Seguridad Informática

Lorenzo Elguea

Objetivos

Al finalizar el curso el alumno(a):

Conocerá la teoría y terminología del área de Ciberseguridad para software y hardware.

Comprenderá la importancia de la seguridad en los sistemas de información.

Detectará puntos de vulnerabilidad.

Será capaz de desarrollar sistemas seguros utilizando las tecnologías adecuadas.

Tema 1

1. Introducción a la ciberseguridad
    - 1.1 Conceptos de seguridad para software
    - 1.2 Conceptos de seguridad para hardware
    - 1.3 Tecnologías de conectividad seguras en Internet
        - 1.3.1 Protocolo de Internet versión 6
        - 1.3.2 Internet de las Cosas
        - 1.3.3 Certificados Digitales
        - 1.3.4 Conexiones Cifradas

Definiciones

Disponibilidad Un sistema posee la propiedad de disponibilidad si, los recursos brindan servicio en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

Autorización: La autorización se refiere al permiso u obligación de hacer uso de los recursos del sistema. Se basa en la posesión de credenciales, que pueden ser: la identidad, la autentificación o la función de una entidad.

Autentificación: La autentificación es el proceso mediante el cual una entidad comprueba su identidad.

Reflexión: ¿Porque los sistemas abiertos “mejoran la disponibilidad”? ¿Qué falla más, la Autorización o la Autenticación? ¿El phishing que es?

Definiciones

Autorización: La autorización se refiere al permiso u obligación de hacer uso de los recursos del sistema. Se basa en la posesión de credenciales, que pueden ser: la identidad, la autentificación o la función de una entidad.

Autentificación: La autentificación es el proceso mediante el cual una entidad comprueba su identidad.

Seguridad para software

La seguridad del software es el concepto de implementar mecanismos en la construcción de la seguridad para ayudarla a permanecer funcional (o resistente) a los ataques. Esto significa que una pieza de software se somete a pruebas de seguridad antes de salir al mercado para comprobar su capacidad para resistir ataques maliciosos.

Un fallo en software, o bug, puede o no poner en riesgo la seguridad.

Si pone el riesgo, se conoce como vulnerabilidad, esto se corrige con un parche o una actualización (Ver versiones)

Si la vulnerabilidad se aprovecha antes de que el desarrollador tenga un parche, se conoce como **Día Cero**.

Seguridad para hardware

El hardware se compone principalmente de componentes mecánicos, eléctricos y/o electrónicos.

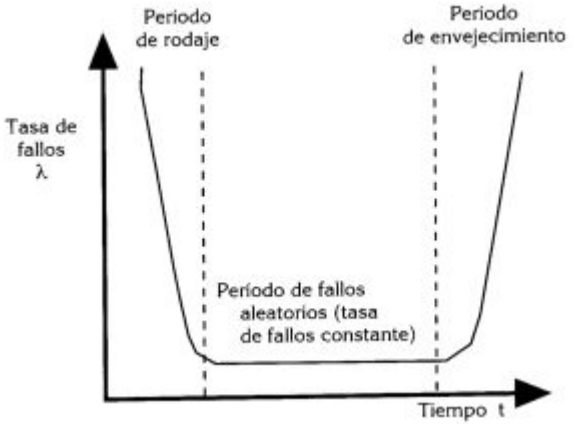
Los componentes mecánicos, sufren desgaste por la fricción, por ejemplo un disco duro o un ventilador.

