



Sobre la autenticidad de lo intangible

Hace tiempo entré a tomar un café en el primer sitio que encontré abierto y resultó ser uno de esos ciber-cafés que tanto se mencionan en la literatura de seguridad cuando las cosas van mal. Mientras me tomaba el café pude observar a una clientela bastante variopinta, en lo que a sus edades se refiere, mientras desarrollaba sus actividades en el ciber-espacio. Lo más curioso de aquella escena era ver con qué concentrada atención miraban todos a sus extrafinas pantallas de cristales líquidos. Como yo estaba de espaldas a las pantallas, sólo conseguía ver cierta luminosidad reflejada en las caras, mayoritariamente atónicas, de aquellos usuarios del ciber-espacio. En aquel momento me di cuenta de que miraban a Internet con los mismos ojos que un profano miraría a una premonitoria bola de cristal en manos de una pitonisa cingara. En ese momento me di cuenta, una vez más, de que la inmensa mayoría de usuarios no son conscientes de que lo que realmente tienen delante a la hora de asomarse a Internet, es sólo eso, una bola de cristal, y no necesariamente la realidad. Este hecho hace que, además de los parámetros técnicos de Internet, también haya que tener muy en cuenta los factores humanos a la hora de analizar incidentes de seguridad, como pueden ser los del actual *phishing*, los del futuro *pharming*, etc.

El usuario común se cree todo lo que ve, e Internet sólo es imagen. Hubo, hace muchos años, una versión "sólo texto" de lo que terminó siendo "La Web", pero duró lo mismo que duraron los terminales VT100. La Web realmente nació cuando ésta se llenó de gráficos, anagramas, colores, información y dinamismo, y su éxito histórico se debe, en parte, a la universalidad y potencia de la interfaz gráfica para los videntes. Cuando el mundo empresarial entendió el potencial de comunicación que supone Internet, y desembarcó en ella para hacer sus negocios, encontró perfectamente natural seguir utilizando colores, anagramas y demás recursos de la publicidad gráfica tradicional como símbolos de identidad, sin darse cuenta de que se metían en un mundo inmaterial esencialmente no-auténtico.

La Web e Internet sólo existen en la pantalla sobre la que el ordenador cliente las "pinta" y puedan así ser vistas por el usuario. Cada uno de los elementos de una página Web es una pieza gráfica, de texto o ejecutables que se envían desde el servidor Web al navegador en uso, para que éste las represente ante los ojos del usuario. Desde el origen de la información hasta las retinas del usuario final hay un largo camino y nadie se responsabiliza

El elevado número de timos que sufren estos días los servicios bancarios que operan en Internet ha puesto de manifiesto, una vez más, que la Web es esencialmente anónima y carece de identidades. Dado que la autenticación es un requisito esencial para poder desarrollar sistemas de valor en la red, conviene que nos paremos a ver cuáles son las características de los sistemas actuales que impiden que funcionen correctamente, y quizás así podamos tener una idea de cómo habría que cambiarlos para hacerlos mejores.

de su seguridad. Puede que los datos en el servidor de un banco sean los correctos pero, por ejemplo, el banco puede no responsabilizarse de ellos una vez salen de sus instalaciones. Cuando esos datos fluyen a través de las redes, el proveedor de conexión se compromete a que la red "técnicamente" funcione pero, en principio, no asegura que el contenido de las transmisiones sea, en todo momento, auténtico. Cuando se llega a las últimas etapas del viaje, esa información pasa



La seguridad de una transacción de valor en Internet no deberá depender de la seguridad de los sistemas operativos diseñados para PCs u otros sistemas generalistas porque, en el caso de hacerlo, tarde o temprano, y con mayor o menor impacto, su inseguridad está plenamente asegurada.

a través de un equipo, de un software y de un sistema operativo, todos ellos "de propósito general", que se encargan de gestionar las conexiones de red, de mostrar en la pantalla lo recibido (o algo parecido), y de esperar a la respuesta del usuario a través del teclado o del ratón.

