

Mientras la tecnología de la información (TI) invade cada rincón de nuestras vidas, la era digital genera serias preocupaciones sobre la seguridad de la información y protección de datos, y la urgente necesidad de una mayor investigación en estas áreas. Desde enero de 2005, de acuerdo con el Centro de Información sobre Derechos de Privacidad, de Estados Unidos (EU), en ese país ocurrieron violaciones a la seguridad informática que involucran más de 218 millones de expedientes con delicada información personal. Las personas cuyos datos personales están implicados se encuentran en riesgo de suplantación de identidad y fraude financiero. Los gobiernos que quieren explotar integralmente la TI están conscientes de la necesidad de adoptar leyes para la protección de datos personales, en particular dentro del sector financiero y biomédico. Sin embargo, la necesidad de asegurar la información digitalizada repercute en varios frentes del mundo de la informática.

**LA SEGURIDAD NO SÓLO
SE INSTITUYE PARA
PROTEGER INFORMACIÓN**

La Escuela de Sistemas de Información (ESI) de la Universidad de Administración de Singapur encabeza una investigación para capitalizar el uso innovador de tecnología en busca de mejorar la seguridad informática. Según el profesor de sistemas de información Li Yingjiu, "la seguridad no sólo se instituye para proteger información. Es también un facilitador de los negocios. Para conservar la confianza y la lealtad de los clientes es importante garantizar la seguridad de la información confidencial y delicada de la clientela, lo cual infunde confianza y sienta los fundamentos de una nueva manera de hacer negocios".

Cinco áreas

Poniendo las cosas en perspectiva, Li recalcó que no hay sistema que satisfaga todas las necesidades de seguridad informática. Específicamente, hay cinco áreas que tienen que atenderse: cifrado de información durante el almacenamiento y la transmisión; sistemas de autenticación al inicio de sesión; detección de intrusiones para descubrir ataques al sistema; aplicaciones de control para eliminar cuestionarios que puedan extraer información personal delicada, y programas de gestión de derechos digitales, que protegen la información con marcas de agua o huellas digitales.

Con este propósito, el laboratorio de seguridad informática y confianza de SIS se enfoca en investigar la aplicación de tecnologías y soluciones novísimas para asegurar la infraestructura de TI, proteger la información de empresas e individuos, y construir confianza entre todas las partes. Trabajando de manera interna y en colaboración con otras instituciones, el equipo de la ESI —encabezado por el profesor de siste-

LA GUERRA INFINITA CONTRA LOS HACKERS



Ali Ashtari (centro), comerciante iraní de bienes electrónicos, al encarar un tribunal revolucionario en Teherán, tras haber sido acusado de espionar en favor de Israel, por lo que fue condenado a muerte ■ Foto Ap

mas de información y decano asociado Robert Deng— está involucrado en una investigación que abarca una gama diversa de proyectos de seguridad informática.

Encriptación de correos electrónicos

Li explicó que se dispone de varias soluciones tecnológicas para el cifrado de datos confidenciales y delicados durante el almacenamiento. Esta información, añadió, está también en peligro cuando se transmite entre direcciones electrónicas. Las soluciones actuales no sirven para administrar copias de correos electrónicos cifrados o para proteger la privacidad de destinatarios múltiples. En consecuencia, en SIS están motivados para desarrollar otro enfoque que doblegue las limitaciones de la actual tecnología de cifrado de correo electrónico.

El cifrado de correos electrónicos para destinatarios múltiples es un reto, pues la práctica actual, por

ejemplo, requiere el encadenamiento de múltiples textos cifrados de correo electrónico que son encriptados con la clave pública de los diversos recipientes. Cada destinatario leerá sólo lo que descifre en su computadora, sin conocer los resultados del desciframiento de otros. Esto acaba con la idea poner a los destinatarios múltiples en la misma página, por así decirlo.

"Nuestra solución prototipo, conocida como cifrado múltiple, es compatible con la actual arquitectura de correo electrónico, pero deben hacerse cambios manuales al servidor y se necesita que los usuarios estén en el mismo dominio de correo electrónico", explicó Li. El profesor Xuhua Ding, de la ESI, investigará también sobre la viabilidad de un nuevo paradigma de cifrado que no requiera la participación de terceros, como ocurre con servidores parcialmente confiables, agregó Li.

Autenticación mediante dos servidores

La autenticación al inicio de sesión impide el acceso de usuarios no autorizados. De acuerdo con Li, una práctica de seguridad largamente establecida es la autenticación con base en contraseñas cuyos detalles se almacenan en una base de datos central. Sin embargo, los hackers lo saben y obtienen de manera ilegal contraseñas de un servidor, lo que tiene serias repercusiones legales y financieras para una organización.

