el envío de mensajes a usuarios locales; en caso contrario, el proceso de entrega del mensaje se repite de un MTA a otro hasta localizar el servidor que contiene la casilla destino, en cuyo caso actuará el MDA.

Cuando el MDA tiene el control del mensaje, dependiendo de la configuración del mismo puede darse alguna de las siguientes

situaciones: el MDA puede enviar el mensaje o procesarlo utilizando un filtro predefinido antes de enviarlo. Luego que el mensaje es enviado, es colocado en la casilla de correo del receptor donde es almacenado hasta que el receptor ejecute alguna acción sobre este (leerlo, borrarlo, etc.) utilizando su MUA.

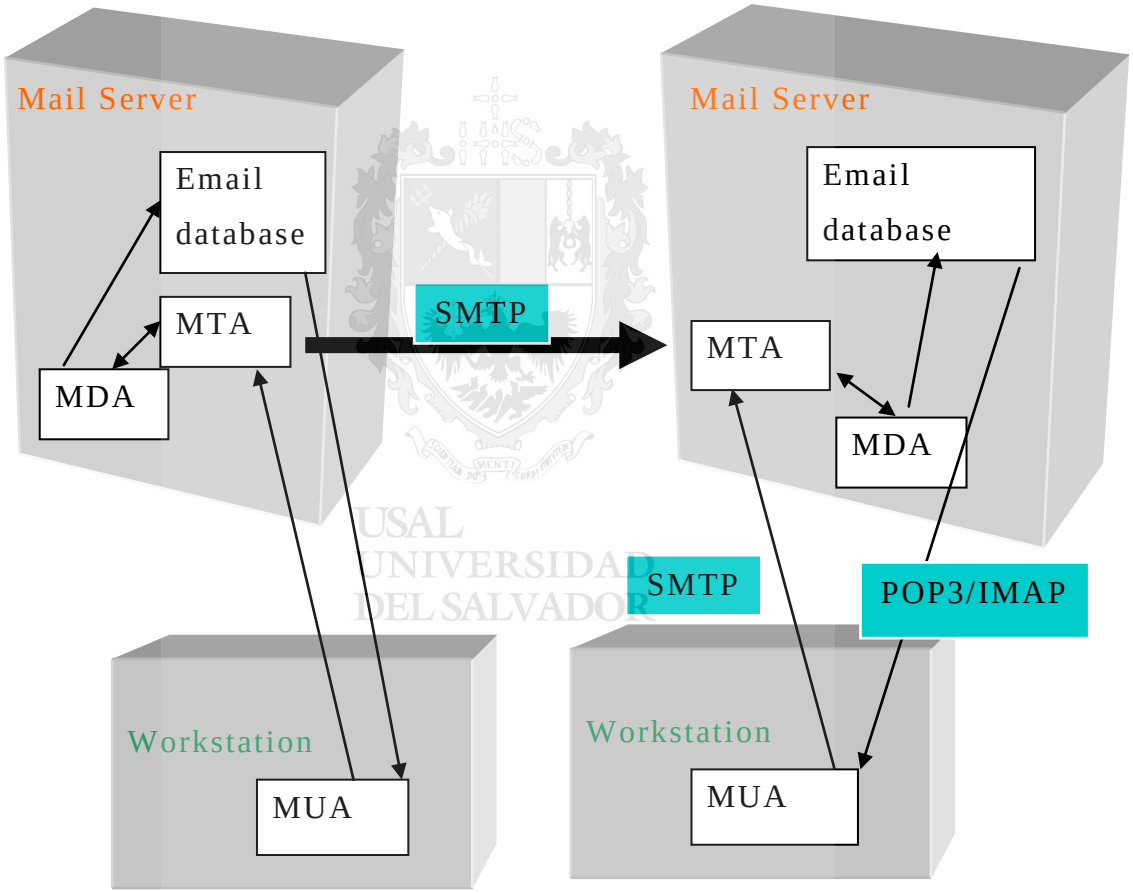

Figura 1 - Esquema del servicio de Correo Básico.

