UNIVERSIDAD DEL CENTRO DEL BAJIO.

LICENCIATURA EN SISTEMAS COMPUTACIONALES.

TÍTULO:

“SERVICIOS DE SEGURIDAD”.

MATERIA:

SEGURIDAD INFORMATICA.

DOCENTE:

FILIBERTO DURAN GARCIA.

PRESENTA

PABLO SÁNCHEZ UGALDE.

Celaya, Guanajuato , 2 de Marzo del año 2019.

Criptografía simétrica.

La criptografía simétrica solo utiliza una clave para cifrar y descifrar el mensaje, que tiene que conocer el emisor y el receptor previamente y este es el punto débil del sistema, la comunicación de las claves entre ambos sujetos, ya que resulta más fácil interceptar una clave que se ha transmitido sin seguridad (diciéndola en alto, mandándola por correo electrónico u ordinario o haciendo una llamada telefónica).

Esquema de criptografía simétrica.

Teóricamente debería de ser más fácil conocer la clave interceptándola que probándola una por una por fuerza bruta, teniendo en cuenta que la seguridad de un mensaje cifrado debe recaer sobre la clave y nunca sobre el algoritmo (por lo que sería una tarea eterna reventar la clave, como comenté en un ejemplo de ataque por fuerza bruta).

Criptografía asimétrica.

La criptografía asimétrica se basa en el uso de dos claves: la pública (que se podrá difundir sin ningún problema a todas las personas que necesiten mandarte algo cifrado) y la privada (que no debe de ser revelada nunca).

Esquema de criptografía asimétrica.

Sabiendo lo anterior, si queremos que tres compañeros de trabajo nos manden un archivo cifrado debemos de mandarle nuestra clave pública (que está vinculada a la privada) y nos podrán mandar de forma confidencial ese archivo que solo nosotros podremos descifrar con la clave privada.

Puede parecer a simple vista un sistema un poco cojo ya que podríamos pensar que sabiendo la clave pública podríamos deducir la privada, pero este tipo de sistemas criptográficos usa algoritmos bastante complejos que generan a partir de la frase de paso (la contraseña) la clave privada y pública que pueden tener perfectamente un tamaño de 2048bits (probablemente imposible de reventar).

Como te has dado cuenta solo cifra una persona (con la clave pública) y la otra se limita a mirar el contenido, por lo que la forma correcta de tener una comunicación bidireccional sería realizando este mismo proceso con dos pares de claves, o una por cada comunicador.

Otro propósito de este sistema es también el de poder firmar documentos, certificando que el emisor es quien dice ser, firmando con la clave privada y verificando la identidad con la pública.

Diferencias entre criptografía simétrica y asimétrica.

Para empezar, la criptografía simétrica es más insegura ya que el hecho de pasar la clave es una gran vulnerabilidad, pero se puede cifrar y descifrar en menor tiempo del que tarda la criptografía asimétrica, que es el principal inconveniente y es la razón por la que existe la criptografía híbrida.

Conceptos básicos sobre elementos de protección en la red.

Conceptos

• “Seguridad de una red” implica la seguridad de cada uno de los dispositivos de la red

• “Hacker”: Experto en programación Suele ser un programador, descubren vulnerabilidades, a veces con ánimo constructivo y otras para actividades delictivas.

• “Cracker”: Persona que rompen los sistemas de seguridad, utiliza sus ataques para sacar beneficio económico

• “Amenaza o ataque” : intento de sabotear una operación o la propia preparación para sabotearla (poner en compromiso) .

• Vulnerabilidad: fallo en la programación que permite la infección o el secuestro de nuestro computador. 8 Tipos de amenazas

• Compromiso: la entidad atacante obtiene el control de algún elemento interno de la red, por ejemplo utilizando cuentas con password triviales o errores del sistema

• Modificación: la entidad atacante modifica el contenido de algún mensaje o texto • Suplantación: la entidad atacante se hace pasar por otra persona

• Reenvío: la entidad atacante obtiene un mensaje o texto en tránsito y más tarde lo reenvía para duplicar su efecto

• Denegación de servicio: la entidad atacante impide que un elemento cumpla su función

Seguridad a nivel aplicación.

La seguridad de aplicaciones web es una rama de la Seguridad Informática que se encarga específicamente de la seguridad de sitios web, aplicaciones web y servicios web.

A un alto nivel, la seguridad de aplicaciones web se basa en los principios de la seguridad de aplicaciones pero aplicadas específicamente a la World Wide Web. Las aplicaciones, comúnmente son desarrolladas usando lenguajes de programación tales como PHP, JavaScript, Python, Ruby, ASP.NET, JSP, entre otros.

Capa de transporte

Pila OSI.

El nivel de transporte o capa de transporte es el cuarto nivel del modelo OSI,1 y está encargado de la transferencia libre de errores de los datos entre el emisor y el receptor, aunque no estén directamente conectados, así como de mantener el flujo de la red. Es la base de toda la jerarquía de protocolo. La tarea de esta capa es proporcionar un transporte de datos confiable y económico de la máquina de origen a la máquina destino, independientemente de las de redes físicas en uno.2 Sin la capa transporte, el concepto total de los protocolos en capas tendría poco sentido.

REFERENCIA.

- **ANÓNIMO**

En el texto: (2019)

Bibliografía: (2019). Retrieved from http://isa.uniovi.es/docencia/SIGC/pdf/seguridad_sigc.pdf

CAPA DE TRANSPORTE

En el texto: ("Capa de transporte", 2019)

Bibliografía: Capa de transporte. (2019). Retrieved from https://es.wikipedia.org/wiki/Capa_de_transporte

GUTIÉRREZ, P.

Tipos de criptografía: simétrica, asimétrica e hibrida

En el texto: (Gutiérrez, 2019)

Bibliografía: Gutiérrez, P. (2019). Tipos de criptografía: simétrica, asimétrica e hibrida. Retrieved from https://www.genbeta.com/desarrollo/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

SEGURIDAD DE APLICACIONES WEB

En el texto: ("Seguridad de aplicaciones web", 2019)

Bibliografía: Seguridad de aplicaciones web. (2019). Retrieved from https://es.wikipedia.org/wiki/Seguridad_de_aplicaciones_web