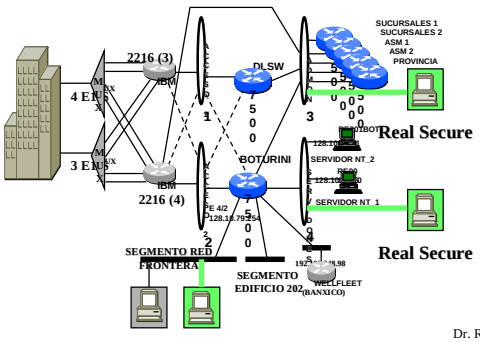
Introducción a la Seguridad Informática

Roberto Gómez Cárdenas
rogomez@itesm.mx
http://webdia.cem.itesm.mx/ac/rogomez

Antecedentes

- Las redes fueron diseñadas para el intercambio de información y compartir recursos.
- La seguridad no era un factor tomado en cuenta en el diseño de las redes.



Haciendo cuentas ...

- Computación electrónica 50 años !
- Redes sólo tienen 30 años de vida !
- Seguridad 23 años !
- Internet 15 años !
- Web 6 años !
- Intranets 3 años...
- Extranets 2 años...

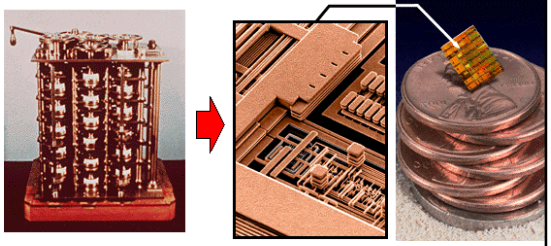


Lámina 4

Dr. Roberto Gómez C. (Seguridad en Redes)

Problema

- Desafortunadamente, este gran crecimiento incluirá (incluye) individuos deshonestos que se introducen a los sistemas de información
- Ninguna institución está libre del asecho de estos individuos.
- Todo el mundo alguna vez ha sido afectado por algún problema de seguridad.

Lámina 5 (Seg Redes)

Amenaza

- Circunstancia o evento que puede causar daño violando la confidencialidad, integridad o disponibilidad
- El termino se refiere a un evento (i.e. tornado, robo, infeccion por virus de computo, etc.)
- Frecuentemente aprovecha una vulnerabilidad

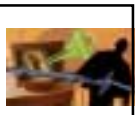
Lámina 6 Dr. Roberto Gómez C. (Seguridad en Redes)

Vulnerabilidad

- Ausencia de una contramedida, o debilidad de la misma, de un sistema informático que permite que sus propiedades de sistema seguro sean violadas.
- Condicion que tiene potencial para permitir que ocurra una amenaza, con mayor frecuencia e impacto.
- La debilidad puede originarse en el diseño, la implementación o en los procedimientos para operar y administrar el sistema.
- En el argot de la seguridad computacional una vulnerabilidad también es conocida como un *hoyo*.

Lámina 7 Dr. Roberto Gómez C. (Seguridad en Redes)

Tiempo vida vulnerabilidad



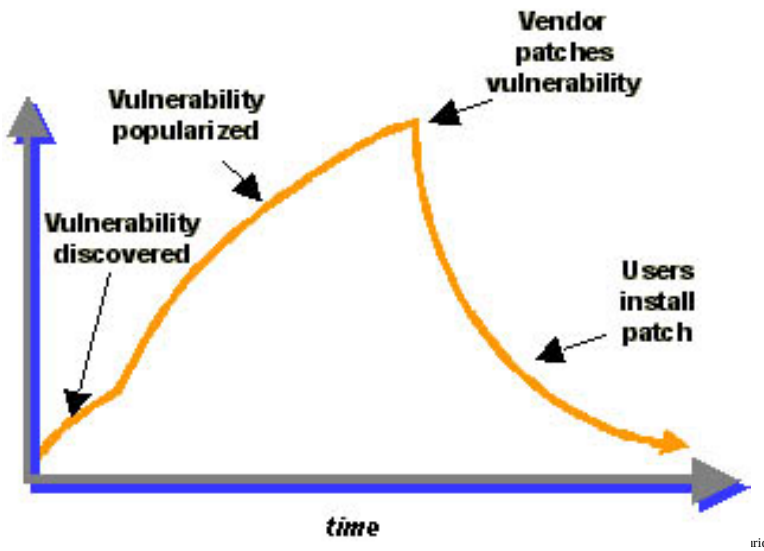
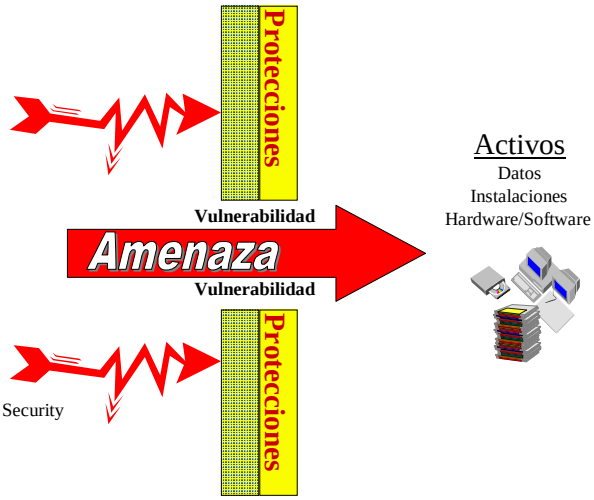


Lámina 8 ridad en Redes)

Vulnerabilidad vs amenaza



Source:
An Introduction to Computer Security
The NIST Handbook
NIST- Serial
Publication 800-12

Lámina 9
Dr. Roberto Gómez C. (Seguridad en Redes)

Riesgo

- El potencial para perdida o falla, como respuesta a las siguientes preguntas:
  - ¿Qué podría pasar (o cual es la amenaza)?
  - ¿Qué tan malo puede ser (impacto o consecuenia)?
  - ¿Qué tan frecuente puede ocurrir (frecuencia)?
  - ¿Qué tanta certidumbre se tiene en las primeras 3 respuestas (grado de confianza)?
- Notese que si no hay incertidumbre, no hay un riesgo per se.

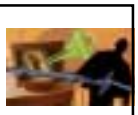
Lámina 10
Dr. Roberto Gómez C. (Seguridad en Redes)

El exploit

- Se refiere a la forma de explotar una vulnerabilidad
  - termino muy enfocado a herramientas de ataque, sobre equipos de computo).
- Aprovechamiento automático de una vulnerabilidad
  - generalmente en forma de un programa/software que realiza de forma automática un ataque aprovechandose de una vulnerabilidad

Lámina 11 Dr. Roberto Gómez C. (Seguridad en Redes)

Los ataques



- Acción o acciones que tienen por objetivo el que cualquier parte de un sistema de información automatizado, deje de funcionar de acuerdo con su propósito definido.
- Esto incluye cualquier acción que causa la destrucción, modificación o retraso del servicio no autorizado.

Lámina 12 Dr. Roberto Gómez C. (Seguridad en Redes)

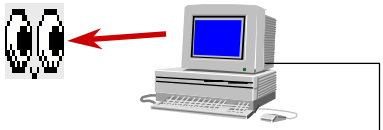
Aclaración ataque

- No es un ataque físico (aunque puede ser).
- Un ataque no se realiza en un solo paso.
- Depende de los objetivos del atacante.
- Puede consistir de varios pasos antes de llegar a su objetivo.

Lámina 13
Dr. Roberto Gómez C. (Seguridad en Redes)

Tipos de Ataques

Ataques Pasivos.



Ataques Activos.

Lámina 14
Dr. Roberto Gómez C. (Seguridad en Redes)

Principales Ataques

- Virus
- Caballo de Troya
- Gusanos (Worms)
- Bugs
- Trapdoors
- Stack overflow
- Pepena
- Bombas lógicas
- Dedos inexpertos
- Falsificación
- Usurpación
- Sniffers
- Spoofing
- Spam
- Grafiti
- Ingeniería Social
- Negación de servicio

Lámina 15 Dr. Roberto Gómez C. (Seguridad en Redes)

alldas.de defacement archive

> displaying from 1 to 138 of 138 defacement(s) found.

