TITULO

Servidor de claves públicas PGP, Cliente Administrador y Cliente para ciframiento y desciframiento de Correo Electrónico.

AUTORES

F. Fabián Redrován Castillo[1], Luis M. Ruiz Ampuero[2], Carmen K. Vaca Ruiz[3], Ricardo E. Yánez Godoy[4] y Guido Alfredo Caicedo Rossi[5].

[1] Ingeniero en Computación ,1998.
[2] Ingeniero en Computación ,1998.
[3] Ingeniero en Computación ,1998.
[4] Ingeniero en Computación ,1998.
[5] Director de Tópico, Ingeniero Eléctrico en Computación, Escuela Superior Politécnica del Litoral, 1985, Máster en Ciencias en Computación en State University of New York at Buffalo, EEUU.

RESUMEN

Basándose en el paradigma Cliente-Servidor bajo la arquitectura TCP/IP, se implementaran tres aplicaciones. Cada aplicación tiene un nombre que refleja su propósito: el Cliente Administrador, el Cliente de Correo Electrónico y finalmente el servidor PGP. Este último ofrece varios servicios, sobresaliendo por su importancia, el proporcionar a quien lo necesite, la clave pública de encriptación PGP (Pretty Good Privacy) de una persona determinada. Para que esto sea posible, dicha persona debió haber generado previamente su par de claves asimétricas utilizando su propia aplicación PGP, y proporcionar la pública al administrador del servicio para que la almacene en el servidor PGP.

El administrador del servicio almacena las claves públicas en el servidor PGP utilizando la aplicación Cliente Administrador, que además del ingreso de claves públicas permite consultar, modificar y eliminar claves e información del propietario (nombre y número de teléfono).

El Cliente de Correo Electrónico, que se usa con un navegador de Internet (Netscape, Internet Explorer u otro), permite enviar mensajes encriptados utilizando la clave pública del destinatario, clave que la aplicación obtiene automáticamente del servidor PGP. Además este cliente es capaz de leer correo electrónico encriptado con PGP, se podrá desencriptarlo proporcionando previamente la clave privada y frase de paso del usuario, requisitos necesarios para poder realizar la desencriptación del mensaje.

INTRODUCCION

Hoy en día, debido al uso frecuente de las facilidades que brinda la Internet, se hace necesario, en ciertos casos, enviar un mensaje que solamente pueda leer el destinatario, aún si cae en manos de otra persona. Para lograr esto, se puede "encriptarlo" o "cifrarlo", es decir, hacerlo ilegible para cualquiera que no sea el destinatario original del mensaje. Esto se consigue usando una clave criptográfica (clave pública) la cual puede ser conocida por cualquier usuario que la requiera. Luego el destinatario usa la llave gemela (clave privada), que solo él conoce, para descifrarlo. El uso de este tipo de ciframiento se conoce como paradigma de llaves asimétricas (clave pública y clave privada). PGP (Pretty Good Privacy) es una de las aplicaciones más difundidas que hace uso de dicho paradigma.

Siendo el correo electrónico una de las aplicaciones más utilizadas en la Internet, resulta de gran utilidad una herramienta que ofrezca mayor privacidad a los mensajes que transporta.

Lo que se hace en este proyecto es incrementar la seguridad a través del uso del ciframiento de los mensajes antes de su envío por la red. Entonces es necesario una aplicación que además de enviar mensajes los encripte previamente y los desencripte a su llegada.

Pero como se dijo anteriormente, se necesita de un par de claves para que esto resulte. Entonces: ¿Cómo consigo la clave de ciframiento de la persona a la que le deseo enviar el mensaje? Podría pedírsela, situación algo molesta y trabajosa si deseamos enviar mensajes a varias personas. Pero, ¿qué tal si puedo obtener todas las claves que necesito de una sola fuente? Es decir, dejando que sea el propio dueño de la clave quien busque la manera de ponerla a disposición de todo el que la requiera. Aquí es donde entra el servidor de claves públicas PGP.

El servidor PGP contendrá las claves públicas. Cada vez que un usuario necesite alguna de estas claves para encriptar un mensaje, la aplicación de correo puede accesar al servidor PGP y solicitarla.

Consecuentemente, es necesario que toda la información que maneja el servidor PGP esté bajo el control de alguna persona encargada. De aquí la importancia de una aplicación administradora: el Cliente Administrador, encargado de consultar, modificar ingresar y eliminar información del servidor PGP.

