>> Jorge Dávila

La guerra por la gestión de identidades y perfiles de usuario en Internet

La posibilidad que tiene un usuario de tener varias identidades distintas en Internet complica bastante la gestión de éstas. Renunciar al uso de pseudónimos abre las puertas a la construcción incontrolada de perfiles de uso y consumo, por lo que se empieza a notar la necesidad de una solución a este problema de gestión de identidades. Microsoft con su *Passport* y un gran número de empresas con la iniciativa *Liberty Alliance*, presentan soluciones enfrentadas pero muy parecidas y, mientras tanto, el usuario final sigue sin tener resuelto el problema. ¿Qué aporta la solución más multitudinaria? ¿Qué diferencias hay entre ambas propuestas?

Con la proliferación de servicios en Internet y con el progresivo y sostenido crecimiento en el número de sus usuarios, la autenticación de estos comienza a ser un tema candente en muchos aspectos. Ya se ha dicho bastante sobre la escasa seguridad de los mecanismos utilizados para tal fin, pero el problema de su gestión desde el punto de vista de los usuarios no ha recibido tanta atención. Para un internauta activo, el número de sitios Web en los que tiene abiertas cuentas empieza a ser una cantidad no despreciable, y en todos ellos tiene que recordar un nombre de usuario y su correspondiente contraseña. Si pretendemos ser cautos y aplicar el principio de compartimentalización, deberíamos utilizar *usernames* y *passwords* diferentes en cada uno de los lugares de la red en los que estamos registrados; sin embargo, eso puede llegar a convertirse en una pesada tarea en la que nuestra memoria (o una clásica libreta azul) tiene que venir en nuestra ayuda. Lo que realmente suele ocurrir es que no se siguen tan recomendables hábitos y los usuarios suelen utilizar la misma identidad en todas partes. Una consecuencia inmediata de este proceder es que se pueden "cruzar" las bases de datos de control de accesos en diferentes sitios y con ello construir *dossiers* que dicen más de nosotros, de nuestras actividades y de nuestros gustos de lo que podemos imaginar.

Este problema técnico no resulta nuevo y ya desde hace bastante tiempo es habitual en las empresas que trabajan con diferentes aplicaciones, cada una de ellas con su propio mecanismo de autenticación de usuarios (¡como debe ser!). Desde la llegada de los mismísimos sistemas operativos multiusuario, un trabajador que debe acceder a varias cuentas y varias máquinas debe recordar cuáles son sus valores de *username* y *password* en cada una de ellas.

La solución de verdad quizá esté en llevar las herramientas de gestión de identidades (pseudónimos) a los equipos propiedad del titular, de tal suerte que queden custodiados por éste. No hay razones técnicas que impidan el desarrollo de esta idea.

Para evitar que en todos los casos se utilicen las mismas identidades y que el compromiso de una cuenta signifique el compromiso automático de todas las demás, éstas deben ser distintas e independientes. En consecuencia, las denominadas técnicas de *single sing-on* han proliferado mucho en las ofertas de sistemas gestores de la seguridad en entornos comerciales.

Con estas herramientas se pretende que la operación de autenticación se haga de una vez por todas y, una vez demostrado que somos quienes somos, poder acceder a todas las cuentas y aplicaciones en las que tenemos derecho y obligación de actuar.

Cualquier entorno comercial es, a fin de cuentas, un entorno controlado y, generalmente, fuertemente jerarquizado, que cuenta con gestores del sistema bien definidos; sin embargo, Internet y el Comercio Electrónico son otra cosa bien distinta. A muchos nos resulta impensable que todos los internautas y prestadores de servicios en Internet vayan a aceptar el arbitraje de un "único" ente central que permitiese, entre otras cosas, montar un sistema de *single sing-on* universal; ante él deberíamos demostrar nuestra identidad y automáticamente se abrirían todas las cuentas que tenemos con nuestros diferentes proveedores de servicios.

