TOKENS DE SEGURIDAD

Keitling Daysi Salinas Hinojosa
Universidad Mayor de San Andrés
Carrera de Informática
Análisis y Diseño de Sistemas
kd_salinas_hinojosa@hotmail.com

RESUMEN

La mayor parte de los sistemas informáticos y redes mantienen de uno u otro modo una relación de identidades personales asociadas normalmente con un perfil de seguridad, roles y permisos.

La falta de supervisión sobre esas aplicaciones y los *tokens* de seguridad empleados pueden significar que una aplicación indeseable de un tercero tenga acceso a los servicios de nube de una compañía, lo que puede conducir a más incidencias en cuanto a datos comprometidos.

Cabe mencionar que entre los principales Tokens de Seguridad se tiene a los *Tokens* OTP y *Tokens* USB.

PALABRAS CLAVES

Token de seguridad, *tokens* OTP (*One-TimePassword*), *tokens* USB, *password*.

1. INTRODUCCION

Los sistemas tradicionales de autenticación utilizan nombre de usuario y contraseña para autenticar pares de usuarios. Esto proporciona una seguridad mínima, ya que muchas contraseñas de usuario son muy fáciles de adivinar.
Ahora dado estos últimos acontecimientos no favorables para la seguridad existe como una opción de ALTO nivel lo que es los Tokens de seguridad cuyo objetivo principal es brindar mejor autentificación, además que los servicios ofrecidos para este dispositivo electrónico establece una relación de confianza entre un cliente y un proveedor de servicios web, a continuación el tema mencionado se presentara mas desarrollado, complementando que es muy interesante y comprensible.

2. MARCO TEORICO

2.1. *TOKEN* DE SEGURIDAD

Definición.- Un *token* de seguridad (también *token* de autenticación o *token* criptográfico, Ver Figura 1) es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Figura 1. *Token* de seguridad.

Es el dispositivo de seguridad utilizado para firmar digitalmente y cifrar mensajes. Tiene un Nivel de Seguridad ALTO, siendo el portador de la llave del usuario para acceder los servicios prestados que requieren Certificados Digitales. Este combina las funcionalidades de una tarjeta inteligente y su lectora en un *hardware* en uno solo; es fácil de manipular, seguro y se puede trasladar a cualquier parte del mundo.
Existe más de una clase de *token*. Están los bien conocidos generadores de contraseñas dinámicas "OTP" (*One Time Password*) y la que comúnmente denominamos tokens USB los cuales no solo permite almacenar contraseñas y certificados, sino que permiten llevar la identidad digital de la persona.

2.2. PRINCIPALES *TOKENS*

2.2.1. *TOKENS* OTP (*ONE TIME PASSWORD* O *PASSWORD* DE UN SOLO USO)

La autenticación con contraseña de un solo uso u OTP (del inglés *One-Time Password*, Ver Figura 2) es una variación de la autenticación con usuario/contraseña. En este método de autenticación se dificulta el acceso no autorizado haciendo que cada contraseña sea válida para una única sesión. Se tiene que usar una contraseña nueva para cada sesión. De esta forma se imposibilita que un atacante que capture el usuario y la contraseña usada, la pueda reutilizar. También hace al sistema más resistente frente ataques de fuerza bruta ya que cada vez que cambia la contraseña los intentos realizados anteriormente para romper la anterior contraseña no sirven para nada y hay que empezar desde cero.

Los sistemas de generación de passwords de un solo uso basados en *hardware*, tradicionalmente usados por la banca privada, ya están al alcance de todo el mundo para mejorar la seguridad en la red.

Figura 2. Ejemplo de tokens OTP (*One-Time Password)*

2.2.1.1. *PASSWORD* (CONTRASEÑA)

Una contraseña o clave (en inglés *Password*) es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.

