

Debemos evitar
que la seguridad
de accesos termine
simplemente en esto...

Llaves Electrónicas vs. PKI/OTP

para Validación de Usuarios

No cabe duda que uno de los principales inconvenientes que enfrenta la gente de seguridad informática es el asociado con la necesidad de poder validar el acceso de los usuarios a aplicaciones críticas por medio de algún método fuerte.

Lo que se pretende es garantizar que no existan "robos de identidades" como sucede habitualmente, sobre todo desde que se han masificado las aplicaciones a través de Internet.

La Norma ISO 17799, en particular, tiene un capítulo dedicado a las recomendaciones respecto de este tema donde se habla de la necesidad de una "Validación FUERTE por DOS FACTORES", como por ejemplo "Algo que tengo" y "Algo que conozco".

Existen distintas tecnologías para lograr mejoras en los niveles de seguridad en la validación de accesos y de la identidad de usuarios, tales como esquemas PKI (usando Certificados Digitales) o dispositivos de generación de claves aleatorias tipo ONE TIME PASSWORD (OTP), pero por lo general son soluciones costosas y que requieren largos plazos para su implementación.

En el caso de PKI, para que realmente se esté validando la identidad de un usuario es necesario

contar con un dispositivo como las llaves criptográficas (tipo iKey, por ejemplo) para proteger y transportar los certificados digitales de los usuarios. Además hay que contar con dispositivos tipo HSM (Hardware Security Module) para proteger el certificado raíz en el lado servidor, así como costosas licencias de software para generar, validar y administrar los certificados digitales emitidos, sus bajas, revocaciones o renovaciones.

En el caso de los esquemas de OTP, también hacen falta dispositivos especiales para los usuarios remotos que generan la "clave aleatoria" y costosas licencias de software para el lado servidor.

Tanto en los esquemas de PKI como en los de OTP,

hay que tener en cuenta que además de los costos de la puesta en marcha luego hay que enfrentar altos costos anuales en abonos de mantenimiento, cambios de dispositivos, renovación de licencias o certificados digitales, y además contar con una estructura interna de especialistas para mantener ésto funcionando en el tiempo.

En la gran mayoría de las instalaciones o aplicaciones donde se necesita una "validación fuerte" de acceso de usuarios, se tiene un acuerdo entre partes respecto a los elementos que se utilizan para esta validación, con lo cual se puede optar por opciones más simples de implementar y de menor costo.

El "Administrador de Passwords" es una especie de SSO (Single Sign-ON), que permite el almacenamiento y administración de passwords, de forma tal que no haga falta recordar las passwords de los sitios y aplicaciones de uso habitual, ya que con sólo insertar la llave HARDkey MIO y el ingreso de su PIN se completará automáticamente estos datos.



El "Disco Privado Virtual Cifrado" permite mantener segura la información almacenada en el disco rígido de una PC o Notebook. Genera una unidad virtual que se puede mapear como una letra más, y todos los datos almacenados en dicha unidad sólo estarán disponibles cuando se inserte la llave de habilitación HARDkey MIO y el ingreso de su PIN. Esta solución permite proteger información confidencial contra robos de equipos o usos no autorizados.

Dentro de las opciones más simples, pero a su vez no tan difundidas, para cumplir con requisitos de "Validación Fuerte por dos Factores de Usuarios" se encuentran las "llaves electrónicas USB" como las HARDkey. Con las HARDkey es posible armar esquemas de validación de accesos de usuarios donde se utilice la llave HARDkey como el "elemento físico" que cumple con lo de "Algo que tengo" y utilizar un PIN o PASSWORD para la parte de "Algo que conozco".

Una de las principales ventajas que tiene el uso de las llaves HARDkey respecto de otros métodos, es la simplicidad de su implementación y la excelente relación COSTO – BENEFICIO que brindan. Para su implementación en cualquier aplicación basta con incorporar unas pocas líneas de código, para que se pueda detectar la presencia de las llaves obteniendo su número de serie o ID, y leer o grabar datos en su memoria como elemento adicional si se desea mejorar el nivel de seguridad.

