Seguridad de la Mensajería Instantánea: desafíos de IPoIM

María Eugenia Corti, Ariel Sabiguero Yawelak
Instituto de Computación - Facultad de Ingeniería
Universidad de la República
Montevideo, Uruguay
{mcorti,asabigue}@{ieee.org,fing.edu.uy}

***Abstract*— La mensajería instantánea es un área de pujante crecimiento en el mundo de las comunicaciones personales. Su utilización se basa más en su practicidad que en su seguridad. Durante el año 2005 en el Instituto de Computación se desarrolló un prototipo de una aplicación, IPoIM, que permite la transmisión de datos codificados como mensajes de texto. Dicho desarrollo evidencia una vulnerabilidad latente de la Mensajería Instantánea que puede ser explotada.**

El presente trabajo introduce el estado del arte en herramientas de gestión de Mensajería Instantánea y los problemas que presenta a las mismas el IPoIM. El foco esta puesto en el impacto en la seguridad empresarial, si bien las vulnerabilidades y problemas discutidos son genéricos para todos los tipos de usuarios del servicio.

Palabras clave: Mensajería instantánea, seguridad, IPoIM

I. Introducción

La mensajería instantánea (Instant Messaging - IM) ha tenido una adopción rápida y masiva durante los últimos años. Inicialmente fue utilizada en los hogares para la comunicación con familiares y amigos, posteriormente adoptada a nivel empresarial. Existen varios problemas de seguridad asociados a la mensajería instantánea y una amplia variedad de herramientas que intentan mitigarlos. Algunos de estos problemas están asociados a la posiblidad que brinda IM de transferir archivos, lo que facilita la propagación de virus o worms. Bloquear la opción de transferencia de archivos y que sólo mensajes de texto puedan ser transmitidos es uno de los controles que muchas organizaciones deciden implementar. De esta forma se restringe la utilización de IM a la transmisión de ”sólo texto”, lo que para muchos no resulta un riesgo de seguridad.

La visión gerencial del fenómeno IM está asociada a la productividad, y no a la seguridad. La concepción general es que el intercambio de mensajes es neutro desde el punto de vista de la seguridad, y que su impacto está fundamentalmente en aspectos de productividad de los usuarios. Las soluciones de mensajería corporativas buscan restringir los contactos a contactos laborales, a tratar de evitar distracciones, spam y recientemente IM-phishing. De todas formas, solamente una fracción de las organizaciones que utilizan IM lo controlan. Los usuarios domésticos básicamente no realizan controles, si bien no son el foco del presente trabajo.

El proyecto de grado ”IPoIM: Internet Protocol over Instant Messaging- [1] del Instituto de Computación de la Facultad de Ingeniería, Universidad de la República, implementó un prototipo que permite establecer un túnel entre clientes de mensajería intantánea. Esta conexión permite el transporte completo de cualquier protocolo IP utilizando ”sólo texto”. Dicho prototipo no sólo habilita la transferencia de archivos en lugares donde está prohibido, sino también el acceso directo a cualquier servicio de la red.

El presente trabajo realiza una breve presentación del estado del arte de los controles de seguridad en IM, introduce los resultados fundamentales del proyecto de grado IPoIM y analiza su impacto en la seguridad de IM. El artículo está organizado de la siguiente manera. La Sección II introduce aspectos y soluciones relevantes de seguridad de IM empresariales. En la Sección III se presentan los resultados fundamentales de IPoIM y se hace una breve descripción de las tecnologías utilizadas. El análisis desde el punto de vista del impacto de IPoIM en la seguridad se realiza en la Sección IV. El artículo concluye en la Sección V.

II. Mensajería Instantánea en la empresa

La mensajería instantánea se ha convertido en una de las herramientas informáticas de comunicación más utilizadas. Esto se debe posiblemente a que resulta en la práctica, menos intrusiva que el teléfono y se obtiene una respuesta más inmediata que en el correo electrónico. Proporciona una manera rápida de comunicarse con clientes, compañeros de trabajo y socios, lo que puede resultar ventajoso en un ambiente de negocios donde segundos pueden hacer la diferencia. Brinda además información presencial de los contactos, indicando si los mismos se encuentran conectados o no y si están disponibles para establecer una conversación. Una descripción de la arquitectura general de servicios de IM se presenta en la Sección III-A.