CONTENIDO

El proyecto consta de los siguientes elementos:

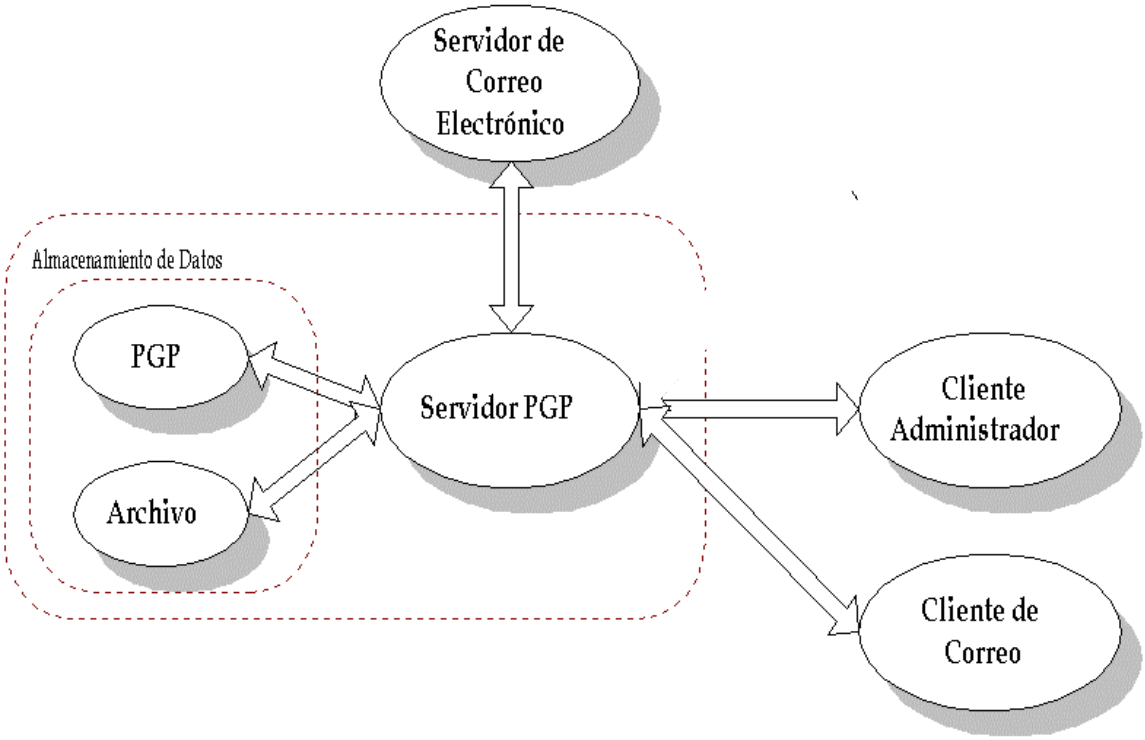

Figura 1.Servidor PGP, programas Clientes y servidor de correo

- Un servidor PGP que se comunica con las aplicaciones Clientes, además de manejar un archivo de información. Aparte de esto, también es usado como "puente" entre el cliente de correo electrónico y los servidores de correo electrónico POPMAIL3 y SMTP[1] que son los encargados de recibir y enviar correo respectivamente.
- Un cliente administrador para el manejo de la información del servidor PGP. Esto incluye consultar, modificar, ingresar y eliminar claves.
- Un cliente de correo electrónico que envía y recibe mensajes utilizando encriptación con PGP.

Aplicación Servidora

El servidor PGP se implementó con un lenguaje de programación orientado a objetos (JAVA versión 1.0), por lo que puede ser utilizado en cualquier sistema operativo que permita ejecutarlo (Windows95/NT™, MAC™ o UNIX™). Así mismo, es necesario que una versión del programa PGP esté instalado en la misma máquina en la que se corre el servidor PGP.

El servidor PGP se encarga de guardar las claves públicas (basándose en un identificador único, en este caso la dirección de correo electrónico), usando para ello la propia aplicación PGP quien posee una forma eficiente de almacenamiento de claves. El servidor PGP maneja la comunicación entre él y la aplicación PGP basándose en comandos. Por otro lado

[1] POPMAIL3: Protocolo utilizado para recibir correo. SMTP (Simple Mail Transfer Protocol): Protocolo utilizado para enviar correo.

el servidor PGP necesita también manejar la información del propietario de la clave (nombre y teléfono) de manera paralela y esto lo realiza mediante el empleo de un archivo de texto.

Entonces, el servidor PGP es capaz de añadir nuevas claves, y, de consultar, modificar y eliminar claves existentes.

