

# Robo de identidad, soluciones multifactor y teléfonos móviles

El uso generalizado del teléfono móvil lo hace el instrumento idóneo para la generación de claves dinámicas que garanticen el proceso de autenticación e identificación personal.



Luis del Ser Toral  
Socio Director de  
Movilok Interactividad Móvil

El 'robo de identidad', es una forma antigua de delito que consiste en que un delincuente recolecta, por distintos medios, datos suficientes como para usurpar la identidad de la víctima ante servicios o instituciones con los que puede realizar operaciones o transacciones. En realidad el término 'robo de identidad' no es estrictamente correcto, ya que la identidad no es algo que pueda robarse o perderse y el delito real es el fraude debido a la usurpación de la identidad de otro individuo.

El desarrollo de servicios a través de Internet y el desarrollo del comercio electrónico dentro de la sociedad, conlleva la necesidad de desarrollar mecanismos de identidad digital: necesitamos identificarnos a través de Internet o en los cajeros automáticos ante nuestro banco, nuestro operador, nuestro supermercado, nuestra agencia de viajes, etc. Por este motivo, el "robo de la identidad digital" utilizando la tecnología (lectores ocultos de bandas de tarjetas, detectores de pulsaciones de teclado, etc.) junto con prácticas denominadas de 'Ingeniería Social' está tomando un nuevo auge en relación con el uso de servicios: El delincuente suplanta a su víctima ante los servicios con alguna finalidad fraudulenta, como conseguir dinero de su cuenta bancaria, cargarle una compra no realizada, hacer uso no autorizado de la copia de respaldo de su agenda de teléfonos guardada un servidor on-line, etc.

El importe de las operaciones fraudulentas no es todavía muy considerable a nivel de cifras absolutas, pero su cifra aumenta mes a mes y con ello se va extendiendo un problema aún mayor: el sentimiento de que los terminales y las redes de datos que dan soporte a los servicios no son

seguras para la realización de transacciones.

Este aspecto empieza a ser especialmente preocupante es España, que llegó a ocupar el tercer puesto mundial en fraude a través de Internet en 2006. Concretamente, el sector de las entidades financieras concentró el 89,7% de los ataques recibidos en diciembre de ese año (fuente: Antiphising Working Group)

Identificar correctamente al usuario que accede a un servicio o a alguno de sus elementos es uno de sus aspectos más críticos, dado que puede comprometer e invalidar el resto de medidas de seguridad que se tomen para proteger ese servicio.

El 'robo de identidad' pone de manifiesto la importancia de los datos personales que nos identifican, porque pueden utilizarse por terceros para suplantarnos en el uso de los servicios electrónicos.

Las contramedidas más habituales es la utilización de alguno de los denominados 'factores':

- La utilización de algo que el usuario conoce (una contraseña)
- La utilización de algo que el usuario posee (una llave, una tarjeta magnética)
- La presentación de que el usuario es (una identificación biométrica)

Es habitual encontramos con accesos a servicios, sistemas o recintos mediante contraseñas, llaves o tarjetas. Su uso está muy generalizado y su principal desventaja se debe a que la suplantación de la identidad se consigue fácilmente con la posesión de ese único elemento de identificación.

Los servicios que se apoyan en este modelo en realidad descargan en el usuario la responsabilidad de 'no perder la identidad' ligándola a lo bien o mal que mantenga en secreto sus contraseñas de acceso a los servicios

Luis del Ser Toral



Socio director y co-fundador de Movilok Interactividad Móvil, empresa especializada en el desarrollo de tecnología móvil interactiva y en productos innovadores apoyados en la movilidad y datos.

Es Ingeniero de Telecomunicación por la ETSIT de la UPM en las Áreas de Telemática y Comunicaciones y Especialista en Dirección y Administración de Empresas por la UPM Madrid.

y a 'no perder de vista' su tarjeta magnética.

La identificación a partir de un rasgo biométrico propio (nuestro iris, huella dactilar o la palma de nuestra mano) ofrece una alta seguridad pero también adolece de una importante desventaja: supone un procedimiento de identificación radicalmente distinto por lo que es todavía necesario educar a los usuarios en su utilización antes de poder conocer realmente si éstos lo aceptan finalmente de forma generalizada.

La seguridad puede incrementarse de forma notable si se utilizan de forma combinada alguno de los factores anteriores en lo que se denomina autenticación multifactor. Lo habitual es combinar dos de los factores: un PIN secreto junto con un generador de claves para obtener contraseñas cambiantes para cada acceso del usuario, una contraseña junto con la lectura del iris o de la huella dactilar, etc.

Aunque las soluciones multifactor son mucho más seguras que las de un único factor, el éxito en su difusión dependerá también de otros elementos no técnicos;

- **Facilidad de uso.** Para que el mecanismo de autenticación sea efectivo, debe poder ser aplicable en circunstancias muy distintas, que tengan en cuenta la operativa real de los usuarios en su entorno y en la Sociedad de la Información.
- **Capacidad *disuasoria*.** Debe ser lo suficientemente complejo para disuadir a atacantes casuales y para retrasar lo suficiente a los posibles atacantes profesionales de forma que éstos puedan ser detectados y se tomen contra ellos las medidas adecuadas.
- **Riesgo Balanceado.** Un mecanismo de autenticación tiene éxito en la medida en la que los dos extremos (proveedor del servicio y usuario del servicio) pongan su máximo interés en proteger lo que consideran importante para mantener la seguridad.
- **Experiencia consistente de acceso.** Es necesario que los usuarios conozcan y acepten el mecanismo de acceso. Cuanto más parecido sea a los actuales de un único factor, es más posible que sea aceptado y utilizado con éxito.

