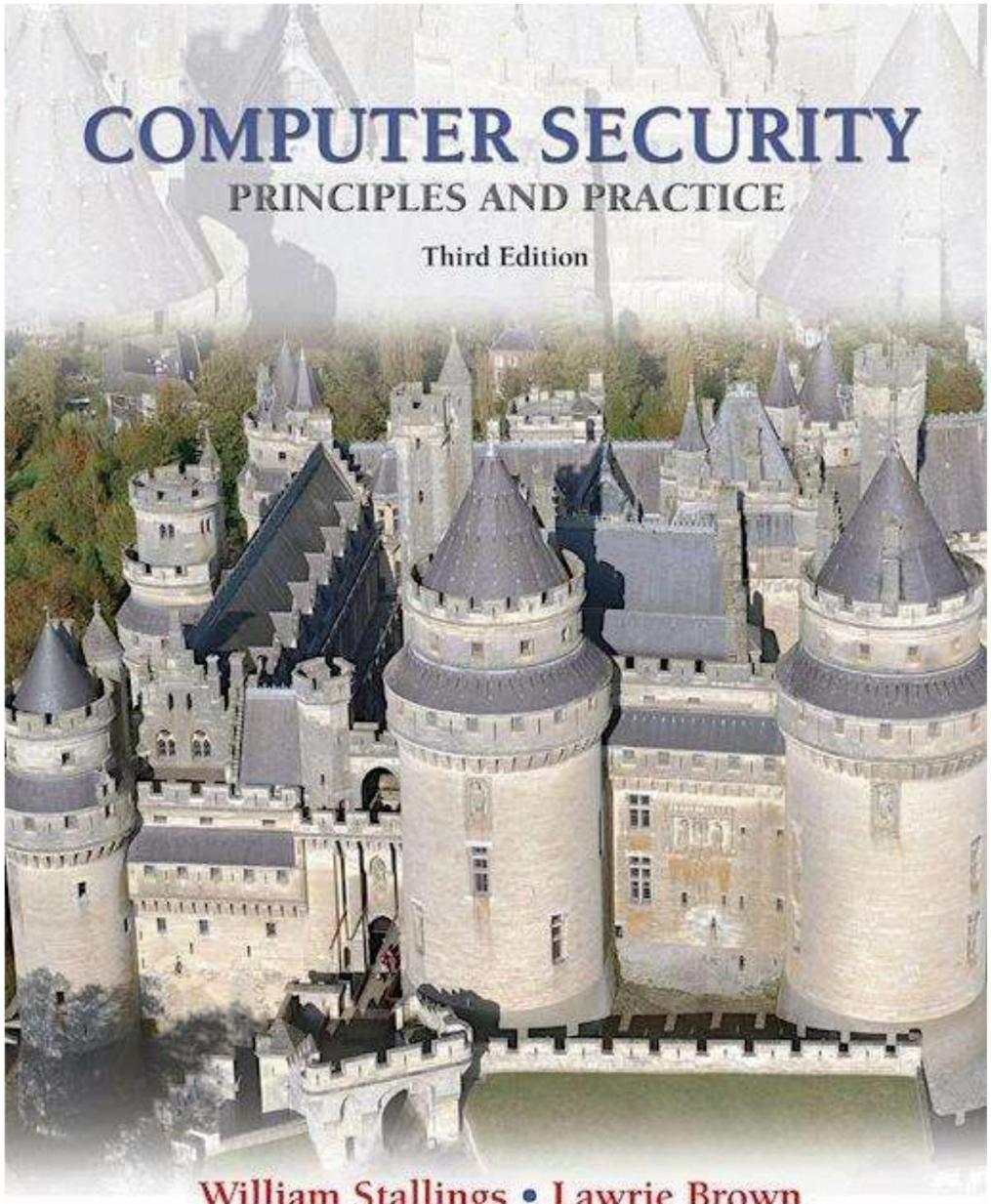


Capítulo 1

Descripción general

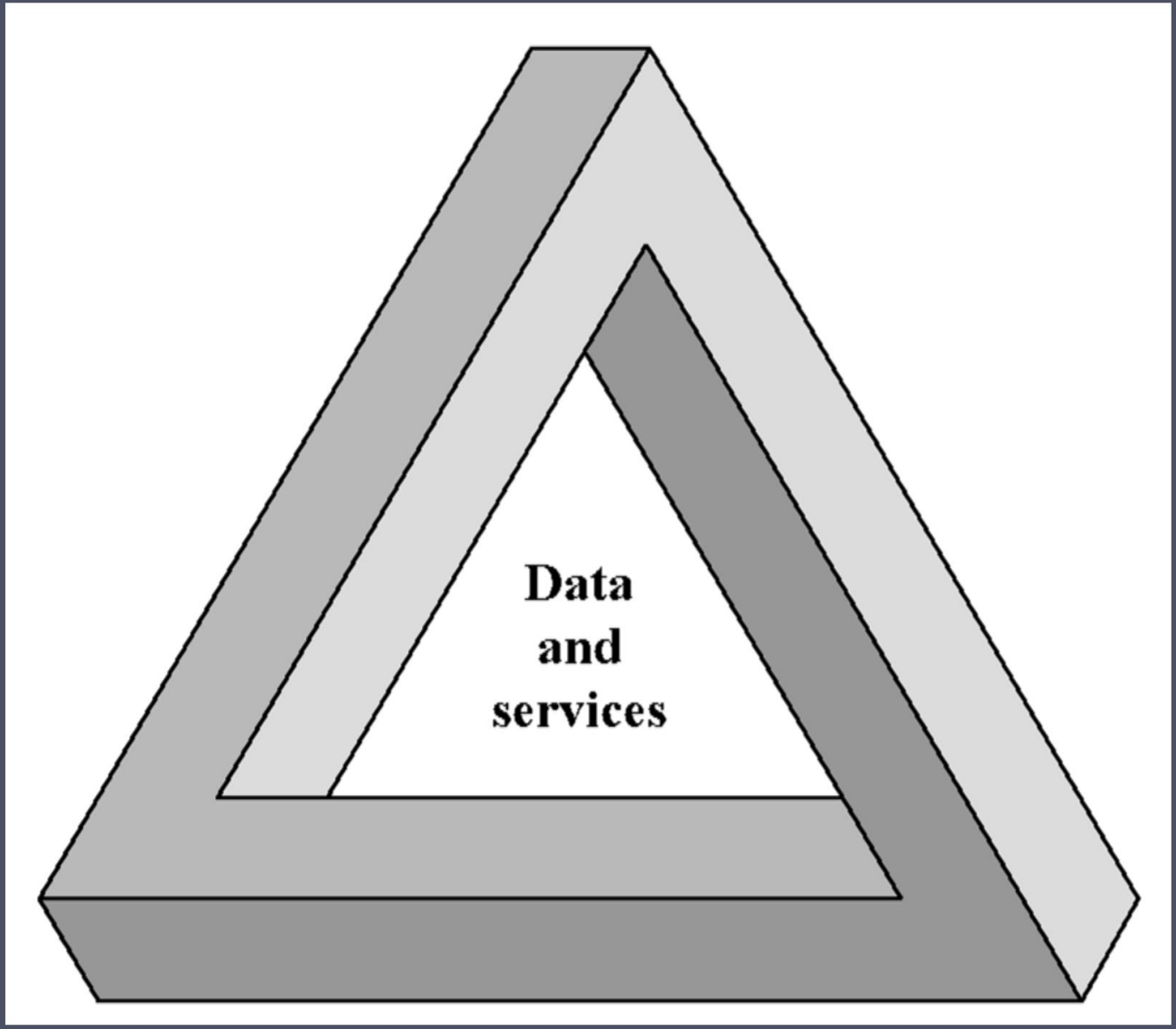
Seguridad informática del NIST

El manual define el término

Seguridad informática como:

"La protección brindada a un sistema de información automatizado para alcanzar los objetivos aplicables de preservar la integridad, disponibilidad y confidencialidad de los recursos del sistema de información" (incluye hardware, software, firmware, información/datos y telecomunicaciones).

La tríada de la CIA



Conceptos clave de seguridad

Confidencialidad

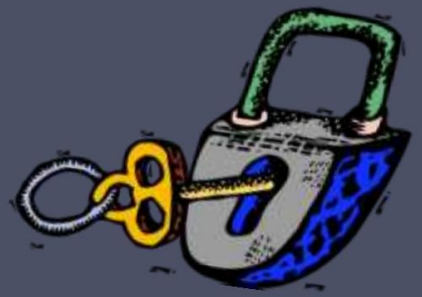
- Preservar las restricciones autorizadas sobre el acceso y la divulgación de información , incluidos los medios para proteger la privacidad personal y la información confidencial.