Adición de claves públicas

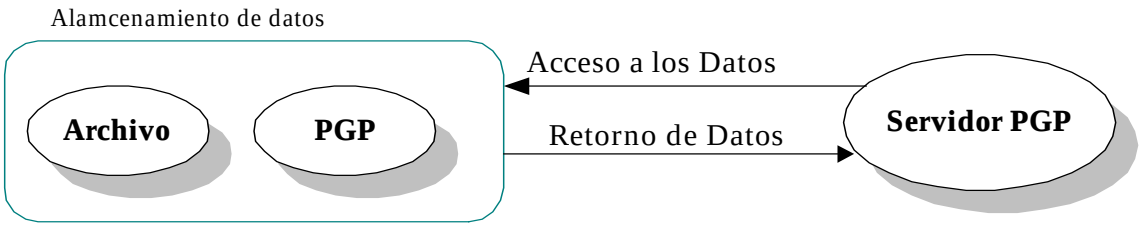

Figura 2. Servidor PGP y almacenamiento de datos

Para añadir una clave, el servidor PGP necesitará toda la información que conlleva esto: El identificador[2], la clave, el nombre del dueño y su teléfono.

Previo a la adición se asegura que la clave sea válida (que tenga formato PGP), que pertenezca al identificador especificado y que no esté duplicada en el servidor PGP.

Una vez que se autorizó el procedimiento, se añade la nueva clave al archivo de claves públicas y el resto de la información en el archivo de datos. Estos dos se asocian con el identificador de la clave.

Consulta de claves públicas

Para consultar una clave, el servidor PGP necesita el identificador de la misma.

Previo a obtener la información de los dos archivos, se verifica que los datos del propietario existan.

Una vez que se autorizó el procedimiento, entrega al cliente los datos necesarios. Si el requerimiento fue hacer una búsqueda, entonces entrega el nombre y la dirección electrónica del propietario de la clave. Si, hace una consulta completa, entonces entrega todos los datos concernientes al propietario.

[2] El identificador de la clave es la dirección de correo electrónico del propietario.

Modificación de claves públicas

Al igual que en la adición, para modificar una clave, el servidor PGP necesitará toda la información que conlleva esto: El identificador, la clave, el nombre del dueño y su teléfono.

Previo a la modificación se asegura que la clave tenga formato PGP, que pertenezca al identificador especificado y que no esté duplicada en el servidor PGP.

Una vez que se autorizó el procedimiento, elimina la clave existente junto con la información del propietario y, añade la nueva clave al archivo de claves públicas y el resto de información en el archivo de datos. Estos dos se asocian con el identificador de la clave.

Eliminación de claves públicas

Para eliminar una clave, el servidor PGP necesita el identificador de la misma.

El servidor PGP sabe que se debió hacer una consulta previa a cualquier intento de eliminar información y, por lo tanto, procede a eliminar la clave deseada y los datos del propietario asociados a la misma.

Aparte de todas estas propiedades el servidor PGP funciona como un "puente" entre el cliente de correo electrónico y el servidor de correo electrónico. Esto permite que el cliente se conecte con cualquier servidor de correo electrónico en el cual tenga una cuenta y, no necesariamente con el de la misma máquina (esta restricción la impone las propiedades de seguridad de JAVA).

Adicionalmente, cada vez que se levante el servidor PGP se crea una copia del archivo de información del propietario y PGP hace lo mismo con el archivo de claves públicas, pero cada vez que éste cambie.

Toda comunicación del servidor PGP hacia la aplicación PGP se hace de manera directa, pero para que PGP se "comunique" con el servidor PGP, se utiliza un archivo. Este archivo recoge la salida del proceso PGP y es analizada por el servidor PGP para luego realizar una acción.

