La seguridad de unos puede ser la inseguridad de otros

Ángel García Baños

Los casos más notorios, sin mencionar los nombres de las instituciones y algunas soluciones inéditas.

Desde hace muchos años existen varias herramientas tecnológicas muy sofisticadas en el campo de la seguridad informática. Sin embargo, su uso incorrecto puede dar lugar a situaciones de falsa seguridad e indefensión, no tanto para las instituciones que las usan, sino para sus clientes.

Desde 1978 en que Rivest, Shamir y Adelman inventaron el cifrado asimétrico RSA y posteriormente se desarrollaron los sistemas de bioidentificación, para garantizar la seguridad informática, disponemos de una serie de herramientas potencialmente más robustas y fiables que la seguridad tradicional de llaves físicas en cerraduras metálicas, y firmas con lapicero sobre papel [1]. Por ejemplo, ahora disponemos de firmas digitales, en vez de firmas en papel; criptografía de clave pública/privada, en vez de dudosos sistemas propietarios de ocultamiento de información; certificados digitales, en vez de cédulas o carnéts; y autenticación biométrica, en vez de confiar en recordar el rostro de cada persona. Sin embargo, a pesar de que efectivamente las herramientas son muy robustas, su pobre implementación en muy diversas instituciones vuelve los sistemas informáticos mucho más frágiles de lo que cabría esperar. Y, lo que es peor, los clientes de esas instituciones quedan indefensos ante fallos, intencionales o no, en esos sistemas informáticos.

Las transacciones en internet habitualmente involucran una institución que ofrece servicios y clientes que quieren utilizarlos. Para que las transacciones sean confiables, ambas partes deben tener certeza que la otra parte es quien dice ser. En ese proceso aparecen tres problemas separados, que se van a tratar en este artículo: en el apartado 2, la autenticación de la institución (que se suele hacer con

certificados digitales); en el apartado 3, la autenticación del cliente (que se suele hacer con contraseñas y con medidas biométricas); y en el apartado 4, la seguridad de los datos en el computador del cliente. En cada caso se muestran situaciones donde, por mala implementación de estos sistemas, las instituciones están dejando a sus clientes en manos de los hackers(1).

Todos los casos aquí expuestos son reales, pero se omiten los nombres de las instituciones involucradas, dado que el objetivo no es denunciar sino instruir.

Problemas en la autenticación de las instituciones

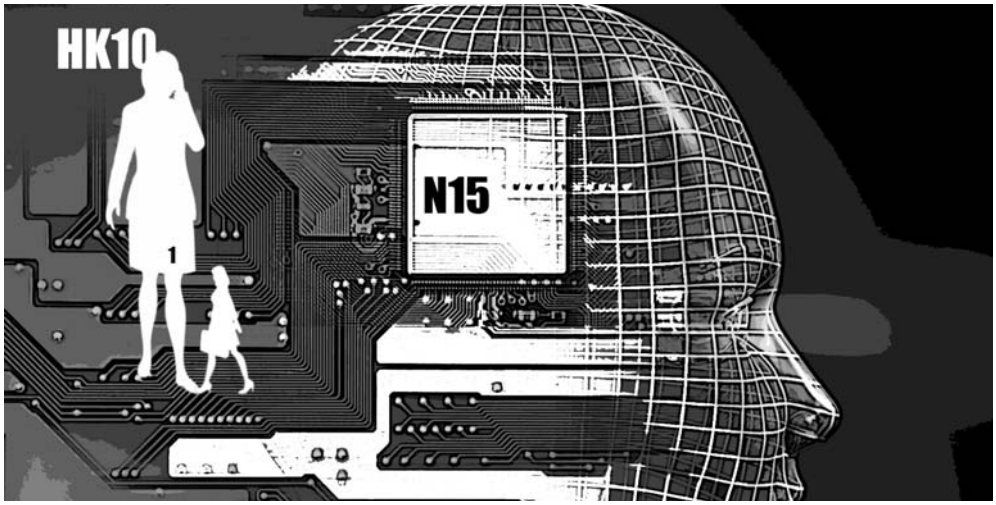
La única forma razonable de autenticar instituciones es a través de certificados digitales. Usando cifrado asimétrico RSA se puede asignar a cada persona o institución un certificado digital [2] [3], que es básicamente como una cédula, carnet o pasaporte, como el medio que asegure que la persona o institución sea realmente quien dice ser. Esto es importante, porque cuando usted navega por internet y entra a la página de su banco, usted quisiera estar absolutamente seguro de que se trata de su banco, y no de un impostor que podría robarle la contraseña de acceso.

