Introducción a la Seguridad

Prof. Isabel Leguías
Universidad Tecnológica de Panamá
Departamento de Programación de Computadoras
Seguridad en Sistemas de Información

Contenido

- Introducción
- Referencias Estadísticas
- Conceptos
- Servicios de Seguridad
- Amenazas, Vulnerabilidades y Ataques de seguridad

Referencias Estadisticas

Tendencias a tener en cuenta en el 2019

- 70% de las organizaciones cree que su riesgo de seguridad creció considerablemente en el 2017.

  IBM https://www.ibm.com/downloads/cas/ZYKLN2E3
- Se estima que para el 2020, el número de contraseñas utilizadas crecerá a 300 billones. SCMagazibe https://www.ibm.com/downloads/cas/ZYKLN2E3
- 43% de los ciberataques afectan a pequeños negocios. (Small Business Trends)
- 230,000 nuevos malware son producidos cada día, y se predice que este número crecerá.

  Panda https://www.ibm.com/downloads/cas/ZYKLN2E3
- 90% de los hackers cubren sus rastros utilizando cifrado.

  Vanson Bournehttps://www.venafi.com/assets/pdf/wp/Venafi_2016CIO_SurveyReport.pdf
- A una compañía le toma entre 6 meses, o 197 días, detectar una brecha de seguridad.

  ZD net https://www.zdnet.com/article/businesses-take-over-six-months-to-detect-data-breaches/
- Windows es el sistema operativo más atacado por hackers, Android viene en segundo lugar..

  Computer Word https://www.computerworld.com/article/2475964/98--of-mobile-malware-targets-android-platform.html
- Hubo más de 3 millones de golpes de crypto jacking entre Enero y Mayo del 2018. (Quick Heal)

  DECCAN Chronicle https://www.deccanchronicle.com/technology/in-other-news/260618/3-million-cryptojacking-hits-detected-in-2018-so-far-research.html

Referencias Estadisticas

Costo de la seguridad Informática

- El mercado de la seguridad informática crecerá un 8.7% en el 2019, llegando a los $124 billones. (Computer Weekly)
- El costo total de un ciberataque exitoso es de más de $5 millones de dólares. (Ponemon)
- El componente más caro de un ataque virtual es la pérdida de datos, que representa un 43% de los costos. (Accenture)
- Se proyecta que el daño relacionado a ciberataques llegará a los $6 trillones de dólares anuales para el 2021. (CyberSecurity Ventures)
- La brecha de seguridad de Equifax le costó más de $4 billones a la empresa. (Time)
- Los dos ataques más frecuentes son los ataques de malware y aquellos basados en la web. Las empresas gastan un estimado de $2.4 millones en defensa. (Accenture)

Referencias Estadisticas

Ransomware

- Ocurren más de 4,000 ataques de ransomware por día. (FBI)
- 75% de las organizaciones infectadas con ransomware tenían protección activa. (Sophos)
- Los daños globales relacionados a ataques de ransomware llegarán a $11.5 billones en el 2019. (Cybersecurity Ventures)
- Se estima que habrá un ataque de ransomware cada 14 segundos para el fin del 2019. Esto no incluye ataques a individuos, que ocurren con mayor frecuencia. (Cybersecurity Ventures)
- 91% de los ataques comienzan con la técnica de spear phishing, que apunta a vulnerar correos e infectar organizaciones. (KnowBe4)

Referencias Estadisticas

Phishing

- En una encuesta realizada a más de 1300 profesionales de TI se descubrió que 56% de las organizaciones identificaron al phishing como su mayor riesgo de seguridad informática. (CyberArk)
- 76% de las negocios reportaron ser víctimas de ataques phishing en el último año. (Wombat Security)
- Verizon reporta que usuarios Estadounidenses abren un 30% de todos los correos maliciosos y un 12% de ellos dan clic al enlace peligroso. (Verizon)
- Kaspersky's ha detectado 246,231,645 intentos de phishing en el 2017, y evidenció un crecimiento de 91 millones con respecto al 2016. (Kaspersky)

Conceptos de Seguridad

- En la actualidad, la seguridad de la información ha adquirido gran auge, dadas las cambiantes condiciones y las nuevas plataformas de computación disponibles.
- Muchas organizaciones han desarrollado documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones con el objeto de obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas.
- Las políticas de seguridad informática (PSI) surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y la sensibilidad de la información y servicios críticos que favorecen el desarrollo de la organización y su buen funcionamiento.

Consideraciones de seguridad

El Porque de la Seguridad

- La “red de redes” interconecta a prácticamente la totalidad de la población mundial, permitiendo la compartición de información a nivel global.

- Internet permite la interactividad entre usuarios, y ahí es donde radica el principal problema de seguridad

Hay que contestar a tres preguntas básicas:

- Que proteger
- De quien protegerlo
- Como protegerlo

Que proteger

- Datos
  - Robo : Puede hacerle muchísimo daño que le roben información confidencial casos de espionaje industrial por la red son cada vez más frecuentes
  - Modificación : Es el ataque más sutil de todos y puede causar grandes daños a la infraestructura de una organización.
  - Destrucción : Que por un descuido toda la información valiosa sea destruida, y se pierda el trabajo realizado durante mucho tiempo.
- Programas
  - Porque son una forma de acceso a los datos, manejan la información y acceden al sistema. Back Orifice (Puertas Traseras).

Qué Proteger

Hardware:

- En algunas ocasiones los hacker prefieren utilizar los recursos disponibles, mas que los propios datos.

  Ejemplo: para iniciar un ataque desde una máquina y así permanecer en el anonimato.

- Utiliza las maquinas como servidores ilegales(FTP) o utiliza los recursos para acceder a servicios a los que normalmente no accedería.

Que Proteger

- Imagen

No hay nada que produzca más desconfianza, que una empresa que ha sido atacada o que ha sido usada como soporte para un ataque a una tercera.

Cuando se encuentra una brecha de seguridad, esta es inmediatamente conocida en la red, lo cual provoca que los ataques se multipliquen a menos que la brecha sea rápidamente contenida.

De Quien Protegerlo

- Existen dos tipos de atacantes por lo que hay q preocuparse los hacker y los Tinyhacker.
- Los ataques pueden clasificarse en 3 tipos genéricos:

  Desmantelamiento de sistemas Son ataques de Denial of Service. Estos ataques tienen como fin colapsar una o más máquinas, haciendo que se “cuelguen”, e incluso provocando la perdida de datos.

  Robo de datos: Para robar datos la forma más básica es conseguir una combinación de login/password de algún usuario.

  Intrusión: Estos ataques consiguen que el hacker tenga acceso remoto a otra máquina, y por tanto puede usar los recursos de esta

Como Protegerlo

- La importancia de los datos a proteger.
- El presupuesto disponible para seguridad
- Es necesario conocer los riesgos asociados a cada servicio que se permita en la red.
- La mayoría de los ataques comienzan desde dentro de la propia organización.
- Añadir seguridad en los equipos finales.

Objetivo de la Seguridad

- Garantizar acceso a los recursos deseados para los usuarios autorizados.
- Garantizar la autenticidad e integridad de los datos.
- Garantizar la identificación de los interlocutores
- Garantizar la confidencialidad de los datos.

Definiciones

- **Seguridad informática**

Consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida, así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.

Seguridad de la información

Conocimiento obtenido a partir de la investigación, el estudio o instrucción, inteligencia, noticias, hechos, datos, una señal o carácter (como en un sistema de comunicación o computadora) representando datos, algo (como un mensaje, datos experimentales o una imagen) que justifique el cambio en una construcción (como un plan o una teoría) que representa la experiencia física o mental u otra construcción (de acuerdo con el diccionario en línea Merriam-Webster (que se encuentra http://www.m-w.com/)).