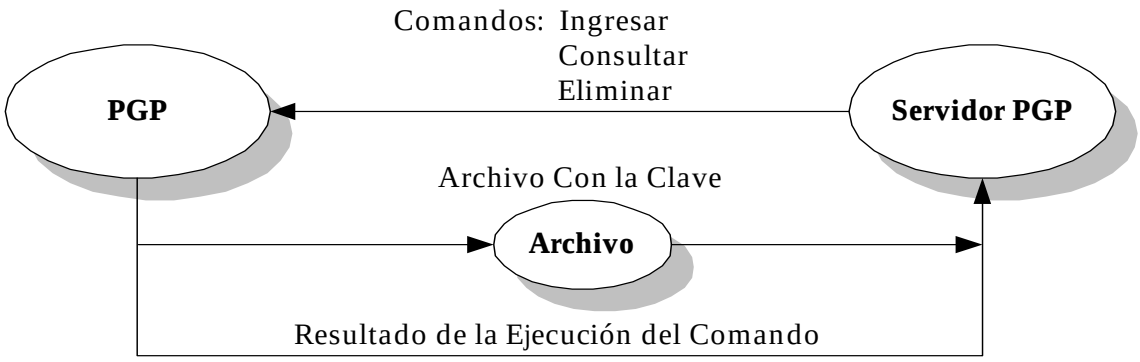

Figura 3. Servidor PGP y aplicación PGP

Aplicación Cliente de Correo Electrónico

Envío de correo

Para que el cliente pueda enviar correo se necesita especificar el nombre del remitente, su dirección de correo electrónico y el servidor de correo SMTP que usará para enviar.

Enviar un mensaje implica solicitarle al servidor PGP que sirva como enlace con el servidor de correo SMTP.

Junto con el mensaje a enviarse debe ir la dirección de correo electrónico del destinatario y el título. Ahora bien, el usuario tal vez quiera enviarlo sin encriptarlo, para lo cual debe darle el permiso respectivo, o se negará el envío de todo mensaje.

Si elige encriptar el mensaje, la aplicación buscará en el servidor PGP la clave pública del destinatario o destinatarios y para cada uno de ellos encriptará el mensaje. Si se trata de *n* destinatarios, y, cada uno de estos posee su propia clave pública, se tendrá *n* mensajes encriptados que hay que enviar. Y, como se dijo antes, sin el permiso correspondiente, los destinatarios que no posean clave no recibirán el mensaje.

En esta parte del cliente de correo electrónico se puede realizar una búsqueda de cualquier clave si desea conocer quienes constan en el servidor PGP.

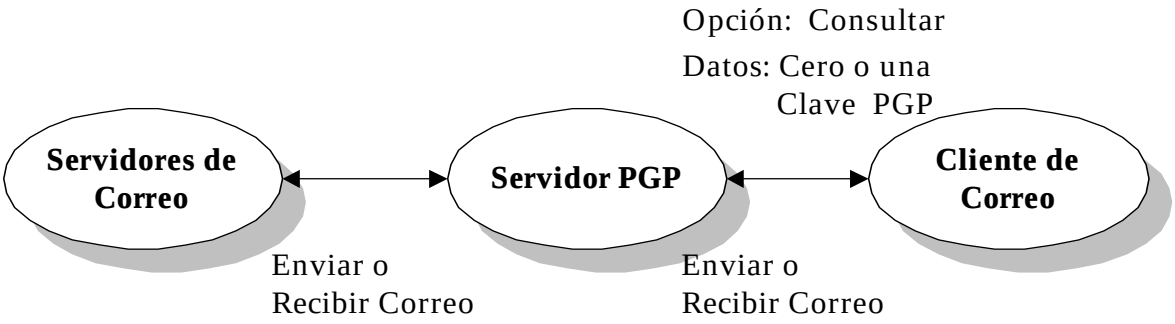

Figura 4. Cliente de Correo y servidor PGP.

Recepción de correo

Para que se pueda recibir correo se necesita especificar el "user", "password" y el servidor de correo POPMAIL3 donde posee una cuenta.

Obtener los mensajes implica solicitar al servidor PGP que sirva como enlace con el servidor de correo.

Una vez recibidos todos los mensajes del servidor PGP, puede elegir cualquiera para leer, e incluso el cliente puede detectar si uno de ellos está encriptado con PGP. De ser así se puede optar por desencriptarlo, pero para esto se necesita que el dueño del mensaje tenga a la mano su clave secreta también llamada privada[3] y que recuerde su frase de paso (todo esto es validado).

Adicionalmente, se puede contestar (reply) los mensajes leídos o reenviarlos (forward), pero solamente si el mensaje es de texto normal, es decir, si está encriptado se debe desencriptarlo previamente.

Aplicación Cliente Administrador

En primer lugar hay que indicar que solamente una aplicación administrador a la vez puede accesar al servidor PGP, es decir, solamente existe un administrador, y, por lo tanto solo hay un usuario y una contraseña.

Como ya se dijo, el servidor PGP tiene el control sobre las claves públicas y sobre la información del propietario, pero es el cliente administrador quien le proporciona los requerimientos para adición, consulta, modificación y eliminación de claves y demás datos.

[3] Hay que recordar que PGP utiliza una clave pública para encriptación y una clave privada para desencriptación.