En este largo peregrinar, los contenidos de la información pueden cambiar en muchos sitios, muchas veces y de formas muy variadas, por lo que en este medio, Internet, basar la autenticidad en factores visuales es una ingenuidad y una temeridad. En Internet los anagramas, las marcas, los colores corporativos, las tipografías, y cualesquiera otros símbolos de identificación habituales en el mundo comercial físico, carecen de sentido; más aún, su uso sólo puede inducir a error al usuario haciéndole creer, en lo que a la autenticidad se refiere, que en Internet las cosas no son como en la vida real.

Incapacidad humana

El mejor y más reciente ejemplo de este incontestable hecho negativo lo encontramos en la esencia, aparición y apoteosis actual del *phishing*. La autenticidad de los sistemas de banca por Internet no puede basarse en los "estilos" corporativos, aunque éstos sean muy útiles en el mundo físico. Cualquiera podría

disponer, en exclusiva, de un servidor de banca por Internet que fuese visualmente indistinguible del servidor original. Cuando nos conectamos a un servicio comercial en Internet no podemos estar seguros de que realmente hemos contactado con él por el mero hecho de que todo "parezca" correcto a simple vista.

El ser humano carece esencialmente de capacidades para evaluar la autenticidad—u otros predicados de la seguridad—de lo que acontece, se transfiere o habita en mundos informáticos como Internet. Un hombre jamás podrá probar

Para tratar los temas de la autenticidad fue para lo que nacieron las así llamadas "Infraestructuras de Clave Pública", y que serían el mecanismo para introducir identidades digitales, reconocidas y reconocibles, en un mundo esencialmente anónimo como el de Internet. En el protocolo SSL, el servidor, en la etapa inicial del establecimiento del canal de comunicaciones, se presenta ante el sistema cliente entregándole su identidad como parte de un documento digital firmado por una (autoproclamada) "Autoridad de Certificación". Es en este punto donde la aplicación cliente puede y debe validar esa identidad aportada por el presunto servidor, y así poder llegar a conocer una identidad concreta en su futuro interlocutor. La seguridad o inseguridad de todo el sistema depende de las etapas en las que se procede a la validación de credenciales.

Según muchos profesionales, la esencia y procedimientos propios de las infraestructuras de clave pública pueden resultar impenetrables para la inmensa mayoría de los usuarios comunes, por lo que los diseñadores de la Web comercial que hoy conocemos decidieron (unilateralmente) "facilitarle la vida" a sus potenciales clientes y suplantaron en su tarea de reconocer, de confiar o no, en una identidad digital; o lo que aún es peor, en reconocer y confiar en toda una catedral de identidades. Este hecho vio la luz el día en el que se aceptó distribuir los navegadores de Internet preñados con numerosos certificados digitales preinstalados. Esos certificados son los de ciertas Autoridades de Certificación, y su presencia ahí hace que los navegadores den por bueno y fiable, de forma automática, cualquier certificado que pertenezca a esas PKIs. Por lo tanto, el usuario que está al otro lado de la pantalla y del teclado o del ratón, no participa de ningún modo en el reconocimiento y aceptación de la identidad del servidor al que se conecta, por lo que es independiente de las consecuencias que éste hecho pudiese causar en adelante.

PKIs y navegadores paternalistas

Los que promovieron esta idea de un "club selecto" de PKIs y de unos navegadores paternalistas que "guiarían" a los usuarios comunes dentro de un paraíso de identidades y autenticidades controladas por ellos, se equivocaron en una cosa: en que podrían controlar la integridad de esa "preinstalación" que les confiere su preeminencia, y esto no es así. Al abrir la caja de Pandora que supone implantar mecanismos para la aceptación y confianza automática en ciertas identidades digitales, sus promotores abrieron la puerta para que "otros" suplantasen a esas

mismas PKIs, o a que se unan a ellas dentro de esos mismos navegadores. Quien logre incluir sus certificados en la base de datos que contiene los certificados de *VeriSign*, *Thawte*, *America Online*, *Entrust*, *Equifax*, *GeoTrust*, *RSA Security*, etc., logrará que sus servidores sean **aceptados "sin rechistar"** por parte de ese navegador. En este caso, el usuario que hay detrás de la pantalla no notará diferencia alguna entre una conexión con un servidor auténtico y otra con un servidor pirata; para él, ambas posibilidades son exactamente las mismas, ya que el candadito seguirá estando cerrado y bien cerrado.

