ANEXO G
IMPLEMENTACION DE UN SERVICIO DE MENSAJERÍA INSTANTÁNEA SEGURO

1. DEFINICIÓN DEL PROBLEMA

Finalmente, dentro de las necesidades de comunicación y trabajo en red identificadas en el grupo objetivo, se consideró la inclusión de mecanismos de comunicación que permitieran la interacción en tiempo real entre los miembros de la Red de Investigación Educativa, y para ello, se optó por la implementación de un Servicio de Mensajería Instantánea.

Este servicio facilitaría el intercambio de experiencias en condiciones bajo las cuales la presencialidad no fuese viable, ni tan importante como para que la interacción no pudiese darse de otra forma.

Aunque el desarrollo del programa de Doctorado en Ciencias de la Educación de RUDECOLOMBIA, requiere para su realización de una constante movilización de sus estudiantes a distintos destinos nacionales, al parecer el contacto que mantienen la mayoría de ellos entre estos intervalos de tiempo, es en realidad poco. Con frecuencia se ha presentado esta situación como algo preocupante para la formación de habilidades investigativas, y el fortalecimiento de vínculos académicos a través de la construcción de relaciones con compañeros, profesores y tutores.

Dados los enormes costos que acarrearía una interacción frecuente a través de un medio como el teléfono, las comunicaciones mediadas por computador han surgido como una alternativa viable para cualquier organización cuyos miembros estén interesados en mantenerse en contacto. Dentro de éstas, la mensajería instantánea se ha destacado por su capacidad para facilitar la comunicación entre las personas, a través del intercambio de mensajes de texto, apoyados en elementos gráficos para la definición de contextos (emoticones), que son de gran utilidad a la hora de darle sentido a palabras que a menudo pueden resultar ambiguas.

Con el fin de estrechar las comunicaciones y las relaciones académicas de los miembros de la Red de Investigación Educativa, a través de medios que permitieran una interacción menos impersonal y que proporcionaran un nivel de percepción mayor sobre el interlocutor, se pensó en que la implementación de un servicio de Mensajería Instantánea, siguiendo la mayoría de las recomendaciones hechas en esta clase de aproximaciones, y entre las cuales sobresale la

importancia de desarrollar procesos de acompañamiento y acercamiento tecnológico, podría contribuir a la generación de sinergia y al aumento de la calidad de las comunicaciones existentes entre los miembros de ieRed.

Con el servicio de mensajería instantánea, se podría, además de permitir que las personas intercambien experiencias mientras conversan, plantear sesiones para la discusión de temas con invitados especiales, tomar decisiones en torno a situaciones sencillas que no requieran complicadas deliberaciones, informar acerca de las novedades del doctorado (ya no a través de un mensaje sino mediante conversación directa con estudiantes, profesores o tutores), y finalmente, contar con un punto de encuentro al alcance de todos, en el cual darse cita para comentar las experiencias tenidas alrededor del desarrollo del programa de Doctorado en Ciencias de la Educación.

Al igual que con los servicios de Correo Electrónico y Disco Virtual, se consideró vital proporcionar un servicio de Mensajería Intantánea que tuviese en cuenta un conjunto mínimo de directrices de seguridad, para garantizar la confidencialidad e integridad de las conversaciones que soportase.

Con esto en mente, para el caso de la Mensajería Intantánea, se consideraron los siguientes aspectos en materia de seguridad:

- Identificación y Autenticación de los usuarios, para permitir el acceso al servicio de mensajería instantánea únicamente a aquellas personas que figuraran como usuarios válidos.

- Cifrado de las conexiones entre el cliente y el servidor para evitar que la información de identificación y autenticación que intercambiaran, se transmitiera de forma insegura, es decir, sin el soporte de una capa de transporte que evitara la interceptación, alteración o interrupción de la comunicación y su contenido.

- Cifrado del contenido de las conversaciones intercambiadas entre los clientes a través del Servidor de Mensajería Instantánea.

Así, se dio inicio a una exploración de alternativas tecnológicas que pudieran suplir los requesitos de seguridad expuesto, y permitieran la configuración de un servicio lo más completo, funcional y usable posible.

2. CONCEPTOS BÁSICOS

2.1 El Servicio de Mensajería Instantánea

La Mensajería Instantánea es un servicio que permite la comunicación a través de mensajes instantáneos de texto (en primera instancia), entre dos o más personas a través de una red como Internet. Se dice que los mensajes de texto son instantáneos, porque a diferencia del correo electrónico, se transmiten en tiempo real, refiriéndonos con ello, al tipo de comunicaciones que se dan en ambos sentidos de forma concurrente, entre un par de interlocutores que actúan tanto como emisores como receptores de la información de comunicación.

