1.1 INTRODUCIÓN

1. Introducción a la seguridad

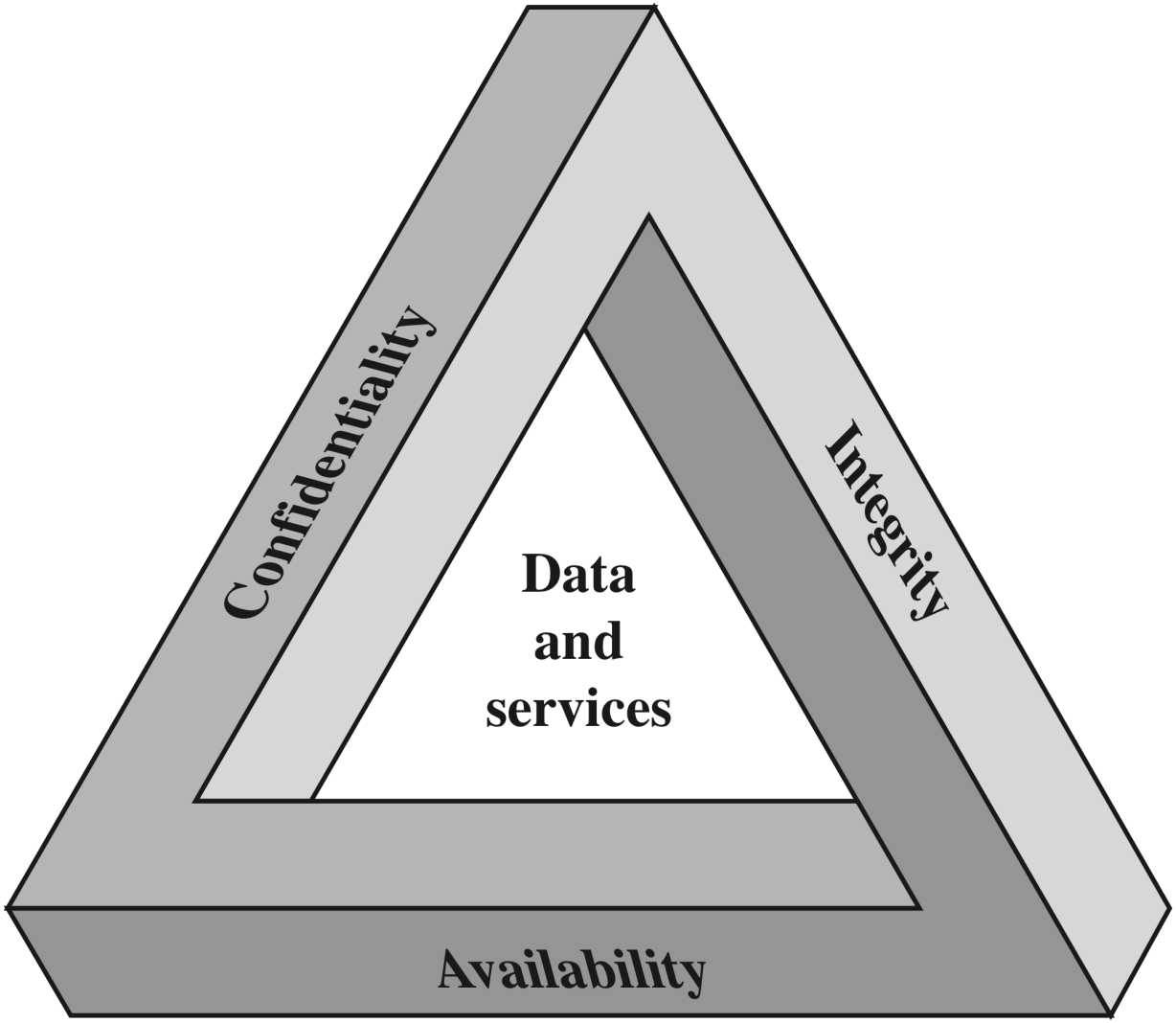
Conceptos de seguridad

- Seguridad de la información: Defensa frente a acceso, uso, revelación, interrupción, modificación, inspección, grabación o destrucción de la información no autorizados
  - El el pasado se proporcionaba con medios físicos y administrativos
  - Con la introducción de los computadores, se necesitaron herramientas automáticas para proteger la información almacenada en ellos
  - Otro cambio importante fue la introducción de las redes de comunicación y de los sistemas distribuidos
- Seguridad informática: Seguridad de la información aplicada a computadores y redes
- Seguridad en redes: Medidas para disuadir, impedir, detectar y corregir violaciones de seguridad que implican la transmisión de información