Integridad

- Protección contra la modificación o destrucción indebida de información , incluida la garantía de la autenticidad y no repudio de la información.

Disponibilidad

- Garantizar el acceso oportuno y confiable a la información y su uso .



Niveles de impacto

Bajo

Se podría esperar que la pérdida tenga un efecto adverso limitado sobre las operaciones de la organización, los activos de la organización o las personas.

Moderado

Se podría esperar que la pérdida tenga un efecto adverso grave en las operaciones de la organización, los activos de la organización o las personas.

Alto

Se podría esperar que la pérdida tenga un efecto adverso grave o catastrófico en las operaciones de la organización , los activos de la organización o las personas.

Seguridad informática

Desafíos

- La seguridad informática no es tan sencilla como podría parecerle a primera vista a un novato.
- Posibles ataques a la
  Se deben tener en cuenta las características de seguridad
- Los procedimientos utilizados para proporcionar determinados servicios suelen ser contraintuitivos.
- Físico y lógico
  Es necesario determinar la ubicación
- Algoritmos adicionales o
  Los protocolos pueden estar involucrados

- Los atacantes solo necesitan encontrar una única debilidad, el desarrollador necesita encontrar todas las debilidades.
- Los usuarios y administradores de sistemas tienden a no ver los beneficios de la seguridad hasta que ocurre una falla. ocurre
- La seguridad requiere un monitoreo regular y constante.
- A menudo es una idea de último momento que se incorpora a un sistema una vez que se completa el diseño .
- Se considera un impedimento para una operación eficiente y fácil de usar.

Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

Attack
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability
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.