Un sistema como ese, al actuar como nuestros "presentadores" ante los lugares en los que estamos inscritos, tendría la habilidad de, entre otras cosas, poder suplantarnos en todos aquellos servidores en los que desarrollamos nuestra existencia cibernética. Así pues, o cargamos con un montón de identidades diferentes, libre y secretamente elegidas por nosotros, o aceptamos que alguien actúe como nuestro "introductor de embajadores" o "ciber-secretario personal" y nos ponemos en sus manos en lo que a nuestra seguridad frente a la suplantación se refiere. El problema es sencillo y, sin embargo, las supuestas soluciones propuestas no lo son.

Hasta el momento sólo se han presentado dos grandes modelos para resolver este problema. Por una parte tenemos la iniciativa universalista de Microsoft a través de su sistema **Passport**[1] y por otra, la de "todos los demás", que ha sido pomposamente bautizada como **Liberty Alliance**[2].

Resulta curiosa esta dicotomía tan poco balanceada, que puede entenderse como "Microsoft contra el mundo" o "el mundo contra Microsoft". Por las fechas en las que aparecen cada una de las iniciativas, más bien estamos ante la segunda interpretación y no ante la primera, ya que fue Microsoft el primero en lanzar el tema a la arena comercial.

Esencialmente, el sistema Passport de Microsoft pretende simplificar la vida a sus subscriptores, relevándolos de la gestión de sus cuentas en diferentes sitios Web comer-

ciales e incluso les lleva su cartera facilitándoles los pagos que puedan realizar en distintos Webs de comercio electrónico. El sistema Passport nos ofrece una especie de mayordomo en la red que se va a encargar de ir abriendo las puertas de todos aquellos sitios en los que nos registremos, encargándose también de guardar todos los números de tarjetas de crédito que vamos a ir utilizando en nuestras compras. Además, este "pasaporte" lo podremos utilizar desde cualquier punto de Internet, ya que toda su seguridad se basa en nuestra autenticación *username/password* (que es muy débil y arriesgada) frente al servidor passport.net.

La idea parece muy cómoda pero, sin embargo, ha recibido muchas críticas empresariales en cuanto a su seguridad y a que pueda suponer un atentado en contra de la libre competencia.

La otra iniciativa, **Liberty Alliance**, pretende ser algo más colectivo y cooperativo que el modelo Microsoft. Esta alianza ha hecho pública una especificación técnica, bastante completa, de un conjunto de protocolos que colectivamente pretenden dar solución a la gestión federada de la identidad en Internet, a la autenticación inter-dominios, y a la gestión de sesiones Web. Esta definición también incluye otros esquemas útiles para el establecimiento de acuerdos entre los participantes comerciales adscritos a ese sistema.

Las "redes federadas de identidad", según sus promotores, constituyen la clave para poner en marcha nuevas taxonomías y oportunidades comerciales. En ese mundo de comerciantes y empresarios federados, la identidad *online* del consumidor, su perfil personal, sus configuraciones personalizadas, sus hábitos de consumo e historial, y sus preferencias a la hora de comprar serían administradas, en principio, por el usuario y "compartidas" con aquellas organizaciones que él haya elegido[3].

La arquitectura de la alianza reconoce a tres actores principales: el usuario de a pie, el proveedor de identidad y el de servicios. El usuario tiene una identidad dada por el proveedor de identidades que le sirve para obtener los servicios que le son propios ante el prestador de servicios. Una vez que los usuarios se autentican ante su proveedor de identidad, éste genera una prueba de autenticidad que es enviada antes y es reconocida por el proveedor de servicios.