Es un hecho el uso de la mensajería instantánea en las organizaciones. Una encuesta realizada por Osterman Research [2] señala que más del 50 % de las organizaciones utilizan aplicaciones de mensajería instantánea y otro 9 % tiene en sus planes su utilización. La misma encuesta muestra además un crecimiento en el uso de IM a nivel empresarial.

II-A. Riesgos de seguridad asociados

El incremento en el uso de IM en las organizaciones no necesariamente significa que el uso de las mismas esté respal-

dado por una decisión corporativa. La mensajería instantánea fue utilizada en sus inicios en los hogares y fue llevada luego a las organizaciones [3]. Los propios empleados fueron quienes instalaron las herramientas y comenzaron a utilizarlas para comunicarse con sus compañeros de trabajo, clientes y familia. Posiblemente haya contribuído el hecho de que las mismas son de fácil acceso, gratuitas y simples de instalar [4]. Esta situación provocó que la instalación se haya realizado, en la mayoría de los casos, sin la supervisión y el consentimiento del personal informático. Una encuesta de Osterman Research [5] señala que sólo en el 40 % de las organizaciones que utilizan IM, la misma esta soportada por el personal de informática. Esta situación es agravada por el fuerte incremento de incidentes de seguridad asociados a la mensajería instantánea. Reportes realizados por IMlogic Threat Center [6] muestran un incremento del 32 % en las amenazas asociadas a IM, durante los cuatrimestres del año 2005. El tipo de amenazas es múltiple: virus, ejecución de programas que resultan atractivos y pretender realizar determinadas acciones cuando en realidad tienen una finalidad oculta (troyanos/gusanos), engañar al usuario para obtener información confidencial (IM-phishing), código malicioso en general (malware) o IM-spam entre otros. A continuación resumimos las principales vulnerabilidades de la mensajería instantánea.

Tráfico inseguro. Aunque actualmente la mayoría de los protocolos de IM soportan encriptación, aún existen servicios donde el tráfico viaja en texto plano. Esto permite que el tráfico interceptado pueda ser leído facilmente. Aún en los casos dónde el tráfico sea encriptado, el mismo es interceptado en el servidor del proveedor del servicio, lo que no garantiza la confidencialidad e integridad de la información transmitida. Significa un riesgo para las organizaciones en las que se utiliza IM para envío de información sensible.

AAA - Authorization, Authentication and Accounting. La utilización de servicios públicos relega en el proveedor del servicio estas tareas tan importantes. Implicitamente, esta confiando a éste información organizacional. Más aun, traspasa la confianza de la autenticación de la contraparte. La autenticación del contacto se realiza en el servidor del proveedor del servicio IM. La misma se realiza utilizando nombre de usuario y contraseña, y ambos datos se almacenan en el servidor del proveedor. La seguridad de esta información depende de un tercero. En caso de falla en la autenticación o el robo de los datos asociados a la misma, cualquiera podría simular ser alguien que no es. Por otro lado no existe ninguna exigencia en el formato de la contraseña, lo que deja a los usuarios vulnerables si utilizan contraseñas débiles.

Los clientes son más que IM. Las herramientas más populares permiten además de la transferencia de mensajes de texto, la transferencia de archivos, espacio de trabajo compartido, telefonía IP, entre otros. Esto permite que información clasificada pueda ser extraída de la organización sin autorización. Este ataque podría ser intencional, realizado por algún empleado o podría ser llevado a cabo por ejemplo por un trojano que se ejecutara en la máquina del empleado. En este último caso el usuario no se enteraría de que la información está siendo transmitida. De la misma manera la opción de transferencia de archivos permite la propagación de trojanos o worms a través de IM.

Desactualización de las herramientas de seguridad. Los antivirus corporativos a nivel de servidor no tienen en cuenta el tráfico de IM para la inspección de virus. A nivel de productos de escritorio muchos ya han comenzado a intalar plug-ins para examinar los archivos provenientes del tráfico de IM.