Li expresó que han propuesto sistemas de contraseñas de servidores múltiples para evitar la vulnerabilidad inherente a la arquitectura de un solo servidor. Ese sistema, sin embargo, es difícil, dijo, porque los usuarios tienen que comunicarse simultáneamente con múltiples servidores, o los protocolos son bastante caros.

Li destacó el éxito de los investigadores de SIS en el desarrollo

de una solución prototipo que divide una contraseña y la almacena de manera novedosa en dos servidores, impidiendo así que los hackers tengan acceso a la contraseña completa en un ataque. Explicó que sólo el servidor frontal contrata con los usuarios, mientras el servidor de control permanece en un segundo plano con la parte restante de la contraseña. La solución podría aplicarse para reforzar los sistemas de contraseñas, protegiéndolos contra ataques conocidos como diccionarios fuera de línea, ejecutados por los virus troyanos que pudieran plantar los hackers en cualquiera de los dos servidores.

Detección de intrusiones

Aunque la autenticación impide el acceso de usuarios no autorizados, los hackers persistirán en sus ataques para explotar las debilidades de los programas de computación. Según Debin Gao, también profesor de la ESI, los reportes de vulnerabilidades de los programas computacionales han crecido de mil 90, en 2000, a 7 mil 239, en 2007.

Una debilidad así, por ejemplo, permite que un atacante inyecte un código que hace que la computadora ejecute el programa del atacante. Por tanto, según Gao, "detectar automáticamente esas intrusiones y analizar las vulnerabilidades es importante para proteger un sistema informático, lo cual es el trabajo de los sistemas de detección de intrusiones (SDI). El SDI evalúa una intrusión sospechosa en cuanto sucede y da la alarma. También permanece en alerta ante ataques que puedan provenir del interior del sistema.

El software de los SDI descubre anomalías al comparar los resultados de vigilar con modelos establecidos que caracterizan el comportamiento y las interacciones normales de los programas. La alarma se produce cuando se detecta una desviación.

Gao explicó: "Obtener lecturas verídicas a partir de los análisis es un desafío, debido en parte a los enormes recursos de las computadoras, la red y las respuestas de los sistemas, lo cual debe ser vigilado y evaluado. Otra dificultad es la mayor sofisticación de los códigos maliciosos inyectados, que pueden imitar el software original, produciendo aun la respuesta correcta durante los ataques. Esto puede causar que el sistema no descubra un ataque, lo que se conoce como 'falso negativo', o que dé la alarma cuando en realidad no hay ataque, lo que se conoce como 'falso positivo'".

Control de inferencia

La vigilancia contra intrusos, o incluso usuarios autorizados que abusan de sus privilegios de acceso a información delicada, es



▶ *Nuevas técnicas de navegación e información en línea revolucionan la exploración en la web*

INMERSOS EN LA RED

Internet ha cambiado mucho desde que surgió, a mediados de los años 90. Las primeras páginas web sólo contenían texto, y existía un gran debate sobre si se deberían permitir fotografías. Hoy es bastante normal que las páginas estén atestadas de fotos, gráficos animados, videoclips, música, segmentos de software y textos. En un aspecto, sin embargo, la red permanece inalterada: se siguen usando hipervínculos interactivos para ir de una página a otra.

Frode Hegland, informático noruego, ha inventado un nuevo tipo de navegación. Su software gratuito, un explorador complementario denominado Hyperwords, convierte en hipervínculo cada palabra o frase, no sólo las que escogen los autores de un sitio web. Si uno da clic sobre cualquier palabra, número o frase, aparecen menús y submenús. Con un segundo clic, es posible traducir el texto a muchas lenguas, obtener conversiones de medidas y monedas, fotos, videos, ensayos académicos, mapas, entradas de Wikipedia y páginas web extraídas por Google, entre otras cosas relacionadas con el tema.

Toda esa información, desde luego, la pueden obtener ya los usuarios de Internet dispuestos a buscarla, abriendo una serie de ventanas o etiquetas de un explorador. El objetivo de Hyperwords, dice Hegland, es "reducir el umbral" de satisfacción de la curiosidad, al hacer más rápida y fácil la búsqueda. Más adelante, este año, Hegland lanzará una nueva versión que despliega esta artimaña más allá del explorador y convertirá cualquier palabra, en cualquier ventana, en un hipertexto.

Hyperword es relativamente una idea nueva, y hasta ahora tiene menos de 200 mil usuarios. Pero es una de las nuevas iniciativas

diseñadas para transformar la búsqueda por Internet, al proporcionar más conexiones entre datos, presentar la información de manera diferente y facilitar una rápida navegación. Otro ejemplo es Cooliris, empresa emergente de Silicon Valley, que ha inventado un navegador complementario llamado Previews. Si se mantiene el indicador del mouse sobre cierto vínculo, aparece una vista previa de la página conexas en una ventana diminuta, lo que facilita decidir si uno quiere entrar en ella. De enero a la fecha, más de 2 millones de personas han descargado el software gratuito.