2.2.2. *TOKENS* USB

Los *tokens* USB son *tokens* electrónicos que tienen un tamaño pequeño que permiten ser cómodamente llevados en el bolsillo o la cartera y son normalmente diseñados para atarlos a un llavero (Ver Figura 3). Los *tokens* electrónicos se usan para almacenar claves criptográficas como firmas digitales o datos biométricos, como las huellas digitales. Algunos diseños se hacen a prueba de alteraciones, otro pueden incluir teclados para la entrada de un PIN.

La familia de *Token* USB de Macroseguridad ofrece una amplia gama de soluciones, desde un dispositivo con el chip con mejor relación coste-beneficio hasta la más reciente innovación que contiene un chip de smartcard de 32 bits de alta performance. Además del innovador *Token* USB que se integra con Biometría, denominado BioPass3000 *Token* USB, la llave interactiva USB con funciones de audio o display, el combo USB Flash + PKI, y así como también la llave que combina la tecnología OTP con PKI.

Figura 3. Un ejemplo de *Tokens* USB y una breve descripcion de a lo que se puede acceder usando este dispositivo.

2.2.2.1. PKI (*PUBLIC KEY INFRASTRUCTURE*)

Una infraestructura de clave pública (o, en inglés, PKI, *Public Key Infrastructure*) es una combinación de *hardware* y *software*, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

3. CONCLUSIONES

Se puede concluir que dado el objetivo principal que presenta un *Token* de Seguridad que es de autentificación (valga la redundancia) este dispositivo electrónico efectúa correctamente su función, además que brinda seguridad al usuario que lo posea.

También cabe recalcar que su única desventaja es que un hacker podría vulnerar los tokens si no se tiene las precauciones adecuadas y deberíamos plantearnos un nuevo interrogante: si grandes compañías como RSA Security (mundialmente conocida por fabricar los tokens de seguridad) fueron comprometidas con mayor o menor nivel de complejidad. ¿Qué podemos esperar de la seguridad de otras empresas?, aca es donde debemos resaltar la importancia de la Seguridad Informatica en un futuro.

4. BIBLIOGRAFIA

[1] Titulo: *Seguridad informática.* Autor: *Harvey Villalobos, Presidente de Biz Net.* Disponible en: *http://www.inteliagencia.net/infotica/TK_Seguridad.htm*
Fecha de acceso: 7/06/13 Hora. 11:35

[2] Titulo: *Autenticación con contraseña de un solo uso.* Disponible en: *http://es.wikipedia.org/wiki/Autenticaci%C3%B3n_con_contrase%C3%B1a_de_un_solo_uso*
Fecha de acceso: 7/06/13 Hora. 12:08

[3] Titulo: *Seguridad de acceso a aplicaciones web: autenticación de dos factores.* Autor: *Antonio Navarro Navarro.* Disponible en: *http://www.ticsconsulting.es/blog/seguridad-acceso-web*
Fecha de acceso: 7/06/13 Hora. 12:30

[4] Titulo: *Usando una memoria USB como Token para autenticarnos en una maquina GNU/Linux* Autor: *Epsilon.* Disponible en: *http://www.rinconinformatico.net/usando-una-memoria-usb-como-token-para-autenticarnos-en-una-maquina-gnulinux/*
Fecha de acceso: 7/06/13 Hora. 12:45

[5] Titulo: *Tokens USB.* Disponible en: *http://www.macroseguridad.net/productos/tokens_usb/*
Fecha de acceso: 4/05/13 Hora. 12:00

[6] Titulo: *Los riesgos bancarios tras el hackeo al proveedor de los tokens SecureID.* Autor: *Sergio Jara Roman.* Disponible en: *http://tecno.americaeconomia.com/noticias/los-riesgos-bancarios-tras-el-hackeo-al-proveedor-del-digipass*
Fecha de acceso: 7/06/13 Hora. 12:30

[7] Titulo: *Contraseña.* Disponible en: *http://es.wikipedia.org/wiki/Contrase%C3%B1a*
Fecha de acceso: 7/06/13 Hora. 13:06

[8] Titulo: *Infraestructura de clave pública.* Disponible en: *http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica*
Fecha de acceso: 7/06/13 Hora. 13:15