Universidad Tecnológica Nacional
Facultad Regional San Nicolás

Seguridad Informática

Técnicas Digitales III

Felipe Poblete, Mariano González - 2023

Noticias

NACIONAL 15 Agosto 2022

El Tribunal Superior de Justicia mediante una acordada declaró días inhábiles hasta el viernes. Hablan de uno de los peores ataques de la historia del país.

Un nuevo ciberataque impacta en el mundo

Ucrania fue el país más afectado de Europa por un virus ransomware. El ataque fue una versión mejorada del anterior. Que el virus informático sea una variante de Petya sugiere que los atacantes serán difíciles de rastrear.

En 2021 se duplicaron los ciberataques en Argentina

Más de la mitad corresponden a casos de phishing

07 de febrero de 2022

Alerta WiFi: así usan los routers para instalar malware y robar datos de tus dispositivos

Una investigación detectó más de 500 vulnerabilidades en routers hogareños, 87 de ellas críticas.

Indice

Definiciones

- **SEGURIDAD INFORMÁTICA**

- Podemos definir la **seguridad informática** o **ciberseguridad** como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica las actividades de proteger contra intrusos el uso de nuestros recursos informáticos, especialmente la información contenida en una computadora o circulante a través de las redes de computadoras, con intenciones maliciosas, con intención de obtener ganancias o incluso la posibilidad de acceder a ellos por accidente.
- La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

Definiciones

- **MALWARE**

- El **malware** (una contracción para soft**ware mal**icioso) es cualquier software diseñado intencionalmente para causar daños a una computadora, servidor, cliente o red informática. Por el contrario, el software que causa daños involuntarios debido a alguna deficiencia se describe típicamente como un error de software (**bug**). Existe una amplia variedad de tipos de malware, incluyendo: **virus informáticos,** gusanos, troyanos, ransomware, spyware, adware, wiper y scareware, entre otros.

Definiciones

- **VIRUS INFORMÁTICO**

- Un **virus informático** es un tipo de programa informático que, cuando se ejecuta, se replica modificando otros programas informáticos e insertando su propio código. Si esta replicación tiene éxito, se dice que las áreas afectadas están "infectadas" con un virus informático, una analogía derivada de los virus biológicos.
- Los virus informáticos generalmente requieren un programa host. El virus escribe su propio código en el programa anfitrión. Cuando se ejecuta el programa, el programa de virus escrito se ejecuta primero, causando infección y daños. Un gusano informático no necesita un programa host, ya que es un programa independiente o fragmento de código. Por lo tanto, no está restringido por el programa anfitrión, pero puede ejecutarse de forma independiente y llevar a cabo ataques de forma activa.

Amenazas actuales

7.5.1 SPYWARE

Cualquier aplicación que recopila la información sobre la actividad en el PC de una persona u organización tanto en línea como fuera de ésta y que es capaz de guardar los datos recopilados localmente o enviarlos a terceros sin que el objeto de espionaje se entere de ello…

7.5.2 ADWARE

Un programa que puede mostrar anuncios mientras se esté ejecutado o mediante otros mecanismos se llama adware. A menudo estos sistemas publicitarios se integran en los programas gratuitos ayudando a los desarrolladores a cubrir los gastos…

7.5.3 ROOTKITS

Se trata de programas diseñados para ocultar objetos como procesos, archivos o entradas del Registro de Windows. Este tipo de software no es malicioso en sí mismo, pero es utilizado por los creadores de malware para esconder evidencias y utilidades en los sistemas infectados…

Amenazas actuales

7.5.4 EXPLOITS

Es una técnica o un programa que aprovecha un fallo o hueco de seguridad - una vulnerabilidad- existente en un determinado protocolo de comunicaciones, sistema operativo, o herramienta informática…

7.5.5 GUSANOS

Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones de la computadora. El objetivo de este malware suele ser colapsar las computadoras y las redes informáticas, impidiendo así el trabajo…

7.5.6 COOKIES

Las cookies son pequeños archivos de texto que el navegador de Internet guarda en la computadora del usuario cuando se visitan páginas web. La información que guardan se utiliza para personalizar la navegación, para recoger información demográfica sobre cuántos usuarios visitan la página y el tiempo que permanecen en ella, etc. Las páginas Web que utilizan cookies deben solicitar la aprobación del visitante para hacer uso de ellas.

Amenazas actuales

7.5.7 HOAX (engaño)

Los “virus” HOAX se difunden por la llamada “ingeniería social”. En general a través de un mensaje de texto se le solicita que lo reenvíe a cuantas personas conozca con motivos más o menos verosímiles. En realidad, el virus es el mensaje…

7.5.8 VIRUS DE EJECUCIÓN ESPECULATIVA

Estos virus se aprovechan de las características de ejecución especulativa de los procesadores, pero especialmente del procesador Intel, usando código que no debería haberse ejecutado pero que el procesador realiza como una de sus propiedades de mejora de la performance…

7.5.9 RANSOMWARE

Un ransomware (del inglés ransom, «rescate» y ware, contracción de software), o «secuestro de datos» en español, es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción…

Amenazas actuales

7.5.10 BOTNETS

Son redes de computadoras con infección de malware que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.

