Criptografía y Seguridad

Ing. Horacio A. Navarro G.

Agenda

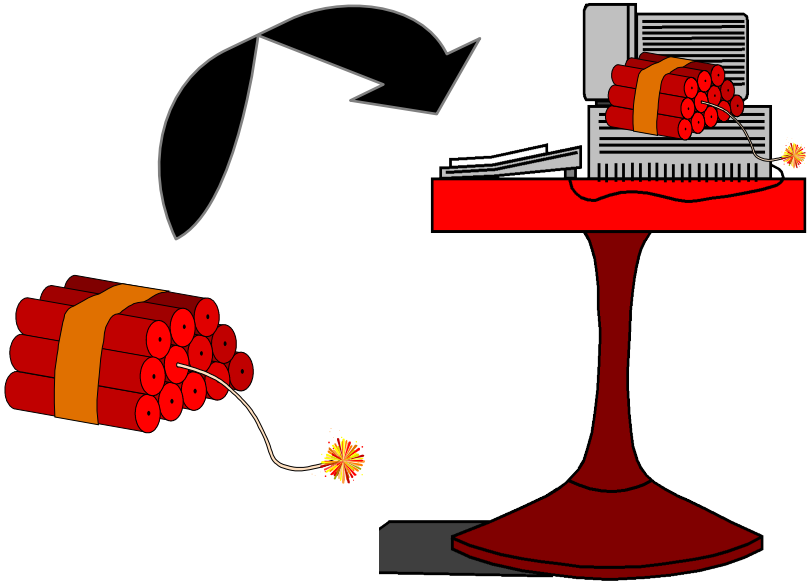
- Definición de seguridad informática
- Criptografía
- Delito informático
- Seguridad física vs seguridad lógica
- Principios de la seguridad informática
- Debilidades
- Amenazas
- Cripto sistemas

¿Cómo definir la seguridad informática?

- Si nos atenemos a la definición de la Real Academia de la Lengua RAE, seguridad es "cualidad de seguro". Buscamos ahora seguro y obtenemos "libre y exento de todo peligro, daño o riesgo".
- Como a partir de estas premisas no podemos decir simplemente que la seguridad informática es "la cualidad de un sistema informático seguro", habrá que buscar una definición más técnica.
- Algo básico: la seguridad no es un producto, sino un proceso.
- Por lo tanto, podríamos aceptar que una primera definición más o menos aceptable de seguridad informática sería:
  - Un conjunto de sistemas, métodos y herramientas destinados a proteger la información, proceso en el cual participan además personas. Concienciarlas de su importancia será un punto crítico.
- Recuerde: la seguridad informática no es un bien medible, en cambio sí podríamos desarrollar diversas herramientas para medir o bien cuantificar nuestra inseguridad informática.

¿Conectado o desconectado?

No podemos aceptar esa afirmación simpática que dice que el computador más seguro ...



... es aquel que está apagado y, por lo tanto, desconectado de la red.

A pesar de todas las amenazas del entorno, que serán muchas y de muy distinto tipo ...

... tendremos que aplicar políticas, metodologías y técnicas de protección de la información.

Acontecimientos en dos últimas décadas

- A partir de los años 80 el uso del ordenador personal comienza a ser común. Asoma ya la preocupación por la integridad de los datos.
- En la década de los años 90 proliferan los ataques a sistemas informáticos, aparecen los virus y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.
- Las amenazas se generalizan a finales de los 90.
- En los años 00s los acontecimientos fuerzan a que se tome en serio la seguridad informática.

¿Qué hay de nuevo?

- Principalmente por el uso masivo de Internet, el tema de la protección de la información se ha transformado en una necesidad y con ello se populariza la terminología técnica asociada a la criptología:
  - Cifrado, descifrado, criptoanálisis, firma digital, ...
  - Autoridades de Certificación, comercio electrónico, ...
- Ya no sólo se comentan estos temas en las universidades. Cualquier usuario desea saber, por ejemplo, qué significa firmar un e-mail o qué significa que en una comunicación con su banco aparezca un candado en la barra de tareas de su navegador y le diga que el enlace es SSL con 128 bits.
- El software actual ya vienen con seguridad añadida.

La criptografía es más o menos esto

Criptografía:

Rama inicial de las Matemáticas y en la actualidad de la Informática y la Telemática, que hace uso de métodos y técnicas con el objeto principal de cifrar y/o proteger un mensaje o archivo por medio de un algoritmo, usando una o más claves. Esto da lugar a diferentes tipos de sistemas de cifra, llamados criptosistemas, que permiten asegurar alguno de estos tres aspectos básicos de la seguridad informática: la confidencialidad, la integridad y el no repudio de emisor y no repudio de receptor.

Una definición menos afortunada...

La criptografía según la RAE:

"Arte de escribir con clave secreta o de modo enigmático"

Desde el punto de vista de la ingeniería y la informática, es difícil encontrar una definición menos apropiada ☹

- Hoy ya no es un arte sino una ciencia.
- No sólo se protegen y escriben cosas o documentos, se generan diversos tipos de archivos y documentos.
- La clave no es única. Muchos sistemas actuales usan dos claves, una de ellas secreta y la otra pública.
- No hay nada de enigmático ☺ en una cadena de bits.

