|  |  |  |
| --- | --- | --- |
| **Asignatura** | **Datos del alumno** | **Fecha** |
| **Técnicas de Identificación Digital** | Apellidos: Paz López | 21 de noviembre del 2021 |
| Nombre: Angel Ramon |

**INTRODUCCION**

En esta época en que vivimos en el siglo donde la Tecnología y las Comunicaciones van creciendo y evolucionando a grandes velocidades, el crecimiento de las redes como Internet, el uso y la evolución de los dispositivos móviles han traído cosas positivas a la sociedad en poder comunicarnos fácilmente con otras personas, el impacto económico ya que hay nuevas formas para competir en el mercado, mejoras de los servicios, pero también conlleva cosas negativas como ser el asociamiento a las amenazas que estas conllevan con respecto a la seguridad que pueden afectar a los Sistemas de Información que estas contengan y a las comunicaciones como ser los ciberdelincuentes que se aprovechan del crecimiento de la tecnología para usar programas actualizados para atacar las vulnerabilidades de los Sistemas y Comunicaciones. Por lo cual por las cosas negativas ya mencionadas en cuanto a seguridad tanto en los Sistemas de Información y Comunicaciones se tienen que implantar medidas de prevención y protección teniendo un Sistema de Gestión de la Seguridad bien estructurado brindando los servicios de seguridad necesarios como Confidencialidad, Integridad, Autenticación y No Repudio para proteger los activos mas importantes de la empresa. En este trabajo estaremos hablando sobre las dos modalidades de Autenticación (Tarjetas Inteligentes, Tokens de Autenticación) y entendemos como autenticación como el método o proceso donde una entidad demuestra que es realmente quien dicha persona o aplicación asegura ser, donde analizaremos las ventajas e inconvenientes y características de ambas modalidades de autenticación.

**TARJETAS INTELIGENTES (SMART CARDS)**

Es una tarjeta que incorpora un chip de microprocesador y circuito integrado pequeño en la cual se puede almacenar y procesar en ella de forma segura material criptográfico como ser claves de cifrado, contraseñas, certificados digitales, firmas mediante algoritmos criptográficos potentes haciendo un buen medio para la criptografía.

Podemos encontrar diferentes clasificaciones de tarjetas inteligentes según las capacidades de su chip:

* Memoria: son un contenedor de ficheros que no contienen en ella aplicaciones ejecutables, se usan normalmente en software de identificación y control de acceso sin ninguno requisito de seguridad.
* Microprocesadas: Estas tarjetas si contiene ficheros y aplicaciones, normalmente se utiliza para pagos con monederos electrónicos y para procesos de identificación.
* Criptográficas: son tarjetas microprocesadas avanzadas ya que contiene un sistema para la ejecución de algoritmos para el cifrado y firmas digitales.

Podemos decir que una tarjeta inteligente viene siendo una mini computadora ya que en ella podemos ver la siguiente estructura en la cual está formada:

1. Contiene una unidad de Central de Procesamiento (CPU), suele contener un procesador de 8 bits, a 5MHz y 5 voltios.
2. Además, contienen Memoria de Solo Lectura (ROM) su memoria interna viene siendo de 12 y 30 kb, es aquí donde las tarjetas también tienen instalado su sistema operativo, todos los procesos de comunicación y todos los algoritmos de seguridad.
3. También tenemos una Unidad de Almacenamiento que se asemeja al disco duro de una computadora la cual se le conoce como EEPROM, aquí se encuentran todos los ficheros, los datos de las aplicaciones que se usan e instalan en ella, claves de seguridad. El acceso a esta unidad está bien protegido por el mismo sistema operativo de la tarjeta.
4. Y por último tenemos la Memoria volátil de Acceso Aleatorio (RAM) en la cual trabaja el procesador.

Con todas estas características mencionadas podemos concluir que una tarjeta inteligente es una mini computadora porque cuenta con los 4 elementos más importantes para armar una computadora personal.

La parte más fundamental de una tarjeta inteligente es su sistema Operativo el mas conocido usado en tarjetas inteligentes se llama SOTI el cual esta programado en el CPU y es la que toma todas las decisiones en ejecución, es grabado en la ROM en la fase de fabricación y esta no puede ser actualizado ni alterado en otras palabras no se puede modificar o actualizar lo cual lo hace un método seguro brindado los servicios de confidencialidad e integridad de los datos. También podemos mencionar otros Sistemas Operativos como JavaCard, MultOS o Windows for smart cards, pero lo que diferencia a SOTI es que hace que cada modelo de tarjeta inteligente sea siempre diferente a los demás dentro del mercado.

**Características Positivas del uso de la tarjeta inteligente.**

* Son empleados según el contexto del Usuario
* Un excelente medio para almacenar información importante de manera segura mediante el cifrado de información.
* El nivel seguridad que brindan tanto en el hardware como en el software son muy altas. Con respecto a la seguridad a nivel de hardware es que debe realizar procesos o utilizar algoritmos que realicen que la tarjeta no pueda ser falsificada, mientras la seguridad a nivel de software se ocupara de controlar todas las ordenes que se ejecuten en la tarjeta.
* Hay una mayor demanda debida debido a la seguridad que brinda ya que es una seguridad multicapas o sea donde un usuario no autorizado no puede iniciar sesión con las credenciales de otra.
* Su facilidad de manejo y porque destaca por su forma y tamaño
* Permiten evitar que procedimientos sean tan largos, ejemplo: Ir al cajero colocar la tarjeta, ingresar el pin o la contraseña y realizar la transacción correspondiente, es mucho más rápido que ir al propio banco de ir a la ventanilla y realizar la misma tarea.