7.5.11 PHISHING

El phishing es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito, etc.

7.5.12 INYECCIÓN DE CÓDIGO SQL

Una inyección de código SQL (por sus siglas en inglés Structured Query Language) es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto le brinda acceso a la información confidencial contenida en la base de datos.

Amenazas actuales

7.5.13 “MAN-IN-THE-MIDDLE”

Un ataque de tipo “Man-in-the-middle” es un tipo de ciberamenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

7.5.14 DENEGACIÓN DE SERVICIO

Un ataque de denegación de servicio es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales.

7.5.15 BACKDOOR

Los virus de puerta trasera son aquellos en los que los hackers acceden a funciones de la computadora de manera oculta y trabajan en segundo plano. Este tipo de virus son, en realidad, una combinación de diferentes amenazas de seguridad y algunos funcionan automáticamente…

Seguridad informática

7.2 ASPECTOS QUE ATAÑEN A LA SEGURIDAD INFORMÁTICA

Las cuatro áreas principales que cubre la seguridad informática son:

1. **Confidencialidad**: Sólo los usuarios autorizados pueden acceder a nuestros recursos, datos e información.
2. **Integridad**: Sólo los usuarios autorizados deben ser capaces de modificar los datos cuando sea necesario.
3. **Disponibilidad**: Los datos deben estar disponibles para los usuarios cuando sea necesario.
4. **Autenticación**: Estás realmente comunicándote con los que piensas que te estás comunicando.

Medidas de mto. y prevención

1. Asegurar la instalación de software legalmente adquirido: por lo general el software legal está libre de troyanos o virus.
2. Actualizar el software y el sistema operativo: esto significa que aprovechará las últimas revisiones de seguridad.
3. Utilizar software antivirus: las soluciones de seguridad detectarán y eliminarán las amenazas. Mantenga su software actualizado para obtener el mejor nivel de protección, con las reglas de configuración y del sistema adecuadamente definidos.
4. Hardware y software cortafuegos: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
5. Uso de contraseñas complejas y grandes: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker no pueda romperla fácilmente.

Medidas de mto. y prevención

6. Cuidado con la ingeniería social: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
7. No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos: podrían estar infectados con malware. No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos.
8. Criptografía, especialmente la encriptación: juega un papel importante en mantener nuestra información sensible, segura y secreta.
9. Evitar el uso de redes Wi-Fi no seguras en lugares públicos: las redes no seguras lo dejan vulnerable a ataques del tipo “Man-in-the-middle”.
10. Tapar la webcam. En general, los distintos sensores de un dispositivo como GPS, micrófono, acelerómetro, etc. podrían ser hackeados.

Criptografía

La **criptografía** es la técnica de escribir de manera secreta u oculta, buscando proteger la información.

Para que un mensaje que, desde que es generado por el emisor, deba atravesar un medio de comunicación inseguro para luego llegar al receptor, desde hace muchos años se emplean métodos para mantenerlo oculto.

7.7.1 CIFRADO SIMÉTRICO

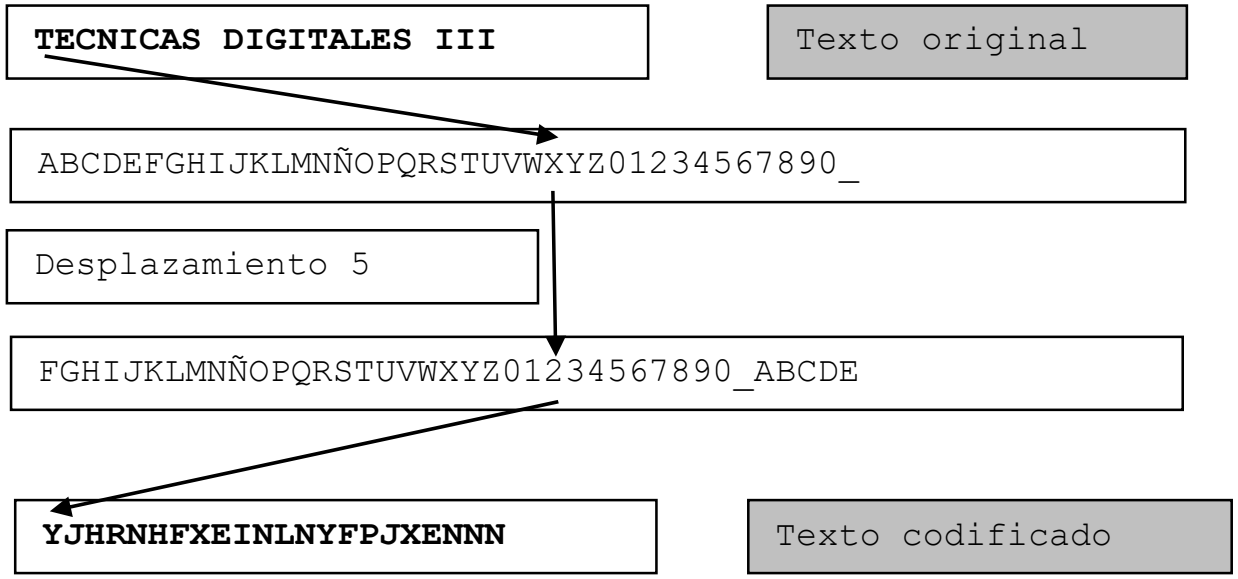
El cifrado simétrico consiste en la codificación mediante una regla (clave) que sólo conocen el emisor y el receptor.