Vulnerabilidades propias. Como muchas otras herramientas de software, las aplicaciones de mensajería instantánea tienen sus propias vulerabilidades. Las mismas pueden ser explotadas por usuarios mal intencionados, dejando expuestas a las organizaciones que la utilizan.

Algunos de los riesgos asociadas a estas amenazas pueden ser reducidos utilizando herramientas comerciales o libres. Varias de estas soluciones se describen en la siguente Sección.

II-B. Soluciones implementadas

Durante el primer trimestre de 2005 el 71.2 % de las organizaciones no bloqueó el tráfico de IM de forma alguna [7]. El complemento de las organizaciones, preocupadas por la amenaza a la seguridad de la información que representa el uso de IM, implementan controles que logran mitigar algunos riesgo. Algunos de estos controles se detallan a continuación:

Filtros en los firewalls

Prevenir el uso de IM filtrando el tráfico TCP en los puertos que utilizan los distintos protocolos de mensajería instantánea no es efectivo. Los clientes IM pueden utilizar los puertos utilizados comunmente para tráfico HTTP y FTP. Los clientes se configuran automáticamente para acceder por estos puertos comunes, en caso de que detecten que los puertos utilizados por defecto han sido bloquedos. Firewalls con capacidad para analizar protocolos pueden filtrar el tráfico IM, ya que los protocolos usados por IM se diferencian del protocolo HTTP. Sin embargo, recientes versiones de clientes IM embeben el tráfico en el protocolo HTTP, salteando a los analizadores de tráfico. Existe la opción de bloquear en los firewalls las direcciones de los servidores de IM. Lamentablemente, existen en Internet muchos servidores proxy, que en forma gratuita, redirigen el tráfico a los servidores correspondientes. Esto obligaría a tener que bloquear las direcciones de estos servidores, y mantener actualizados estos filtros, lo que se convirtie en una tarea administrativa costosa.

Políticas corporativas

Utilizar políticas a nivel corporativo, que definan claramente cuales son los objetivos del uso de IM en la organización, que es lo permitido y denegado y cuales son las sanciones en caso de no cumplimiento de las mismas, es otra medida que se puede tomar para mitigar el riesgo. De todas formas, se debe poder controlar si las políticas establecidas están siendo cumplidas, para lo que se necesitan herramientas para monitorear las acciones.

IM Corporativo

Utilizar soluciones corporativas de IM como Sun ONE Instant Messaging [8], IBM Lotus Instant Messaging [9], Microsoft Office Live Communications Server [10] y Jabber [11] (una versión de software libre), que permiten a las organizaciones tener sus propios servidores de IM preveniendo de esta forma que los datos sean interceptados. Mantienen el tráfico de mensajería instantánea de la organización dentro de la misma. Ofrecen además autenticación, autorización, encriptación y registro. Algunos tienen integradas herramientas para el control de spam y análisis de virus en el contenido de los mensajes y los archivos transferidos.

IM Gateway

Adquisición y uso de IM Gateways, que ofrecen acceso controlado a mensajería instantanea de tipo empresarial y pública. Funcionan como proxys monitoreando la comunicación. Permiten examinar el tráfico, reforzando las políticas de seguridad establecidas. Pueden por ejemplo, determinar qué usuarios tienen permitido el acceso a las aplicaciones de IM, qué clientes de IM están permitidos y si pueden realizar transferencia de archivos o no. Un ejemplo de este tipo de aplicación es el IMlogic IM Manager [12] de Symantec.

En la Sección IV veremos como afecta IPoIM a las prácticas de seguridad actuales.

III. IPoIM: Internet Protocol over Instant Messaging

Durante el año 2005 se llevó a cabo en el Instituto de Computación, Facultad de Ingeniería, Universidad de la República el proyecto de grado denominado *"IPoIM: Internet Protocol over Instant Messaging"* [1]. El mismo tuvo como objetivo implementar un prototipo que permitiese validar la idea ingenua que la IM puede ser utilizada para transportar un protocolo de comunicaciones como IP. Las siguientes Secciones introducen los conceptos y principales resultados aportados por el proyecto de grado.