El cifrado asimétrico se basa en el uso de dos claves por cada persona o institución: una clave pública, que todo el mundo conoce; y una clave privada, que sólo el respectivo propietario conoce. Para generar y asignar dichos certificados digitales se necesita una autoridad global (una especie de notario electrónico), cumpliendo el siguiente proceso:

1.La institución que requiere un certificado digital se acerca físicamente a la autoridad que los emite, llevando su propia clave pública así como su cédula, certificado de cámara de comercio, etc. que la identifique como normalmente hacemos.

2.La autoridad global también posee su juego de claves asimétricas (la pública y la privada). Entonces crea un mensaje que contiene varios campos entre los que cabe destacar los datos de la institución (nombre real, dirección física, dirección electrónica y clave pública de la institución). Después encripta este mensaje con su clave privada. A esto se le llama el certificado digital de la institución.

La autoridad global está actuando como un notario, asociando indisolublemente la clave pública de cada persona o institución con sus datos del mundo real. Nadie puede hacer esto de modo que se pueda recuperar esa información con la clave pública de la autoridad global (que, recorde-



mos, al ser pública la conoce todo el mundo); es decir, la autoridad global está firmando digitalmente ese certificado, asegurando así que la información que lleva asociada (dirección, clave pública, etc.) es veraz.

En la práctica no hay una única autoridad mundial sino un pequeño conjunto (entre las que cabe destacar VeriSign, AOL, America Online, Digital Signature Trust, etc.). Los certificados de estas autoridades se llaman de "clase 1", están autofirmados y vienen incluidos automáticamente en todos los navegadores web.

Como sería incómodo y caro acercarse físicamente a estas autoridades para pedir un certificado, lo que se ha hecho es que ellas certifican digitalmente la existencia de autoridades secundarias a nivel regional (de clase 2), y éstas a su vez certifican digitalmente la existencia de autoridades locales (de clase 3) que se supone que están más cerca de su domicilio.

Entonces, usted o su empresa pueden pedir un certificado a las autoridades de clase 3, que a su vez está firmado por las autoridades de clase 2 y firmado por las de clase 1. Y estas últimas se puede comprobar que son verdaderas porque el respectivo certificado está dentro de su navegador web.

Cada vez que usted navega y llega a una página segura (con protocolo https en vez de http, y donde aparece un candado cerrado en alguna esquina), se pide automáticamente el certificado digital de esa página y se sigue la cadena de entidades certificadoras hasta llegar a la de clase 1, comparándolo con el que tiene almacenado internamente el navegador. Si la comparación sale correcta y la cadena no está rota en ningún sitio, significa que

la página a la que acabamos de entrar es realmente de quien dice ser.

Esto no es trivial, como podría parecer. Actualmente, el fenómeno de phising(2) está en expansión, y son los certificados digitales quienes nos permiten distinguir páginas web legales de las falsificaciones.

Vemos así que los certificados digitales son la salvación. Los clientes pueden confiar en las páginas web de las instituciones si éstas tienen correctamente configurados sus certificados digitales. Pero a veces nos encontramos con todo lo contrario, como veremos en unos ejemplos a continuación.

Situaciones donde se dan malas implementaciones

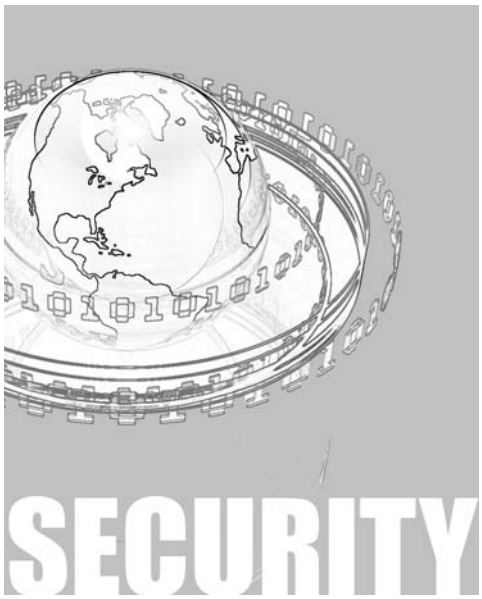
Sin certificado

El caso peor, obviamente, es cuando la institución no tiene ningún tipo de certificado en su página web. Si es así, sus clientes nunca estarán seguros de si están visitando una página web legítima o una falsificada. Por ejemplo, ¿es http://www.bancoXXX.siteYYY.com/ una página legítima del banco XXX?. Probablemente no, ya que cualquier propietario del dominio siteYYY puede crearla.