El término apropiado es cifrar

Cifra o cifrado:

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica o secreto, no será posible descifrarlo o recuperarlo.

No obstante, la RAE define cifrar como “Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar” ... también muy poco técnica ☹.

En algunos países de Latinoamérica, por influencia del inglés, se usará la palabra encriptar. Aunque se entienda, esta palabra todavía no existe y bien podría ser el acto de “introducir a alguien dentro de una cripta”, ... ✞☠✞ ... como puede ver, algo bastante distinto a lo que deseamos expresar... ☺.

Unas cuantas definiciones previas

Criptología: ciencia que estudia e investiga todo aquello relacionado con la criptografía: incluye cifra y criptoanálisis.

Criptógrafo: máquina o artilugio para cifrar.

Criptólogo: persona que trabaja de forma legítima para proteger la información creando algoritmos criptográficos.

Criptoanalista: persona cuya función es romper algoritmos de cifra en busca de debilidades, la clave o del texto en claro.

Texto en claro: documento original. Se denotará como M.

Criptograma: documento/texto cifrado. Se denotará como C.

Claves: datos (llaves) privados/públicos que permitirán cifrar.

¿Es atractivo el delito informático?

- Suponiendo que todos entendemos más o menos qué es un delito informático, parece ser que es un buen negocio:
  - Objeto pequeño: la información está almacenada en contenedores pequeños: no es necesario un camión para robar un banco, llevarse las joyas, el dinero, etc.
  - Contacto físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del propio delincuente.
  - Alto valor: el objeto codiciado tiene un alto valor. El contenido (los datos) puede valer mucho más que el soporte que los almacena: computador, disco, CD, etc.
- La solución será el uso de técnicas criptográficas.

Seguridad Física vs Seguridad Lógica

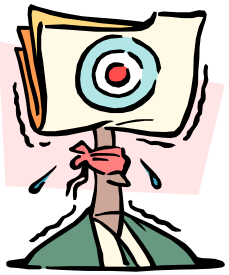
- El estudio de la seguridad informática podríamos plantearlo desde dos enfoques distintos aunque complementarios:
  - La Seguridad Física: puede asociarse a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc.
  - La Seguridad Lógica: protección de la información en su propio medio, mediante el enmascaramiento de la misma usando técnicas de criptografía. Este enfoque de las aplicaciones criptográficas, es el que será tratado a lo largo de los capítulos de este libro.
  - La gestión de la seguridad está en medio de la dos: los planes de contingencia, políticas de seguridad, normativas, etc. Aunque muy brevemente, este tema será tratado en un próximo capítulo.
  - No obstante, tenga en cuenta que esta clasificación en la práctica no es tan rigurosa. En resumidas cuentas, podríamos decir que cada vez está menos claro dónde comienza una y dónde termina la otra.

Principios de la seguridad informática

- Veremos a continuación los tres principios básicos de la seguridad informática: el del acceso más fácil, el de la caducidad del secreto y el de la eficiencia de las medidas tomadas.
- Tras los acontecimientos del 11/09/2001 y del 11/03/2004, que echaron por tierra todos los planes de contingencia, incluso el más paranoico, comenzamos a tener muy en cuenta las debilidades de los sistemas y valorar en su justa medida la seguridad.

Es necesario aprender de los errores ☹

1er principio de la seguridad informática



PREGUNTA:

¿Cuáles son los puntos débiles

de un sistema informático?

- "El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque"
- Existirá una diversidad de frentes desde los que puede producirse un ataque. Esto dificulta el análisis de riesgos porque el delincuente aplicará la filosofía del ataque hacia el punto más débil.

2º principio de la seguridad informática

PREGUNTA:
¿Cuánto tiempo deberá protegerse un dato?

- "Los datos confidenciales deben protegerse sólo hasta que ese secreto pierda su valor como tal"
- Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
- Esto nos llevará a la fortaleza del sistema de cifra.

3er principio de la seguridad informática

- "Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio"
  - Que funcionen en el momento oportuno.
  - Que lo hagan optimizando los recursos del sistema.
  - Que pasen desapercibidas para el usuario.

Medidas de control

» Y lo más importante: ningún sistema de control resulta efectivo hasta que debemos utilizarlo al surgir la necesidad de aplicarlo. Junto con la concienciación de los usuarios, éste será uno de los grandes problemas de la Seguridad Informática.

Debilidades del sistema informático

HARDWARE - SOFTWARE - DATOS

MEMORIA - USUARIOS

Los tres primeros puntos conforman el llamado Triángulo de Debilidades del Sistema:

- Hardware: pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- Software: puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.
- Datos: puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

Debilidades del sistema informático

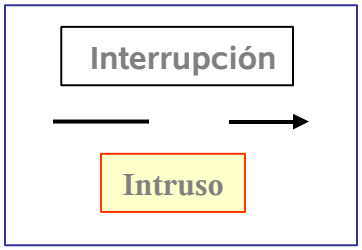
  - Memoria: puede producirse la introducción de un virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
  - Usuarios: puede producirse la suplantación de identidad, el acceso no autorizado, visualización de datos confidenciales, etc.