Escapan al alcance del presente trabajo servicios adicionales como transferencia de archivos o VoIP, generalmente asociados a IM (ya existentes y fácilmente interceptados en firewalls). Estos servicios son empaquetados en las aplicaciones de IM, pero utilizan protocolos independientes. Generalmente sus conexiones de datos son independientes de las utilizadas para IM y se establecen directamente entre los usuarios. El presente trabajo se concentra en la utilización de los propios mensajes de texto para el encapsulado y transmisión de información.

III-A. Mensajeria instantánea

En la presente Sección describiremos la arquitectura general de los servicios de IM. El marco de referencia general de IM está dado por los RFC 2778 y 2779 [13], [14]. La mayoría de los servicios de IM se basan en protocolos no estándar y no interoperables de diferentes prestadores de servicio. Más alla de este hecho, los servicios existentes sobre Internet comparten varias características. La primera de ellas es que se basan en la utilización de servidores, tanto para mantener la información de presencia, como para el envio de mensajes. Debido a requerimientos de carga, los servidores se organizan en grupos o *farms*, y entre ellos comparten y distribuyen la tarea. La Figura 1 muestra conceptualmente dos clientes A y B conectados a través de un servicio brindado sobre internet.

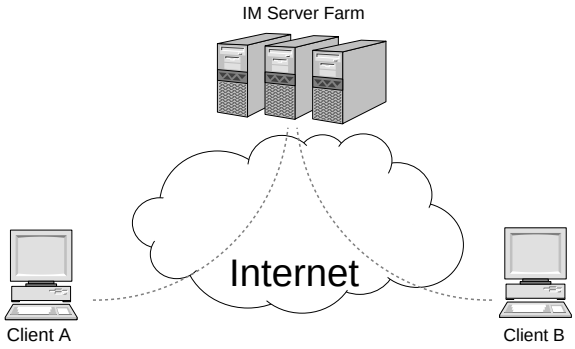

Fig. 1. Arquitectura general de los servicios de IM

Ambos clientes establecen sus respectivas conexiones TCP con servidores en direcciones conocidas que reenvian los mensajes entre los clientes.

III-B. Cliente IPoIM

IPoIM es construido componiendo un túnel con un cliente de IM. La herramienta utilizada para el armado del túnel es OpenVPN [15], y el cliente de IM es Gaim [16]. El túnel, OpenVPN, es utilizado para realizar tareas de networking a nivel de interfaz con el sistema operativo, configuración del dispositivo de red virtual y ruteo. El cliente de IM reemplaza la comunicación standard provista por OpenVPN. Gaim sustituye el mecanismo de comunciación basado en UDP provisto por OpenVPN en base a la transmision del datagrama como mensaje instantáneo.

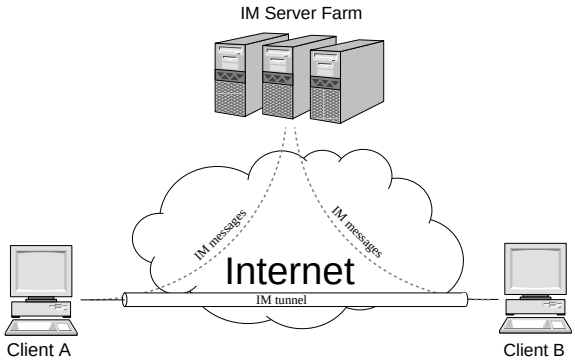

Fig. 2. Arquitectura conceptual de IPoIM

La Figura 2 ilustra conceptualmente el túnel que se establece entre los clientes, si bien el tráfico intercambiado entre los mismos utiliza la mensajería instantánea para su transporte. Una funcionalidad adicional provista por OpenVPN es la capacidad de comprimir y encriptar el tráfico. OpenVPN utiliza SSL/TLS [17] como mecanismo de encriptación. Es

consecuencia directa que IPoIM provea un canal de comunicación seguro entre ambos clientes, independiente de las características de seguridad propias del protocolo de IM y la organización subyacente.

III-C. Algunos resultados experimentales

El prototipo fue desarrollado para plataformas POSIX y win32. El mismo fue compilado y ejecutado en OpenSuSE Linux, asi como en sistemas windows. Se realizaron diversos tests para probar tanto la interoperabilidad de la solución como la validez de su implementación. Las mismas siguieron las recomendaciones provistas por el RFC 2398: *Some Testing Tools for TCP Implementors* [18]. Se seleccionaron los tests basados en las herramientas NetPerf [19], TcpTrace [20] y TTcp [21]. Los mismos permiteron realizar pruebas relevantes en las plataformas destino. Se realizaron pruebas sobre Internet utilizando el servicio de mensajería MSN [22], [23] y pruebas en una LAN utilizando Jabber (XMPP) [24]–[26].