> date	> original site	> archive	> attacked by	> OS	> comments	> nmap	> class-C
23/01/2002	www.republicain-niger.com	mirror	S4t4n1c_S0uls	Solaris	none	view	history
22/01/2002	www.megaplus.ch	mirror	S4t4n1c_S0uls	Unknown	none	view	history
22/01/2002	www.colbayns.org.uk	mirror	S4t4n1c_S0uls	Windows	none	view	history
22/01/2002	www.traumgirl.ch	mirror	S4t4n1c_S0uls	Unknown	none	view	history
20/01/2002	www.onix.de	mirror	S4t4n1c_S0uls	Linux	none	view	none
20/01/2002	www.globo-insurance.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
20/01/2002	www.atleticaitaliana.it	mirror	S4t4n1c_S0uls	Windows	none	view	none
20/01/2002	www.jacksonholebuilder.com	mirror	S4t4n1c_S0uls	Linux	none	view	none
19/01/2002	www.cdt.br	mirror	S4t4n1c_S0uls	Windows	none	view	none
15/01/2002	www.brainchainfreedom.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
15/01/2002	www.co.macon.nc.us	mirror	S4t4n1c_S0uls	Windows	Redefacement	view	history
12/01/2002	www.rottenpeaches.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
12/01/2002	www.forumsec.org.fi	mirror	S4t4n1c_S0uls	Windows	Redefacement	view	history
11/01/2002	eisenpower.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
11/01/2002	www.thedga.com	mirror	S4t4n1c_S0uls	Windows	none	view	history
11/01/2002	merchantsofsouthgaylord.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
10/01/2002	lewisandroth.org	mirror	S4t4n1c_S0uls	Windows	none	view	none
10/01/2002	www.cbbound.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
07/01/2002	www.melissa.org	mirror	S4t4n1c_S0uls	Windows	none	view	none
07/01/2002	www.cpinyc.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
07/01/2002	www.mmitech.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
07/01/2002	www.fgi.org	mirror	S4t4n1c_S0uls	FreeBSD	none	view	history
06/01/2002	www.efashionjewelry.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
04/01/2002	www.honda.com.sg	mirror	S4t4n1c_s0uls	Windows	Redefacement	view	history
04/01/2002	www.lasvegaseventphoto.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
04/01/2002	www.lasvegas2000.com	mirror	S4t4n1c_S0uls	Windows	none	view	history
04/01/2002	www.haquewater-lasvegas.com	mirror	S4t4n1c_S0uls	Solaris	none	view	none
03/01/2002	www.harmonyproperties.com	mirror	S4t4n1c_S0uls	Windows	none	view	none
03/01/2002	www.svuc.se	mirror	S4t4n1c_S0uls	Windows	none	view	none
01/01/2002	www.consiglio.regione.tos.it	mirror	S4t4n1c_S0uls	Windows	none	view	none
01/01/2002	www.hdc.ru	mirror	S4t4n1c_S0uls	Windows	none	view	none
30/12/2001	www.bibc.de	mirror	S4t4n1c_S0uls	Windows	none	view	none
30/12/2001	www.optimeq.com	mirror	S4t4n1c_S0uls	FreeBSD	none	view	none

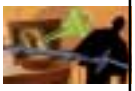
Seguridad Computacional

El conjunto de políticas y mecanismos que nos permiten garantizar la ***confidencialidad***, la ***integridad*** y la ***disponibilidad*** de los recursos de un sistema.

En la actualidad, el activo más importante en una organización es la información.

Lámina 17
Dr. Roberto Gómez C. (Seguridad en Redes)

Confidencialidad



Un sistema posee la propiedad de *confidencialidad* si, la información manipulada por éste no es disponible ni puesta en descubierto para usuarios, entidades o procesos no autorizados.

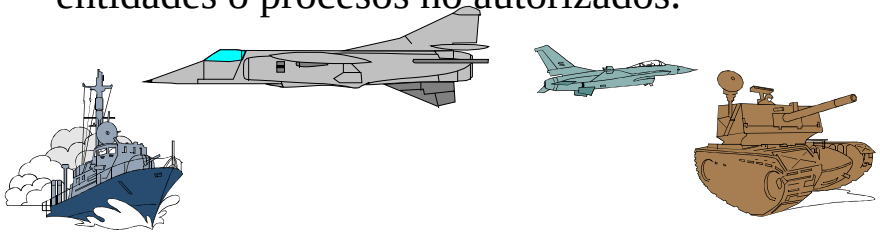


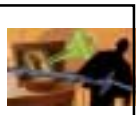
Lámina 18
Dr. Roberto Gómez C. (Seguridad en Redes)

Integridad

Un sistema posee la propiedad de integridad si los datos manipulados por éste no son alterados o destruidos por usuarios, entidades o procesos no autorizados.

Lámina 19
Dr. Roberto Gómez C. (Seguridad en Redes)

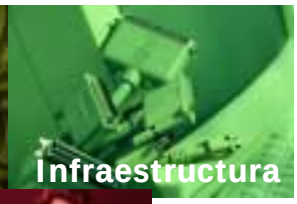
Disponibilidad



Un sistema posee la propiedad de *disponibilidad* si, la información es accesible (está disponible) en el momento en que así lo deseen los usuarios, entidades o procesos autorizados.

Lámina 20
Dr. Roberto Gómez C. (Seguridad en Redes)

La seguridad involucra 3 dimensiones (no sólo una)



Diseñar pensando en la seguridad
Roles y responsabilidades
Auditar dar seguimientos y rastrear
Mantenerse al día con el desarrollo de seguridad

Falta de conocimiento
Falta de comrpomiso
Falla humana

Los productos no cuentan con funciones de seguridad
Demasiado difícil mantenerse al día
Muchos problemas no se ven abordados por estándares técnicos (BS 7779)
Los productos tienen problemas

Lámina 21
Dr. Roberto Gómez C. (Seguridad en Redes)

El principio básico

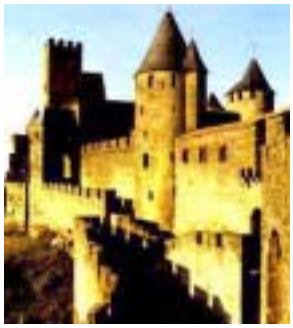


Lámina 22
Dr. Roberto Gómez C. (Seguridad en Redes)

La estrategía es un ciclo

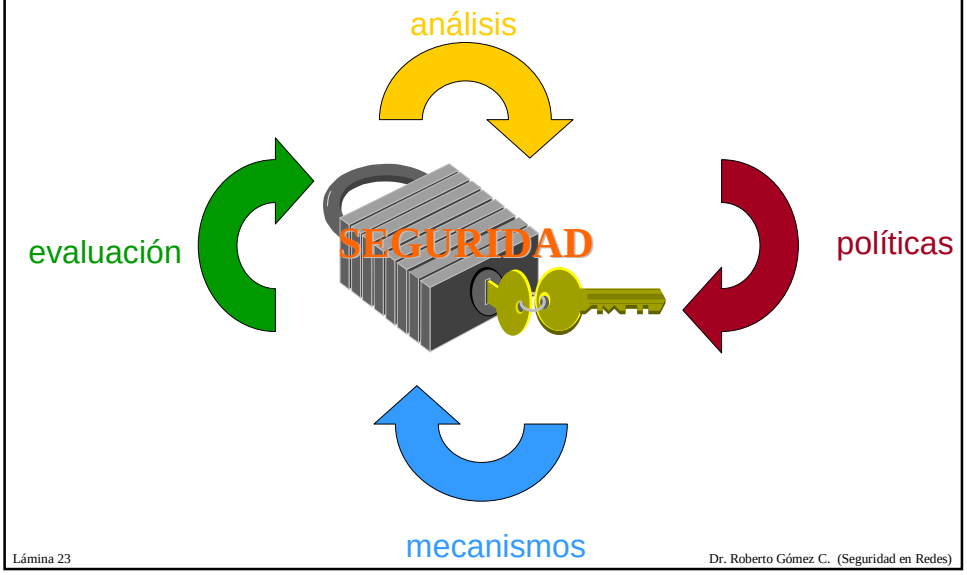


Lámina 23
Dr. Roberto Gómez C. (Seguridad en Redes)

Asegurando el sistema

- Objetivo
  - minimizar los riesgos potenciales de seguridad
- Análisis de riesgos
  - análisis amenazas potenciales que se pueden sufrir,
  - las pérdidas que se pueden generar
  - y la probabilidad de su ocurrencia
- Diseño política de seguridad
  - definir responsabilidades y reglas a seguir para evitar tales amenazas o
  - minimizar sus efectos en caso de que se produzcan
- Implementación
  - usar mecanismos de seguridad para implementar lo anterior

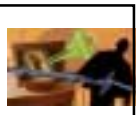
Lámina 24
Dr. Roberto Gómez C. (Seguridad en Redes)

Análisis de riesgo: plan estratégico

- Es el proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo que significaría la prevención de este suceso.
- Su análisis no sólo nos lleva a establecer un nivel adecuado de seguridad, sino que permite conocer mejor el sistema que vamos a proteger.