Otra de las ventajas es que no es necesario invertir en un software costoso, o licencias para el lado servidor de la aplicación, ya que todo lo necesario para la implementación se entrega sin cargo en la primera compra de llaves dentro del KIT DE DESARROLLO (o SDK).

Para algunos usuarios especiales se puede mejorar el nivel de seguridad por medio de uso de un esquema de "password aleatoria o dinámica" que se puede almacenar en la memoria de la llave, y cambiarla cada vez que el usuario se conecta a las aplicaciones, generando de esta forma algo equivalente a un ONE TIME PASSWORD (OTP).

Con las HARDkey se logra una "solución escalable" donde en una primera instancia se puede implementar simplemente chequeo de la presencia de la llave y la validación de su número de serie o ID

contra una base de datos, en reemplazo de todo acceso a aplicaciones con USUARIO y PASSWORD. Ésto es sólo un primer paso, pero resuelve los principales problemas de seguridad para la gran mayoría de los usuarios.

Se puede dejar para una segunda etapa la incorporación, para los usuarios más críticos, de otros tipos de controles adicionales más elaborados que los mencionados anteriormente.

De esta forma se divide en etapas el proyecto total, dejando la implementación de estas opcio-

nes más elaboradas para más adelante permitiendo incluso repartir en el tiempo la carga de trabajo que implican la implementación y puesta en marcha de todo esquema de seguridad.

En el caso de las llaves HARDkey MIO (modelo de llaves electrónicas con 4 Kbytes de memoria y PIN de acceso) también se puede incorporar en una segunda etapa un CSP (Cryptographic Service Provider) para almacenar certificados digitales en su memoria, permitiendo protegerlos y transportarlos.

Incluso en un futuro, para ciertos usuarios, se

Para cualquier esquema donde se use una validación de acceso con USUARIO y PASSWORD, es muy sencillo mejorar su seguridad incluyendo el chequeo de una llave HARDkey para identificar el acceso a las aplicaciones u operaciones críticas que necesiten la garantía que la persona que las realiza es quien tiene la llave HARDkey de habilitación y conoce su PIN o PASSWORD.

Normalmente en toda implementación existen distintos niveles de requisitos, y sólo un grupo reducido de usuarios necesitan altos niveles de seguridad, y para la gran mayoría bastará con la posibilidad de validar su identidad por medio del chequeo de la presencia de una llave HARDkey, y el ingreso de su PIN.



puede incorporar a las llaves HARDkey MIO la integración a otras soluciones como las contenidas en la HARDkey MIO Security Suite, que utilizando este esquema de validación fuerte por medio de las llaves electrónicas, permiten proteger el acceso a la información almacenada en las PCs contra accesos no autorizados.

La HARDkey MIO Security Suite contiene tres módulos principales: un "Control de LOGON a la PC", un "Administrador de Passwords" y un "Disco Privado Virtual Cifrado".

Respecto de casos de éxito podemos citar: Telefonía de Argentina, Automotora Gildemeister (Chile), Mercado de Valores de Mendoza, y Mercado Abierto de Buenos Aires, por ejemplo, que ya han implementado las HARDkey para la validación de accesos de usuarios.

La clave de este tipo de soluciones es obtener una propuesta escalable, siempre bajo el concepto de "todo con una sola llave", y lograr rápidamente en una primera etapa accesos seguros por medio de una "Validación Fuerte de Dos Factores": "algo que tengo" una llave HARDkey y "algo que conozco" su PIN, y en el futuro incorporar medias de seguridad adicionales para los usuarios que sean necesarias. ■

El "Control de LOGON a la PC" permite reemplazar el logon estándar de Windows por la detección de la presencia de la llave HARDkey MIO y el ingreso de su PIN, y luego se completa automáticamente el nombre de usuario y password leyéndolos de la memoria de la llave HARDkey MIO. Ésto permite utilizar "passwords fuertes" (largas y con caracteres raros) ya que no hay que recordarlas ni tipearlas.