PicLens, otra aplicación de Cooliris, extrae imágenes de Google, Flickr, Facebook, eBay y otros sitios web y las despliega, sin el desorden de las imágenes de las páginas web, sobre una pantalla espectacular, en 3D. Los espectadores pueden moverse rápidamente a izquierda y derecha, utilizando el zoom, para explorar cientos de imágenes en segundos. Se puede hacer clic sobre las imágenes para verlas a pantalla completa, o verlas en el contexto de su página web original. El software gratuito ha sido descargado más de 5 millones de veces. De manera similar, una nueva versión, que se lanzó en abril, convierte las búsquedas de YouTube en un muro ordenado de videos. Austin Shoemaker, director de tecnología en Cooliris, dice que los usuarios de Internet se "frustran inconscientemente" al tener que seguir pasando ventanas para ver el contenido.

Búsqueda por inmersión

PicLens da un indicio del futuro posible de la red: un ambiente tridimensional donde los usuarios se mueven a través de grupos de páginas que parecen flotar en el espacio, apartando las no deseadas y reuniendo otras en agrupaciones lógicas. Esta propuesta aprovecha la memoria espacial de las personas. John Maeda, director de la Escuela de Diseño de Rhode Island, dice que la gente encuentra difícil navegar en dos dimensiones sobre el torrente de información

en línea, y raras veces abre más de unas cuantas ventanas al mismo tiempo. Con un navegador de 3D pueden visualizarse más de 100 ventanas en forma inmediata, incluso en la pantalla de laptop.

Hasta hace poco, Maeda, investigador del Instituto Tecnológico de Massachusetts, trabajaba en un navegador de 3D llamado E15, que usa un mouse especial para que los usuarios circulen en un espacio de 3D. Durante años, los investigadores han trabajado en exploradores de 3D, pero nunca obtuvieron mucho. Apenas el año pasado las conexiones ultrarrápidas de Internet y las computadoras poderosas se han vuelto lo bastante abundantes para hacer posible un mercado masivo de 3D.

LA COMUNIDAD ENTERA TRABAJA ARDUAMENTE PARA "TRANSITAR AL SIGUIENTE PARADIGMA"

SpaceTime, nueva empresa neoyorquina, ha desarrollado un navegador de 3D que ha sido descargado más de 2 millones de veces desde su lanzamiento, en enero. El director de SpaceTime, Eduardo Bakhsh, dice que se inspiraron en los videojuegos y los gráficos animados del iPhone de Apple. Los desarrolladores de software compiten, desde luego, pero Bakhsh dice que existe la sensación de que la comunidad entera trabaja arduamente para "transitar al siguiente paradigma".

La evolución tendrá otro empujón a finales de julio, cuando Second Life, el popular mundo virtual de 3D, incorpore una característica que permitirá que los habitantes pongan páginas web en las paredes. Joe Miller, vicepresidente de tecnología en Linden Labs, la empresa que administra Second Life, dice que explorar en una red de dos dimensiones es, por lo general, un acto solitario. Explorar en Second Life, en cam-

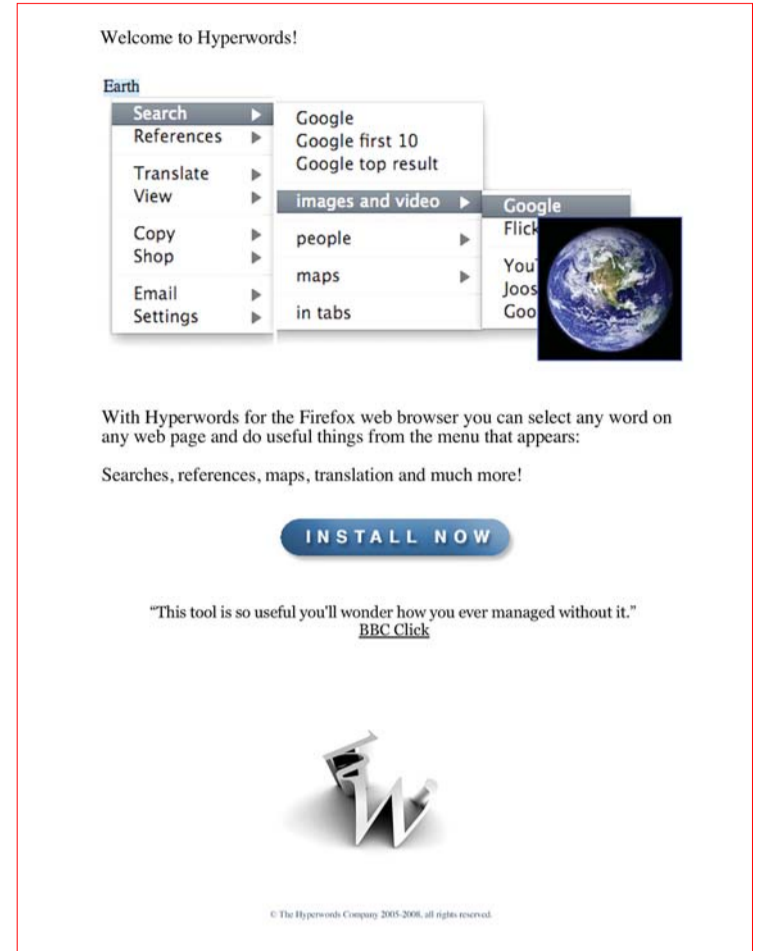
datos delicados. "Los usuarios pueden todavía evadir el control de acceso combinando solicitudes de información no delicada a partir de la cual se puedan inferir valores delicados", remarcó Li. "Esas inferencias no serían capturadas por el control de acceso tradicional, ya que las preguntas son, en apariencia, inocentes."