Lámina 25 Dr. Roberto Gómez C. (Seguridad en Redes)

Información del análisis de riesgo



- Información que se obtiene en un análisis de riesgo:
  - Determinación precisa de los recursos sensibles de la organización.
  - Identificación de las amenazas del sistema.
  - Identificación de las vulnerabilidades específicas del sistema.
  - Identificación de posibles pérdidas.
  - Identificación de la probabilidad de ocurrencia de una pérdida.
  - Derivación de contramedidas efectivas.
  - Identificación de herramientas de seguridad.
  - Implementación de un sistema de seguridad eficiente en costes y tiempo.

Lámina 26 Dr. Roberto Gómez C. (Seguridad en Redes)

Pasos en un análisis de riesgos

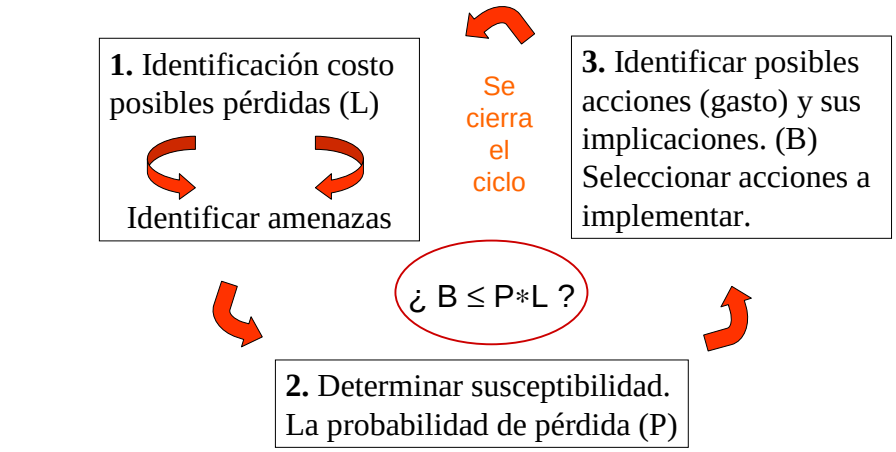


Lámina 27 Dr. Roberto Gómez C. (Seguridad en Redes)

Política de Seguridad

- Especifica las características de seguridad que un sistema debe observar y proveer
  - conjunto de reglas que deben respetarse para mantener la seguridad de la información.
- Especifica las amenazas contra las que la organización debe protegerse y cómo debe protegerse
- Depende de los objetivos y metas de la organización.
- Generalmente es expresada en un lenguaje o idioma.
- Típicamente establecida en términos de *sujetos* y *objetos*.

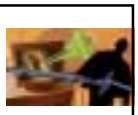
Lámina 28 Dr. Roberto Gómez C. (Seguridad en Redes)

Objetos y Sujetos

- Un objeto es todo recurso “pasivo” del sistema. Por ejemplo, la información, un archivo, el código de un programa, un dispositivo de red, etc.
- Un sujeto es toda entidad “activa” en el sistema. Por ejemplo, un usuario, un programa en ejecución, un proceso, etc.

Lámina 29 Dr. Roberto Gómez C. (Seguridad en Redes)

¿Qué hace una política?



- La política define la seguridad de un sistema de cómputo.
  - Un sistema es seguro si vive dentro sus políticas de seguridad.
- La política especifica qué propiedades de seguridad el sistema debe proporcionar.
- La política define la seguridad de cómputo para una organización, especificando:
  - Propiedades del sistema
  - Responsabilidades de seguridad de la gente

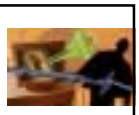
Lámina 30 Dr. Roberto Gómez C. (Seguridad en Redes)

Paradigmas

- *Paranoico*: Nada está permitido.
- *Prudente:* Lo que no está expresamente permitido, está prohibido.
- *Permisivo*: Lo que no está expresamente prohibido, está permitido.
- *Promiscuo:* Todo está permitido.

Lámina 31 Dr. Roberto Gómez C. (Seguridad en Redes)

Algunas políticas de seguridad



- Políticas administrativas
  - Procedimientos administrativos.
- Políticas de control de acceso
  - Privilegios de acceso del usuario o programa.
- Políticas de flujo de información
  - Normas bajo la cuales se comunican los sujetos dentro del sistema.

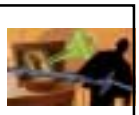
Lámina 32 Dr. Roberto Gómez C. (Seguridad en Redes)

Aspectos administrativos

- Políticas administrativas
  - Se establecen aquellos procedimientos de carácter administrativo en la organización como por ejemplo en el desarrollo de programas: modularidad en aplicaciones, revisión sistemática, etc.
  - Se establecen responsabilidades compartidas por todos los usuarios, cada uno en su nivel.

Lámina 33 Dr. Roberto Gómez C. (Seguridad en Redes)

Control de accesos



- Políticas de control de acceso
  - Política de menor privilegio
    - Acceso estricto a objetos determinados, con mínimos privilegios para los usuarios.
  - Política de compartición
    - Acceso de máximo privilegio en el que cada usuario puede acceder a todos los objetos.
  - Granularidad
    - Número de objetos accesibles.
    - Se habla entonces de granularidad gruesa y fina.

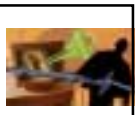
Lámina 34 Dr. Roberto Gómez C. (Seguridad en Redes)

Control de flujo

- Políticas de control de flujo
  - La información a la que se accede, se envía y recibe por:
    - ¿Canales claros o canales ocultos? ¿Seguros o no?
  - ¿Qué es lo que hay que potenciar?
    - ¿La confidencialidad o la integridad?
    - ¿La disponibilidad? ... ¿El no repudio?
    - Según cada organización y su entorno de trabajo y servicios ofrecidos, habrá diferencias.
    - En algunos sistemas primarán unos más que otros, en función de cuán secreta es la información que procesan.

Lámina 35 Dr. Roberto Gómez C. (Seguridad en Redes)

Ejemplo de Política (en lenguaje natural)



- Sólo se permitirá el intercambio de correo electrónico con redes de confianza.
- Toda adquisición de software a través de la red debe ser autorizada por el administrador de seguridad.
- Debe impedirse la inicialización de los equipos mediante disco.

Lámina 36 Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos de seguridad

- Son la parte más visible de un sistema de seguridad.
- Se convierten en la herramienta básica para garantizar la protección de los sistemas o de la propia red.
- Se dividen en:
  - prevención
  - detección
  - recuperación

Estrategias de protección
- Evitación
- Prevención
- Detección
- Recuperación

Lámina 37
Dr. Roberto Gómez C. (Seguridad en Redes)

Evitación

- No exponer activos a amenazas.
- Organizar las tareas de modo de evitar amenazas.
- Definición y uso de áreas y/o equipos restringidos o aislados.

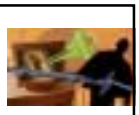
Lámina 38

Prevención

- Incluye funciones de seguridad en hardware y software.
- Debe incluir la definición y observancia de políticas de seguridad.
- Incluye controles administrativos.
- Es la estrategia más ampliamente usada.