Objetivos de la seguridad informática

- Confidencialidad (*confidentiality*)
  - Confidencialidad de datos: Garantiza que la información privada o confidencial no es revelada a individuos no autorizados
  - Privacidad: Garantiza que los individuos controlan qué información personal puede ser recolectada y almacenada y por quién y para quién puede ser revelada esa información
- Integridad (*integrity*)
  - Integridad de datos: Garantiza que la información y los programas son modificados solo de la forma especificada y autorizada
  - Integridad de sistemas: Garantiza que un sistema realiza su función sin impedimentos y libre de manipulación no autorizada, ya sea deliberada o involuntaria
- Disponibilidad (*availability*)
  - Garantiza que un sistema trabaja sin demora y que el servicio no es denegado a los usuarios autorizados

Tríada CIA [FIPS PUB 199]



Conceptos adicionales

- Autenticidad (*authenticity*)
  - Asegura la validez de una transmisión, de un mensaje o del origen de un mensaje
- Responsabilidad o atribución (*accountability*)
  - Asegura que las acciones de una entidad son atribuidas de manera única a esa entidad

Desafíos de la seguridad informática

- La seguridad no es sencilla
- Se deben considerar los ataques potenciales
- Los procedimientos pueden ser poco intuitivos
- Es necesario decidir dónde usar los distintos mecanismos de seguridad
- Requiere monitorización constante
- Se suele pensar en ella demasiado tarde
- Los mecanismos de seguridad típicamente implican más de un algoritmo o protocolo particular
- Es una batalla de ingenio entre un infractor y el diseñador
- Se percibe poco beneficio de la inversión en seguridad hasta que ocurre un fallo en la misma
- Se ve como impedimento a la operación eficiente y amigable

Estándares

- *National Institute of Standards and Technology* (NIST)
  - Agencia federal de Estados Unidos
  - Publica *Federal Information Processing Standards* (FIPS) y *Special Publications* (SP) con impacto mundial
- *Internet Society* (ISOC)
  - Sociedad profesional a nivel mundial
    - *Internet Engineering Task Force* (IETF) e *Internet Architecture Board* (IAB)
  - Publica estándares y especificaciones como *Requests for Comments* (RFCs)
- *International Telecommunication Union-Telecommunication Standardization Sector* (ITU-T)
  - Agencia especializada de la ONU, antiguamente llamada CCITT
  - Publica recomendaciones en series: X (*Data networks, open system communications and security*), Y (*Global information infrastructure, Internet protocol aspects and next-generation networks*)…
- *International Organization for Standardization* (ISO)
  - Compuesta por representantes de organizaciones nacionales de estándares
    - ISO/IEC (*International Electrotechnical Commission*) *Joint Technical Committee*
  - Publica estándares (ISO[/IEC] [IS]), informes técnicos (ISO[/IEC] TR), especificaciones técnicas (ISO[/IEC] TS o PAS) y guías (ISO[/IEC] *Guide*)

Historia

- 1960s: Los comienzos del *hacking*
  - El significado original de la palabra *"hack"* se inició en el MIT para referirse a una forma elegante, ingeniosa e inspirada de hacer algo
- 1970s: *Phreaks* (*phone+freaks*) y *Cap'n Crunch*
  - John Draper (*"Cap'n Crunch"*) descubre que un silbato de regalo con una caja de cereales da una señal de 2600Hz que permite acceder al sistema de conmutación de larga distancia de AT&T
  - Draper construye una *"blue box"* que, con el silbato, permite realizar llamadas gratis
  - Steve Wozniak y Steve Jobs, futuros fundadores de Apple Computer, construyen y venden estas *"blue boxes"*

Historia

- 1980s: La era dorada
  - 1980: BBSs (*Bulletin Board System*) y grupos de *hackers*
    - Se forma *Legion of Doom* (USA) y *Chaos Computer Club* (Alemania)
  - 1983: Película “Juegos de guerra”
  - 1984: Revistas de hackers (2600 y *Phrack*)
  - 1985: Se publica *“The Hacker's Handbook”* en Reino Unido
  - 1986: Se aprueba la ley de fraude y abuso de computadores (USA)
    - Es delito entrar en computadores sin permiso
  - 1988: Robert T. Morris lanza un gusano en ARPANET
    - Creación del primer CERT (*Computer Emergency Response Team*)
  - 1989: Los alemanes, la KGB y Kevin Mitnick
    - *Hackers* alemanes arrestados por vender datos americanos a la KGB
    - *“The Mentor”*, desde la cárcel, publica *“Hacker's Manifesto”* en *Phrack*
    - Kevin Mitnick es condenado por primera vez