Gestión de derechos digitales

La preocupación por los derechos de propiedad de la información digitalizada, que puede copiarse fácilmente, ha promovido la evolución de la gestión de derechos

digitales (DRM, por sus siglas en inglés), tecnología que siembra marcas de agua digitales en el producto. En su investigación, tomó la página de una tecnología bien establecida, que agregaba marcas de agua a documentos multimedia, y la personalizó para bases de datos interrelacionadas, expresó Li. "Pretendemos desarrollar un nuevo esquema de base de datos que agregue marcas de agua digitales, y que pueda usarse para proteger la propiedad públicamente comprobable. Nuestra propuesta tiene ciertas propiedades únicas".

De acuerdo con Li, estas características incluyen una clave



Ventana de inicio para instalar Hyperwords, el futuro del hipertexto ■ Foto <http://www.hyperwords.net/>

bio, será una actividad social, porque los usuarios que dan un paseo virtual pueden reunirse y charlar a un lado de las páginas web.

El navegador 3B, desarrollado por una empresa londinense del mismo nombre, también socializa la búsqueda. Los usuarios buscan un producto y las fotografías de los resultados se organizan en los pasillos de una tienda virtual. Los compradores pueden dar vueltas para verlos mejor, y chatear con otras personas que buscan cosas similares. Más de 200 empresas de ventas, entre ellas Barnes & Noble, Wal-Mart y Gap, exhiben sus mercancías en 3D. Algunas emplean dependientes para contestar las preguntas de los compradores. Nicky Morris, director de la empresa, dice que el negocio es "absolutamente fenomenal", porque las mujeres, en particular, permanecen más en las tiendas cuando no están solas.

También Microsoft desarrolla un navegador móvil de 3D, llamado Deepfish. Están en proyecto

muchos otros navegadores de 3D. Esta seductora tecnología puede parecer maravillosa. Dave Farber, científico de Carnegie Mellon, y uno de los padres fundadores de la Internet, dice que el entusiasmo por los videos será sustituido por la conciencia de que la navegación en 3D es una herramienta muy necesaria. Piensa que Hyperwords será ampliamente utilizado (e imitado), ya que permite hacer conexiones más interesantes. Un usuario puede agregar una opción, digamos, para buscar cualquier palabra o frase en sus periódicos favoritos bolivianos y peruanos. Los usuarios de Hyperwords pueden, también sin esfuerzo, colocar textos en un blog, correo electrónico, mensaje instantáneo o perfil de Facebook. Estas nuevas conexiones agregan "profundidad" a las palabras y a las ideas, dice Farber, pero crean redes increíblemente complejas. Sin mapas de 3D, señala, podríamos perdernos en la red.

FUENTE: EIU

▶ otro aspecto de la seguridad informática. Li declaró que, en este caso, la atención se centra en especial en las bases de datos, como la información del censo nacional.

"El software de control estadístico de inferencia es necesario para proteger la privacidad de datos delicados y el acceso, mientras se encuentra un equilibrio proveniente de la creciente necesidad de datos estadísticos precisos", agregó Li. Sobre el control de inferencia, aseguró que el acceso a la información confidencial es controlado por el software, que rehúsa responder preguntas sobre

de agua. Agrega Li: "Nuestro esquema es sólido. Es difícil que los ataques tradicionales invaliden la detección de marca de agua y prueba de propiedad".

Li afirmó que los usuarios apreciarán la técnica de marcas de agua debido a su uso práctico en el mundo real para proteger la propiedad de bases de datos. Concluye que la investigación de la ESI en seguridad contribuirá a proteger los sistemas informáticos y la Internet; y a salvaguardar la integridad de los productos digitales y de los derechos de propiedad.

FUENTE: EIU