- Es muy difícil diseñar un plan que contemple minimizar de forma eficiente todos estos aspectos negativos.
- Debido al principio de acceso más fácil, el responsable de seguridad informática no se deberá descuidar ninguno de los cinco elementos susceptibles de ataque al sistema.

Amenazas del sistema

- Las amenazas afectan principalmente al hardware, al software y a los datos. Éstas se deben a fenómenos de:
  - Interrupción
  - Interceptación
  - Modificación
  - Generación

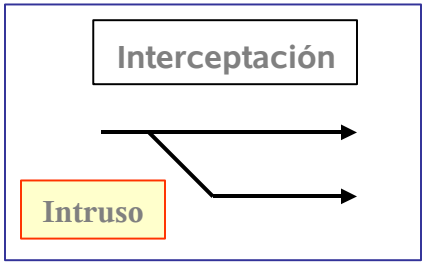
Amenazas de interrupción



- Se daña, pierde o deja de funcionar un punto del sistema.
- Su detección es inmediata.

Ejemplos: Destrucción del hardware.
Borrado de programas, datos.
Fallos en el sistema operativo.

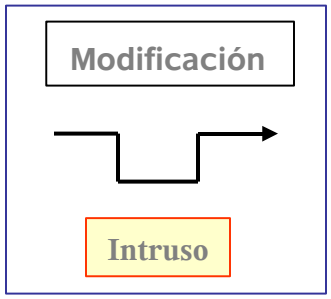
Amenazas de interceptación



- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Su detección es difícil, a veces no deja h

Ejemplos: Copias ilícitas de programas.
Escucha en línea de datos.

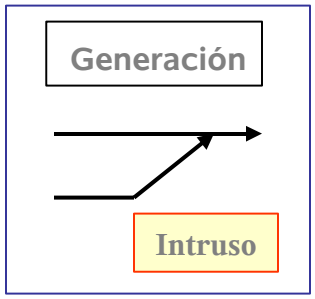
Amenazas de modificación



- Acceso no autorizado que cambia el entorno para su beneficio.
- Su detección es difícil según las circunstancias.

Ejemplos: Modificación de bases de datos.
Modificación de elementos del HW.

Amenazas de generación



- Creación de nuevos objetos dentro del sistema.
- Su detección es difícil: delitos de falsificación.

Ejemplos: Añadir transacciones en red.
Añadir registros en base de datos.

Ataques característicos

- Hardware:
  - Agua, fuego, electricidad, polvo, cigarrillos, comida.
- Software:
  - Además de algunos típicos del hardware, borrados accidentales o intencionados, estática, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.
- Datos:
  - Tiene los mismos puntos débiles que el software. Pero hay dos problemas añadidos: no tienen valor intrínseco pero sí su interpretación y, por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público: hay leyes que lo protegen.

Confidencialidad, integridad y disponibilidad

- Confidencialidad
  - Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.
- Integridad
  - Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.
- Disponibilidad
  - Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Requisitos de un criptosistema

- Algoritmo de cifrado y descifrado rápido y fiable.
- Posibilidad de transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado.
- La seguridad del sistema deberá residir solamente en el secreto de una clave y no en las funciones de cifra.
- La fortaleza del sistema se entenderá como la imposibilidad computacional (tiempo de cálculo en años que excede cualquier valor razonable) de romper la cifra o encontrar la clave secreta a partir de otros datos de carácter público.

Fortaleza: tipos de ataques

Conociendo el algoritmo de cifra, el criptoanalista intentará romper la cifra en uno de estos escenarios:

1. Contando únicamente con el criptograma.
2. Contando con texto en claro conocido.
3. Eligiendo un texto en claro.
4. A partir de texto cifrado elegido.

ATAQUE POR FUERZA BRUTA

Un algoritmo de cifra será fuerte si, conociendo su funcionamiento o código, conociendo el texto cifrado y conociendo el texto en claro, el ataque a la clave de cifra secreta es computacionalmente muy difícil.

Clasificación de los criptosistemas

- Sistemas de cifra: clásicos versus modernos
  - Clasificación histórica y cultural (no técnica).
- Sistemas de cifra: en bloque versus en flujo
  - Clasificación de acuerdo a cómo se produce la cifra.

- Sistemas con clave: secreta versus pública
  - Clasificación de acuerdo al uso de una única clave secreta (simétricos) o bien con dos claves, una de ellas pública y la otra privada (asimétricos).

Cifrado en bloque y cifrado en flujo

- CIFRADO EN BLOQUE:
  - El mismo algoritmo de cifra se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave. El bloque de texto o información a cifrar normalmente será de 64 ó 128 bits.
- CIFRADO EN FLUJO:
  - El algoritmo de cifra se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y de mayor longitud que el mensaje. La cifra se hace carácter a carácter o bit a bit.

Referencias

- Curso de seguridad informatica y criptografia

  Dr. Jorge Ramio Aguirre
- Hispasec www.hispasec.com