Lámina 39

Mecanismos prevención



- Aumentan la seguridad de un sistema durante el funcionamiento normal de éste.
- Previenen la ocurrencia de violaciones a la seguridad
- Ejemplos mecanismos:
  - encripción durante la transmisión de datos
  - passwords difíciles
  - firewalls
  - biométricos

Lámina 40

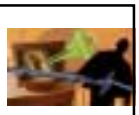
Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos prevención más habituales

- Mecanismos de autenticación
  - hacen posible identificar entidades del sistema de una forma única
  - posteriormente, una vez identificadas, son autenticadas (comprobar que la entidad es quién dice ser)
- Mecanismos de control de acceso
  - usados para proteger objetos del sistema (archivos, recursos..)
  - controlan todos los tipos de acceso sobre el objeto por parte de cualquier entidad del sistema
  - dos tipos discrecional (DAC) y mandatorio/obligatorio (MAC)

Lámina 41 Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos prevención …



- Mecanismos de separación
  - permiten separar los objetos dentro de cada nivel
  - evitar el flujo de información entre objetos y entidades de diferentes niveles siempre que no exista una autorización expresa del mecanismo de control de acceso
- Mecanismos de seguridad en las comunicaciones
  - protegen la integridad y privacidad de los datos cuando se transmiten a través de la red
  - la mayor parte se basan en la criptografía
  - uso de protocolos seguros

Lámina 42 Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos autenticación

- Basados en algo que se sabe
  - passwords, frases y números de identificación personal, NIP
  - siguen siendo el sistema de autenticación más usado hoy en día.
- Basados en algo que se es
  - biométricas y comportamiento
  - se realiza una medición física y se compara con un perfil almacenado con anterioridad,
- Basadas en algo que se tiene
  - usar un objeto físico que llevan consigo y que de alguna forma comprueba la identidad del portador
  - tokens, tarjetas inteligentes y pases.

Lámina 43 Dr. Roberto Gómez C. (Seguridad en Redes)

Basados en lo se tiene

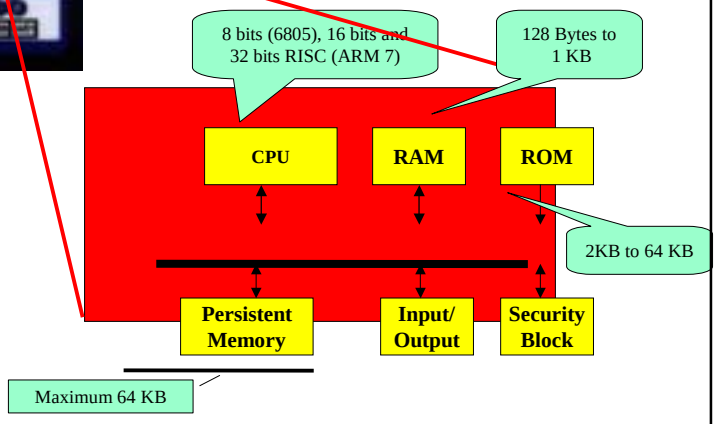
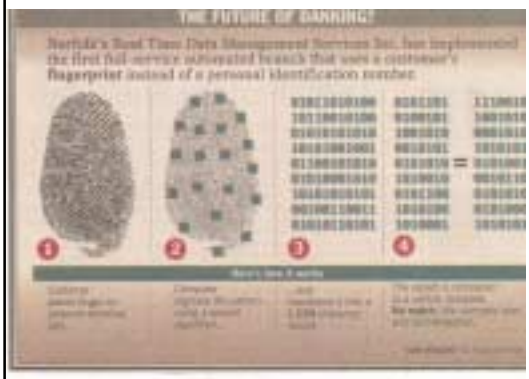


Lámina 44 Dr. Roberto Gómez C. (Seguridad en Redes)

Basados en lo que és



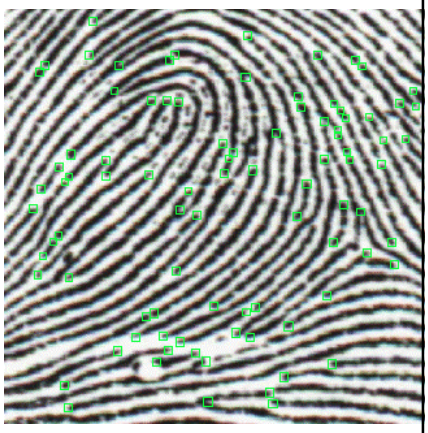


Lámina 45
Dr. Roberto Gómez C. (Seguridad en Redes)

Basados en algo que se sabe

- Primeros sistemas de autenticación se basaron en claves de acceso: nombre usuario y una clave de acceso.
- Son fáciles de usar y no requieren de un hardware especial.
- Siguen siendo el sistema de autenticación más usado hoy en día.

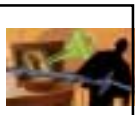
Lámina 46
Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos de control de acceso

- La autenticación pretende establecer quién eres.
- La autorización (o control de accesos) establece qué puedes hacer con el sistema.
- Dos modelos: DAC y MAC
- Control de acceso discrecional (DAC),
  - un usuario bien identificado (típicamente, el creador o 'propietario' del recurso) decide cómo protegerlo estableciendo cómo compartirlo, mediante controles de acceso impuestos por el sistema.
- Control acceso mandatorio (MAC)
  - es el sistema quién protege los recursos.
  - todo recurso del sistema, y todo usuario tiene una etiqueta de seguridad.

Lámina 47 Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos de separación



- Definición de un perímetro de seguridad
- Definir las zonas “abiertas” y las zonas cerradas.
  - DMZ: Zona desmilitarizada
- Mecanismos que sirven para delimitar una frontera
  - Filtros de paquetes
  - Firewalls
  - Wrappers
  - Proxies

Lámina 48 Dr. Roberto Gómez C. (Seguridad en Redes)

Detección

- Busca descubrir incidentes al momento en que ocurren o lo antes posible.
- Debe permitir detectar eventos para reducir el daño.
- Permite identificar y perseguir culpables.
- Revela vulnerabilidades.

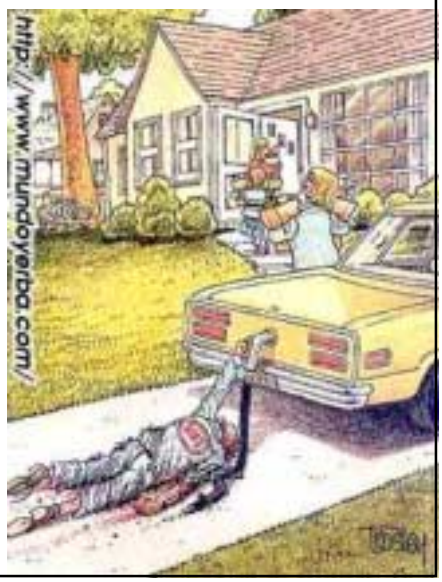


Lámina 49

Mecanismos detección

- Son aquellos que se utilizan para detectar violaciones de la seguridad o intentos de violación.
- Ejemplos de estos mecanismos
  - IDS
    - Tripwire
    - Snort
  - Detectores de vulnerabilidades
    - Nessus
    - ISS

Lámina 50

Dr. Roberto Gómez C. (Seguridad en Redes)

Recuperación

- Se pone en marcha después de un incidente de seguridad.
- Incluye la restauración de los recursos dañados.
- Debe remediar las vulnerabilidades que permitieron el incidente.