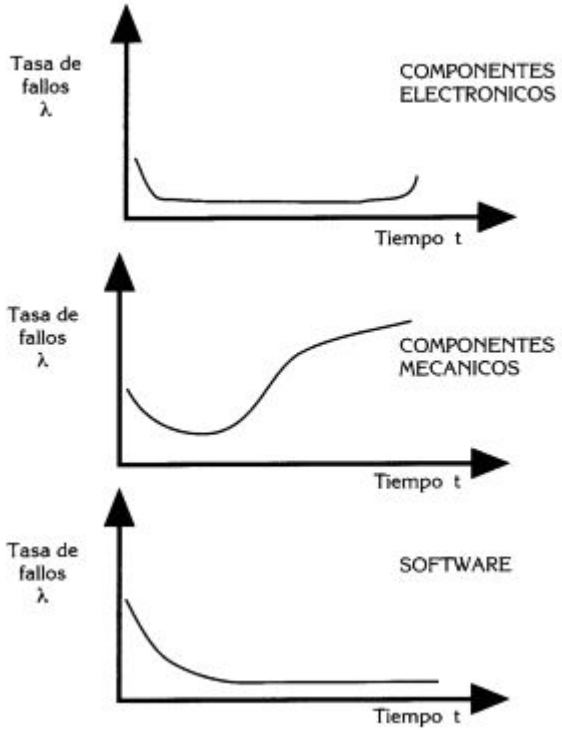
Los componentes eléctricos, son sensibles a variaciones de voltaje o fuera de especificaciones (ejem Temperatura en los sites)

¿Los componentes electrónicos se desgastan?

¿Qué hace la NASA?

Curvas de fallas (Bañera)





Tecnologías de conectividad seguras en Internet

IPv4 tiene 40 años

¿Que es obsoleto según la RAE?

LO QUE DEBES SABER SOBRE IPV6

LORENZO ELGUEA FERNÁNDEZ

TEMARIO

Que es IPv6

Para que se crea IPv6

Principales Diferencias con IPv4

Beneficios

Pruebas de Conectividad

Otros…

5 Pasos

¿QUÉ ES IPV6?

Es el mecanismo de Evolución de IPv4 para redes con base en TCP/IP

El protocolo IPv6 presenta **mejoras en rendimiento y seguridad y es más eficiente.**

Busca principalmente solucionar el problema de falta direcciones publicas.

Implementa desde el principio la seguridad, y aunque es opcional, facilita las cosas.

PARA QUE SE CREA IPV6

En 1969 la Agencia de Proyectos de Investigación Avanzada (Defense Advanced Research Projects Agency o DARPA) del Ejército de los EEUU desarrolla la ARPAnet.

1974 Se publica la primera norma TCP/IP.

¿48 años en tecnología es mucho o poco?

Se le quitaron campos que no se usan.

- Otros campos que no se usan, simplemente no se usan.

Se implementó NAT, para que alcanzara para todos.

Se le “pego” la seguridad.

SE CREA para solucionar muchos de las deficiencias de IPV4.

IPV4 VS IPV6

32 bits vs 128

4294967296 vs 3.402823669209384634633746074317 7e+38.

En IPv6 es más sencillo el direccionamiento.

El segmento mas pequeño en IPv6 es el /64 (18446744073709551616 hosts)

Encabezado con soporte para autenticación y encapsulación.

Mejor seguridad con Ipsec ya que se contempla desde el inicio.

BENEFICIOS DE IPV6

No es necesario recalcular la redundancia, ya que no existe.

Mejoras en Calidad de Servicio (QoS), además que se agregan etiquetas de flujo en el encabezado.

Desde un inicio se incluye la movilidad, con mayor eficiencia.

Jumbo Frames: Video streaming mejorado.

Bidireccional: Con NAT, se pierde la conexión en un sentido.

Para todos por igual. Todos con IPv6 tenemos direcciones, con IPv4 no.

DUALSTACK proporciona muchos beneficios. Puede ser de gran ayuda para la alta disponibilidad…

PRUEBAS DE CONECTIVIDAD

En IPv4, se usa: http://www.msftncsi.com/ncsi.txt

Ip4.me

En IPv6, se usa: http://ipv6.msftconnecttest.com/connecttest.txt

Ip6.me

También están: https://test-ipv6.com/

https://ipv6-test.com/

https://ipv6test.google.com/

OBSOLETO

RAE: **obsoleto** (Del lat. obsolētus).