Certificado mal configurado

Pero otro caso, casi tan malo como el anterior es cuando, por desconocimiento o por ahorrar dinero, las instituciones proporcionan certificados de seguridad autofirmados por ellas mismas, o que no hacen referencia (a través de una cadena continua) a una autoridad mundial.

También a veces vemos certificados correctos pero que han expirado. Aclaramos aquí que, para aumentar la seguridad, cada certificado incluye fechas de inicio y de fin, proporcionando al certificado típicamente un periodo de validez de 2 años. Si el certificado no se renueva oportunamente cuando caduca, el navegador web que usa el cliente le advertirá a éste de la situación anómala.



El navegador también dispara mensajes de advertencia al cliente en el caso de que el enlace web de la institución no coincida con el que está dentro del certificado. Por ejemplo, si estamos navegando en http://www.bancoXXX.com/ pero el certificado pertenece a http://www.banco-XXX.com/ (obsérvese que hay un guión de más).

En todos estos casos (cadena rota de certificados que no alcanzan a una autoridad mundial, fecha de expiración superada, inconsistencia en los nombres) el navegador web dispara mensajes de advertencia al cliente y le da la posibilidad de continuar o de cancelar la operación.

Y allí está el problema: los clientes necesitan hacer operaciones y, habitualmente, continuan el proceso haciendo caso omiso de las advertencias. Incluso cuando el cliente es consciente de lo que ello significa, lo más que puede hacer es llamar telefónicamente a la institución. Y la respuesta que suele obtener es "no se preocupe, que el certificado es correcto. Lo que ocurre es que... [cualquier excusa administrativa]"

Desgraciadamente esta forma de operar permite a los hackers hacer ataques de tipo "man in the middle"(3) o de "phising", proporcionando páginas web idénticas a las legítimas, idénticas en todo excepto en el certificado de seguridad. Al cliente de la institución le aparecerá de nuevo (como siempre) el aviso en el navegador, advirtiéndole que la página web que va a visitar no parece ser la legítima, pues el certificado de seguridad es incorrecto. Y, como siempre, entrenado paulovianamente por su institución, lo más probable es que el cliente pulse el botón de CONTINUAR, quedando en manos de los hackers.

Varios certificados mal configurados

Como caso excepcional se puede mencionar un banco que se hace phising a si mismo: tiene dos dominios web distintos, pero con la misma información (www.bancoxxxxx.com y www.xxxx.com.co). Y, lo que es peor, ambos sitios web tienen rota la

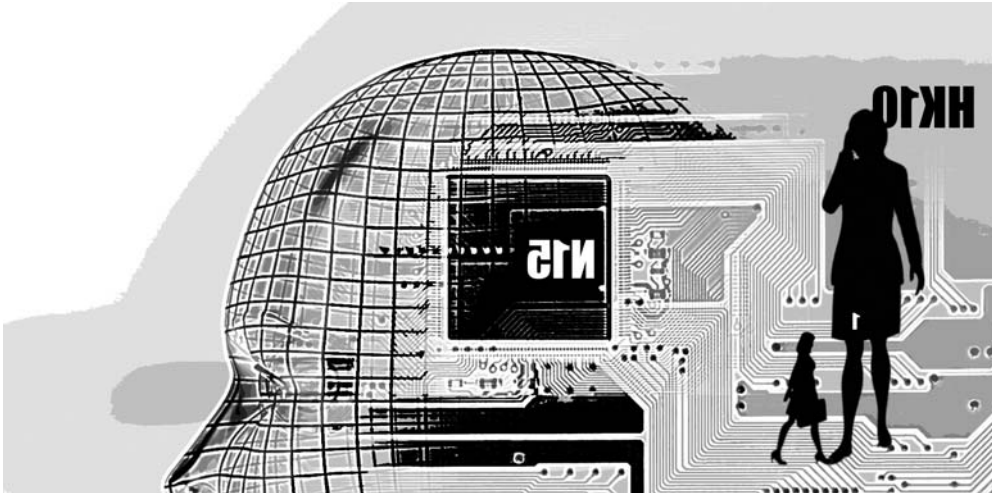
cadena de certificados. Un usuario sensato no sabría cual de los dos es el auténtico y evitaría entrar a ambos. Un usuario inexperto entraría a cualquiera de los dos y, acostumbrado a ello, también entraría a cualquier otro sitio similar (por ejemplo, www.bancoxxxxx.hacker.com) que un hacker quiera ponerle como anzuelo).

