HARDkey – La mejor alternativa a esquemas de PKI /OTP para Validación de Accesos 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 17799/27001, 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".

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

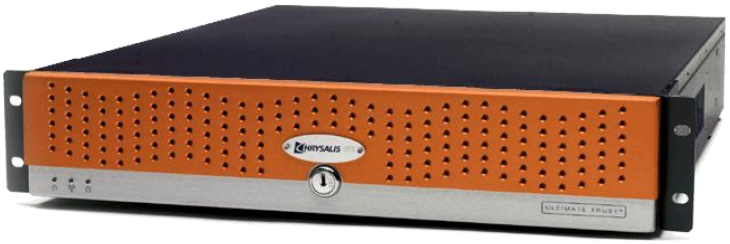
Existente distintas tecnologías para lograr mejoras en los niveles de seguridad en la validación o autenticación de accesos y de la identidad de usuarios, tales como esquemas PKI (usando Certificados Digitales) o dispositivos de generación de claves aleatorias tipo ONE TIME PASSWORD (OTP), pero por lo 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.

Si estos certificados se dejan, como ocurre por defecto, en el repositorio de certificados en el disco fijo de una computadora, cualquiera que conozca la password con la cual están protegidos puede utilizarlos. Esto sería equivalente a dejar una chequera bancaria o un block de hojas firmadas en blanco guardadas en un cajón, el que tenga acceso a ese cajón podrá completar los cheques o las hojas firmadas en blanco y vaciarnos nuestra cuenta bancaria o hacer lo que quiera con notas "supuestamente" firmadas por nosotros.

Además en los esquemas de PKI para poder ser una Autoridad Certificante "homologable" en Argentina por la ONTI (Oficina Nacional de Tecnologías de la Información) se debe contar con dispositivos tipo HSM (Hardware Security Module, como el LUNA SA) para proteger el certificado raíz en el lado servidor.

Llaves "iKey"



Equipo LUNA SA (HSM)

Si no se tiene la tecnología para generar, validar y administrar los certificados digitales emitidos, y controlar sus bajas, revocaciones o renovaciones, también hace falta contratar a empresas como VERISIGN para que nos brinden el asesoramiento, capacitación y Know – How para implementar un esquema PKI, debiendo pagar altos costos por licencias, costos de certificados y renovación anual de los mismos. También hay que contemplar varios meses para la puesta en marcha de un esquema PKI.

En el caso de los esquemas con dispositivos de generación de claves aleatorias (OTP) son necesarios dispositivos especiales para que los usuarios remotos puedan identificarse contra el servidor .

También hacen falta capacitaciones y costosas licencias de software para el lado servidor.

Dispositivos OTP

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 dispositivos, renovación de licencias o certificados digitales, y además contar con una estructura interna de especialistas para mantener esto 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.

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 primer compra de llaves dentro del KIT DE DESARROLLO (o SDK).

En 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.

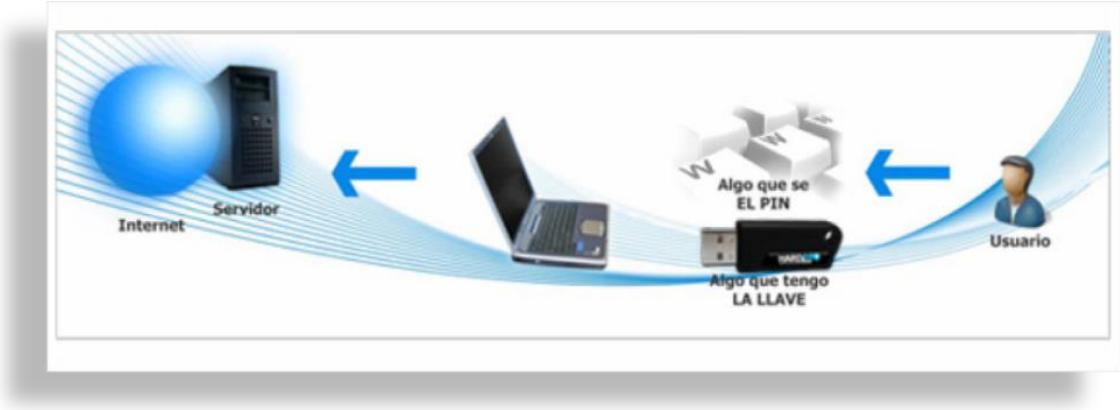
Control de acceso a sección de soporte

Autenticación segura de admistradores

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).