Seguridad falsa

Para complicar más la situación actual, algunos aconsejan —e incluso parecen llegar a exigir—, que los usuarios hagan doble clic en el candadito cerrado para poder leer, personalmente, cuáles son los campos del certificado que se ha aceptado, y cuál es la identidad raíz, dentro del selecto club, que otorga identidad fiable a ese servidor en concreto. Este proceder es muy desaconsejable ya que **induce al usuario del navegador a tener una sensación de seguridad falsa**, y la razón de ello es bien sencilla: también se pueden suplantar los certificados preinstalados de esas PKIs. Cuando alguno de nosotros utiliza cualquier navegador para conectarse a cualquiera de los genuinos servidores que están dentro de alguna de las PKIs preinstaladas, lo que nosotros tenemos que hacer es: nada, absolutamente nada. La autenticación y aceptación del servidor se hace independientemente de quién sea el usuario que solicita la conexión.

Este funcionamiento supone que el navegador ha echado mano de una pequeña base de datos, que tiene entre sus ficheros, y en la que guarda los certificados de las PKIs que da "automáticamente" por buenos. El hecho de que el usuario no haya tenido que hacer nada pone de manifiesto que el fichero con esos certificados **carece de cualquier tipo de control de integridad o que, de tenerlo, éste es de naturaleza puramente software e independiente**. En ambos casos, cualquier aplicación que pudiese tener acceso al fichero con los certificados que constituyen "el credo" del navegador, podría cambiar los auténticos por otros falsos, o lo que es más divertido para el atacante, podría **incluir otros certificados nuevos (y falsos) que en sus campos humanamente legibles pusiese lo mismo que en los originales a los que suplantán o con los que compiten**. Por mucho que haga el usuario doble clic en cualquier candadito cerrado, éste leerá lo que haya querido que lea el que "amplió o modificó" el credo del navegador.

Hemos visto que, examinando la representación gráfica de una página Web, es humanamente imposible saber si es auténtica o no. Es fácil entender que si vemos un candadito cerrado al pie del navegador, éste no es más que un pequeño

GIF colocado en un rincón de la ventana del navegador; si hacemos doble clic en él, aparecerán unos campos literales contenidos en diferentes certificados digitales, en los que podremos leer cualquier cosa pero que en ningún caso prueban que se trate de un certificado digital auténtico. Por último, **el hecho de que un determinado certificado esté instalado como "fiable" en el credo de un navegador, no supone que el usuario deba confiar en él**, por lo que la cadena de confianza no puede extenderse hasta el usuario final, sino que termina en el fabricante del navegador utilizado.

PCs particulares y sistemas operativos

Supongamos que procedemos correctamente y que un futuro sistema compuesto por un hardware, un software y un usuario común, llegase a establecerse correctamente un canal de comunicación confidencial y con autenticación mutua del tipo SSL; con esto nos quitaríamos de encima los peligros que acechan en la red, aunque todavía nos quedarían los que tenemos "dentro de casa", en nuestro PC.



El hecho de que un determinado certificado esté instalado como "fiable" en el credo de un navegador, no supone que el usuario deba confiar en él, por lo que la cadena de confianza no puede extenderse hasta el usuario final, sino que termina en el fabricante del navegador utilizado.

Un sencillo *keylogger* en software sería capaz de capturar todas nuestras claves simétricas (usuario, cualquier palabra o número clave, matrices de acceso, parámetros bancarios, etc.) tan pronto como las utilizásemos, y transmitirlos en secreto a servidores que ni conocemos, ni sospechamos. Este riesgo nace de la inseguridad del sistema operativo sobre el que se ejecuta la aplicación que invocó el canal SSL, y éste no puede hacer nada para mitigarlo.

Desde hace tiempo el panorama de los PCs particulares ha mejorado en cuanto a su seguridad general se refiere, y eso ha sido gracias a la posibilidad que hay hoy en día de mantenerlos actualizados utilizando las distintas herramientas (automáticas) que traen consigo casi todas las distribuciones de los sistemas operativos. Sin embargo, no podemos olvidar que el PC es una máquina de propósito general, que es propiedad del usuario y que, sin duda, éste la utilizará para navegar por sitios que nada bueno aportan a la seguridad del PC, y que en él se instalarán todo tipo de aplicaciones software bajo el único criterio y saber hacer de su dueño. **Estos hechos son incompatibles con el mantenimiento de la seguridad de cualquier sistema operativo**. Así pues, el sistema operativo de un PC de propósito general, en principio administrado y mantenido por su dueño,

y dedicado a las actividades e intereses normales para cualquier usuario común, **nunca podrá ser considerado como un sistema software seguro**.