Otro caso extraño es de una institución que tiene un único dominio web, y que por razones de balanceo de carga utiliza dos computadores servidores. El error consiste en que asignaron un certificado distinto a cada computador. Si estuvieran firmados por una autoridad mundial no habría problema. Pero cada uno de ellos está autofirmado.

Aún cuando no exista una cadena de certificados que lleven a una autoridad mundial, un usuario consciente puede apuntar en un papel el certificado que le muestra el navegador. De este modo, obtiene un buen grado de seguridad si, cada vez que entre a esa página web, le coincide el certificado que muestra el navegador con el del papel.

Sin embargo, si la institución tiene varios certificados autofirmados, y aparecen a veces unos y a veces otros, la conclusión errónea a la que llega el cliente es que continuamente hay phising.

Como resumen, vemos que aunque la percepción que la institución tiene de si misma es buena, la percepción que tiene el cliente es de confusión (le faltan herramientas para decidir si una página web es legítima o no) e incluso indefensión (como todo siempre ha funcionado mal, cuando aparece un hacker de verdad los mensajes de advertencia pasan inadvertidos).



Problemas en la autenticación del cliente

Los clientes se suelen autenticar (es decir, que las instituciones se aseguren de que los clientes sean quienes dicen ser) mediante contraseñas apoyadas o no en certificados digitales y también con medidas biométricas.

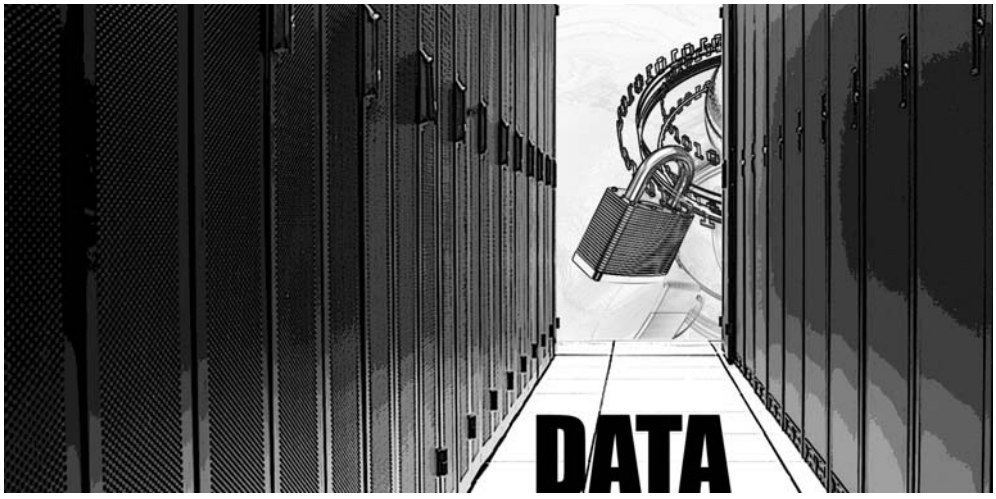
Certificados y contraseñas del cliente

Hasta ahora hemos visto que los certificados autentican la identidad de las instituciones. Pero también pueden servir para autenticar a los clientes. Por ejemplo, si un banco quisiera estar seguro de la identidad de los clientes que entran a hacer operaciones, podría exigirles que tuviera cada uno de ellos su propio certificado obtenido a través de una entidad certificadora mundial e instalado en su navegador web. En la práctica, el manejo de los certificados requiere conocimientos que no se pueden exigir a los clientes comunes, por lo que nadie emplea este método. En su lugar, cada cliente se autentica utilizando una contraseña que sólo él conoce; cuando el cliente quiere cambiar su contraseña puede hacerlo él mismo.