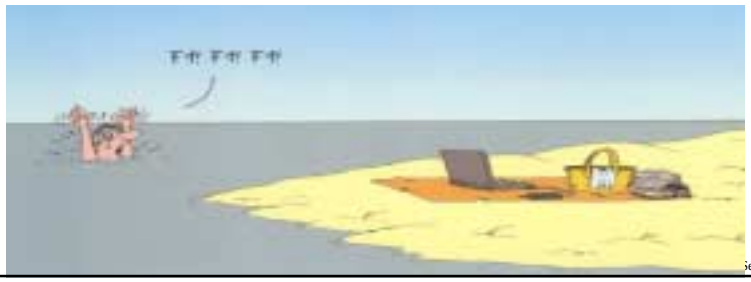


Lámina 51
Dr. Roberto Gómez C. (Seguridad en Redes)

Mecanismos de recuperación

- Son aquellos que se aplican cuando una violación del sistema se ha detectado, para retornar a éste su funcionamiento correcto.
- Ejemplos
  - respaldos
  - redundancia
  - bitácoras
  - BCP
  - DRP
- Subgrupo
  - mecanismos de análisis forense

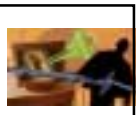
Lámina 52
Dr. Roberto Gómez C. (Seguridad en Redes)

Los respaldos

- Es una copia de los datos escrita en cinta u otro medio de almacenamiento duradero.
- De manera rutinaria se recuerda a los usuarios de computadoras que respalden su trabajo con frecuencia.
- Los administradores de sitios pueden tener la responsabilidad de respaldar docenas o incluso cientos de máquinas

Lámina 53 Dr. Roberto Gómez C. (Seguridad en Redes)

Accountabilty: loggin: bitacoras



- Se refiere al procedimiento a través del cual un sistema operativo registra eventos conforme van ocurriendo y los preserva para un uso posterior.
- Es posible configurar los sistemas de tal forma que los eventos:
  - se escriban en uno o en distintos archivos,
  - se envien a través de la red a otra computadora,
  - se transmitan a algún dipositivo.
- Algunos comandos en linux
  - lastlog
  - last

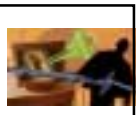
Lámina 54 Dr. Roberto Gómez C. (Seguridad en Redes)

DRP y BCP

- DRP (Disaster Recovery Planning)
  - recuperar la operación de los servicios computacionales y de telecomunicaciones después de un desastre
  - desastre es un evento no planeado que ocasiona la “no disponibilidad” de los servicios informáticos por un periodo de tiempo tal que, para restablecer estos servicios, es necesario utilizar facilidades alternas de cómputo y telecomunicaciones en otra localidad
- BCP (Business Continuity Planning)
  - capacidad para mantener la continuidad de las operaciones
  - dirigido a situaciones catastróficas (no problemas rutinarios)

Lámina 55 Dr. Roberto Gómez C. (Seguridad en Redes)

Planes de contingencia



- Consiste en un análisis pormenorizado de las áreas que componen una organización para establecer una política de recuperación ante un desastre.
  - es un conjunto de datos estratégicos de la empresa y que se plasma en un documento con el fin de protegerse ante eventualidades.
- Además de aumentar su seguridad la empresa también gana en el conocimiento de fortalezas y debilidades.
- Si no lo hace, se expone a sufrir una pérdida irreparable mucho más costosa que la implantación de este plan.

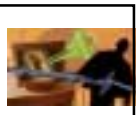
Lámina 56 Dr. Roberto Gómez C. (Seguridad en Redes)

Desastres naturales y su prevención

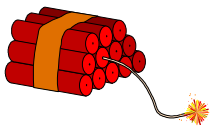
- Desastres naturales
  - Huracán
  - Tormenta
  - Inundación
  - Tornado
  - Vendaval
  - Incendio
  - Otros
- Medidas prevención
  - Emplazamientos adecuados
  - Protección fachadas, ventanas, puertas

Lámina 57 Dr. Roberto Gómez C. (Seguridad en Redes)

Vandalismo informático y su prevención



- Terrorismo
- Sabotaje
- Robo



- Virus
- Programas malignos

- Medidas de prevención
  - Fortificación entradas
  - Guardia Jurado
  - Patrullas
  - Circuito cerrado TV
  - Control de accesos
  - Protección de software y hardware con antivirus, cortafuegos, etc.

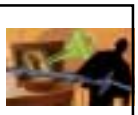
Lámina 58 Dr. Roberto Gómez C. (Seguridad en Redes)

Amenazas del agua y su prevención

- Amenazas
  - Inundaciones por causas propias de la empresa
  - Inundaciones por causas ajenas
  - Pequeños incidentes personales (botella de agua, taza con café)
- Medidas prevención
  - Revisar conductos de agua.
  - Localizar la sala con los equipos más caros en un sitio libre de estos problemas.
  - Instalar sistemas de drenaje de emergencia.
  - Concienciar empleados.

Lámina 59
Dr. Roberto Gómez C. (Seguridad en Redes)

Amenazas del fuego y su prevención



- Amenazas
  - Una mala instalación eléctrica.
  - descuidos personales como fumar en la sala de ordenadores.
  - Papeleras mal ubicadas en la que se tira un cigarrillo no apagado.
  - Vulnerabilidades del sistema por humo.
- Medidas prevención
  - Detector humo y calor.
  - Materiales ignífugos.
  - Almacén de papel separado de máquinas.
  - Estado del falso suelo.
  - Extintores revisados.
    - Es la amenaza más temida por su rápido poder destructor.

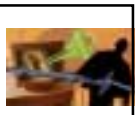
Lámina 60
Dr. Roberto Gómez C. (Seguridad en Redes)

¿Qué sucede si se produce una catástrofe?

- Las empresas dependen hoy en día de los equipos informáticos y de todos los datos que hay allí almacenados (nóminas, clientes, facturas, ...).
- Dependen también cada vez más de las comunicaciones a través de redes de datos.
- Si falla el sistema informático y éste no puede recuperarse, la empresa puede desaparecer porque no tiene tiempo de salir nuevamente al mercado con ciertas expectativas de éxito, aunque conserve a todo su personal.

Lámina 61 Dr. Roberto Gómez C. (Seguridad en Redes)

Tiempos de recuperación ante desastres



- Período máximo de paro de una empresa sin poner en peligro su supervivencia:
  - Sector Seguros: 5,6 días
  - Sector Fabricación: 4,9 días
  - Sector Industrial: 4,8 días
  - Sector Distribución: 3,3 días
  - Sector Financiero: 2,0 días

Ref. Estudio de la Universidad de Minnesota (1996)

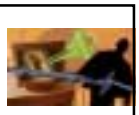
Lámina 62 Dr. Roberto Gómez C. (Seguridad en Redes)

Pérdidas por no contar con un plan

- Pérdida de clientes.
- Pérdida de imagen.
- Pérdida de ingresos por beneficios.
- Pérdida de ingresos por ventas y cobros.
- Pérdida de ingresos por producción.
- Pérdida de competitividad.
- Pérdida de credibilidad en el sector.

Lámina 63
Dr. Roberto Gómez C. (Seguridad en Redes)

Implantación de medidas básicas



- Plan de emergencia
  - Vidas, heridos, activos, evacuación personal.
  - Inventariar recursos siniestrados.
  - Evaluar el coste de la inactividad.
- Plan de recuperación
  - Acciones tendentes a volver a la situación que existía antes del desastre.

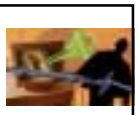
Lámina 64
Dr. Roberto Gómez C. (Seguridad en Redes)

BCP: Plan de continuidad

- Instalaciones alternativas
  - Oficina de servicios propia.
  - Acuerdo con empresa vendedora de HW y SW.
  - Acuerdo recíproco entre dos o más empresas.
  - Arranque en frío; sala vacía propia.
  - Arranque en caliente: centro equipado.
  - Sistema Up Start: caravana, unidad móvil.
  - Sistema Hot Start: centro gemelo.