El prototipo se desempeñó correctamente a lo largo de la totalidad de las pruebas realizadas, permitiéndonos confiar en la validez de la implementación. Cabe notar que a lo largo de los tests ejecutados, los valores numéricos hallados fueron consistentes. El ancho de banda estimado utilizando el servicio MSN a través de Internet es de 22Kbps, similar al de un modem telefónico analógico. Otro resultado obtenido es el que se extrae de la medición del *round-trip-time* (RTT) de los mensajes ICMP `echo-request / echo-reply` enviados a través del túnel. El valor medio de RTT observado es de $5{,}5 \times 10^2 ms$. Dichas mediciones fueron consistentes a diferentes horas del día y a lo largo de diferentes días. El jitter observado siempre fue bajo en condiciones de no saturación del canal.

Los resultados presentados son preliminares. Una investigación en curso busca profundizar el conocimiento de las capacidades de IPoIM.

IV. Consecuencias de IPoIM sobre la seguridad en IM

La implementación del prototipo IPoIM evidencia una vulnerabilidad latente en la mensajería instantánea. A continuación se presentan los principales problemas de seguridad asociados al uso de IPoIM y posibles soluciones a implementar para disminuir el riesgo asociado.

IV-A. Principales problemas

La utilización de un cliente de VPN da otro alcance a IPoIM. Al crear nuevos recursos de red en el host en el que se ejecuta, permite que tanto tráfico propio, como de la red a la que está conectado sea transmitido por el túnel. La Figura 3 ilustra la conexión de hosts de la red donde se ejecuta el cliente con el host (o la red) remota a través del túnel.

Utilizando IPoIM cualquier empleado de una organización podría dejar accesible los servicios de red de la organización a cualquier persona ajena a la misma o incluso usarla para beneficio propio. La conexión podría establecerse desde cualquier lugar, sin que los administradores de TI lo notaran. Un usuario

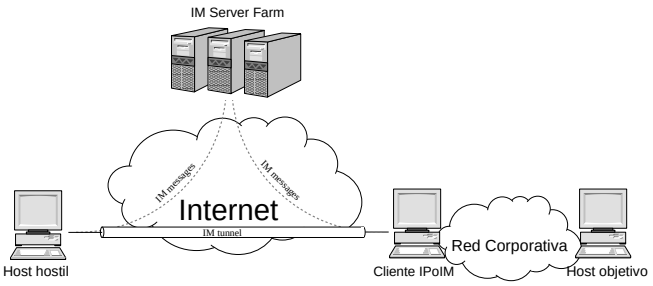

Fig. 3. Alcance y escala del impacto de la vulnerabilidad.

podría establecer una conexión a su casa y acceder desde allí a todos los servicios de red de la organización, el acceso a estos servicios sólamente estará limitado por los controles que proveean los distintos servicios. Sería potencialmente posible, y con escasa complejidad técnica realizar NAT/PAT desde dicho host para evitar problemas de ruteo y poder comunicar las diferentes redes. Otro escenario válido podría ser la utilización de protocolos de ruteo como RIP u OSPF sin un buen nivel de seguridad. En este caso se podría avisar la nueva tabla de rutas a todos los equipos de la organización, y utilizando métricas adecuadas, se podría redirigir tráfico conteniendo información sensible de la empresa. Aunque esta última opción podría eventualmente dejar registro de los cambios de rutas que pueden ser vistos por los administradores de red.

De forma similar, trojanos podrían utilizar IPoIM para transmitir información sin ser detectados. Un trojano que se instale en la máquina cliente, puede ejecutar IPoIM en esta máquina y establecer una conexión desde cualquier lugar a la red de la organización. Por otro lado, los trojanos/spyware actuales requieren de direcciones de red a las que transmiten la información que obtienen. Dicha dirección permite rastrear el origen del atacante. Variantes de este tipo de ataque que utilicen IPoIM para transportar la información fuera de la empresa son más difíciles de detectar, pues la dirección destino es desconocida.