Situaciones donde se dan malas implementaciones de contraseñas

El problema fundamental de la implementación de contraseñas es cómo asignar la inicial a cada cliente. Las instituciones emplean para ello varios métodos. Vamos a enumerar algunos de ellos, empezando por los más seguros y costosos y terminando por los más inseguros y baratos:

Entrega personalizada (en mano, en sobre de seguridad y con acuse de recibo) de una contraseña única y generada al azar, de forma irrepetible.



Entrega masiva (por correo ordinario) de contraseñas únicas generadas al azar. El riesgo aquí radica en que la contraseña no llegue al destinatario (ya que el correo ordinario no es muy seguro), sino a otra persona que podría utilizarla para hacer operaciones ilegítimas.

Entrega masiva de un algoritmo sencillo para generar la contraseña de cada cliente. Por ejemplo: la contraseña es la primera letra del nombre, seguida del número de cédula, y seguida de la primera letra del primer apellido.

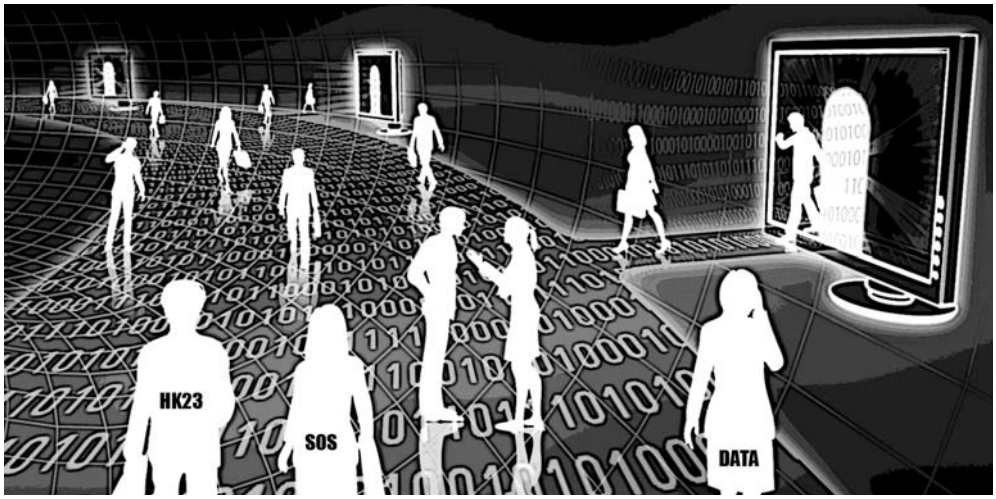
El último método se sigue empleando en varias instituciones hoy día, seguramente por ser el más barato. Pero es absolutamente inseguro, ya que todos los clientes conocen el algoritmo y, por tanto, pueden averiguar las contraseñas de todos los demás. Hay un periodo de tiempo que suele oscilar entre unas horas y varios días, mientras cada cliente se percata del problema y cambia su clave insegura por otra secreta y personal. Mientras eso ocurre, todas las cuentas están abiertas.

Son momentos de pánico: cada cliente sabe que su contraseña es trivial y teme que sea demasiado tarde para cambiarla. A consecuencia de ello sé que se han producido incidentes leves (robo de cuentas e identidades), rápidamente corregidos, pero podría haber problemas más graves.

Autenticación biométrica

Cuando en la vida cotidiana reconocemos a una persona y la distinguimos de las otras, lo hacemos gracias a que hay una serie de características biométricas sutiles que son únicas (o casi únicas) en cada persona. Entre ellas están la forma del rostro, la manera de caminar, el timbre de la voz, las huellas de los dedos, los vasos capilares en el iris de los ojos, las firmas digitalizadas(4), los anticuerpos del sistema inmune que están circulando por la sangre, etc. [4].

Actualmente existe en el mercado un tipo de sensor muy barato que, al poner el dedo en él, captura el equivalente a una fotografía de la huella del dedo. Esa foto se puede almacenar después en un computador(5). En el



futuro es de esperar que sigan apareciendo sensores que midan otras características biométricas(6).