Una vez de acuerdo, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra usando la misma clave.

El inconveniente de este método es que se debe enviar al receptor la clave de cifrado con algún método seguro y si el receptor se encuentra lejos esto puede ser costoso.

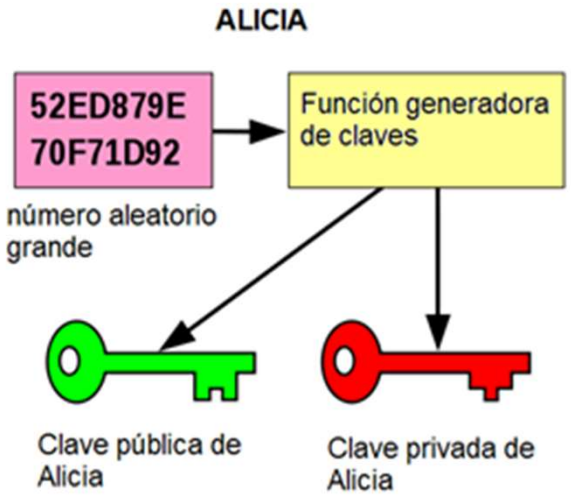
Criptografía - Ejemplo

El texto original es “**TECNICAS DIGITALES III**” y el método de cifrado es incrementar en 5 la posición de cada letra. Disponemos de una lista de letras ordenadas y luego la misma lista pero desplazada 5 posiciones. Para la primera letra (T) corresponde (Y), luego para la segunda letra (E) corresponde (J) y así sucesivamente. Se obtiene “**YJHRNHFXEINLNYFPJXENNN**” que es incomprensible.

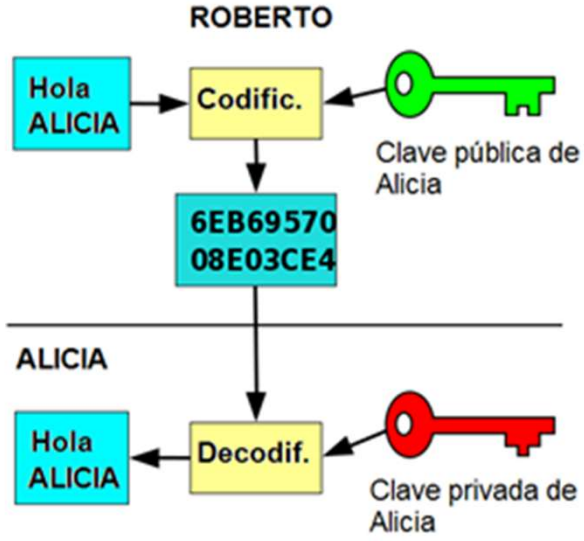


Cifrado asimétrico

Este método, atribuido a Diffie y Hellman, consiste en la generación matemática de dos claves. Una de ellas, llamada privada, es conocida sólo por el emisor y la otra, llamada pública es enviada al receptor. Los textos codificados con la clave privada pueden luego decodificarse con la clave pública. Esto facilita la distribución de claves en los sistemas de comunicación actuales y da lugar a la PKI (Public Key Infrastructure).



Generación de clave



Envío de mensaje

Cifrado híbrido

Un sistema de cifrado híbrido usa tanto el cifrado simétrico como el asimétrico. Funciona mediante el uso de una clave pública para compartir una clave privada para el cifrado simétrico. El mensaje que se esté enviando en el momento, se cifra usando la clave y enviándolo al destinatario. Ya que compartir una clave simétrica no es seguro, la clave usada es diferente para cada sesión. La clave de sesión es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave de sesión y acto seguido usa la clave de sesión para descifrar el mensaje.