Al igual que la gran parte de las aplicaciones telemáticas conocidas, su funcionamiento se basa en una arquitectura Cliente/Servidor, donde los clientes usualmente son programas que deben ser instalados dependiendo del protocolo del servicio de mensajería al cual desee conectarse.

Se puede considerar a la mensajería instantánea como una evolución de los antiguos servicios de conversación en Internet, aún vigentes como el IRC (*Internet Relay Chat*, Sala de Conversación Moderada en Internet) y las salas convencionales de chat, en donde, mediente el uso de un programa cliente, un usuario puede conectarse a un servidor y proporcionar información sobre su estado de conexión (disponible, ausente, ocupado, etc.).

Los servicios de mensajería instantánea públicos más populares son AOL Instant Messenger, Yahoo Messenger, .NET Messenger Service e ICQ.

2.2 Protocolos de Mensajería Intantánea

Dentro de la iniciativas más importantes que han existido para la normalización y estandarización del servicio de mensajería instantánea, figuran: los protocolos SIP (*Session Initiation Protocol*, Protocolo de Inicio de Sesión) y SIMPLE (*SIP for Instant Messaging and Presence Leverage*, SIP para la Mensajería Instantánea y la notificación presencial) de la IETF, APEX (*Application Exchange*), PRIM (*Presence and Instant Messaging Protocol*, Protocolo de Presencia y Mensajería Instantánea), y XMPP (*Extensible Messaging and Presence Protocol*, Protocolo de Mensajería Extensible y Presencia) que se encuentra basado en XML y es mejor conocido como Jabber.

La mayoría de los intentos de crar un estándar unificado para la mayoría de los proveedores del servicio de mensajería intantánera (AOL, Yahoo y Microsoft), han fracasado, y cada uno continúa utilizando su propio protocolo propietario.

Algunas aplicaciones cliente de mensajería instantánea, intentan combinar varios de los protocolos bajo un solo cliente unificado. A estos clientes se les denomina "multiprotocolo", y algunos de los más conocidos son: Trillian y Gaim, entre otros. Ante este problema, el protocolo Jabber intenta una aproximación distinta, delegando la labor de comunicarse a otros servicios de mensajería, a los servidores, para lo cual hace uso de un conjunto de "transportes".

Dentro de los protocolos de Mensajería Instantánea más utilizados, figuran: Gadu-Gadu, Gale, OSCAR (AIM e ICQ), Jabber, Lotus Sametime, .NET Messenger Service, SIMPLE, TOC protocol (AIM), Yahoo! Messenger y Zephyr Notification Service.

En cuanto a los clientes, los más comunes son: AOL Instant Messenger, Fire, Gadu-Gadu, Gaim, ICQ, MSN Messenger, Trillian y Yahoo! Messenger.

2.3 El Protocolo Jabber[1]

Como se pueden encontrar en la documenatción oficial[2], Jabber es un conjunto de protocolos XML de flujos de descarga (streaming) y tecnologías que permite que dos entidades en Internet intercambien mensajes, presencia, y otra información estructurada en tiempos cercanos al real. Jabber Se encuentra soportado en miles de servidores de Internet y es usado por más de 6 millones de personas en todo el mundo. Aunque se encuentra mucho menos difundido que muchos sistemas propietarios. Las siguientes son algunas de sus ventajas[3]:

- Es un protocolo abierto: Cualquiera puede implementar un servidor o un cliente y actualmente existen muchos disponibles.

- No está centralizado: Cualquiera puede correr un servidor Jabber en su dominio, y si así lo desea interoperará perfectamente con los contactos situados en servidores ajenos.

- Es extensible: Se le pueden añadir extensiones de todo tipo que funcionarán sobre el protocolo original, gracias a lo cual no se limitan a la Mensajería Instantánea. Las extensiones comunes son manejadas por la Jabber Software Foundation.

- Es seguro: Cualquier servidor Jabber puede ser aislado del exterior. El servidor de referencia soporta SSL para comunicaciones Cliente/Servidor y varios clientes soportan la extensión GPG para firmar la presencia y encriptar las

1 Para mayor información: http://www.jabber.org

2 http://www.jabber.org/about/overview.php

3 http://es.wikipedia.org/wiki/Jabber

comunicaciones punto a punto, usando cifrado asimétrico. En la actualidad, se está desarrollando una implementación de seguridad más robusta usando claves de sesión y SASL.