Las opciones de seguridad, mencionadas anteriormente, parecen no ser factibles para controlar IPoIM:

Firewalls

Los filtros en el firewall no impiden que se establezca la conexión. Si las reglas de los firewalls autorizan la utilización de IM, entonces tambiń se podrá utilizar IPoIM. IPoIM encapsula el tráfico en el protocolo utilizado por la herramienta IM. Esto impide que el firewall detecte el establecimiento del túnel. Aunque el mismo tenga la capacidad de inspeccionar el contenido del tráfico a nivel de aplicación (layer 7 filtering), el firewall únicamente verá tráfico de IM, el cual en caso de estar autorizado por las políticas de seguridad, no será denegado.

IM corporativo

Para las soluciones corporativas de IM, en las que las organizaciones implementan sus propios servidores de mensajería, IPoIM no representa una amenaza externa siempre y cuando no interoperen con servidores de mensajería públicos,

o permitan que se establezcan conexiones con contactos ubicados fuera de la organización. En estos casos, no existe la posibilidad de que algún usuario establezca una conexión con alguna red externa a la de la organización. Sin embargo, si el servicio de IM corporativo interopera con servidores públicos, existe el riesgo de que se pueda establecer el túnel hacia una dirección ajena a la organización.

Aún en el caso de una organización cerrada, existe la posibidad que un usuario al que se le ha negado la opción de realizar transferencias de archivos utilizando la herramienta IM, pueda mediante IPoIM conectarse con otro empleado dentro de la empresa y transferir archivos. Esto permitiría a un atacante que se encuentre en una zona con altos niveles de seguridad, en la que le prohiban sacar la información que maneja en cualquier medio, transferir el contenido sensible hacia zonas de niveles de seguridad menores, facilitando asi la tarea de extraerla de la empresa. Por otra parte, también es posible utilizar IPoIM para acceder a zonas de la red en las que no tiene permisos, siempre y cuando pueda establecer el túnel requierido utilizando la solución de IM corporativo.

IM Gateways

El uso de IM Gateways permite examinar el tráfico de IM y denegar el mismo utilizando técnicas de Pattern Matching. Esto tampoco es un impedimento para la utilización exitosa de IPoIM de por si. Las técnicas utilizadas están orientadas a la busqueda de patrones conocidos par el filtrado del tráfico. En el caso de IPoIM este método de filtrado puede no resultar exitoso, dado que dependerá fuertemente de las reglas que se apliquen. Por la forma en que esta implementado el prototipo, el tráfico es codificado en Base64, siendo difícil encontrar expresiones regulares que permitan identificar el contenido enviado.

En la siguiente Sección veremos posibles soluciones, no testeadas aún, que podrían identificar conexiones de IPoIM.

IV-B. Posibles soluciones a IPoIM

Como señalamos anteriormente IPoIM evidencia una nueva amenaza a la utilización de la mensanjería instantánea. A continuación se discuten algunas soluciones que podrían ser utilizadas para disminuir el riesgo asociado a esta amenaza, detectando y controlando el mismo.

Identificadores de texto

Algunas soluciones de seguridad, como mencionamos en Secciones anteriores, permiten implementar filtros para evitar el envío de mensajes con determinado contenido identificado como sensible para la organización. Estas soluciones utilizan técnicas de Patern Matching para identificar expresiones regulares determinadas. Utilizando estas mismas técnicas, se podría implementar una solución que controlara que el texto de los mensajes enviados este formado por palabras válidas en algún diccionario. De esta forma la codificación Base64 utilizada por IPoIM en la traducción de paquetes IP en mensajes de texto, que no se identifica con palabras válidas en ningún diccionario, sería descartada. Por un tema de usabilidad, donde es natural que se cometan errores en la escritura y en el caso de la mensajería instantánea donde es más importante la velocidad que la correctitud del texto, se debe permitir un margen de error en la correspondencia con palabras del diccionario. Por otro lado en la mensajería instantánea se utilizan muchas veces palabras y símbolos que no se encuentran en diccionarios convencionales, por lo que la correspondencia de palabras debería buscarse con diccionarios específicos.