Lámina 65 Dr. Roberto Gómez C. (Seguridad en Redes)

El computo forense



- Se refiere al proceso de aplicar técnicas científicas y analíticas a infraestructura de cómputo, para identificar, preservar, analizar y presentar evidencia de manera que sea aceptable en un procedimiento legal
- ¿Que clase de evidencia ?
  - la computadora involucrada de forma directa.
  - la computadora involucrada de forma indirecta.
- Meta: reconstrucción de eventos pasados
  - reconstruir que pasó, que lo ocasionó y deslindar responsabilidades

Lámina 66 Dr. Roberto Gómez C. (Seguridad en Redes)

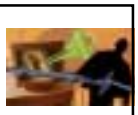
Clasificación mecanismos seguridad

Mecanismos de seguridad

- **prevención**
  - autenticación
    - en lo que se sabe
    - en lo que se tiene
    - en lo que es
  - control acceso
    - discrecional
    - mandatorio
  - separación
    - filtros
    - firewall
    - wrappers
    - proxies
  - seguridad comunicaciones
- **detección**
  - IDS
  - scanner vulnerabilidades
- **recuperación**
  - respaldos
  - redundancia
  - bitácoras
  - BCP
  - DRP
  - análisis forense

Lámina 67
Dr. Roberto Gómez C. (Seguridad en Redes)

Algunos principios de Seguridad



- Propuestos por la OECD en 1992
- Entre los más importantes encontramos
  - Accountability (Responsabilidad / Rendición de Cuentas)
  - Awareness (Sensibilización)

Lámina 68
Dr. Roberto Gómez C. (Seguridad en Redes)

Accountability

- Propiedad que asegura que las acciones de una entidad deben llevar unicamente a dicha entidad (ISO 7498-2)
- La propiedad que habilita actividades en un sistema ADP que conducen (trace) a individuos que pueden ser declarados responsables de dichas actividades (DOE 5636.2A)

Lámina 69

Awareness (Sensibilización)

- Todas las partes deben poder conocer las medidas de seguridad, practicas y procedimientos.
- Una motivación para este principio es forzar la confianza en los sistemas de información.

Lámina 70

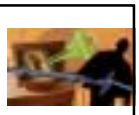
Servicios propuestos por OSI

Norma 7498-2

- Autentificación.
- Control de Acceso.
- Confidencialidad.
- Integridad de Datos.
- No Repudiación.

Lámina 71
Dr. Roberto Gómez C. (Seguridad en Redes)

Autentificación



- La autentificación se refiere a demostrar la identidad de las entidades involucradas en la transacción. Evita que alguien tome la identidad de otro. Generalmente toma dos formas:
  - Autentificación del proveedor de bienes o servicios.
  - Autentificación del cliente.

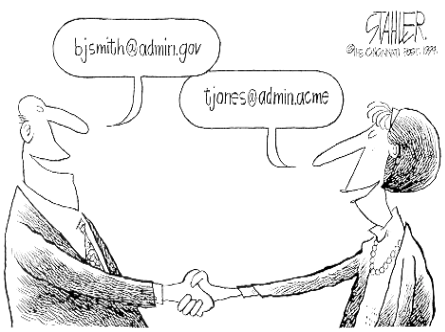


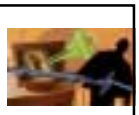
Lámina 72

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.

Lámina 73 Dr. Roberto Gómez C. (Seguridad en Redes)

Control de Acceso.



- Como ejemplos de mecanismos para este servicio podemos mencionar:
  - Los permisos en los archivos de Unix..
  - Los niveles de autorización en un sistema militar.

Lámina 74 Dr. Roberto Gómez C. (Seguridad en Redes)

Confidencialidad.

- Servicio que garantiza la privacidad de los datos:
  - En local.
  - En conexiones.
  - En modo no conectado.
  - En campos selectos.
  - En flujo de datos.
- Principal mecanismo para implementar este servicio es la criptologia

Lámina 75
Dr. Roberto Gómez C. (Seguridad en Redes)

Integridad de Datos.

- Permite proteger los datos contra ataques activos.
  - Con recuperación de datos.
  - Sin recuperación de datos.
  - En campos selectos.
- Los mecanismos principales son:
  - CRCs
  - huellas digitales.

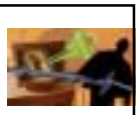
Lámina 76

No Repudiación.

- Permite comprobar las acciones realizadas por el origen o destino de los datos.
  - Con prueba de origen.
  - Con prueba de entrega.
- Los mecanismos principales son los certificados, la notarización y las firmas digitales.

Lámina 77
Dr. Roberto Gómez C. (Seguridad en Redes)

No repudiación



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

Lámina 78

La AAA

- Authentication, authorization, y accounting
  - consiste de un framewok que proporciona los tres servicios
- El objetivo del grupo de trabajo AAA es definir un protocolo que implemente autenticación, autorización y accounting lo suficientemente general para ser usado en aplicaciones diferentes.
- Definición de la arquitectura
  - de Laat, C. & Gross, G. & Gommans, L. & Vollbrecht, J. & Spence, C., Generic AAA architecture, Internet Draft (work in progress), January 2000.

Lámina 79 Dr. Roberto Gómez C. (Seguridad en Redes)

Esquema general

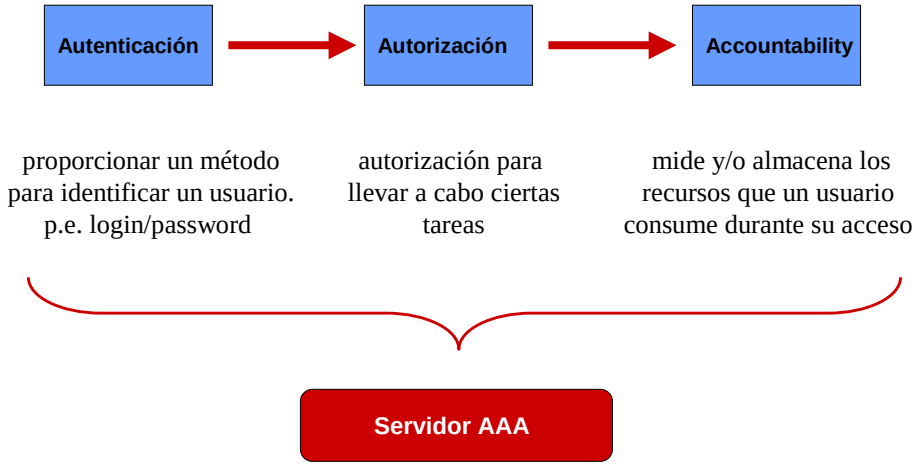


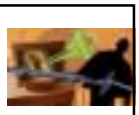
Lámina 80 Dr. Roberto Gómez C. (Seguridad en Redes)

Modelos de seguridad

- Modelo de Bell LaPadula (BLP)
  - Rígido. Confidencialidad y con autoridad.
- Modelo de Take-Grant (TG)
  - Derechos especiales: tomar y otorgar.
- Modelo de Clark-Wilson (CW)
  - Orientación comercial: integridad.
- Modelo de Goguen-Meseguer (GM)
  - No interferencia entre usuarios.
- Modelo de Matriz de Accesos (MA)
  - Estados y transiciones entre estados
    - Tipo Graham-Dennig (GD)
    - Tipo Harrison-Ruzzo-Ullman (HRU)

Lámina 81 Dr. Roberto Gómez C. (Seguridad en Redes)

Criterios y normativas de seguridad



- Criterio de evaluación TSEC
  - Trusted Computer System Evaluation Criteria, también conocido como Orange Book.
- Criterio de evaluación ITSEC
  - Information Technology Security Evaluation Criteria.
- Criterio de evaluación CC
  - Common Criteria: incluye los dos anteriores.
- Ley Orgánica de Protección de Datos LOPD (1999, España)
  - Establece un conjunto de medidas de seguridad de debido cumplimiento por parte de empresas y organismos.
- Normativa internacional 17799
  - Desarrolla un protocolo de condiciones mínimas de seguridad informática de amplio espectro.

Lámina 82 Dr. Roberto Gómez C. (Seguridad en Redes)

La normativa 17799

Código de buenas prácticas para la Gestión de la Seguridad de la Información: PNE-ISO/IEC 17799

- Antecedentes
- Introducción
- Objeto y campo de la aplicación
- Términos y definiciones
- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de los archivos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad del negocio
- Conformidad

En 70 páginas y diez apartados, presenta unas normas, recomendaciones y criterios básicos para establecer unas políticas de seguridad. Éstas van desde los conceptos de seguridad física hasta los de seguridad lógica. Parte de la norma elaborada por la British Standards Institution BSI, adoptada por International Standards Organization ISO y la International Electronic Commission IEC.

Lámina 83
Dr. Roberto Gómez C. (Seguridad en Redes)

Los protagonistas

hackers, crackers y ...