La seguridad de una transacción de valor en Internet no deberá depender de la seguridad de los sistemas operativos diseñados para PCs u otros sistemas generalistas porque, en el caso de hacerlo, tarde o temprano, y con mayor o menor impacto, **su inseguridad está plenamente asegurada**. Tampoco mejora el panorama si se utilizan sistemas tradicionalmente considerados como "de alta seguridad" (lectores de huellas palmarias, dactilares, de iris o de retina, tarjetas inteligentes, llaves criptográficas USB, etc.), ya que si el atacante controla total o parcialmente el sistema operativo sobre el que se ejecuta la aplicación de valor, el adversario siempre encontrará el modo de subvertir cualquier hardware periférico que utilizemos, aunque éste sea realmente bueno.

Con este panorama podría pensarse que no es posible utilizar Internet para hacer negocios o para facilitar la vida de los ciudadanos en los temas considerados "serios". Pensar eso sería tan erróneo como lo es pensar que los sistemas actuales son seguros en cuanto a la autenticación de

del servicio que se quiere proteger, los sistemas a utilizar deberían ser estándar y, en parte, independientes (al estilo de la filosofía EDI) de la compañía que realiza las transacciones y el negocio. Si se definiere e hiciese pública la esencia y el contenido de aplicaciones como, por ejemplo, las de banca por Internet, las de comercio electrónico, las que llevan las relaciones de los pacientes con los servicios de salud, las encargadas de las relaciones con las distintas administraciones, etc., para su explotación se podrían utilizar sistemas mixtos software y hardware, a prueba de modificaciones, que fuesen sometidos a revisión pública permanente; esta última característica sería la base real sobre la que establecer la confianza general en el sistema, y no una falsa confianza impuesta.

Esta definición no necesariamente debería ser hecha por todos los agentes del mercado, sino que podría ser realizada por cualquiera de ellos que tuviese capacidad para ponerla en explotación. El hecho de que sus desarrollos o propuestas de estándares fuesen públicos no harían perder negocio a su promotor, ya que su cometido no es principalmente la definición de estándares sino otro muy distinto; sin embargo, ese promotor tendría una posición aventajada por haber sido de los primeros.

En lo que al usuario común se refiere, el hecho de que se construyan con máxima publicidad los sistemas que éste utiliza no aumenta su conocimiento técnico sobre dichos sistemas, pero sí le permite confiar en ellos siguiendo mecanismos que le son más naturales. Si un sistema es abierto y cualquiera puede ver cómo esta hecho y, aún así, funciona, es seguro y lo usa con satisfacción mucha gente, entonces a cualquier ciudadano mínimamente interesado le es razonable pensar que también es aceptable para él, y lo asumirá libremente y con mucha más tranquilidad que en otras circunstancias. Cualquier sistema en marcha que sea una imposición de facto al usuario común puede terminar siendo aceptado, pero el que lo impone debe saber que se queda sólo a la hora del reparto de responsabilidades cuando las cosas vayan mal.

El problema aquí planteado está abierto y su solución es perfectamente posible si se cuenta con la colaboración real y responsable de diferentes agentes (Industria, Administración, Investigación, Academia, etc.) El no solucionarlo y dejar las cosas como están no va a frenar el fraude telemático que ya tenemos, y esto terminará haciendo que la sociedad en general, los usuarios comunes, abandonen irremisiblemente una tecnología que puede hacer mucho bien a toda la sociedad. ■

JORGE DÁVILA MUÑOZ

Consultor independiente y Director Laboratorio de Criptografía LSIIS – Facultad de Informática – UPM jdavila@fi.upm.es

Revisión pública

Dado que, en general, el diseño, el desarrollo, la implementación, la prueba y la puesta en marcha de sistemas de seguridad no suelen ser parte esencial del negocio o de la cadena de valor