Situaciones donde se dan malas implementaciones de autenticación biométrica

Vamos a centrarnos en el problema de la huella del dedo, pero todo lo que se diga es aplicable a los demás datos biométricos.

La tradicional huella del dedo índice la empleamos desde hace muchos años, para autenticarnos en notarías, bancos, contratos, etc. Actualmente, el sensor de huella se utiliza en muchos sitios: en notarías; para obtener permiso de entrada a ciertos edificios; en "casas de cambio" para enviar dinero de una ciudad a otra; etc. A veces nos piden poner un solo dedo en el sensor. A veces nos piden poner los diez dedos de las manos, para autenticarnos mejor.

Todo el valor de la huella de los dedos radica en que va unida indisolublemente al resto de nuestro cuerpo. Desgraciadamente, al digitalizarla y guardarla en un computador, se pierde esta característica fundamental.

De modo que nuestras huellas se encuentran ahora repartidas en muchas bases de datos, en muchos computadores. ¿Estarán bien protegidas? Porque nuestra identidad depende de ello, ya que si con una huella recién digitalizada puedo firmar un documento, con una huella digitalizada, almacenada y recuperada exactamente igual años después, también puedo firmar documentos.

El problema es grave, y para aclararlo basta un ejemplo: si nos roban en un banco, se puede cambiar la clave, se puede cambiar la cuenta, se puede

cambiar el banco. Pero si nos roban las huellas digitalizadas, no hay forma de cambiarlas y nuestra identidad la pueden usar los hackers por toda la vida. El asunto se agrava porque quienes almacenan nuestras huellas digitalizadas (notarías, casas de cambio, porteros de edificios) habitualmente no tienen la infraestructura de seguridad, ni los conocimientos, ni la experiencia adecuadas para protegerlas. Están ya en demasiados sitios inseguros.

La consecuencia desastrosa de ello es que, por el empleo ingenuo de las huellas digitalizadas, su función como autenticador se perdió desde el primer momento. No tienen ya ninguna validez. Por ejemplo, puedo poner en duda la legitimidad de cualquier documento que aparezca firmado con mis huellas digitalizadas, puesto que mis huellas no las controlo yo ya en exclusividad.

La seguridad en el computador del cliente

Aunque los certificados bien configurados dan un alto nivel de seguridad a la información en tránsito por internet, no existe ninguna garantía mientras la información reside en los computadores. Obviamente, las instituciones protegen la información de sus propios computadores usando una variedad de métodos. Pero el cliente permanece desprotegido, pues su propio computador es permanente objetivo de ataque de hackers (ver Figura 1).

En muchas instituciones bancarias nos advierten que es peligroso realizar operaciones desde cafés-internet o computadores localizados en sitios públicos. Y que sólo hay seguridad desde el propio computador, en el hogar o en la oficina. Pero esto no es del todo así, pues incluso en el hogar y la oficina navegamos por internet,

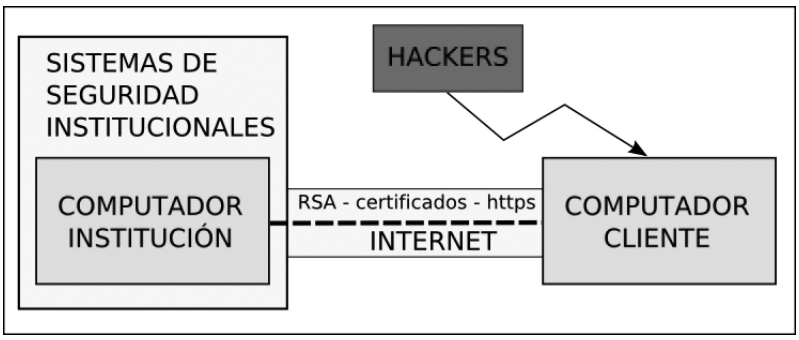
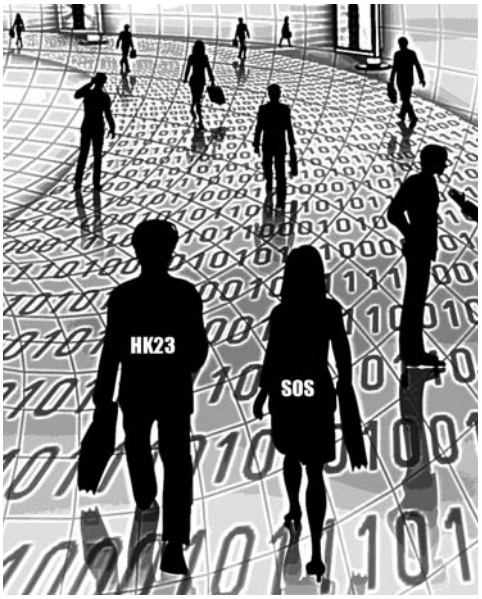