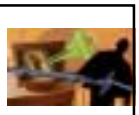
Lámina 84
Dr. Roberto Gómez C. (Seguridad en Redes)

Los protagonistas

- Los hackers
- Los crackers
- Los phreakers
- Los script kidies

Lámina 85
Dr. Roberto Gómez C. (Seguridad en Redes)

El Hacker: La Vieja Guardia



- Origen del término a finales de los 60.
- Programador con alto dominio de su profesión, capaz de solucionar problemas a través de hacks (segmentos de código muy ingenioso).
- Verdaderos conocedores de la tecnología de cómputo y telecomunicaciones (85-93).
- La búsqueda del conocimiento siempre fue su fuerza impulsora.

Lámina 86
Dr. Roberto Gómez C. (Seguridad en Redes)

El cracker

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas computacionales.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado.
- No necesariamente tiene el mismo nivel de conocimientos que el hacker.

Lámina 87
Dr. Roberto Gómez C. (Seguridad en Redes)

Los phreakers

- Aquella persona que en forma persistente realiza intentos hasta obtener acceso a sistemas telefónicos privados.
- Una vez logrado el acceso produce daños a los recursos del sistema atacado, o se beneficia del mismo.

Lámina 88

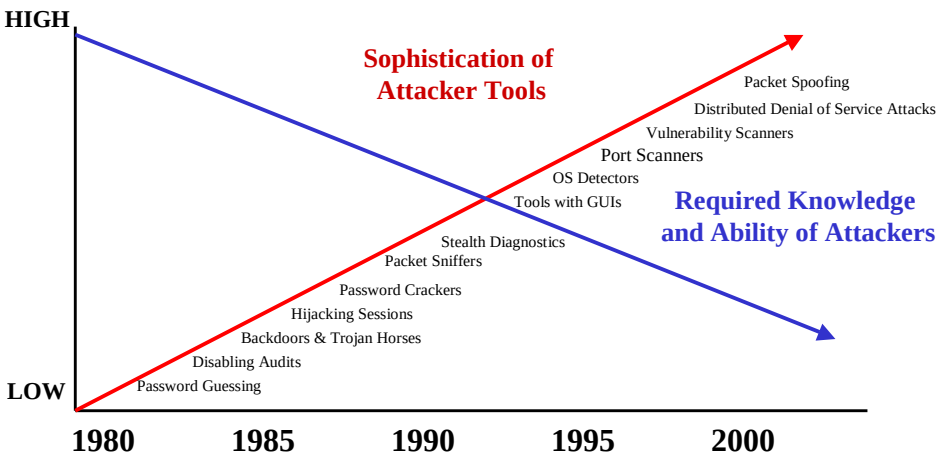
El Hacker: la nueva generación o los ¨Script-kidies¨

- 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¨.

Lámina 89
Dr. Roberto Gómez C. (Seguridad en Redes)

External Threats: Hacker Tool Explosion

Recent Web Search for "Hacker Tools" returned over 2100 hits



I get scanned dozens of times everyday. Less than 20% of those scans are US based

ISS User

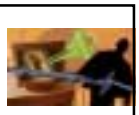
Lámina 90
Dr. Roberto Gómez C. (Seguridad en Redes)

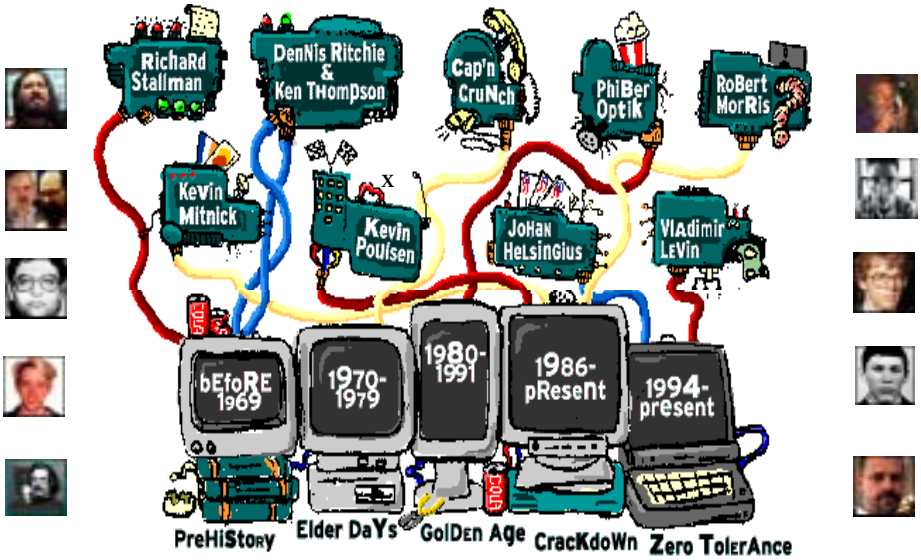
El Hacker: ¿cómo lo ven el resto de los usuarios?

- ¿Qué es eso?
- Eso pasa solo en las películas.
- Así como los de ¨The Net¨
- Yo soy hacker.
- Yo apenas sé como se usa una computadora.
- Bill Gates se va a encargar de ellos.

Lámina 91
Dr. Roberto Gómez C. (Seguridad en Redes)

El hall de la fama de los hackers





www.discovery.com/area/technology/hackers/hackers.html

Lámina 92
Dr. Roberto Gómez C. (Seguridad en Redes)

¿Qué hicieron?

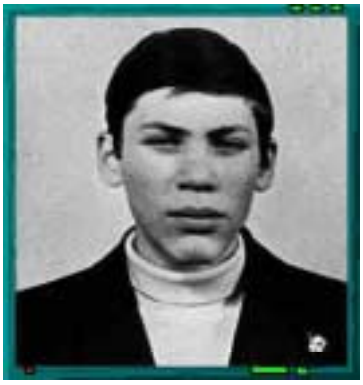
- Kevin Poulsen
  - In 1990 Poulsen took over all telephone lines going into Los Angeles area radio station KIIS-FM to win a call-in contest.
- Johan Helsingius
  - Operated the world's most popular anonymous remailer, called penet.fi, until he closed up shop in September 1996.
- Phiber Optik (Mark Abene)
  - Inspired thousands of teenagers around the country to "study" the internal workings of our nation's phone system.
- Cap Crunch (John Draper)
  - Figured out how to make free phone calls using a plastic prize whistle he found in a cereal box.

Lámina 93 Dr. Roberto Gómez C. (Seguridad en Redes)

El hacker Kevin Mitnick

Lámina 94 Dr. Roberto Gómez C. (Seguridad en Redes)

Vladimir Levin (Russian Hacker).