Entre algunos inconvenientes del uso de las tarjetas inteligentes podemos tener:

* Son caros de producir
* Pueden tener problema de compatibilidad y no está disponible en todos los lugares

Principales usos de la tarjeta inteligente:

* Tarjetas de Crédito y Débito: Muy usados para hacer transacciones bancarias mediante cajeros, lo cual nos permite ahorrar tiempo en realizar la transacción de forma rápido en comparado en ir al banco directamente
* Sistemas de seguridad informática
* Identificación Segura. (Nuevas tarjetas de Identidad)
* Los navegadores de Internet pueden usar la tecnología de las tarjetas inteligentes y mejorar todas las transacciones realizadas por Internet para una mayor seguridad de los datos.
* Pagos electrónicos de servicios o bienes mediante monederos electrónicos o digitales, lo cual nos permite también realizar transacciones y tareas muy rápido y ahorrándonos tiempo.
* También son utilizados en la telefonía móvil con las tarjetas SIM del celular.

**TOKENS DE AUTENTICACION**

Los tokens vienen siendo un control que nos valida y nos garantiza que un usuario ha pasado el mecanismo de autenticación en una sistema o aplicación, en la cual el usuario autenticado recibe una cadena de caracteres encriptada como respuesta como prueba de que ha sido autenticado en el sistema y con ello el usuario informa al servidor que ha pasado con éxito el proceso de autentificación para después realizar cualquier operación en el sistema o app. El clave token es un código de seguridad para sistemas de autenticación de dos factores, que se genera de manera aleatoria y normalmente consta de 6 dígitos, esa clave que género es irremplazable y no se volverá a generar en ninguna otra ocasión ni para otro usuario, dicha clave cambia o se actualiza en un lapso de tiempo ya sea 30 a 60 segundo depende a como este programado.

Características del token de seguridad:

* Pueden almacenar claves criptográficas los cuales pueden utilizarse para generar una firma digital, datos biométricos.
* Se utilizan como un complemento de seguridad como doble factor junto con la contraseña para una autenticación segura y así validar la identidad del usuario. Sirve como una llave electrónica para acceder a un sistema.

Podemos encontrar dos tipos de Tokens:

1. Físicos o de Hardware: Son dispositivos físicos con un token incorporado que los usuarios pueden utilizar para la autenticación, y deben cumplir ciertos requisitos como: Formato de Respuesta (Contraseña de un solo uso OTP basada en tiempo de seis dígitos), Algoritmo (OATH OTP basado en tiempo) y Entrega de Semillas (Archivo OATH PSKC)
2. Virtuales: Actualmente son los que mas se utilizan, generalmente se usan en un teléfono móvil, donde al usuario le llegan las claves las cuales se generan de una forma aleatoria.

**Beneficios del uso de un token de seguridad.**

* Mayor seguridad minimizando los riesgos a que se produzcan fraudes y otros delitos electrónicos.
* No genera ningún costo
* Facilidad de manejo y uso.

**Principales usos del token de seguridad:**

* Normalmente lo usan la mayoría de entidades bancarias para hacer cualquier tipo de transacciones bancarias, la cual solo se debe solicitar a la entidad para poder usarlo.
* Lenguajes de programación para la creación de aplicaciones Web realizan una autenticación basada en token, el estándar que mas se utiliza es el JSON Web
* Tokens (JWT)

**Inconvenientes o Desventajas del uso de Tokens de Autenticación:**

* Sería para el programador, realizar la creación de ello en un sistema o aplicación ya que exige un grado de dificultad programar dichos procedimientos.

**REFERENCIAS**

* Torres, J. (s. f.). Nuevo Marco de Autenticación para Tarjetas Inteligentes en Red. https://e-archivo.uc3m.es/bitstream/handle/10016/781/Tesis\_Doctoral-Joaquin\_Torres\_Marquez.pdf;jsessionid=C8D573E19944FD0BB49B084DAB54E908?sequence=1
* La seguridad en las tarjetas inteligentes. (s. f.). Recuperado 1 de noviembre de 2021, de http://spi1.nisu.org/recop/al02/chesco/index.html
* Token de seguridad. (2021). En Wikipedia, la enciclopedia libre. https://es.wikipedia.org/w/index.php?title=Token\_de\_seguridad&oldid=136808570
* ¿Qué es un token y cómo hace sus transacciones más seguras? (2016, mayo 19). Saber más, ser más. https://www.sabermassermas.com/token-como-hace-transacciones-seguras/
* *Tokens de Hardware*. (s. f.). Recuperado 8 de noviembre de 2021, de https://www.watchguard.com/help/docs/help-center/es-xl/Content/en-US/authpoint/tokens\_hardware.html