Definiciones

seguridad informática

Es *una serie de mecanismos que minimizan la vulnerabilidad de bienes y recursos,* donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene.

Para ello, se han desarrollado protocolos y mecanismos adecuados, para preservar la seguridad

Definiciones

Seguridad en Redes

- Un conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o de la información en ellos contenida.
- Mantener bajo **protección los recursos que se** cuenta en la red, a través de procedimientos basados en una **política de seguridad informática (PSI).**

No existe la seguridad total: ante cualquier coraza de protección, siempre se podrá encontrar un elemento capaz de romperla.

Definiciones

Seguridad de los Sistemas de Información

Es la protección de los sistemas de información respecto al acceso no autorizado o modificación de la información en el almacenamiento, proceso , tránsito y contra la denegación de servicio para los usuarios autorizados, incluyendo aquellas medidas necesarias para detectar, documentar y contrarrestar dichas amenazas (según *INFOSEC Glossary 2000)*.

Sistema de Seguridad

Es un conjunto de elementos que permiten al usuario realizar ciertas operaciones en función del nivel de responsabilidad que le ha sido asignado. Este nivel de responsabilidad depende del puesto que ocupe el usuario del sistema

Otras Definiciones

- OSI 7498
  - Seguridad está relacionada con la reducción de las vulnerabilidades
  - "**seguridad de una red**" implica la seguridad de cada uno de las dispositivos de la red
  - Vulnerabilidades son debilidades que pueden ser exploradas para la violación de sistemas o informaciones
  - Amenaza
    - potencial violación de seguridad
    - condición o acción que compromete la seguridad
  - "Amenaza o ataque"**:** intento de sabotear una operación o la propia preparación para sabotearla (poner en compromiso)
- Riesgo: se define como el daño potencial que puede surgir por un proceso o evento ya sea presente o futuro.

Servicios de Seguridad

El servicio que mejora la seguridad de los sistemas de procesamiento de datos y la transferencia de información de una organización.

- Confidencialidad o Secreto
- Autenticación
- Integración
- No repudiación
- Disponibilidad

Servicios de Seguridad

Confidencialidad

- ¿lo ha interceptado alguien más?
- Los componentes del sistema serán accesibles sólo por aquellos usuarios autorizados.

- Servicio que garantiza la privacidad de los datos:
  - En local.
  - En conexiones.
  - En modo no conectado.
  - En campos selectos.
  - En flujo de datos.
- Entre los mecanismos que implementan este servicio están:
  - PGP, SSL, RSA, DES,

Servicios de Seguridad

Autenticación

Demostrar la identidad de las entidades involucradas en la transacción. Evita que alguien tome la identidad de otro. Generalmente toma dos formas:

- Autenticación de origen. Cuando se garantiza que la entidad origen de la comunicación es quien dice ser.
- Autenticación de destino. Cuando se garantiza que la entidad destino de la comunicación es quien dice ser

Algunos ejemplos de los mecanismos que permiten implementar este servicio son:

login, password.

Kerberos.

S/Key.

Servicios de Seguridad

Control de Acceso

- Permite definir quién puede tener acceso a ciertos recursos, dependiendo de los privilegios o atributos que posea.
- Permite proteger los recursos del sistema contra el uso no autorizado.
- Se basa en credenciales o atributos .
- Se aplica a los usuarios y procesos que ya han sido autentificados.
- Como ejemplos de mecanismos para este servicio podemos mencionar:
  - Los permisos en los archivos de Unix.
  - Los *tickets* en Kerberos.
  - Los niveles de autorización en un sistema militar

Servicios de Seguridad

Integridad

- ¿puedo asegurar que este mensaje esta intacto?
- Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

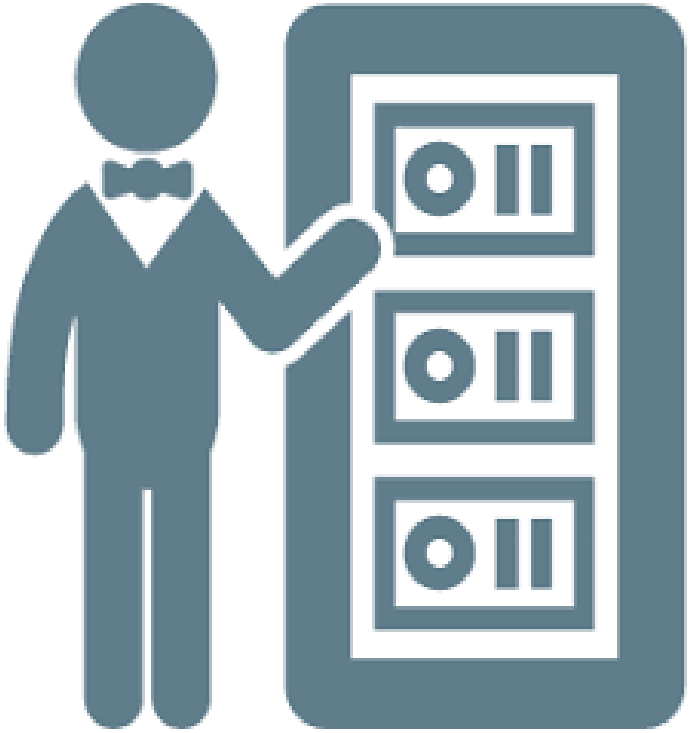
- Permite proteger los datos contra ataques activos.
  - Con recuperación de datos.
  - Sin recuperación de datos.
  - En campos selectos.

- Se aplican mecanismos por ejemplo mediante un hash criptográfico con firma.
- La integridad de secuencia de datos asegura que la secuencia de los bloques o unidades de datos recibidas no ha sido alterada.

Servicios de Seguridad

Disponibilidad

Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.



Servicios de Seguridad

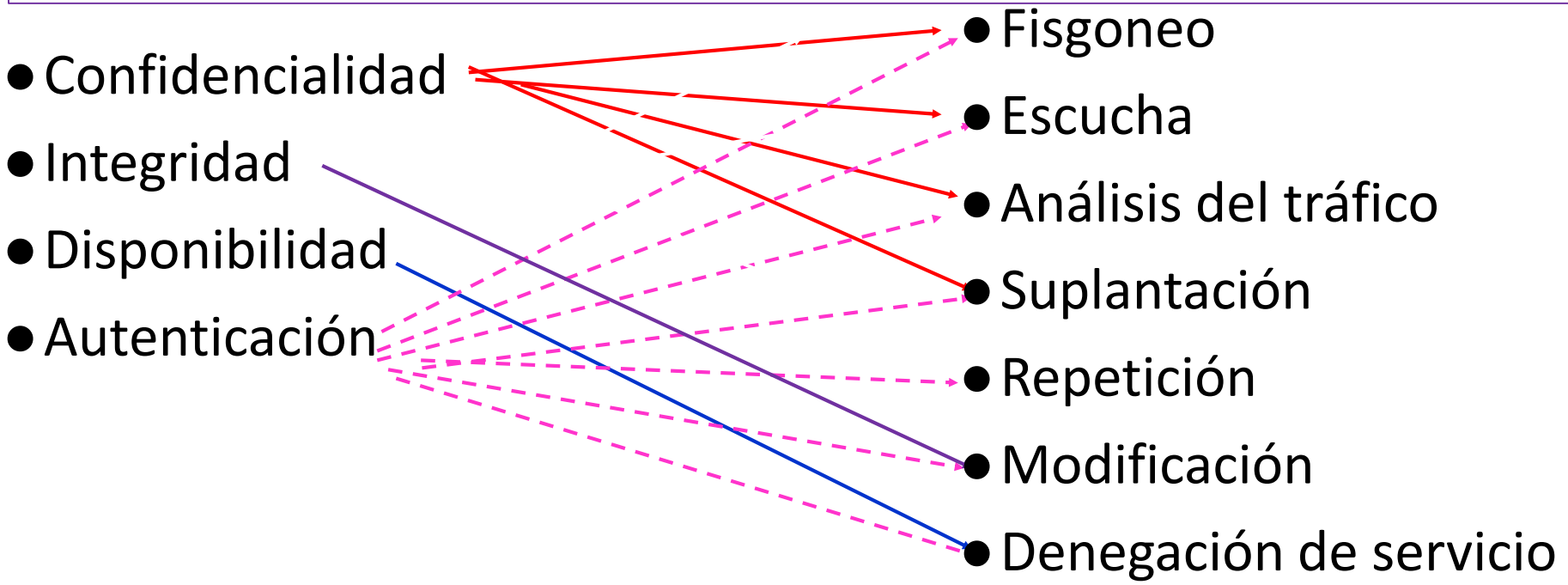
No Repudio:

¿ha enviado/recibido esto realmente? mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

- **No repudio con prueba de origen**: en este caso, el receptor del mensaje adquiere una prueba, demostrable ante terceros, del origen de los datos recibidos. En muchos casos puede bastar las garantías que el emisor introduce en el mensaje cuando aplica los mecanismos que aseguran la autenticación del origen de los datos
- **No repudio con prueba de envío**: el receptor o el emisor del mensaje adquieren una prueba, demostrable ante terceros, de la fecha y hora en que el mensaje fue enviado.
- **No repudio con prueba de entrega**: el emisor del mensaje adquiere una prueba, demostrable ante terceros, de que los datos han sido entregados al receptor adecuado.

- Es necesario garantizar que alguien que haya efectuado un pago no pueda negar haberlo hecho

Servicios y ataques



Seguridad Lógica

Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

- ✓Los objetivos que se plantean serán:
- ✓Restringir el acceso a los programas y archivos.
- ✓Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓Que la información recibida sea la misma que ha sido transmitida.
- ✓Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓Que se disponga de pasos alternativos de emergencia para la transmisión de información.

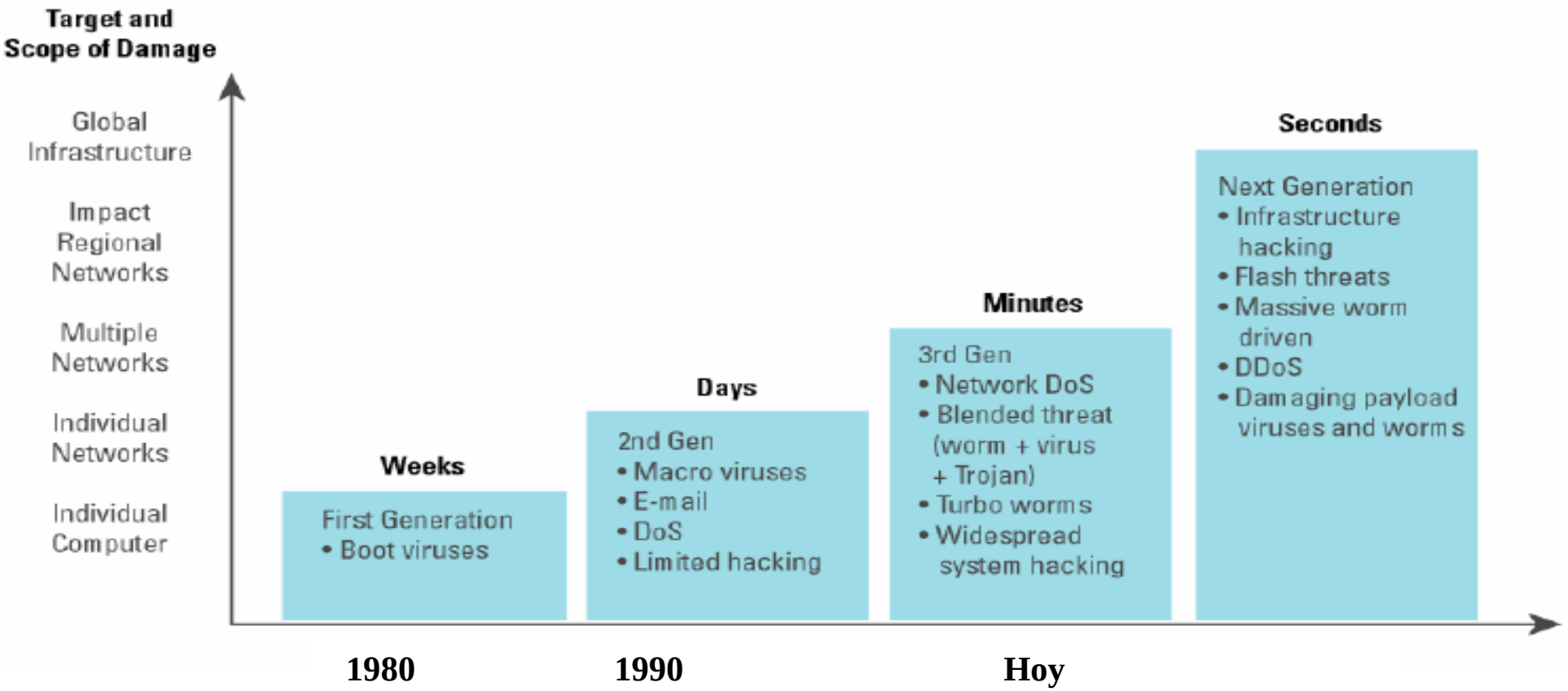
Amenazas Vulnerabilidades y Ataques

El Reto en la Seguridad

- Los sistemas de Tecnologías de la Información…
  - … cambian rápidamente
  - … son cada vez más complejos

Y los “Hackers” son más sofisticados, y hacer “Hacking” cada vez más fácil.

Ataques: pasado y presente



Atacantes

☹Personas llevadas por desafío intelectual o por aburrimiento

☹(Ex)Empleados vengativos

☹Personas (empleados, clientes, delincuentes) que buscan beneficio económico

☹Delincuencia organizada que quiere ocultar actividades ilegales

☹Espías de compañías o países rivales con fines económicos, políticos o militares

☹Terroristas o naciones que intentan influir en la política de un estado

☹Usuario que mete la pata

☹Fenómeno de la naturaleza (huracán, terremoto, …) que causa catástrofes

Tipos de atacantes

Hackers:

- Definición inicial de los ingenieros del MIT que hacían alardes de sus conocimientos en informática. Pirata Informático.

Se refiere a un experto, son las personas que poseen mayor conocimiento en informática, dentro de las áreas de programación, redes de computadoras, sistemas operativos, etc. un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas. El cual usa sus conocimientos para actos lícitos o no lícitos en algunos casos.

Tipos de atacantes

Cracker:

- Persona que intenta de forma ilegal romper la seguridad de un sistema por diversión o interés.
- No existe uniformidad de criterios en su clasificación; no obstante, su acción cada día se vuelve más técnica, sofisticada y debemos implementar medidas para proteger nuestra información ante tales ataques.