La alianza promueve el establecimiento de "federaciones" entre proveedores de identidad y de servicios para que funcione el sistema. Dentro de esta iniciativa se reconocen cuatro protocolos principales: (1) el de *Single Sign-On* y *Federación*, (2) el de *Registro de Nombres* (protocolo en el que el proveedor de servicios puede registrar un descriptor "opaco" de su usuario reconocido), (3) el de *Terminación de una federación* (protocolo en el que un proveedor notifica a otro de que el reconocimiento de una identidad deja de cursar efecto) y, por último, (4) el de *Single Log-out* (protocolo con el que los proveedores notifican a otros los eventos de *log out* del usuario).

En este esquema, los proveedores de identidad asignan a sus usuarios unos *identificadores de nombre* que serán aceptados por todos los servidores (proveedores) federados con él[4]. Estos identificadores se construyen con valores pseudo-aleatorios que, en principio, no pueden ser relacionados por nadie con el usuario a excepción, claro está, del proveedor de identidad que los fabrica. Este proceder no es otra cosa que utilizar meros pseudónimos generados y gestionados por el proveedor de identidad. Del mismo modo, en el momento de la federación, el proveedor de identidad genera otro identificador opaco a favor del proveedor de servicio y ambos los relaciona en el proceso de autenticación mutua.

La tendencia a proponer sistemas basados en intermediarios o tutores quizá esconda otros interes relacionados con la confección de estadísticas de uso y perfiles de consumo.

A la vista de todo lo anterior, la propuesta de la Liberty Alliance tan sólo modifica, en lo esencial, el hecho de que en la iniciativa de Microsoft es esta empresa la única que conoce todas las identidades del sistema, cosa que "todos los demás" no quieren aceptar. A fin de cuentas, tal dualidad de modelos sólo parece ser un intento más de que Microsoft reparta el pastel con los demás actores del teatro informático, pero no hay ninguna razón técnica significativa, de seguridad o intimidad, que haga preferir a los usuarios de a pie una opción respecto a la otra.

Ambos sistemas se basan en la delegación de la identidad de usuario a los servidores de Microsoft o a los de la Alianza, por lo que el usuario está otorgándoles las capacidades necesarias para actuar en su nombre y monitorizar todas sus actividades de autenticación en Internet.

Muchos usuarios, por el tipo y frecuencia de sus actividades, verán ventaja en quitarse de encima la carga de conocer y administrar sus identidades a pesar de entregarle a alguien su identidad, y confiarán que les protejan los contratos de prestación de servicios que firmen con sus proveedores de identidad. Para otros tal riesgo no podrá ser asumido y seguirán custodiando y administrando su identidad en la red.

Estas soluciones, en realidad, no lo son. Aunque estos sistemas no propagan el valor del par *username/password* a terceros (identidad estricta), atentan contra el principio básico de que el titular es agente único de lo que su identidad le permite, ya que en ambos esquemas se delega el ejercicio de las potestades del titular a los servidores de la Alianza o a los de Microsoft.

La solución de verdad quizá esté en llevar las herramientas de gestión de identidades (pseudónimos) a los equipos propiedad del titular y custodiados por este, y facilitar ahí su uso. No hay razones técnicas que impidan el desarrollo de esta idea, por lo que la tendencia a proponer sistemas basados en intermediarios o tutores, como ocurre con los anteriores, quizá esconda otros intereses relacionados con la confección de estadísticas de uso y perfiles de consumo. Todavía queda mucho que hacer para poder "ser" en Internet. n

Jorge Dávila Muro
Director
Laboratorio de Criptografía
LSSI – Facultad de Informática – UPM
jdavila@fi.upm.es

1 http://www.passport.net/Consumer/Default.asp?lc=3082
2 http://www.projectliberty.org/
3 Esto salvaría el principio de libre competencia y desbancaría el pretendido monopolio de Microsoft. Sin embargo, no cambia en nada la desproporción contractual entre el usuario individual y los proveedores empresariales.
4 Este procedimiento lo que implementa en la Red es el viejo modelo de los "clubes privados" en los que los socios se inscriben y el club los representa ante un conjunto de servicios y proveedores.