Adición de claves públicas

Lo primero que el cliente envía al servidor PGP es el identificador de la clave que va a añadir, y éste le responderá si puede ingresarla o no. Cuando acepta el requerimiento, lo siguiente que se le pide al usuario administrador es ingresar el nombre del propietario, el teléfono y clave pública, esta última sujeta a verificación de falla o duplicación.

La adición de las claves se la hace una a una previa verificación.

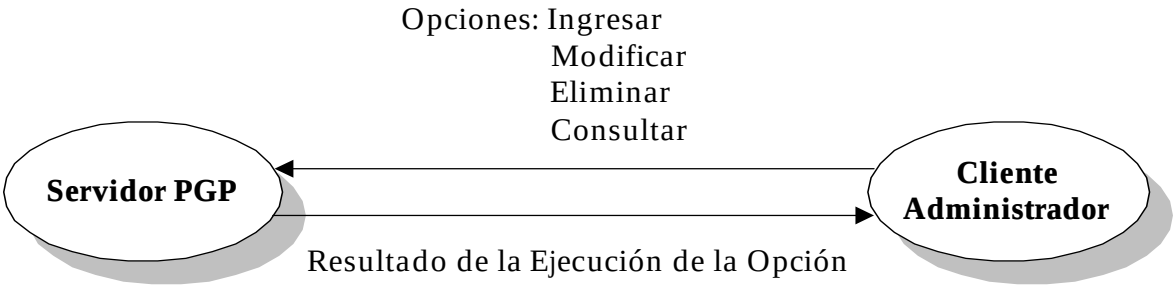

Figura 5. Comunicación Cliente Administrador con el Servidor PGP

Consulta de claves públicas

Al igual que en el anterior, lo primero que se envía al servidor PGP es el identificador de la clave o un patrón de la misma (también puede ser un patrón del nombre del propietario). En caso de ser un patrón que dé como resultado varias ocurrencias, éstas aparecen listadas por nombre del propietario de la clave y su identificador[4], con lo que se puede elegir uno para ver más detalles como el teléfono y la clave. Esto es importante si tomamos en cuenta que a partir de la consulta, y solo así, se puede modificar información o eliminarla.

Así, ya sea en el caso de que se envíe el identificador de la clave de manera exacta o de que se halla elegido alguno de los de una lista de ocurrencias, lo siguiente que se muestra al usuario administrador es toda la información de la clave. Desde esta información se puede modificar cualquier campo (incluso la misma clave por otra) o eliminarla por completo.

Modificación de claves públicas

Posterior a una consulta, se puede modificar la información recibida en todos sus campos excepto el identificador (si quisiera hacer algo así, previamente tendría que eliminarlo todo).

Cuando se modifica el campo de la clave, previo a actualizar todos los campos, el servidor PGP revisa la validez de la clave y si no está duplicada.

[4] Cabe recordar que el identificador de la clave es la dirección de correo electrónico del dueño de la clave.

Eliminación de claves públicas

De la misma manera, una vez consultada toda la información, esta puede ser eliminada con una simple confirmación de parte del usuario.

Para esto lo único que el cliente envía al servidor es el identificador de la clave que deseo eliminar.

CONCLUSIONES

Java es una herramienta de programación orientada a objetos muy poderosa debido a su gran flexibilidad, transportabilidad y facilidad, junto a la aplicación PGP, tan ampliamente difundida para diversas plataformas y de fácil manejo, constituyeron las mejores herramientas para el tipo de proyecto.

Con la utilización del paradigma de par de claves asimétricas se ha logrado cumplir uno de los principales objetivos planteados: Suplir la deficiencia de seguridad en el transporte de correo a través de la Internet, recayendo dicha seguridad en la responsabilidad con que los propietarios manejen sus claves.

La comunicación entre servidores y clientes es posible gracias a la arquitectura de comunicación TCP/IP, que ha alcanzado una envidiable popularidad gracias a su eficiencia puesta a prueba día a día en la Internet.

REFERENCIAS

1. Douglas E. Comer, Redes globales de información con Internet y TCP/IP: Principios básicos, Protocolos y Arquitectura. (3ra. Edición, México: Prentice-Hall Hispanoamericana S.A., 1996).
2. Douglas E. Comer y David L. Stevens, editores Internetworking with TCP/IP, Volumen III: Client-Server Programming and Applications, Windows Socket Version. (New Jersey: Prentice-Hall, 1997).
3. Weber, Using JAVA 1.1 (3ra. Edición, QUE Corporation, Indianápolis, 1997).
4. Internet, http://www.pgp.com
5. Internet, http://www.Inter_PGP-Home.html