Tipos de atacantes

Lammers

- Individuos con ganas de hacer Hacking
- Carecen de cualquier conocimiento.
- Son individuos que apenas si saben lo que es un computador, pero el uso de este y las grandes oportunidades que brinda Internet, convierten al nuevo internauta en un obsesivo ser que rebusca y relee toda la información que le fascina y que se puede encontrar en Internet.
- El grupo que más peligro acontece en la red ya que ponen en práctica todo el Software de Hackeo que encuentran en la red

Copyhackers

- Nueva raza.
- Emplean la ingeniería social para convencer y entablar amistad con los verdaderos Hackers, les copian los métodos de ruptura y después se los venden a los " bucaneros ".
- Poseen conocimientos de la tecnología y son dominados por la obsesión de ser superiores, pero no terminan de aceptar su posición. Por ello " extraen " información del verdadero Hacker para terminar su trabajo.
- La principal motivación, el dinero.

Tipos de atacantes

- **Bucaneros**
  - Son peores que los Lamers, ya que no aprenden nada ni conocen la tecnología.
  - Buscan el comercio negro de los productos entregados por los Copyhackers.
  - Los bucaneros sólo tienen cabida fuera de la red, ya que dentro de ella, los que ofrecen productos " Crackeados " pasan a denominarse " piratas informáticos "
  - Es simplemente un comerciante, el cual no tienen escrúpulos a la hora de explotar un producto de Cracking a un nivel masivo.

- **Phreaker**
  - Es una extensión del Hacking y el Cracking.
  - Es conocido en la Red por sus conocimientos en telefonía.
  - Posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. También de tarjetas prepago, ya que la telefonía celular las emplea habitualmente.

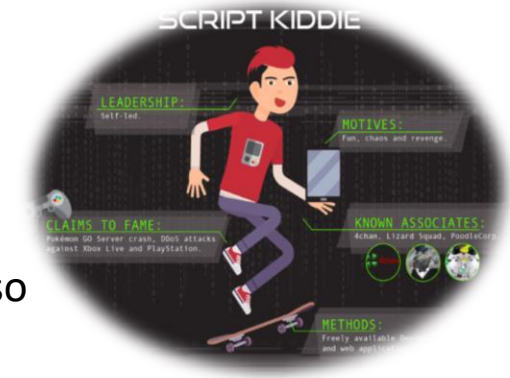
Tipos de atacantes

Newbie

- Es un novato o más particularmente es aquel que navega por Internet, tropieza con una página de Hacking y descubre que existe un área de descarga de buenos programas de Hackeo.
- Al contrario que los Lamers, los Newbies aprenden del Hacking siguiendo todos los cautos pasos para lograrlo y no se mofa de su logro, sino que aprende.

Script Kiddie

- Denominados Skid kiddie o Script kiddie
- son el último eslabón de los clanes de la Red.
- Son simples usuarios de Internet, sin conocimientos sobre Hack o el Crack en su estado puro.
- En realidad son devotos de estos temas, pero no los comprenden. Simplemente son internautas que se limitan a recopilar información de la Red. En realidad se dedican a buscar programas de Hacking en la Red y después los ejecutan sin leer primero los ficheros Readme de cada aplicación.
- Sueltan un virus, o se cansan de ellos mismos su propio ordenador.
- Les llaman los “ pulsa botones “ de la ReD. Los Kiddies en realidad no son útiles en el progreso del Hacking.



Tipos de atacantes

Spammer:

- Persona o grupo dedicados a la distribución de correo electrónico no deseado, spam o spamdexing. La actividad suele resultarles sumamente lucrativa, pero está muy mal vista por la mayoría de los usuarios y empresas de internet, de hecho es ilegal en muchos países.

Wannabe:

Término creado por los hackers para designar a aquellos que podrán llegar a ser un hacker, pero que aún le falta conocimiento para serlo.

Tipos de atacantes

White hat

- Son profesionales que prueban que tan vulnerable es un sistema, y realizar un reporte detallado el cual servirá para mejorar el sistema, son conocidos como auditores de seguridad informática.
- Contenido de calidad.
- Generan contenido propio.
- Uso adecuado de palabras claves.
- Consiguen enlaces éticamente.
- Se integran a una comunidad.
- Protegen la reputación de la marca.

Black hat

- Vulneran un sistema, extraen información sensible.
- Contenido oculto.
- Copian contenido.
- Repetición ilógica de una palabra clave.
- Hacen granjas de enlaces (link farming).
- Comentan en blog cosas sin sentido (SPAM).
- No les interesa la reputación de la marca para la que trabajan.

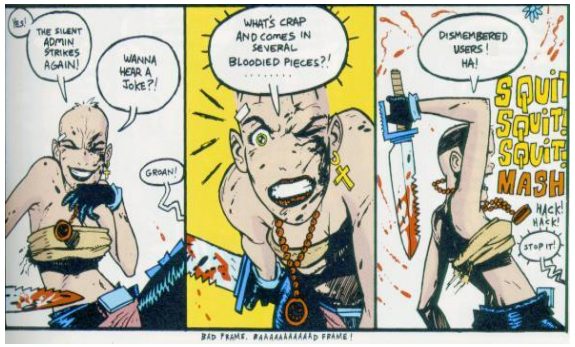
Grey hat

Son aquellos que un día son buenos, y quizás en el mismo día, son también malos. Su comportamiento se identifica cuando son los que detectan vulnerabilidades, y en el caso de que no se les contrate para subsanarlas, son los mismos que las explotan, y así consiguen su cometido a la buena o a la mala.

Tipos de atacantes

La nueva generación o los ¨Scripters¨

- Gente con la capacidad de buscar un programa en la red y ejecutarlo.
- No hay una meta fija.
- Necesidad de pertenencia, aunque sea al inframundo.
- No hay preocupación por las consecuencias reales de sus actos.
- Se sienten muy ¨cool¨.



Ingeniería Social

"Usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Lo único que se necesita es un llamado a un empleado desprevenido e ingresan sin más. Tienen todo en sus manos." **Kevin Mitnick.**

Ingeniería social

Nos referimos a un proceso de estudio tomado por personas, el cual consiste en tomar técnicas sicológicas y habilidades sociales, utilizadas para llegar a obtener algún tipo de información o algún material requerido por la persona, así mismo recaudando esta información de manera penal o no legalizada por la ley.

Cibercrimen

- Infección en varios barcos de la Royal Navy, pierden acceso a correo electrónico e Internet
- Hospitales de Sheffield infectados, +800 PCs
- 3 hospitales de Londres sin red por infección
- Houston, infección en juzgados obliga a suspender arrestos
- Parte de la red de los US Marshals (división del Departamento de Justicia de Estados Unidos) tuvo que ser desconectada para limpiar una infección.

- Apertura de centro contra cibercrimen. http://www.elmundo.es/elmundo/2013/01/11/union_europea/1357921246.html
- http://conacytprensa.mx/index.php/tecnologia/tic/9327-los-mecanismos-y-costos-del-cibercrimen
- http://www.lanacion.com.ar/1921344-cibercrimen-el-auge-de-los-delitos-de-acoso-virtual

Ciberterrorismo.

- Considerar ahora a una nación como su objetivo de ataque; el ciberterror como evolución del terrorismo tradicional y el cibercrimen como la transformación de la delincuencia en medios informáticos y electrónicos.
- El ciberterrorismo es la convergencia entre el terrorismo y el ciberespacio, una conjunción de fuerzas que utilizando las ventajas y capacidades del terrorismo físico, ahora basado en fallas y vulnerabilidades tecnológicas, logran intimidar o presionar a un estado y sus ciudadanos.
- Algunos establecen que el ciberterrorismo esta relacionado con las vulnerabilidades propias de las infraestructuras críticas de una nación: energía eléctrica, producción, almacenamiento y suministro de gas y petróleo, telecomunicaciones, bancos y finanzas, sistemas de suministro de agua, transporte, servicios de emergencia y operaciones gubernamentales, aquellos sistemas que hacen parte de la dinámica de la economía de un país y el bienestar de los ciudadanos.