Estándares del Transporte de Correo

Para asegurar la compatibilidad e interoperabilidad entre varias aplicaciones de correo, fueron establecidos los estándares del transporte de correo (Mail Transport Standards). En el escenario mas simple, un mensaje es enviado de un usuario local a otro usuario local, para este caso actúa solamente el MDA, quien es responsable de entregar el mensaje al destinatario. Cuando el mensaje es enviado a un usuario que no se encuentra en el servidor local, un MTA es requerido para enviar el mensaje desde el servidor local al servidor remoto. Dependiendo del sistema involucrado, diferentes MTA pueden ser utilizados, que podrán utilizar diferentes protocolos de transferencia.

El protocolo de transferencia más común es el Simple Mail Transfer Protocol (SMTP), el cual es un estándar de facto en Internet para enviar mensajes de correo. Así cualquier sistema de mensajería en Internet debe soportar el SMTP para facilitar la comunicación con otras aplicaciones de correo.

Simple Mail Transfer Protocol (SMTP)

En agosto de 1982, Jon Postel de la universidad del sur de California desarrolló el SMTP que es un protocolo básico de transferencia de correo, como lo establece la RFC 821 “SMTP fue desarrollado para asegurar una más confiable y eficiente manera de transportar mensajes”. SMTP es el lenguaje mínimo

que define el protocolo de comunicación para entregar mensajes de correo.

Cuando un usuario envía un correo, el cliente o MUA contacta al servidor SMTP y establece una comunicación usando el lenguaje SMTP. El MUA es generalmente parte de la aplicación cliente de correo (Oultlook, Eudora, etc.). Si el MUA no se encuentra disponible, el mensaje de correo puede ser enviado utilizando un cliente telnet.

Limitaciones del esquema SMTP/822

1. SMTP no puede transmitir archivos ejecutables u otro tipo de objetos binarios. Si bien existe un gran número de esquemas que convierten en archivos binarios en texto que pueda ser utilizado por SMTP, incluso el popular Uuencode/Uudecode utilizado en Unix, ninguno de estos esquemas se ha convertido en un estándar.

2. SMTP no puede transmitir texto que incluya caracteres que son representados por códigos de 8 bits con valores superiores al 128 decimal, además SMTP esta limitado al ASCII de 7 bits.

3. Los servidores SMTP pueden rechazar los mensajes superiores a cierto largo.

4. Los gateways SMTP que se comunican a redes que utilizan X.400, no pueden manejar los caracteres especiales que son incluidos en los mensajes X.400

5. Algunas implementaciones SMTP no adhieren completamente al estándar SMTP definido en la RFC 821. Esto genera los siguientes problemas:

   - ✓ Borrado, Agregado y cambios de posición de los caracteres de retorno de carro y fin de línea
   - ✓ Truncado de líneas mayores a 76 caracteres
   - ✓ Borrado de caracteres de espacios en blanco y tabulaciones
   - ✓ Relleno en líneas del mensaje para que sean del mismo largo
   - ✓ Conversión de caracteres de tabulación en múltiples espacios en blanco.

Extended Simple Mail Transfer Protocol (ESMTP)

Cuando el número de usuarios de correo electrónico creció, fueron necesarias nuevas funcionalidades en los clientes y en los servidores SMTP. En 1993, la RFC 1425 introduce el concepto de extensiones al servicio SMTP; ésta luego es reemplazada por la RFC 1651 y 1869. Estas RFC agregaron tres piezas al esquema SMTP:

- Nuevos comandos SMTP (RFC 1425)

- Registro de las nuevas extensiones al servicio SMTP (RFC 1651)
- Parámetros adicionales para los comandos SMTP MAIL FROM y RDPT TO (RFC 1689)

Para ser compatible con los anteriores servidores SMTP fue necesario un método para que el cliente pueda determinar si el servidor al cual se estaba conectando soportaba las nuevas extensiones. Esto fue logrado a través del comando "enhanced hello" (EHLO). Cuando el cliente se conecta al servidor, este envía un comando EHLO, si el servidor soporta las extensiones SMTP, este dará una respuesta satisfactoria y una lista de extensiones soportadas, en cambio si el servidor no soporta las nuevas extensiones enviará una respuesta de falla advirtiendo al MUA que envíe el comando estándar HELLO.
Los servidores que soportan las extensiones SMTP son conocidos como SMTP Extendido o Extended SMTP (ESMTP).