Figura 1: Conexión con seguridad (protocolo https), pero con el cliente desprotegido.



recibimos correos electrónicos y compartimos disquetes y CDs con otros usuarios de otros computadores. Todos estos procedimientos pueden servir como puerta de entrada para virus que instalen un keylogger en nuestro computador. Un keylogger es un pequeño programa que monitorea las teclas pulsadas por el usuario en su computador, sin que éste lo advierta. El objetivo principal de los keyloggers es capturar contraseñas, que luego envían a hackers por medio de internet.

Este problema es el más difícil de resolver, y aunque realmente no es responsabilidad de las instituciones garantizar que los computadores de sus clientes estén libres de keyloggers, sí pueden ayudarles a evitar este problema, con un sencillo método que se explicará a continuación.

La idea es que las instituciones podrían proporcionar a sus clientes un LIVE-CD(7) que ellos garanticen razonablemente libre de virus y keyloggers. Este LIVE-CD podría estar basado, por ejemplo, en una distribución gratuita de OpenBSD (que es bastante segura) y debería incluir un sistema operativo básico y únicamente dos aplicaciones: un navegador

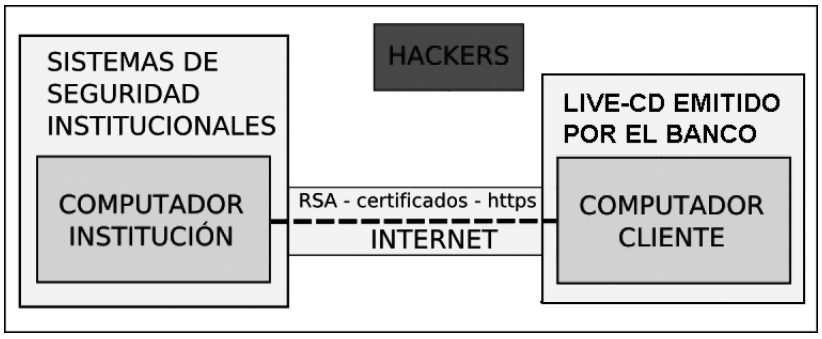


Figura 2: Conexión con seguridad (protocolo https), con el cliente protegido, usando un LIVE-CD. El hacker no dispone de ningún punto de penetración.

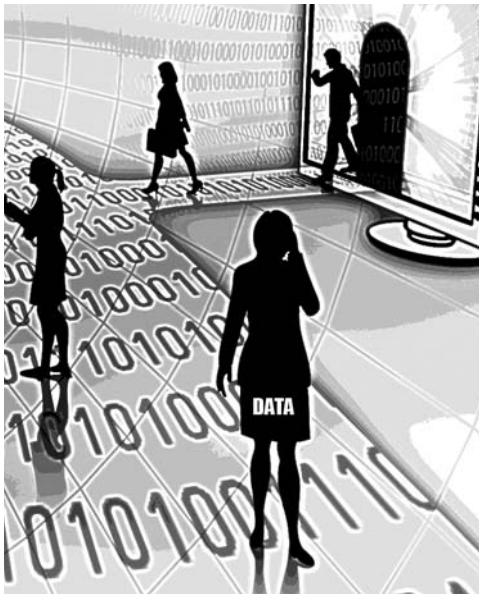
web con los certificados adecuados para acceder a la institución; y un firewall con las reglas adecuadas que impidan navegar a otros sitios. Con ello (ver Figura 2) darán al usuario la garantía de seguridad total punto a punto desde el computador de la institución hasta el computador del usuario (incluyendo el propio computador del usuario).