- http://cxo-community.com/articulos/blogs/blogs-seguridad-publica/5271-cibercrimen-y-ciberterrorismo-dos-amenazas-emergentes.html
- http://mundo.sputniknews.com/tecnologia/20160604/1060407678/kaspersky-ciberterrorismo.html

Ciberterrorismo

- DDoS sobre la república asiática de Kyrgyzstan (MyDoom)
- Grupo chino hackea la página web del consulado ruso en Shangai
- NYPD, ataque para entrar en su red interna; 70.000 intentos diarios, provenientes principalmente de China
- Webs, principalmente gubernamentales, de Estados Unidos y Corea del Sur fueron víctimas de un ataque DDoS
- Ataque contra diversos sitios gubernamentales de Polonia. El ataque, de nuevo, venía desde Rusia.
- Ministro suizo de exteriores víctima de un ataque dirigido por parte de hackers

ELPAIS.com > Sociedad > Domingo

REPORTAJE: LA GUERRA DE LOS CIBERESPÍAS

España, blanco de más de cuarenta ciberataques

España sufrió más de 40 ataques informáticos "graves" en 2009. Instituciones clave fueron el objetivo de 'troyanos' diseñados al efecto. El Centro Nacional de Inteligencia (CNI) es uno de los organismos 'tocados'

JOSEBA ELOLA 24/01/2010

Vota ☆☆☆☆☆ Resultado ★★★★½ 181 votos Comentarios - 81

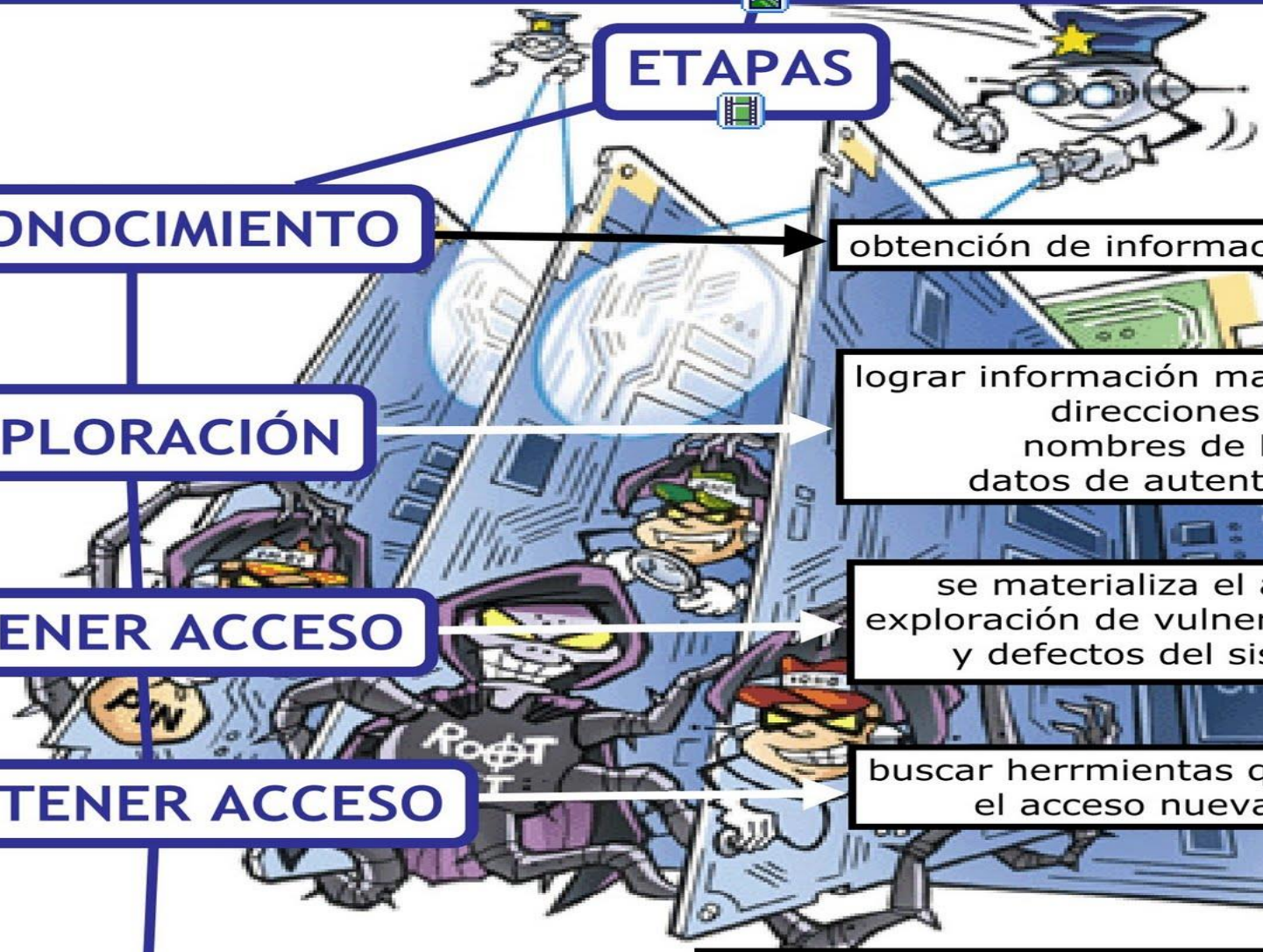
Ciberespías que escudriñan los correos electrónicos de sus enemigos. Que se infiltran en redes vitales para la seguridad mundial. El caso Google ha puesto en el ojo del huracán la batalla de espionaje que China y Estados Unidos libran en la Red. Pues bien, España, aunque está lejos de los niveles de tensión que respiran las dos potencias, no vive ajena a los intentos de ciberespionaje.

Noticias

- http://revista.seguridad.unam.mx/numero25/tic-internet-y-ciberterrorismo-iii
- http://blogs.protegerse.com/laboratorio/category/cibercrimen-2/
- http://www.enhacke.com/tag/cibercriminales/
- http://www.elmundo.es/espana/2016/04/08/5706bead22601dae7a8b45bd.html
- http://www.lexnews.es/la-comprension-psicojuridica-de-los-ciberdelincuentes-y-cibercriminales/
- http://highsec.es/2013/03/introduccion-a-la-navegacion-anonima-tor/
- http://tic-seguridad.blogspot.com/p/definiciones-fundamentales.html

ANATOMÍA DE UN ATAQUE INFORMÁTICO

ETAPAS



RECONOCIMIENTO → obtención de información

EXPLORACIÓN → lograr información mas detallada:
direcciones IP
nombres de host
datos de autenticación

OBTENER ACCESO → se materializa el ataque
exploración de vulnerabilidades
y defectos del sistema

MANTENER ACCESO → buscar herrmientas que permitan
el acceso nuevamente

BORRAR HUELLAS → borrar huellas dejadas en la intrusión:
(archivos de registro),
alarmas de sistema de detección de intrusos (IDS)

Principales vulnerabilidades **en un sistema informático**

- De configuración:
  - Si la gestión administrable por el usuario es tal que hace que el sistema sea vulnerable, la vulnerabilidad no es debida al diseño del mismo si no a cómo el usuario final configura el sistema.
  - También se considera error de este tipo cuando la configuración por defecto del sistema es insegura, por ejemplo una aplicación recién instalada que cuenta de base con usuarios por defecto.
- Validación de entrada:
  - Este tipo de vulnerabilidad se produce cuando la entrada que procesa un sistema no es comprobada adecuadamente de forma que una vulnerabilidad puede ser aprovechada por una cierta secuencia de entrada.
- Inyección SQL :
  - una vulnerabilidad informática en el nivel de base de datos de una aplicación. El origen es el filtrado incorrecto de las variables utilizadas en las partes del programa con código SQL.
  - Una inyección de código SQL sucede cuando se inserta un trozo de código SQL dentro de otro código SQL con el fin de modificar su comportamiento, haciendo que ejecute el código malicioso en la base de datos.