Historia

- 1990s: La caza de *hackers* y la *Web*
  - 1990: Operación *Sundevil*
    - Agentes del servicio secreto americano capturan *hackers* en 14 ciudades, provocando un colapso en la comunidad, con miembros informando sobre otros a cambio de inmunidad
  - 1993: Primera conferencia de *hacking Def Con* en Las Vegas
    - Fiesta para reemplazar los BBSs por la Web que pasó a ser anual
  - 1995: Captura de Mitnick y los rusos
    - Mitnick, el *hacker* más buscado de USA, es arrestado de nuevo por entrar en sistemas corporativos y robar información personal de celebridades, números de tarjetas de crédito y código fuente
    - Hackers rusos transfieren 10 millones de dólares de Citibank
  - 1998: Un adolescente entra en el sistema telefónico de Bell Atlantic
  - 1999: Más ataques
    - Páginas *web* del Pentágono, MIT, FBI…
    - Chantajes a empresas

Historia

- 2000s: Ataques DoS, a DNS, *desfiguraciones* Web…
  - 2000: DDoS masivos
    - Ataque DDoS en algunos de los sitios con más tráfico de Internet (yahoo.com, cnn.com, amazon.com, fbi.gov…)
      - Saturó los encaminadores durante varias horas con paquetes ICMP de gran tamaño (*ping flood*) enviados desde servidores infectados con un troyano
  - 2001: Ataque a DNS
    - Se corrompen las entradas DNS de los sitios *web* de Microsoft
    - Se detecta en pocas horas, pero impide a millones de usuarios acceder a las páginas de Microsoft durante dos días
  - 2003: Se forma el grupo hacker *Anonymous*
  - …

1.2 VULNERABILIDADES Y AMENAZAS

1. Introducción a la seguridad

Vulnerabilidades y amenazas [RFC 4949]

- Vulnerabilidad
  - *“A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy”*
- Amenaza
  - *“A potential for violation of security, which exists when there is an entity, circumstance, capability, action, or event that could cause harm (unauthorized access, destruction, disclosure, or modification of data, or denial of service)”*

Vulnerabilidades

- Un sistema puede tener vulnerabilidades en su:
  - Diseño o especificación
  - Implementación
  - Operación y gestión
- Pueden ser de diversa naturaleza:
  - Física: interceptación (*wire tapping*)
  - *Hardware*: sistemas y dispositivos de red
  - *Software*: sistema operativo, servicios...
  - Protocolos de red (Ethernet, TCP/IP...): escuchas (*sniffing*) y suplantación (*spoofing*)
  - Personal: fallos de configuración, descuidos...
  - Procedimental: políticas incorrectas…