Un ejemplo de implementación para destacar es el de TELEFONICA DE ARGENTINA, ellos en el año 2003 quisieron certificar la Norma ISO 17799/27001 para un data center donde unos 200 operadores manejaban las tarifas de sus clientes principales con un “simple” esquema de usuario y password.

La empresa que hizo la auditoría para esta certificación, les objeto este “endeble” esquema de seguridad para una aplicación tan crítica como esa, y debieron analizar alternativas para mejorar la seguridad.



Evaluaron las tres tecnologías mencionadas en esta nota:

(1) Utilizar un esquema de PKI con tokens criptográficos para los 200 usuarios.
Con un costo del orden de los U$S 120.000, entre licencias, capacitación, certificados y tokens, y una implementación en un plazo 4 o 5 meses.

(2) Utilizar dispositivos tipo OTP, con un costo también en el orden de U$S 120.000, entre licencia servidor, dispositivos, capacitación, etc. y un plazo de implementación de 3 a 4 meses.

(3) Utilizar las llaves HARDkey, para que cada operador se valide contra una aplicación de login especial con la presencia de su llave HARDkey más su PIN, logrando una autentificación por dos factores: “algo que tengo” la llave y “algo que conozco” su PIN. Con un costo estimado de U$S 4.000 a U$S 5.000 para los 200 puestos.

Obviamente, ante semejante diferencia de presupuesto decidieron analizar en profundidad la opción de HARDkey, y con nuestra asistencia en pocas horas, lograron hacer satisfactoriamente las primeras pruebas, y en menos de una semana tenían todo el esquema funcionando.

En el momento de definir que tecnología aplicar, optaron por elevar al directorio las tres opciones para que decidieran por cual optar, donde obviamente a la gente de finanzas les llamó la atención la gran diferencia entre los costos entre las dos primeras opciones y la última. Y cuando preguntaron cuanto tiempo tardaban en evaluar la opción de HARDkey, se encontraron con la respuesta de los técnicos de que ya estaba funcionando esta opción dado que se trataba de una alternativa novedosa y tuvieron que dedicarle una semana para evaluarla y dada la facilidad de implementación de la solución la dejaron funcionando.

Con lo cual no cabe duda porque opción se inclinó el directorio, y lograron certificar la Norma ISO 17799/27001 utilizando las HARDkey con una implementación en tiempo record y con un presupuesto muy económico.

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. Esto 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 como los mencionados anteriormente.

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

Respecto de otros casos de éxito podemos citar: Automotora Gildemeister (CHILE), MERCADO DE VALORES DE MENDOZA, BANELCO y MERCADO A TERMINO DE BUENOS AIRES (MATBA).

www.MATBA.com.ar

En el caso de MATBA tienen un servicio por internet para que sus operadores puedan “firmar digitalmente” operaciones en forma remota. En una primera etapa implementaron la validación del acceso de los operadores con el simple chequeo de la presencia de una llave HARDkey del lado remoto, y luego en una segunda etapa han incluido, para mejorar la seguridad, el almacenamiento de la “clave privada” de un certificado digital dentro de la llave HARDkey, y la utilización de esto para la firma de de boletos de compra venta.

Sin duda la utilización de las llaves HARDkey para autenticación o validación de acceso de usuarios a aplicaciones o sitios web es la mejor alternativa por su excelente relación COSTO – BENEFICIO y su rápida implementación.

Con solo agregar unas pocas líneas de código en cualquier aplicación se puede lograr una “Autenticación Fuerte de Accesos de Usuarios por Dos Factores”, cumpliendo con los requisitos de la Norma ISO 17799/27001, mejorando la seguridad de acceso reemplazando o cumplimentando el uso de usuario y password.

Esto es aplicable no solo para páginas o sitios web que manejen información restringida para usuarios VIPs o especializados, sino también para cualquier aplicación contable, industrial o de gestión en general donde se desee restringir el acceso a operaciones sensibles a los usuarios que se autentiquen por medio de un elemento físico como son las HARDkey.

Una de las aplicaciones principales de esta autenticación con HARDkey es sin duda la validación de acceso de los “administradores” de las aplicaciones, para evitar que cualquiera que consiga su usuario y password pueda realizar operaciones críticas sin autorización y terminar con la “integridad” de los sistemas. Otros caso son los técnicos o responsable del mantenimiento de los sistemas, que por lo general tienen accesos sin controles para realizar operaciones correctivas.

La implementación de las llaves HARDkey permite transformar en “tangible” la seguridad de acceso y mejorar con muy poco esfuerzo los endebles esquemas de usuario y password de los sistemas y aplicaciones web.