Principales vulnerabilidades **en un sistema informático**

- **Inyección de código**:
  - **Inyección directa de código estático:** el software permite que las entradas sean introducidas directamente en un archivo de salida que se procese más adelante como código, un archivo de la biblioteca o una plantilla
  - **Evaluación directa de código dinámico:** el software permite que las entradas sean introducidas directamente en una función que evalúa y ejecuta dinámicamente la entrada como código
  - **Inclusión remota de archivo PHP:** vulnerabilidad existente únicamente en paginas dinámicas escritas en PHP
- **Error de búfer**:
  - **El desbordamiento del búfer:** un búfer se desborda cuando, de forma incontrolada, al intentar meter en él más datos de los que caben, ese exceso se vierte en zonas del sistema causando daños.
  - **El agotamiento del búfer:** es un estado que ocurre cuando un búfer usado para comunicarse entre dos dispositivos o procesos se alimenta con datos a una velocidad más baja que los datos se están leyendo en ellos.
- **Errores numéricos**:
  - **El desbordamiento de entero (integer overflow):** un desbordamiento del número entero ocurre cuando una operación aritmética procura crear un valor numérico que sea más grande del que se puede representar dentro del espacio de almacenaje disponible.
  - **El agotamiento de entero (integer underflow):** consiste en que un valor se resta de otro, que es menor que el valor mínimo del número entero, y que produce un valor que no es igual que el resultado correcto.

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 suelta, 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.
- **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,

Amanazas

- **Físicas:**
  - La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.
- **Lógicas:**
  - Nos referimos a todo tipo de programas que de una forma u otra pueden dañar a nuestro sistema, creados de forma intencionada para ello (*software* malicioso, también conocido como *malware*) o simplemente por error (*bugs* o agujeros).

Amenazas Físicas

- Principales amenazas
  - Desastres naturales, incendios accidentales, tormentas e inundaciones.
  - Amenazas ocasionadas por el hombre.

    Disturbios, sabotajes internos y externos deliberados.

- Controlar el ambiente y acceso físico permite:
  - Disminuir siniestros.
  - Trabajar mejor manteniendo la sensación de seguridad.
  - Descartar falsas hipótesis si se produjeran incidentes.
  - Tener los medios para luchar contra accidentes.

Amenazas

- Amenazas accidentales:

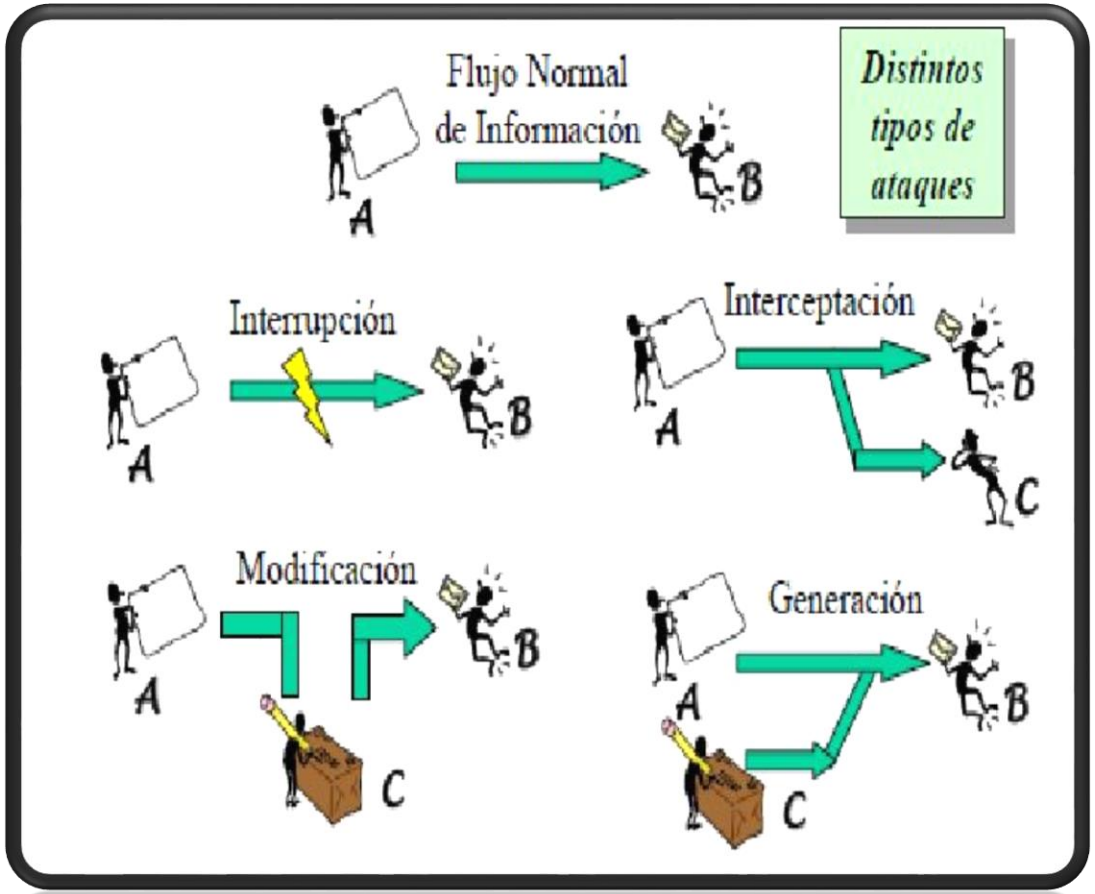
Son las que aparecen de forma no premeditada.

- Amenazas intencionales:

Se producen cuando existe voluntad de uso indebido de ciertos recursos.

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**

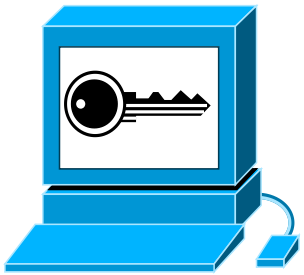


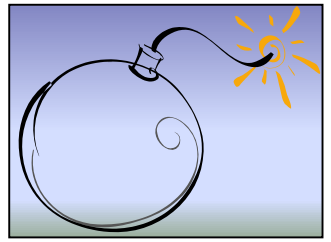
Amenazas

- Intercepción de datos en tránsito
- Acceso a programas o datos en anfitriones remotos
- Modificación de programas o datos en anfitriones remotos
- Modificación de datos y programas al vuelo.