Tabla 1.1

Computadora Seguridad Terminología y

RFC 4949, Internet
Glosario de seguridad,
Mayo de 2000

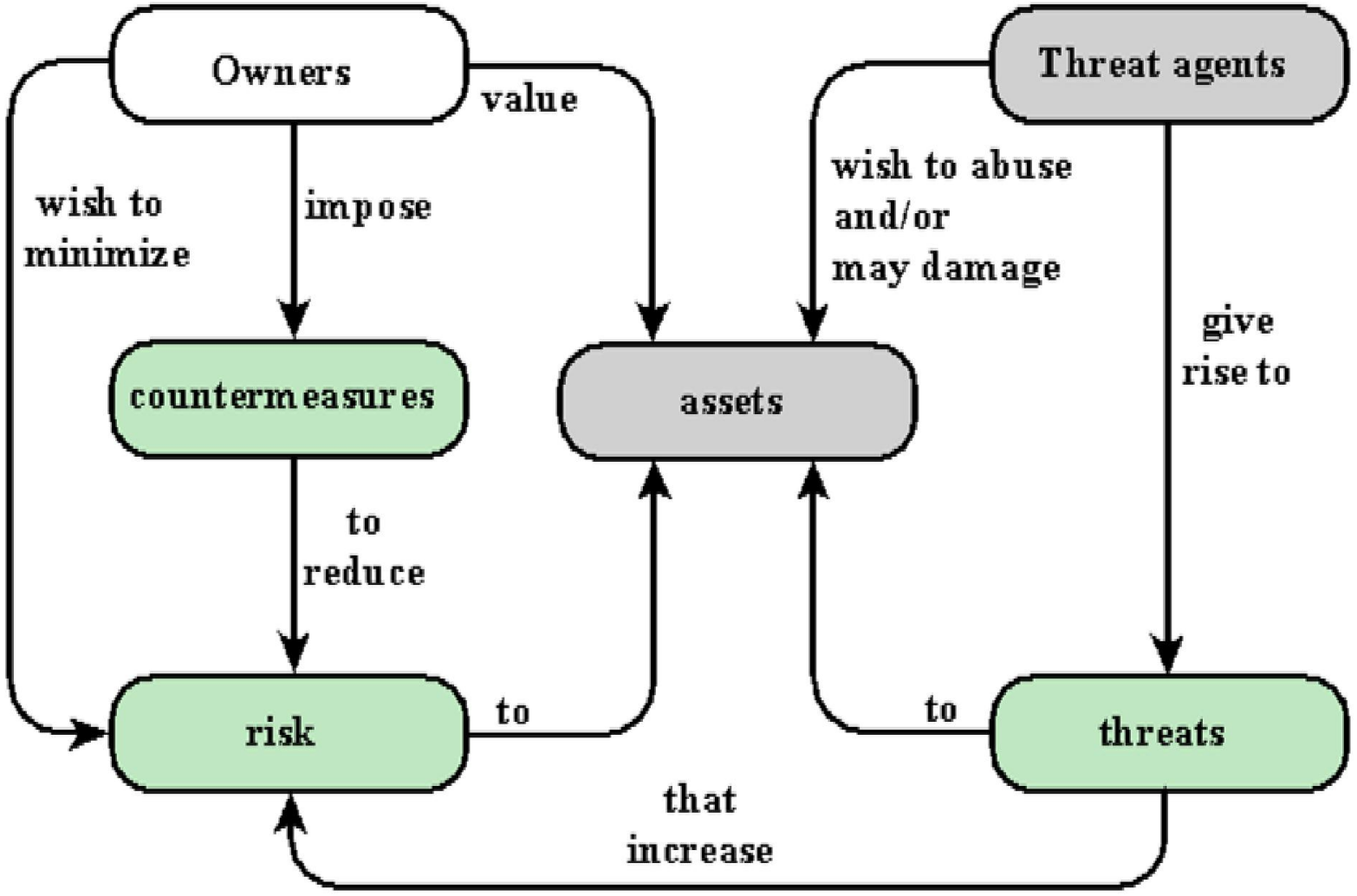
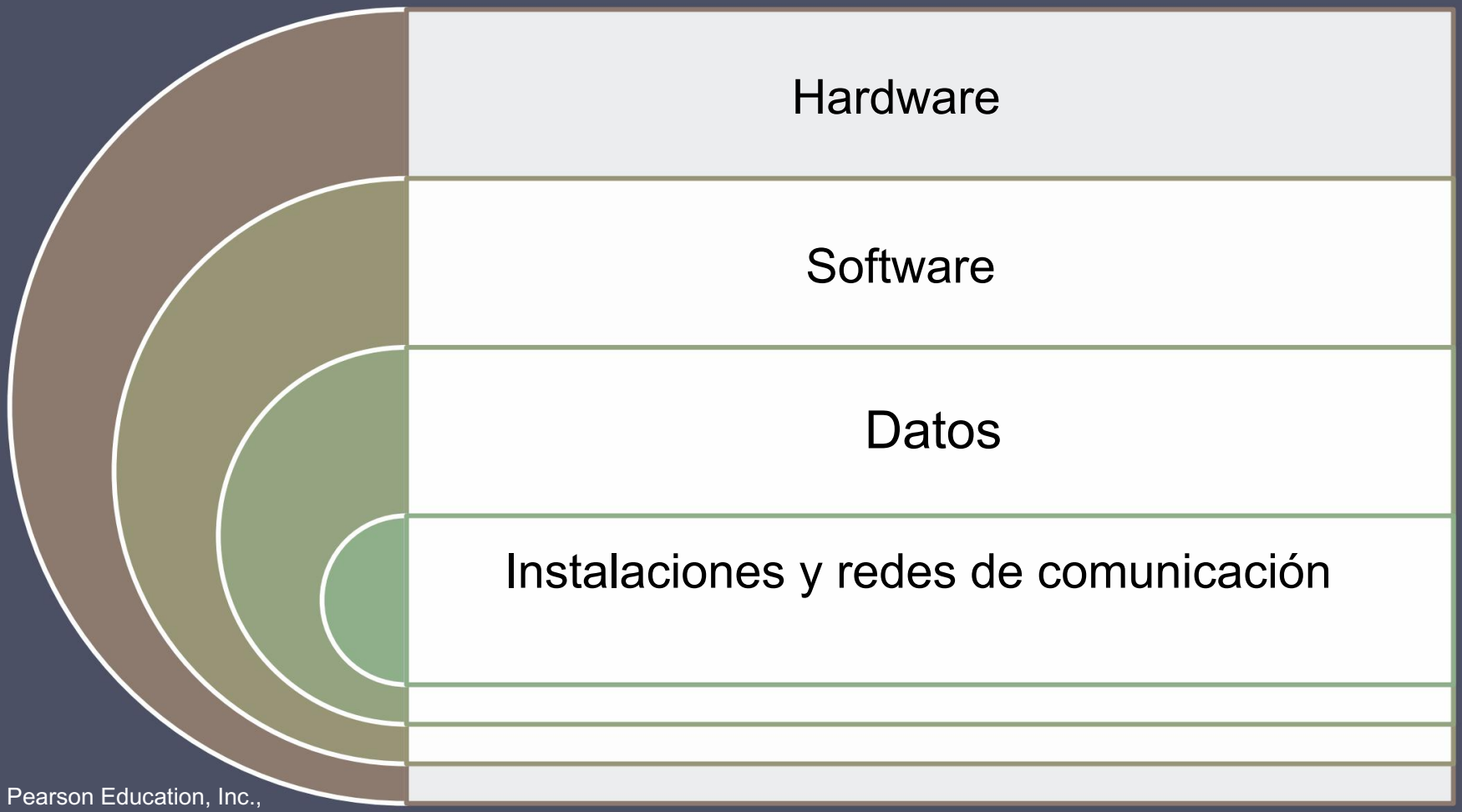