Este tipo de soluciones basadas en el reconocimiento de patrones son una solución transitoria hasta que se encuentre una codificación alternativa que no pueda ser reconocida por los patrones. Sabiendo que se aceptan palabras de algún diccionario, una simple forma de construir codificaciones válidas se basaría en el mapeo de bytes en palabras del diccionario de forma unívoca. La principal contra de este mecanismo de codificación es su overhead, más alto aún que el de Base64. El siguiente paso para resolver este mecanismo, estaría dado por un análisis sintáctico/semántico de los mensajes, algo que probablemente no pasarían la mayoría de los mensajes humanos actuales.

Cabe notar que el foco puesto en el overhead se debe a aspectos prácticos y concretos del transporte de IP sobre IM. Con la codificación actual se manejan tiempos de *round-trip-time* no inferiores a los $550ms$ para paquetes de 64 bytes. Mecanismos de codificación con mayor overhead pueden comprometer el transporte de IP, más específicamente, de TCP o UDP o de aplicaciones estándar.

Monitores de tráfico

De las herramientas implementadas para solucionar problemas de seguridad de la mensajería instantánea, algunas de ellas manejan la opción de monitorear y registrar el tráfico. Estos registros permiten obtener información estadística de cantidad de conexiones, cantidad de logins, cantidad de mensajes enviados y recibidos, etc. Una revisión frecuente de estos registros permitiría detectar casos en que exista un incremento inusual en la cantidad de mensajes enviados y recibidos. Una revisión detallada a estos mensajes, mostraría que el texto enviado no contiene palabras que se puedan corresponder con la utilizadas en algún diccionario, indicando un posible uso de IPoIM. De esta forma se podría detectar el uso de IPoIM, pero las revisiones manuales deberían realizarse en forma frecuente para que la detección pueda realizarse en forma temprana y poder controlarla a tiempo.

Otra alternativa es la utilización de técnicas automáticas para la detección de patrones de utilización anómalos. Aún no se dispone de registros específicos que nos permitan caracterizar una conexión.

Control de ancho de banda utilizado

Existen herramientas que permiten registrar y controlar el ancho de banda utilizado para la transmición de mensajes. Esto permitiría identificar aquellas conexiones que utilizan un ancho de banda fuera de lo normal. Un análisis detallado de estas conexiones podría determinar el uso de IPoIM. Microsoft estima una utilización de ancho de banda promedio de 1.6

kilobits por segundo (kbps), por usuario en un período de 8 horas [27]. En base a caracterizaciones de este tipo sería posible aislar conexiones que puedan estar siendo utilizadas de forma anómala.

El análisis anterior se basa en el estudio de conexiones ya establecidas, en las que ya se transmitió información fuera de la organización. Es deseable lograr esto con la menor cantidad de información comprometida, y de ser posible, con la transmisión de 0 bytes de contenido sensible.

El proyecto de grado del Instituto de Computación de la Facultad de Ingeniería de la Universidad de la República, "IM_SEC: Seguridad en Mensajería Instantánea", actualmente en ejecución, tiene como uno de sus objetivos el estudio de soluciones que logren detectar y controlar el uso de herramientas similares a IPoIM.

V. Conclusiones

El uso de la mensajería instantánea en las empresas continúa creciendo, acompañado de un incremento en el número de incidentes de seguridad, amenazas y vulnerabilidades. El prototipo IPoIM implementado en el Instituto de Computación muestra empíricamente que es posible la transferencia de tráfico IP usando la mesajería instantánea como transporte[1]. Los mensajes de texto pueden ser más que "sólo texto". Desde el punto de vista de la seguridad, esta implementación evidencia una vulnerabilidad en IM.

La vulnerabilidad evidenciada se aplica a un 70 % de las empresas y a la casi totalidad de los usuarios domésticos. Es por consiguiente una amenaza muy grande desde el punto de vista de su impacto y potencialidad. Más aun, la escasez de controles en la creación de cuentas en servidores públicos de IM hace muy difícil rastrear a la persona responsable por el uso de una cuenta. Variantes de malware que utilicen IPoIM tendrán consecuencias tanto en los proveedores de servicio de IM como en los usuarios del servicio. La explotación de estas vulnerabilidades pueden ser un freno para el crecimiento del sector.