Nota: El cifrado tiene una complejidad que excede el alcance de nuestra asignatura y de este apunte. Si desea más información, se cita un excelente trabajo de tesis en: https://repository.unad.edu.co/bitstream/handle/10596/40365/rtorrescar.pdf?sequence=3&isAllowed=y.

También se puede consultar el artículo "GNU privacy guard" en https://www.gnupg.org/gph/es/manual/c190.html

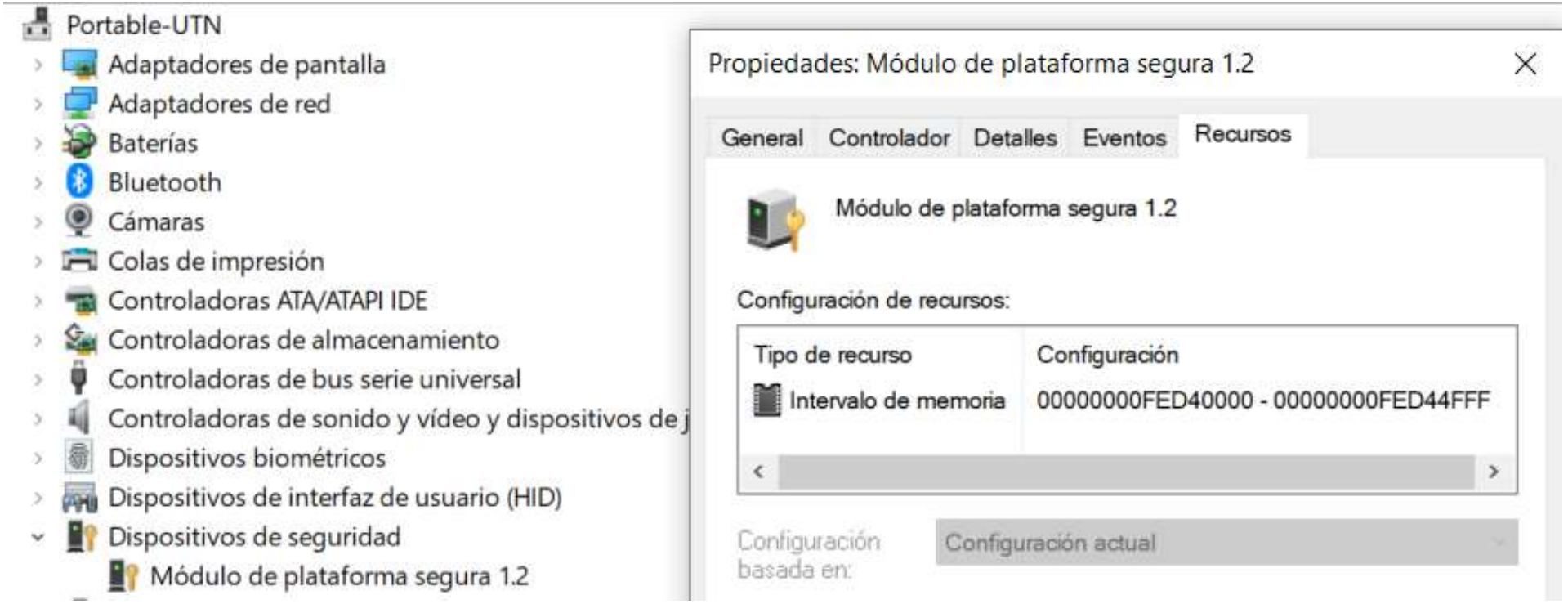
Módulo de plataforma confiable

Trusted Platform Module (TPM, también conocido como ISO /IEC 11889) es un estándar internacional para un criptoprocesador seguro, un microcontrolador dedicado diseñado para proteger el hardware a través de claves criptográficas integradas. El término también puede referirse a un chip que cumple con el estándar. El mismo proporciona:

- Un generador de números aleatorios por hardware
- Facilidades para la generación segura de claves criptográficas para usos limitados.
- Atestación remota: crea un resumen de clave hash casi indescifrable de la configuración de hardware y software. El software encargado de “hashear” los datos de configuración determina el alcance del resumen. Esto permite a un tercero verificar que el software no se ha cambiado.
- Enlace: Cifra los datos utilizando la clave de enlace TPM, una clave RSA única descendiente de una clave de almacenamiento.
- Sellado: Similar al enlace, pero, además especifica el estado TPM para los datos que se descifrará.
- Otras funciones de Trusted Computing (Computación confiable) para que los datos se descifren.

Módulo de plataforma confiable

En el administrador de dispositivos de Windows se muestra la descripción del módulo TPM, si el mismo está disponible.



Para verificar si su PC tiene habilitado el módulo TPM, se puede ejecutar el comando de consola tpm.msc.

Fin de la presentación

Técnicas Digitales III – UTN – FRSN

https://www.frsn.utn.edu.ar/tecnicas3