1. adj. Poco usado.

2. adj. Anticuado, inadecuado a las circunstancias actuales.

¿QUIÉNES USA IPV6?

Google: 2607:f8b0:4000:804::1012

Facebook: 2a03:2880:10:cf07:face:b00c:0:1

Nasa: 2600:1404:0:1::48f6:3718

Yahoo: 2001:4998:f011:1fe::3000

Apple: 2600:1404:0:1::48f6:3713

Netflix: 2406:da00:ff00::36f3:696b

Wikipedia: 2620:0:861:ed1a::1

Mozilla: 2620:101:8008:5::2:1

Bing: 2600:1404:0:1::48f6:3709

Comcast: 2001:418:3801:6::cc02:de38

IBM: 2600:141c:2000:390::1e89

5 PASOS (PARA LOS QUE NO TIENE YA IPV6)

Registrarse en http://www.tunnelbroker.net para un segmento ::/64 o un ::/48 o en IAR para un ::/48 propio.

Configurar los servicios básicos: Clientes, DNS, WEB, FTP, antivirus, etc.

Poner uno o dos segmentos de nuestra red en pruebas.

Capacitarnos.

Ponerlo en productivo.

Internet de las Cosas

Demo Sensor Sonoff

Certificados Digitales

El certificado digital es un mecanismo que sirve para poder verificar tu identidad real de forma “inequívoca”

La encriptación o cifrado es un mecanismo de seguridad que permite modificar un mensaje de modo que su contenido sea ilegible, salvo para su destinatario. De modo inverso, la desencriptación o descifrado permitirá hacer legible un mensaje que estaba cifrado.

Hay mecanismos de cifrado simétrico y asimétrico

Cifrado Simétrico

Un sistema de cifrado simétrico **es un tipo de cifrado que usa una misma clave para cifrar y para descifrar**.

Hay varios estándares “modernos” para eso.

AES, DES, 3DES y TDEA

Cifrado Asimétrico

Un sistema de cifrado asimétrico **es un tipo de cifrado que usa una clave para cifrar y otra diferente para descifrar**.

Diffie-Hellman.

RSA.

DSA.

Cifrado ElGamal.

Criptografía de curva elíptica.

Criptosistema de Merkle-Hellman.

Goldwasser-Micali.

Goldwasser-Micali-Rivest.

Cifrado, Certificados y Firmas

Si se cifra el mensaje utilizando la llave privada, cualquiera puede descifrarlo utilizando su llave pública correspondiente. De esta forma se logra la identificación y autenticación del remitente, ya que sólo él pudo haber utilizado su llave privada.

La firma digital se basa en el hecho de que un documento cifrado utilizando la llave privada de una persona sólo puede ser descifrado utilizando la llave pública asociada a esa misma persona. La firma digital es un digesto o huella del documento, el cual se cifra utilizando la llave privada del firmante.

Integridad de los datos: algoritmos Hash

El verificar la no alteración de los datos es crítico en las transacciones electrónicas.

Los sistemas criptográficos utilizan funciones “hash” para realizar el chequeo de integridad, mediante la generación de una “huella digital” o digesto (digest).

Ejemplos MD2, MD5, SHA-1, SHA-256, SHA-384, SHA-512, CRC32

Se usan para descargar archivos, en comunicaciones de redes y ….

https://dencode.com/en/hash

TAREA:

Criptografía

Ariel Maiorano

https://books.google.com.mx/books?id=j7F1EAAAQBAJ&pg=PR4&dq=criptograf%C3%ADa+de+Ariel+Maiorano&hl=en

Cuando la Criptografía Falla

Arturo Quirantes Sierra

https://www.amazon.com.mx/Cuando-criptograf%C3%ADa-Arturo-Quirantes-Sierra-ebook/dp/B00ARPJ9E6