- Puede interoperar con otras redes: Los transportes, que corren en los servidores, permiten que los usuarios puedan acceder a sus contactos de otros sistemas de Mensajería Instantánea a través de Jabber. Es posible suscribir transportes situados en servidores distintos al servidor donde se encuentra la cuenta desde la cual se suscriben. Existen transportes para MSN, ICQ, AOL y Yahoo, entre otros.

3. ALTERNATIVAS DE SOLUCIÓN CONSIDERADAS Y JUSTIFICACIÓN DE LAS SOLUCIÓN ESCOGIDA

A diferencia de los demás servicios implementados, la escogencia del Servidor de Mensajería Intantánea tuvo en realidad pocos candidatos, porque en su mayoría, tanto los protocolos como sus implementaciones eran propietarias, cerradas, y especialmente, costosas. Las dos excepciones importantes fueron Jabber y SIMPLE, pero existía una comunidad de usuarios más sólida y un proyecto de desarrollo más maduro para el primero, por lo cual la alternativa seleccionada fue Jabber. Por otro lado, lo que se tenía en mente era la implementacion segura de un Servicio de Mensajería Instantánea, y Jabber seguía ofreciendo la alternativa más segura y robusta, al lado de sus contrapartes propietarias.

En cuanto a los clientes, existe un gran abanico de programas que soportan el protocolo Jabber[4], pero se examinaron de cerca, las opciones más usables y recomendadas para los Sistemas Operativos Microsoft Windows.

De todo el abanico de clientes disponible tanto bajo licencias gratuitas, como libres y comerciales, se preseleccionaron tres: Exodus, PSI y Neos. Con este par de candidatos, se realizaron un conjunto de pruebas heurísticas de usabilidad, para determinar con cuál se iba a trabajar del lado de los clientes, y en donde se probó la facilidad que se tenía para establecer el estado de conexión, agregar nuevos usuarios a la lista de contactos, configurar una conexión si el computador se encontraba detrás de una pasarela proxy, y otros aspectos relativos a la funcionalidad y el diseño gráfico, y se optó por Neos 1.0.79, que es un cliente multiprotocolo gratuito, más no libre, con soporte para transferencia de archivos, voz y video, y que posee una interfaz gráfica limpia y agradable.

4 http://www.jabber.org/software/clients.php

4. IMPLEMENTACIÓN DE LA SOLUCIÓN

Para implementar el servicio de Mensjería Instantánea se instaló el paquete disponible para la versión estable de Debian, que sugería dos paquetes más. Específicamente, los paquetes fueron: jabber 1.4.2a-12 (daemonio de Jabber), jabber-jud 0.4-7 (paquete para el soporte de los directorios de usuarios jabber), y jabber-muc 0.5.2-6 (Multi User Chat module, Módulo para Salas de Conversación Multiusuario).

El soporte SSL necesario para asegurar que las conexiones al servidor se hicieran bajo una capa de transporte, que garantizara no sólo un proceso de autenticación seguro, sino que todo la conversación estuviese cifrada, se obtenía con OpenSSL. Éste ya había sido implementado debido a los requerimientos que el servidor Web y el servidor de Correo, tenían en materia de seguridad.

Se configuró el demonio para que sólo soportara conexiones seguras (que por defecto escucha en el puerto 5223), y se procedió a probar con clientes de mensajería Neos desde equipos corriendo Windows 2000 y XP Professional.

Sólo una persona con cuenta en el sistema podría acceder, de tal forma que se unifico la autenticación del servicio de mensajería instantánea con la del sistema para las cuentas de correo y disco virtual.

En el trabajo de aproximación y aprendizaje tecnológico en torno a los servicios implementados para la Red de Investigación Educativa, se explicó como descargar, instalar y configurar el cliente de mensajería Neos, y se realizaron las pruebas del servicio (conversaciones individuales y en grupo, creación de salas de conversación, etc.) con este cliente, aunque cualquier cliente de mensajería para jabber funcionaría bien. Se hicieron pruebas con Exouds, PSI y GAIM y los resultados fueron muy satisfactorios.

5. RECOMENDACIONES Y TRABAJO FUTURO

Se recomienda el estudio de escenarios específicos de aplicación del servicio de Mensajería Instantánea de forma tal que se aprovechen plenamente las ventajas de las conversaciones a distancia, en situaciones en las que la presencia física no sea una alternativa, por motivos de costos o de tiempo.

Se debe propender por la difusión de servicios basados en estándares abiertos tales como Jabber, de forma tal que los usuarios no se vean obligados a utilizar varios servicios incompatibles entre sí, sólo porque a las compañías que los administran no les interesa ni la interoperabilidad ni prescindir de prácticas monopolísticas que les aseguren ciertas ventajas sobre sus competidores.