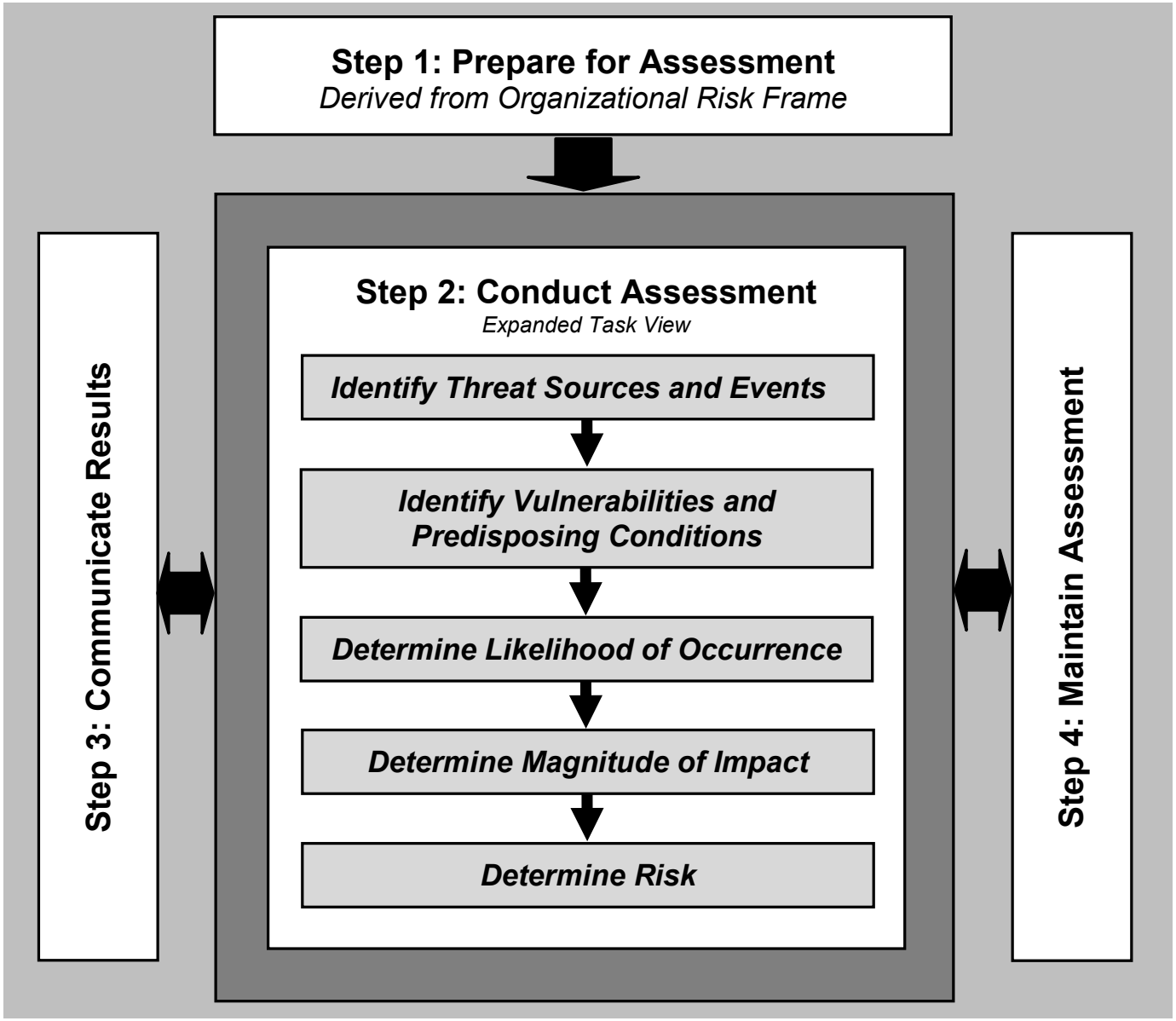
Amenazas

- Pueden ser de dos tipos:
  - Accidentales: Posibilidad de error humano u omisión, mal funcionamiento de un equipo o desastre natural (fuego, inundación, terremoto…)
  - Intencionales o inteligentes: Posibilidad de un ataque por una entidad inteligente (*cracker* individual u organización criminal)
- Las amenazas inteligentes se caracterizan por:
  - La vulnerabilidad que podría ser la base del ataque
  - El agente amenazante (persona, organización, gobierno…), guiado por una motivación (económica, política, publicitaria…)
  - El supuesto método de ataque
  - El recurso de sistema que podría ser atacado