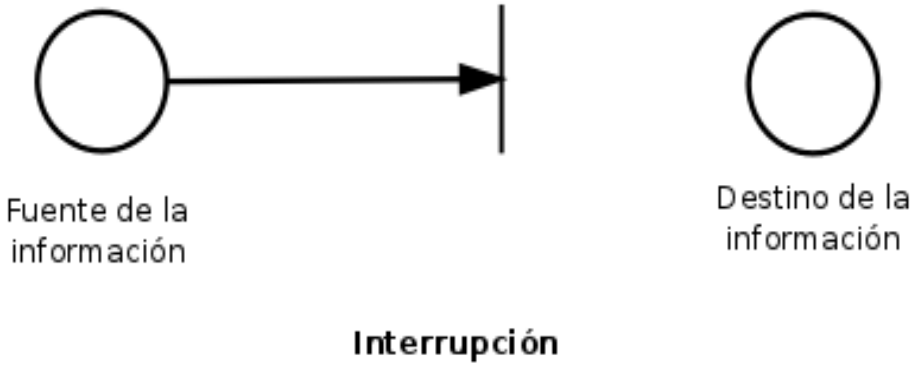
Amenazas (Threats)

- Suplantación de un usuario para añadir comunicaciones
- Inserción de una repetición de una secuencia
- Bloqueo de tráfico selecto
- Denegación del servicio
- Ejecución de un programa en un anfitrión remoto
- Interrupción de servicios (DoS)
- Intercepción (Ataque a la confidencialidad)
- Modificación
- Fabricación (Ataque a la autenticidad)
- Violación de autorización
- Masquarade
- Repudiación
- Spoofing
- Penetración al sistema
- Ingeniería Social





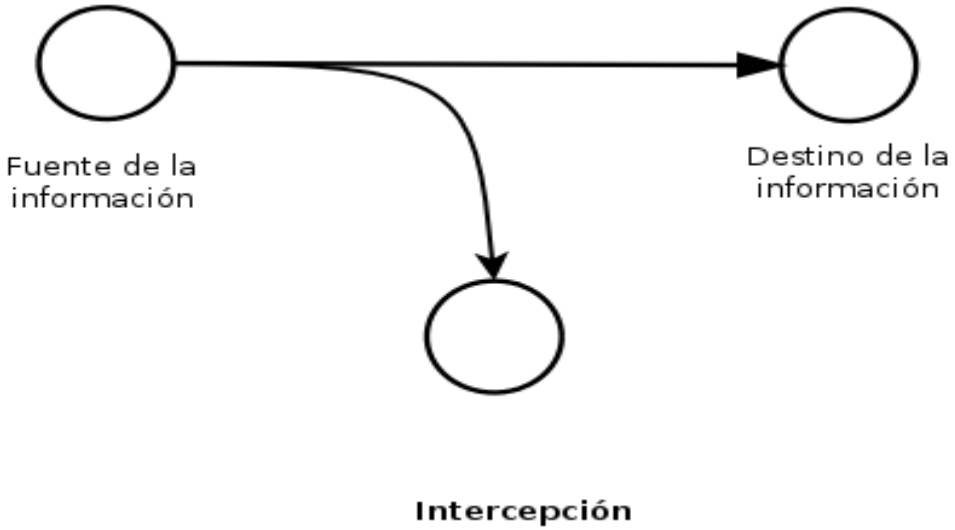
Amenazas de Interrupción



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

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

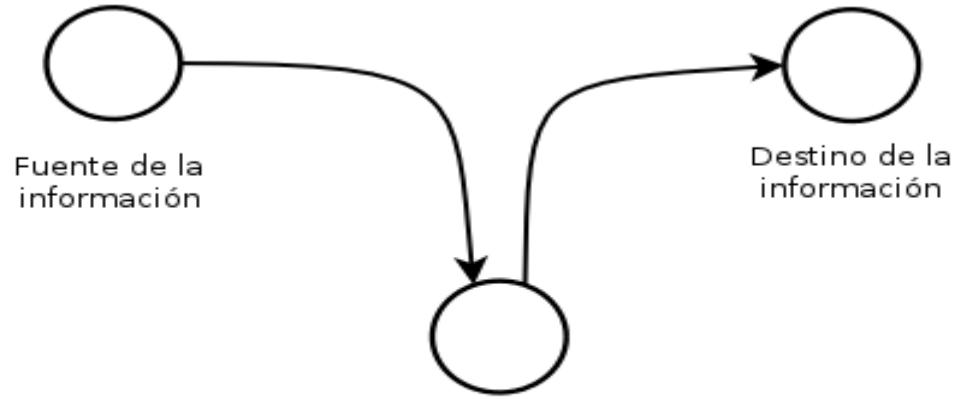
Amenazas de Intercepción



- Una entidad no autorizada consigue acceder a un recurso. Esto es un ataque contra la confidencialidad

Ejemplos: Escucha en un canal de comunicación para obtener datos.
Obtención de datos con troyanos, copia ilícita de archivos o programas

Amenazas de Modificación

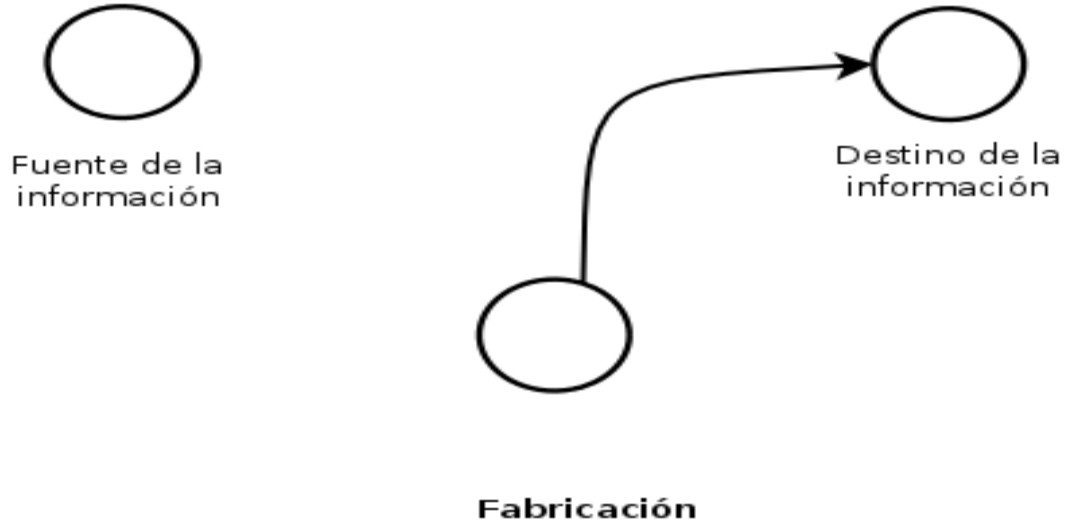


Modificación

- Acceso no autorizado que cambia los datos para su beneficio.
- Su detección es difícil según las circunstancias.
- Amenaza la integridad