Figure 1.1 Security Concepts and Relationships

Activos de una computadora

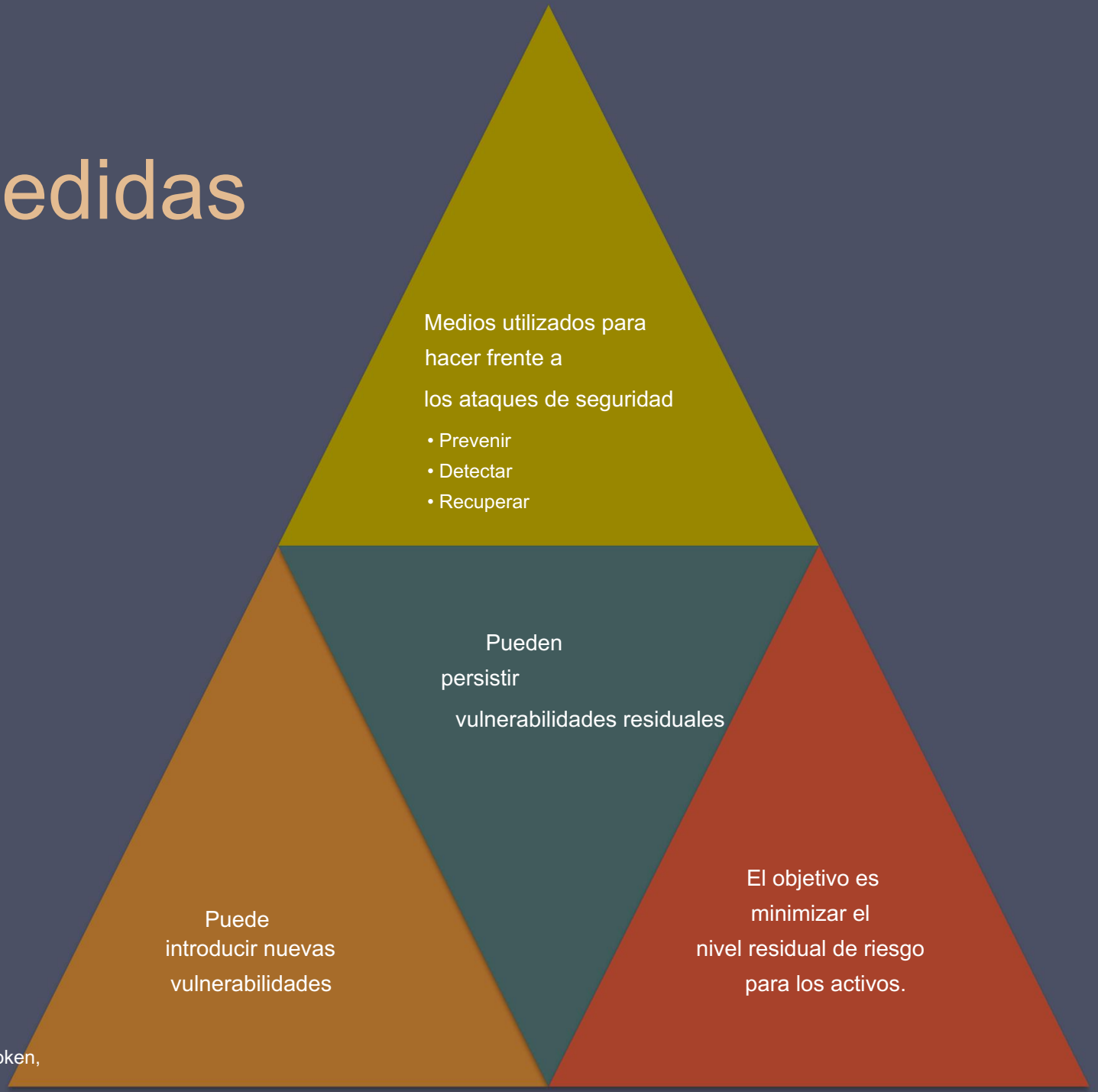
Sistema



Unerates, retas y ataques

- Categorías de vulnerabilidades
  - • Corrupto (pérdida de integridad) •
  - Con fugas (pérdida de confidencialidad)
  - • No disponible o muy lento (pérdida de disponibilidad)
- Amenazas
  - • Capaz de explotar vulnerabilidades •
  - Representar un daño potencial a la seguridad de un activo
- Ataques (amenazas realizadas)
  - • Pasivo: intento de aprender o hacer uso de la información del sistema.
    que no afecta los recursos del sistema
  - • Activo: intento de alterar los recursos del sistema o afectar su funcionamiento. •
  - Interno: iniciado por una entidad dentro del parámetro de seguridad. •
  - Externo: iniciado desde fuera del perímetro.