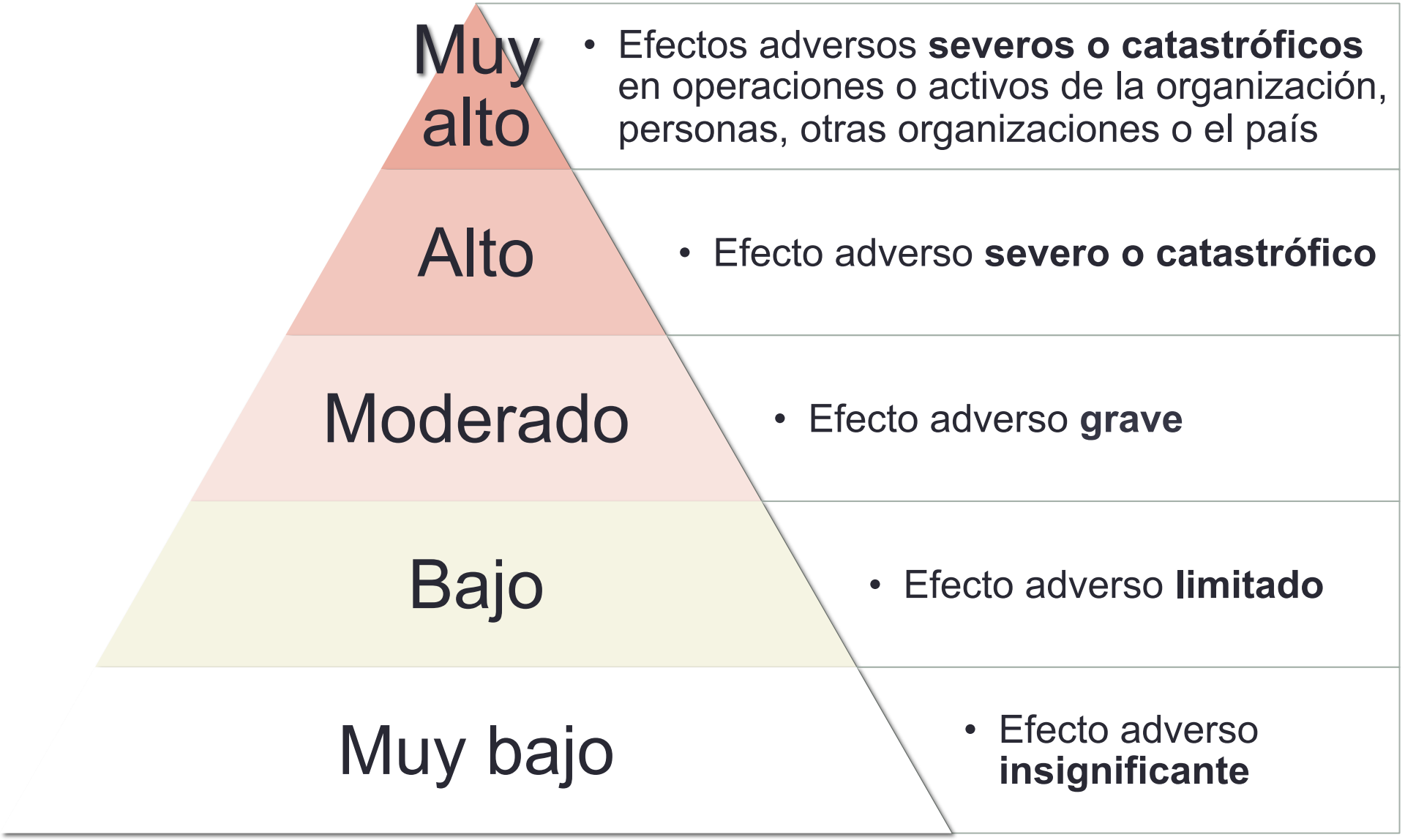
Hackers

- ***Black hat***: alguien que rompe la seguridad, normalmente por razones maliciosas o beneficio personal
  - ***Cracker*** o **cibercriminal**, sinónimo de *hacker* para algunos
- ***White hat***: especialista de seguridad que realiza pruebas de intrusión (conocidos como *hackers* **éticos**)
  - Mismas habilidades y técnicas, pero usadas con **autorización**
- ***Grey hat***: combinación de los dos anteriores
  - *Hacker black hat* trabajando temporalmente dentro de la ley (contratado para realizar una prueba de intrusión)
  - *Hacker white hat* que ocasionalmente se salta la legalidad
- ***Script kiddie*** (*skiddie*): no experto que usa herramientas automáticas escritas por otros con poco entendimiento
- ***Hacktivist***: alguien que usa técnicas de *hacking* para anunciar un mensaje social, ideológico, religioso o político

Análisis de riesgos [NIST SP 800-30]



Análisis del impacto



Determinación del riesgo

Impacto

Probabilidad	Muy bajo	Bajo	Moderado	Alto	Muy alto
Muy alta	Muy bajo	Bajo	Moderado	Alto	Muy alto
Alta	Muy bajo	Bajo	Moderado	Alto	Muy alto
Moderada	Muy bajo	Bajo	Moderado	Moderado	Alto
Baja	Muy bajo	Bajo	Bajo	Bajo	Moderado
Muy baja	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Medidas de respuesta [NIST SP 800-39]

- Aceptación
  - Permitir que el sistema funcione con un riesgo conocido
  - Muchos riesgos bajos son simplemente aceptados
- Eliminación
  - Eliminar el aspecto vulnerable del sistema o el propio sistema
- Mitigación o reducción
  - Arreglar, anticipar, reaccionar, recuperar…
  - Es la respuesta más común
- Compartición o transferencia
  - Reducir el impacto en la organización mediante la transferencia o compartición del riesgo
    - Cualitativamente → externalizar
    - Cuantitativamente (e.g. impacto económico) → asegurar
- Una combinación de los anteriores