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

Amenazas de Fabricación



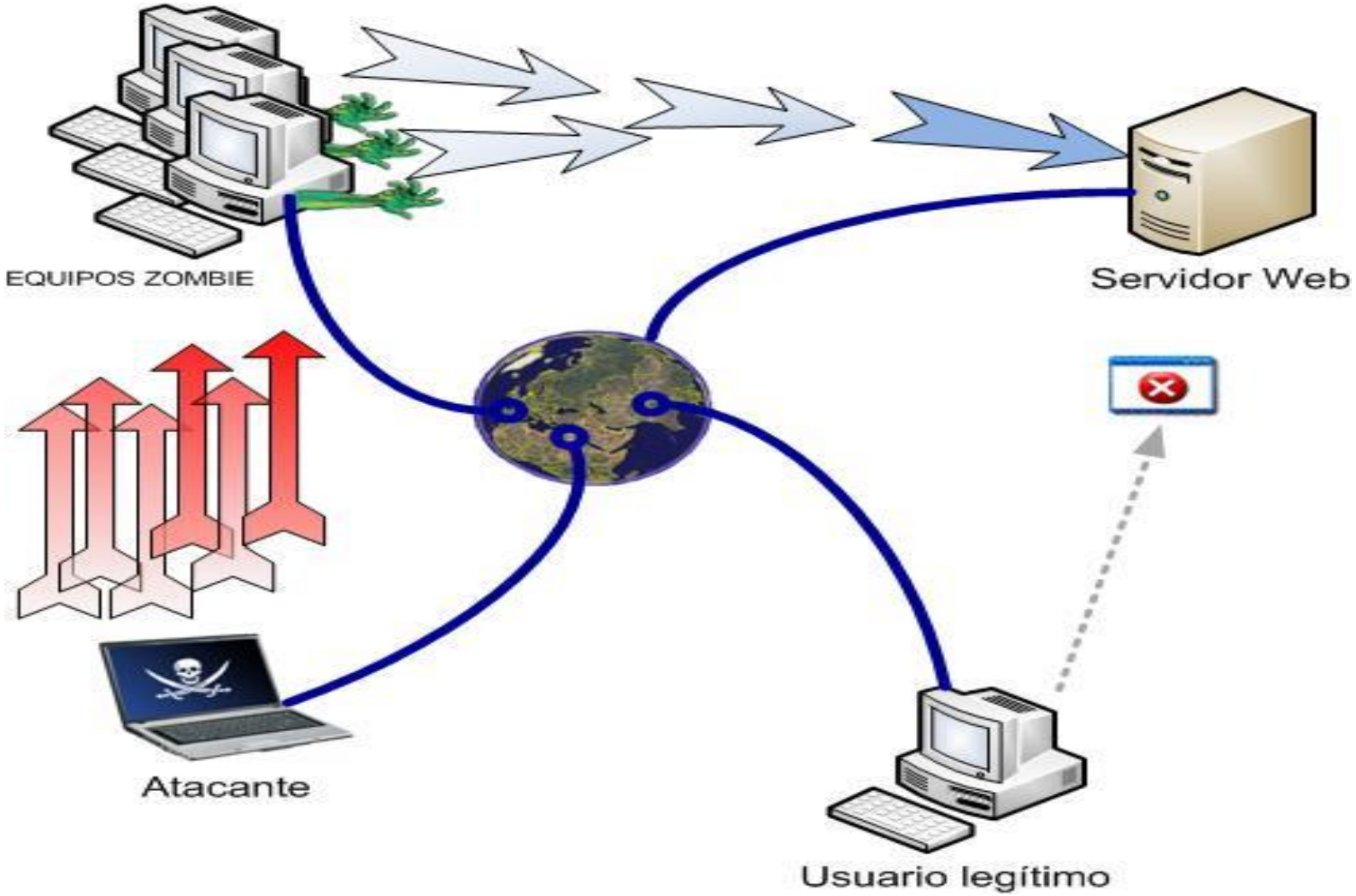
- Una entidad no autorizada inserta objetos falsificados en el sistema.
- Es un ataque contra la autenticidad.

Ejemplos: Inserción mensajes falsos en una red
Añadir datos a un archivo.

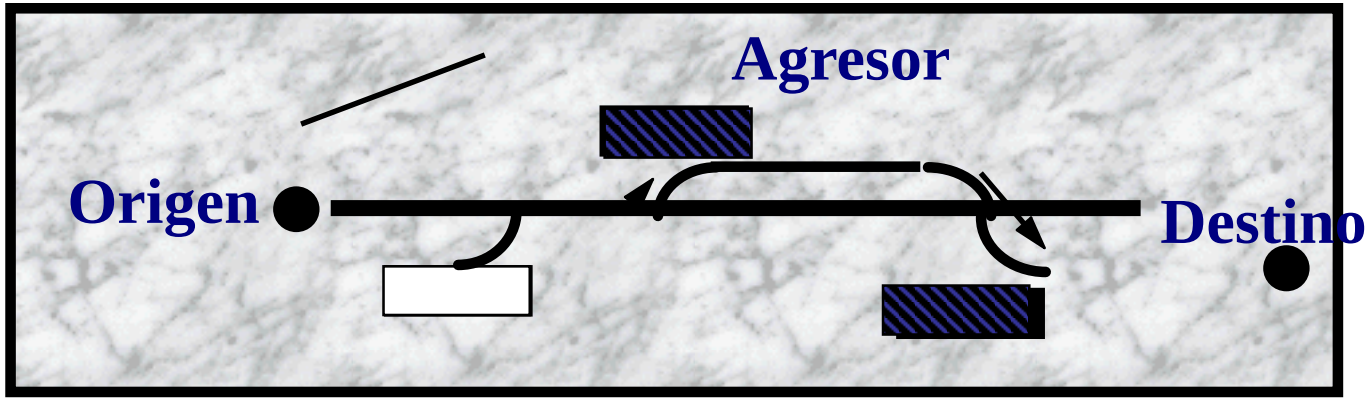
Modalidad de algunos ataques a la Seguridad de Redes

- Virus, gusanos, troyanos, tormentas, spam, espías, malware, adware …
- Ransomware: Secuestro de Documento/Carpeta mediante la encriptación
- SCAM: correos engañosos
- Spoofing: falsedad en dirección IP
- Phishing: recomendar una página Web falsa
- Eavesdropping y Packet Sniffing: pasiva intercepción (sin modificación) del tráfico de red
- Snooping y Downloading: obtener la información sin modificarla
- Flooding: Inundación (Negación de servicio)
- Tampering o Data diddling: la modificación no autorizada de los datos, o al software instalado en un sistema
- Ingeniería Social

- Amenazas - Ejemplos



- *Garantizar autenticidad e integridad de los datos*



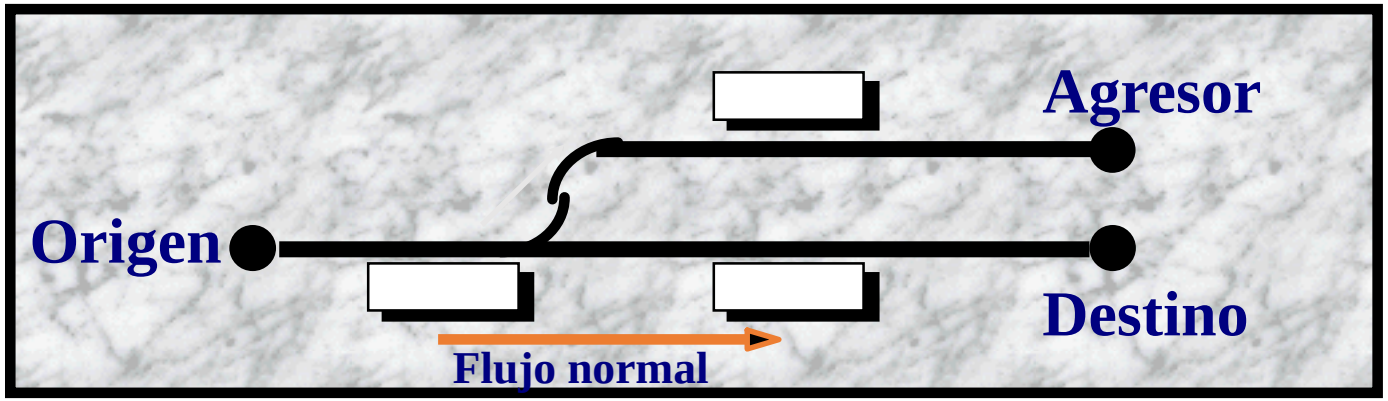
- *Replay* de mensajes antiguos
- Forjar mensajes

Amenazas - Ejemplos

- *Garantizar la identificación de los interlocutores*

Agresor enmascarado

Amenazas - Ejemplos



- Escucha (interceptación de mensaje
- *elemental, recursos poco sofisticados*

Amenazas - Ejemplos

- *Verificar la ocurrencia de evento*

- Renuncia de envío/recepción
- Tercera parte, neutra, árbitro
- Ej.: servicios de correos