Conclusiones

El rápido desarrollo de las nuevas tecnologías de la información no va acompañado de una toma de conciencia sobre sus peligros, que son completamente nuevos para el común de la gente. En general, los riesgos que se introducen con las nuevas tecnologías no son nuevos, pero si son mayores, alcanzan más gente y pueden desarrollarse con más rapidez.

Cuando las instituciones implementan mal esos mecanismos de seguridad, dejan completamente indefensos a sus clientes, no solo a los comunes sino incluso a los experimentados. Este argumento se ha resaltado a lo largo del artículo.

También se ha presentado una propuesta efectiva que podrían ofrecer las instituciones a sus clientes, para mejorar la seguridad total de extremo a extremo en la comunicación a través de internet.



Referencias

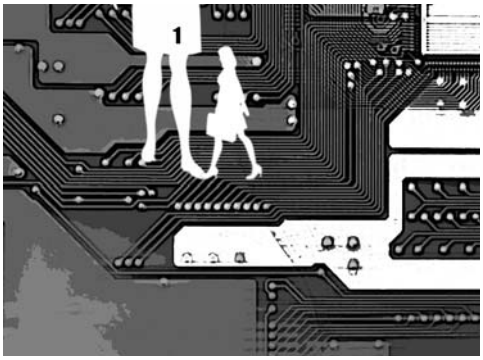
[1] Charles P. Pfleeger, "Security in Computing", Prentice Hall, New Jersey, 1989.
[2] http://es.wikipedia.org/wiki/Certificado_digital (Consultado: 2008-03-02)
[3] http://www.rsa.com/node.aspx?id=2604 (Consultado: 2008-03-02)
[4] http://en.wikipedia.org/wiki/Biometrics (Consultado: 2008-03-02)

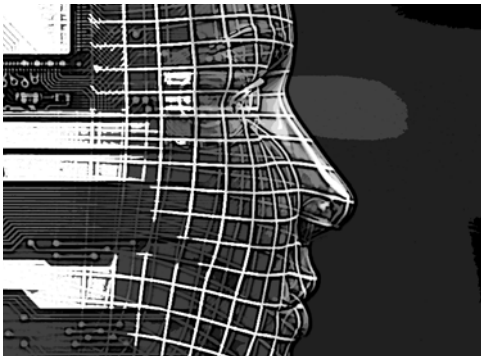
Notas

(1) La palabra adecuada sería cracker (persona que hace daños) frente a hacker (persona con muchos conocimientos), pero desgraciadamente ya se ha impuesto esta última.

(2) Phising: consiste en falsificar hasta en sus mínimos detalles una página web (típicamente de una entidad bancaria) para que el cliente se confíe e introduzca allí sus datos (username/password), que llegan de esta manera al propietario real de la página, un hacker, que los usará para acceder a su cuenta bancaria y desvalijarlo.

(3) Alguien que está escuchando una transacción legítima, y que altera para su propio provecho algunos de los datos en tránsito.





(4) Las firmas digitalizadas son simplemente algo así como una fotografía de la firma normal con lápiz sobre el papel, con sus ventajas e inconvenientes (fácil de falsificar). Mientras que la firma digital es una secuencia de números obtenida a través de algoritmos basados en RSA que, hasta el momento no se ha podido falsificar; si un documento está firmado digitalmente por una persona, las propiedades matemáticas de esos algoritmos permiten demostrar que sólo la mencionada persona pudo haber firmado el documento en cuestión.

(5) A veces no se almacena la fotografía de la huella completa, sino sólo los artefactos más relevantes. Pero ello no invalida la discusión que se va a dar, puesto que es trivial convertir lo uno en lo otro.

(6) De hecho, ya existen, pero por razones de su alto costo todavía no se emplean masivamente.

(7) Es un CD (o DVD) que incluye un sistema operativo y un pequeño conjunto de aplicaciones. No necesita instalarse en el disco duro (ni siquiera lo usa), ya que se ejecuta al introducir el CD en la correspondiente unidad, en el momento de prender el computador. Incluso, para mayor seguridad, debería desconectarse o deshabilitarse el disco duro.

Ángel García Baños. *Doctor Ingeniero de Telecomunicación; Director del Programa de Ingeniería de Sistemas, Escuela de Ingeniería de Sistemas y Computación, Universidad del Valle, Cali, Colombia.*