Evaluación de la seguridad [NIST SP 800-115]

- Proceso de determinar la eficacia con la que una entidad cumple objetivos de seguridad específicos
- Métodos de evaluación:
  - Entrevista: discusiones con individuos o grupos
  - Revisión: inspeccionar y estudiar el sistema (documentación, registro, reglas, configuración, análisis de tráfico…)
  - Prueba: ejercitar el sistema bajo unas condiciones específicas para comparar el comportamiento real y el esperado
- Pruebas:
  - Identificación y análisis: descubrimiento de red, identificación de puertos y servicios, exploración de vulnerabilidades…
  - Validación de vulnerabilidades: romper contraseñas, pruebas de intrusión, ingeniería social…
  - Pueden ser externas o internas y de caja blanca, negra o gris

1.3 ANATOMÍA DE UN ATAQUE

1. Introducción a la seguridad

Ataque [RFC 4949]

- *“An intentional act by which an entity attempts to evade security services and violate the security policy of a system”*
  - Esto es, un asalto real a un sistema que se deriva de una amenaza inteligente

Tipos de ataques [RFC 4949 y X.800]

- Según la intención:
  - Pasivo: el atacante intenta aprender o usar información del sistema pero no afecta a los recursos del sistema
  - Activo: el atacante intenta alterar los recursos del sistema o afectar a su funcionamiento
- Según el punto de iniciación:
  - Interno: iniciado por una entidad dentro del perímetro de seguridad (*insider*)
  - Externo: iniciado desde fuera del perímetro de seguridad, por un usuario no autorizado o ilegítimo (*outsider*)
- Según el modo de direccionamiento:
  - Directo: el atacante envía paquetes a la víctima
  - Indirecto: el atacante envía paquetes a una tercera parte (*reflector*), que responde enviando paquetes a la víctima

Ataques pasivos

- Se trata de escuchas (*eavesdropping*) o monitorización de transmisiones
- El objetivo del atacante es obtener información que está siendo transmitida
- Ejemplos:
  - Captura de paquetes (*sniffing*): Obtención del contenido de los paquetes
  - Análisis de tráfico: Adivinar los detalles de la comunicación basándose en patrones de mensajes

Ataques activos

- Conlleva alguna modificación en el flujo de datos o la creación de un flujo de datos falso
- Ejemplos:
  - Suplantación (*masquerade*): Una entidad se hace pasar por otra
    - Normalmente incluye una de las otras formas de ataque
  - Repetición (*replay*): Se capturan de datos de forma pasiva y se retransmiten posteriormente para producir un efecto no autorizado
  - Modificación (*modification*): Se altera una porción de un mensaje legítimo, o se retardan o reordenan los mensajes para producir un efecto no autorizado
  - Denegación de servicio (*denial of service*): Impide el uso o gestión normal de redes o sistemas

Ataques comunes

- Reconocimiento
  - *Sniffing*, *footprinting*, *fingerprinting*…
- Acceso
  - *Man-in-the-middle*, *session hijacking*, *code injection*…
- Denegación de servicio (*Denial of Service*, DoS)
  - *Flooding*, *amplification/reflection*…
- Software malicioso (*malware*)
  - *Virus*, *worms*, *Trojan horses*, *back doors*…

Fases de un ataque

1. Reconocimiento (*reconoissance*, *footprinting*)
   - Búsqueda en Internet y en DNS
   - Ingeniería social
2. Exploración (*scanning*, *fingerprinting*)
   - Exploración de redes y puertos
   - Identificación de servicios y análisis de vulnerabilidades
3. Obtención de acceso
   - Explotación de vulnerabilidades y escalado de privilegios
4. Mantenimiento del acceso
   - Descifrado de contraseñas, *rootkits* y *backdoors*
   - Movimientos laterales
5. Ocultación de pistas
   - Desactivado de auditoría y borrado de registros
   - Corrupción de datos

1.4 SERVICIOS Y MECANISMOS DE SEGURIDAD

1. Introducción a la seguridad

Security Architecture for Open System Interconnection [X.800 e ISO 7498-2]