References

[1] L. Rodríguez. (2006) IPoIM: Internet Protocol over Instant Messaging. http://www.fing.edu.uy/~asabigue/prgrado/2005ipoim/docum_ipoim.pdf.

[2] M. Osterman. (2005, May) Business use of IM is up, suervey shows. http://www.networkworld.com/newsletters/gwm/2005/0404msg1.html.

[3] D. Frase. (2002) The Instant Messaging Menace: Security Problems in the Enterprise and Some Solutions. http://www.sans.org/reading_room/papers/download.php?id=479&c=80c9dec08d4b581d738caceb89082798.

[4] H. de Vos, H. ter Hofte, H. de Poot. (2004) Adoption of Instant Messaging in a Knowledge Worker Organisation. http://csdl.computer.org/comp/proceedings/hicss/2004/2056/01/205610019a.pdf.

[5] Osterman Research Inc. (2003) http://www.networkworld.com/newsletters/gwm/2003/0929msg1.html.

[6] IMlogic Threat Center. (2005) http://www.imlogic.com/pdf/Q305_IMThreatReport.pdf.

[7] Osterman Research Inc. (2006) http://www.ostermanresearch.com/.

[8] Sun ONE Instant Messaging. (2006) http://www.sun.com.

[9] IBM Lotus Instant Messaging. (2006) http://www.lotus.com/lotus/offering1.nsf.

[10] Microsoft Office Live Communications Server. (2006) http://office.microsoft.com/livecomm/.

[11] Jabber. (2006) http://www.jabber.org/.

[12] IMlogic IM Manager. (2006) http://www.imlogic.com/products/im_manager.asp.

[13] M. Day and J. Rosenberg and H. Sugano. (2000) RFC 2778: A Model for Presence and Instant Messaging. http://www.rfc-editor.org/in-notes/rfc2778.txt.

[14] M. Day and S. Aggarwal and G. Mohr and J. Vicent. (2000) RFC 2779: Instant Messaging / Presence Protocol Requirements. http://www.rfc-editor.org/in-notes/rfc2779.txt.

[15] James Yonan. (2006, May) OpenVPN - An Open Source SSL VPN solution. http://openvpn.net/.

[16] (2006, May) Gaim - A multi-protocol instant messaging (IM) client. http://gaim.sourceforge.net/.

[17] Eric A. Young. (2006, May) OpenSSL - The Open Source toolkit for SSL/TLS. http://openvpn.net/.

[18] S. Parker and C. Schmechel. (1998) RFC 2398: Some Testing Tools for TCP Implementors. ftp://ftp.rfc-editor.org/in-notes/rfc2398.txt.

[19] (2006, May) NetPerf - Benchmarking Methodology Working Group (BMWG). http://www.netperf.org/netperf/NetperfPage.html.

[20] S. Ostermann. (2006, May) tcptrace - Official Homepage. http://www.tcptrace.org/.

[21] (2006, May) TTCP is a benchmarking tool for determining TCP and UDP performance between 2 systems. http://renoir.csc.ncsu.edu/ttcp/.

[22] (2006, May) Microsoft Online Services - MSN Messenger Overview. http://messenger.msn.com/.

[23] R. Movva and W. Lai. (1999) MSN Messenger Service 1.0 Protocol. http://www.hypothetic.org/docs/msn/ietf_draft.txt.

[24] (2006, May) Jabber - Open Instant Messaging and a Whole Lot More, Powered by XMPP. http://www.jabber.org/.

[25] P. Saint-Andre. (2004) Extensible Messaging and Presence Protocol (XMPP): Core. ftp://ftp.rfc-editor.org/in-notes/rfc3920.txt.

[26] ——. (2004) Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence. ftp://ftp.rfc-editor.org/in-notes/rfc3921.txt.

[27] M. Corp. (2006) Deploying Office Live Comunication Server 2005. http://www.microsoft.com/technet/itsolutions/msit/infowork/lcs2005twp.mspx.

[1] Actualmente está en curso un proyecto de grado estudiando mecanismos para mitigar los riesgos evidenciados por el prototipo IPoIM