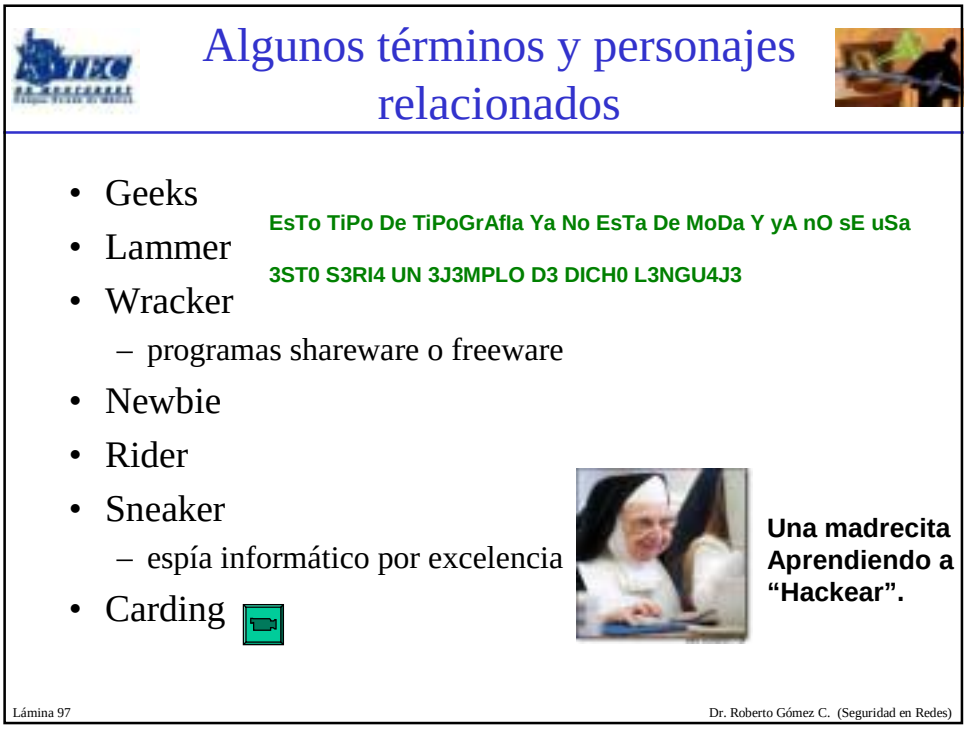
Hacked the City Bank $ 10,000,000

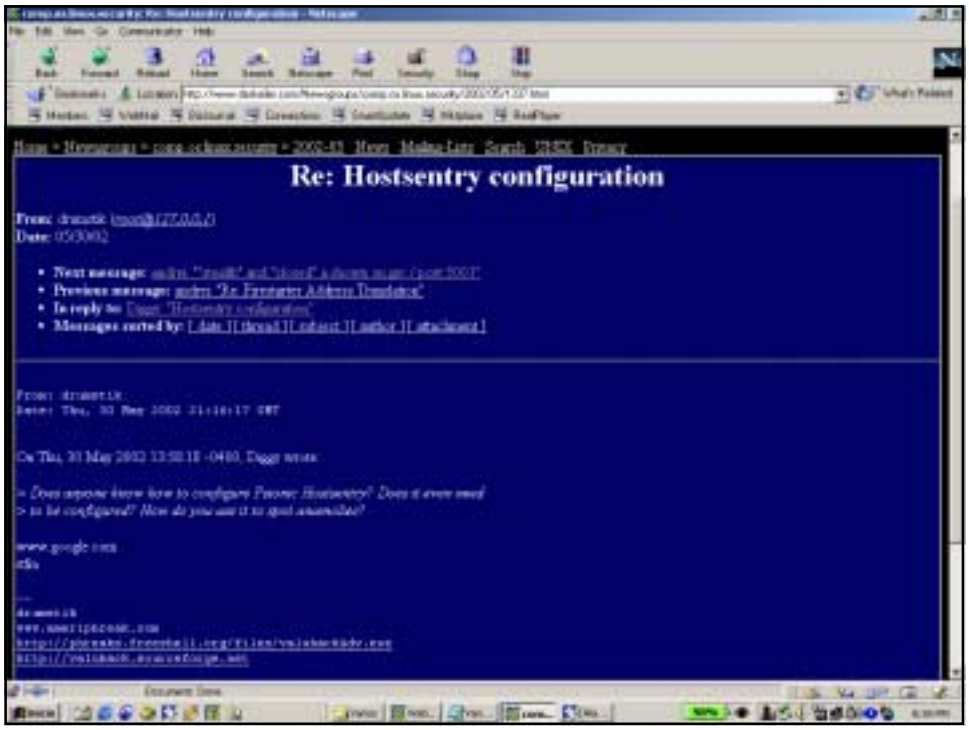
Lámina 95 Dr. Roberto Gómez C. (Seguridad en Redes)

Algunos otros

- Steve Wozniak
- Tsutomu Shimomura
- Linus Torvalds

Lámina 96 Dr. Roberto Gómez C. (Seguridad en Redes)


Algunos términos y personajes relacionados
• Geeks
• Lammer
• Wracker
– programas shareware o freeware
• Newbie
• Rider
• Sneaker
– espía informático por excelencia
• Carding
EsTo TiPo De TiPoGrAfIa Ya No EsTa De MoDa Y yA nO sE uSa
3ST0 S3RI4 UN 3J3MPLO D3 DICH0 L3NGU4J3
Una madrecita Aprendiendo a "Hackear".
Lámina 97
Dr. Roberto Gómez C. (Seguridad en Redes)

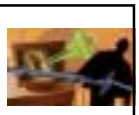

Re: Hostsentry configuration

Algunos grupos

- Chaos Computer Club
- Cult of the Dead Cow
- DC2600.org
- AntiOffline removing the Dot in Dot.com
- The gethohackers
- DARK CLAW
- LoD

Lámina 99
Dr. Roberto Gómez C. (Seguridad en Redes)

¿Y cómo diferenciar a los buenos de los malos?



- Recomendaciones de terceros
- Prestigio de las compañías
- Certificaciones
  - A las instituciones
    - ISO 17799
  - A los individuos
    - CISSP

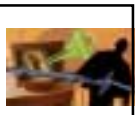
Lámina 100
Dr. Roberto Gómez C. (Seguridad en Redes)

ISO

- Bajo ISO 17799 una organización puede optar a implantar y "certificar" su sistema de gerencia en la gestión de integridad y seguridad en el manejo de información y datos.
  - comprende de elementos y cláusulas enfocados a prácticas y métodos fundamentales de seguridad contemporánea
- La precursora de ISO 17799 es la adopción de la normativa británica BS 7799.
  - La BS 7799 se publicó en febrero del 1995 y se revisó en mayo del 1999.
  - Esta normativa aplica invariablemente a organizaciones pequeñas, medianas y multinacionales.

Lámina 101 Dr. Roberto Gómez C. (Seguridad en Redes)

Areas control ISO 1799



1. Security Policy
2. Security Organization
3. Asset Control and Classification
4. Personnel Security
5. Physical & Environmental Security
6. Communications & Operations Management
7. Acces Control
8. Systems Development & Maintenance
9. Business Continuity Management
10. Compliance

Lámina 102 Dr. Roberto Gómez C. (Seguridad en Redes)

CISSP

- No es una asociación, es el título que ostenta el profesional certificado
  - Certified Information Systems Security Professional
- Ser CISSP es un privilegio que se debe ganar y mantener
- Otorgado por la $(ISC)^2$
  - International Information Systems Security Certification Consortium
  - Organismo independiente
  - Creado para realizar la certificación de profesionales en seguridad informática

Lámina 103 Dr. Roberto Gómez C. (Seguridad en Redes)

Common Body of Knowledge

- Access Control Systems & Methodology
- Telecommunications & Network Security
- Security Management Practices
- Applications & Systems Development Security
- Cryptography
- Security Architecture & Models
- Operations Security
- Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)
- Law, Investigations & Ethics
- Physical Security

Lámina 104 Dr. Roberto Gómez C. (Seguridad en Redes)

Referencias

- Computer Security Handbook by Arthur E. Hutt (Editor), Seymour Bosworth (Editor), Douglas B. Hoyt (Editor), 3rd edition (September 1995), John Wiley & Sons
- Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage by Clifford Stoll, Pocket Books; (October 3, 2000)
- Secure Computing: Threats and Safeguards, Rita C. Summers, 1997, McGraw-Hill, ISBN 0-07-069419-2
- Computer Crime: A Crime Fighter's Handbook, David Icove, Karl Seger, and William VonStorch, 1995, O'Reilly and Associates, ISBN 1-56592-086-4

Lámina 105 Dr. Roberto Gómez C. (Seguridad en Redes)

Páginas para mayor información

- Security Focus: www.securityfocus.com
- CERT : www.cert.org
- SANS: www.sans.org
- Securiteam: www.securiteam.com
- Snort: www.snort.com
- ISS: www.iss.net
- Página seguridad RSA: www.rsasecurity.com
- Cypherpunks: www.vnunet.com
- Bruce Scheneider: www.counterpane.com
- Security Space: www.securityspace.com
- Ernst&Young: www.esecurityonline.com

Lámina 106 Dr. Roberto Gómez C. (Seguridad en Redes)

Más páginas

- Linux Security: www.linuxsecurity.com
- Diccionario del hacker: www.hack.gr/jargon/
- Defaced pages 1: www.attrition.org/ (deshabilitada)
- Defaced pages 2: www.alldas.org/
- Criptología: www.criptored.upm.es
- Packetstorm: http://www.packetstorm.com
- (ISC)^2: http://www.isc2.org
- Noticas 1: http://www.xatrix.org/
- Noticias 2: http://www.mountainwave.com/
- Noticias 3: http://www.cyberdefenders.com/privacynews.htm

Lámina 107
Dr. Roberto Gómez C. (Seguridad en Redes)