- Mecanismo de seguridad
  - *"A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack"*
- Servicio de seguridad
  - *"A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization"*
- Los servicios de seguridad implementan políticas de seguridad y son implementados por mecanismos de seguridad

Categorías de servicios en X.800

- Autenticación
- Control de acceso
- Confidencialidad de datos
- Integridad de datos
- No repudio o no negación

Autenticación

- Garantiza que una comunicación es auténtica
  - En el caso de un único mensaje, garantiza al receptor que el mensaje proviene del origen del que indica proceder
    - *Data origin authentication*
  - En el caso de una interacción continuada, garantiza que las dos entidades participantes son auténticas y que una tercera parte no puede suplantar a una de las dos partes legítimas
    - *Peer entity authentication*

Control de acceso o autorización

- Capacidad de limitar y controlar el acceso a sistemas y aplicaciones
  - Cada entidad que intente obtener acceso debe primero ser identificada, o autenticada, para que los permisos de acceso puedan ser personalizados para esa entidad
    - *Access control*

Confidencialidad de datos

- Protección de datos transmitidos frente a ataques pasivos
  - El servicio más amplio protege todos los datos transmitidos
    - *Connection confidentiality*
  - Formas más específicas del servicio protegen mensajes individuales o incluso campos específicos de estos
    - *Connectionless confidentiality*
    - *Selective field confidentiality*
- Protección del flujo de datos frente a análisis de tráfico
  - Requiere que el atacante no sea capaz de observar el origen y destino, frecuencia, tamaño u otras características del tráfico
    - *Traffic flow confidentiality*

Integridad de datos

- Puede aplicarse a un flujo de mensajes, a un mensaje único o a campos seleccionados de un mensaje
  - Un servicio de integridad orientado a conexión trata con flujos de mensajes y garantiza que los mensajes son recibidos tal y como se enviaron, sin duplicación, inserción, modificación, reordenación o repetición
    - *Connection integrity with recovery*
    - *Connection integrity without recovery*
    - *Selective field connection integrity*
  - Un servicio de integridad sin conexión trata con mensajes individuales sin considerar su contexto y generalmente solo proporciona protección frente a modificación
    - *Connectionless integrity*
    - *Selective field connectionless integrity*

No repudio

- Evita que el emisor o el receptor puedan negar la emisión o recepción de un mensaje
  - Cuando se envía un mensaje, el receptor puede probar que el presunto emisor realmente envió el mensaje
    - *Non-repudiation with proof of origin*
  - Cuando se recibe un mensaje, el emisor puede probar que el presunto receptor realmente recibió el mensaje
    - *Non-repudiation with proof of delivery*

Mecanismos de seguridad en X.800

- Específicos: pueden incorporarse a la capa de protocolos apropiada para proporcionar alguno de los servicios de seguridad
  - Cifrado
  - Firma digital
  - Control de acceso
  - Integridad de datos
  - Intercambio de autenticación
  - Relleno de tráfico
  - Control del encaminamiento
  - Certificación
- Genérico: no específicos de un servicio de seguridad o de una capa de protocolos particular
  - Funcionalidad de confianza
  - Etiqueta de seguridad
  - Detección de eventos
  - Registro de auditoría de seguridad
  - Recuperación de seguridad

1.5 ASPECTOS LEGALES Y ÉTICOS

1. Introducción a la seguridad

Delitos informáticos y ciberdelitos

- Hay dos categorías:
  - Los que usan datos, programas o sistemas informáticos como instrumento para cometer delitos
  - Los que tienen como objetivo los propios datos, programas o sistemas informáticos
- Antiguamente, solo la primera era castigada con la misma pena que el equivalente no informático
- Ahora la segunda también está penada
  - "El que… borrase, dañase, deteriorase, alterase, suprimiese, o hiciese inaccesibles datos, programas informáticos o documentos electrónicos ajenos…"
  - "El que… obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos…"
  - "El que… acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo…"

Ley Orgánica 5/2010 por la que se modifica la Ley Orgánica 10/1995 del Código Penal

Resumen

- Introducción
  - Seguridad de la información, seguridad informática y seguridad en redes
  - Requisitos
  - Estándares
  - Historia
- Vulnerabilidades y amenazas
  - *Hackers*
  - Análisis de riesgos
  - Evaluación
- Anatomía de un ataque
  - Tipos de ataques
  - Ataques comunes
  - Fases de un ataque
- Servicios y mecanismos de seguridad
- Aspectos legales y éticos