## La seguridad puede incrementarse notablemente con la autenticación multifactor

La solución de factor-2 más extendida en el mercado está basada en la generación de contraseñas dinámicas: cada vez que un usuario desea acceder al servicio, sistema o máquina, genera una contraseña válida para el siguiente uso a partir de los elementos:

- Algo que él sólo conoce y que mantiene en secreto: un PIN
- Algo que sólo él posee: un generador de claves específico de ese usuario (un token)

El funcionamiento es muy sencillo, el usuario introduce su PIN secreto en el dispositivo token que posee utilizando para ello su teclado. El token genera la contraseña de forma local y la presenta en su pantalla para que el usuario pueda utilizarse en el siguiente acceso.

La principal ventaja es que con este mecanismo de token factor-2 el acceso no cambia básicamente respecto al más utilizado en la actualidad: una contraseña. La única diferencia es que esta contraseña es variable. El usuario tan solo tiene que utilizarla en el siguiente acceso y una vez utilizada dejará de ser válida. No tiene por qué preocuparse de si es observado o si alguien se la copia, porque una contraseña utilizada ya no es válida.

Hay distintos esquemas para la generación de estas contraseñas permitiendo incluso que éstas caduquen en un tiempo si no se consumen en un tiempo razonable después de su generación.

La mayor parte de las soluciones del mercado utilizan un dispositivo hardware específico para la genera-

La principal diferencia de este mecanismo multifactor, es que la contraseña es variable. Una vez utilizada dejará de ser válida

Sólo se hace uso de la capacidad de cálculo del teléfono móvil, por lo que la contraseña nunca viaja al exterior del teléfono

## Para generar la contraseña sólo hay que teclear el PIN secreto en la aplicación

ción de claves. Este dispositivo funciona como una calculadora por lo que su uso es muy sencillo: se introduce en PIN por el teclado y presenta en su pantalla la contraseña.

La solución es muy segura, pero adolece de una desventaja de uso: supone llevar encima 'un dispositivo más'. Esto hace que no pueda considerarse una solución generalizable para todas las situaciones y que en la práctica su uso actual se aplique como solución de acceso a recursos corporativos en las empresas o con clientes tipo 'vip' de determinados servicios.

En nuestro intento de aprovechar las muchas ventajas de las soluciones token factor-2, hemos desarrollado una solución de autenticación que utiliza como generador de claves algo que todos (y de forma ya universal) llevamos encima en nuestra vida diaria: nuestro teléfono móvil.

Mediante una aplicación software que se instala en el teléfono y que se activa de forma personal para cada usuario, éste puede utilizarse para generar claves dinámicas:

- Introducimos por el teclado del teléfono nuestro PIN secreto (asignado por el proveedor del servicio)
- La aplicación en el teléfono genera (de forma local) la contraseña y la presenta en la pantalla para que la utilicemos donde sea necesario.
- El usuario lee esta contraseña de la pantalla de su teléfono y la in-

## El uso de soluciones factor-2 está aceptado por las empresas como solución segura

troduce en el sistema o servicio al que desea acceder.

Cabe resaltar que a pesar de utilizar nuestro teléfono móvil sólo se hace uso de su capacidad de cálculo: la contraseña se genera de forma local y nunca viaja al exterior del teléfono. Esto permite generar claves en cualquier situación independientemente de la cobertura.

Esta solución sería aplicable en una de las situaciones cotidianas en las que más se centran los 'amigos de la identidad ajena': los cajeros bancarios. Si en lugar de utilizar siempre la misma contraseña al sacar dinero de un cajero automático pudiéramos introducir uno válido solamente para ese acceso, cesaría el interés de terceros con oscuras intenciones por capturar ese PIN ya que no podría volver a ser utilizado con posterioridad de forma fraudulenta.

Entre las principales ventajas de este enfoque destacan:

- **Facilidad de uso:** En nuestra vida diaria actual siempre tenemos nuestro teléfono móvil a mano para poder generar la contraseña siguiente allí donde lo necesitemos. Para generar la contraseña sólo hay que teclear el PIN secreto en la aplicación y ver la contraseña en la pantalla del teléfono.
- El uso de soluciones factor-2 está aceptado por las empresas como solución segura para la autenticación; la flexibilidad que aporta el teléfono móvil hace que pueda ser aplicable de forma generalizada en los servicios hacia los clientes.
- El teléfono móvil es un dispositivo personal y aceptado, es 'nuestro teléfono móvil' y cada vez podemos utilizarlo en más contextos. Por este motivo el interés del usuario en manejar de forma responsable su teléfono está garantizada.
- **Uso consistente con el actual:** La interacción con el cajero automático no varía, por lo que no es necesaria ningún tipo de formación ni cambio de uso de los usuarios clientes.

Una ventaja adicional, para la entidad bancaria, es que esta solución no requiere modificaciones en el propio cajero: el usuario continúa introduciendo su contraseña de forma habitual como lo hace actualmente. 