Contramedidas



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Tabla 1.2

Amenaza

Consecuencias,

y el

Tipos de

Acciones de amenaza

Esa causa

Cada

Consecuencia

Residencia en

RFC 4949

**La tabla está en la página 20 del libro de texto.

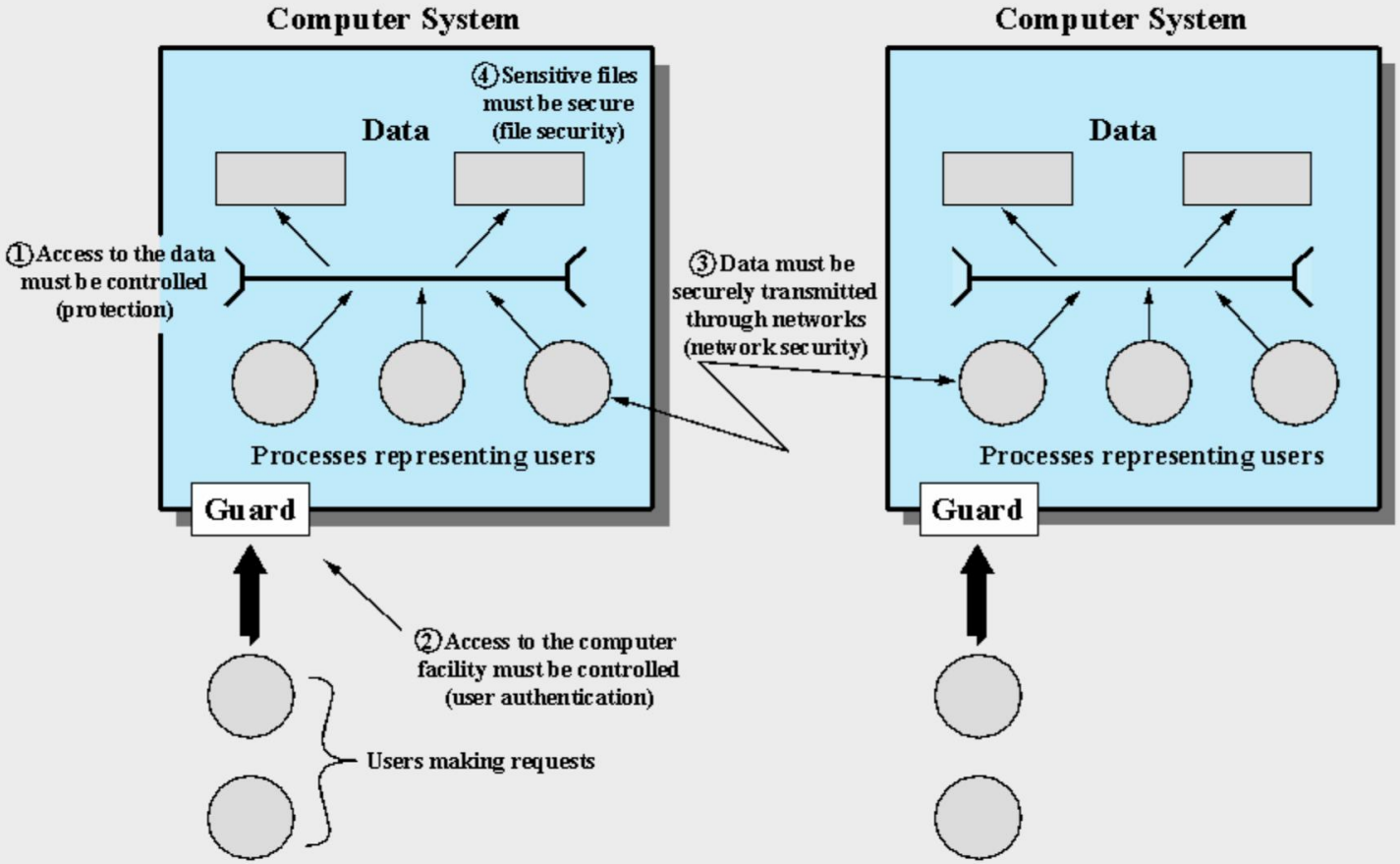


Figure 1.2 Scope of Computer Security. This figure depicts security concerns other than physical security, including control of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Tabla 1.3

Activos informáticos y de red, con ejemplos de amenazas

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

assve un ctve Ataques

Ataque pasivo

- Intenta aprender o hacer uso de la información del sistema pero no afecta los recursos del sistema.
- Escuchas clandestinas o monitoreo de transmisiones
- El objetivo del atacante es obtener la información que se está transmitiendo .
- Dos tipos:
  - o Liberación del contenido del mensaje
  - o Análisis de tráfico

Ataque activo

- Intenta alterar los recursos del sistema o afectar su funcionamiento.
- Implican alguna modificación del flujo de datos o la creación de un flujo falso.
- Cuatro categorías:
  - o Repetir
  - o Mascarada
  - o Modificación de mensajes
  - o Denegación de servicio

Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Tabla 1.4

Seguridad Requisitos

(PUBLICACIÓN FIPS 200)

(pagina 1 de 2)

(La tabla se puede encontrar en la página 26 del libro de texto).

Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Tabla 1.4

Seguridad Requisitos

(PUBLICACIÓN FIPS 200)

(pagina 2 de 2)

(La tabla se puede encontrar en la página 27 del libro de texto).

unamenta seguridad

Principios de diseño

Economía de mecanismo	Valores predeterminados a prueba de fallos	Mediación completa	Diseño abierto
Separación de privilegios	Mínimo privilegio	El menos mecanismo común	Aceptabilidad psicológica
Aislamiento	Encapsulación	Modularidad	Capas
El menor asombro			

Superficies de ataque

Consiste en las vulnerabilidades alcanzables y explotables en un sistema.

Ejemplos:

- Puertos abiertos en la cara exterior Servidores web y otros, y código que escucha en esos puertos
- Servicios disponibles dentro de un firewall
- Código que procesa datos entrantes, correo electrónico, XML, documentos de oficina y formatos de intercambio de datos personalizados específicos de la industria
- Interfaces, SQL y formularios web
- Un empleado con acceso a información confidencial vulnerable a un ataque de ingeniería social

Categorías de superficies de ataque

Red Ataque Superficie

Vulnerabilidades en una red empresarial, una red de área amplia o Internet

En esta categoría se incluyen las vulnerabilidades del protocolo de red, como las utilizadas para un ataque de denegación de servicio, la interrupción de los enlaces de comunicaciones y varias formas de ataques de intrusos.

Software Ataque Superficie

Vulnerabilidades en el código de aplicaciones, utilidades o sistemas operativos

El enfoque especial se centra en el software del servidor web.

Ataque humano Superficie

Vulnerabilidades creadas por personal o personas externas, como ingeniería social, error humano y personas internas de confianza.

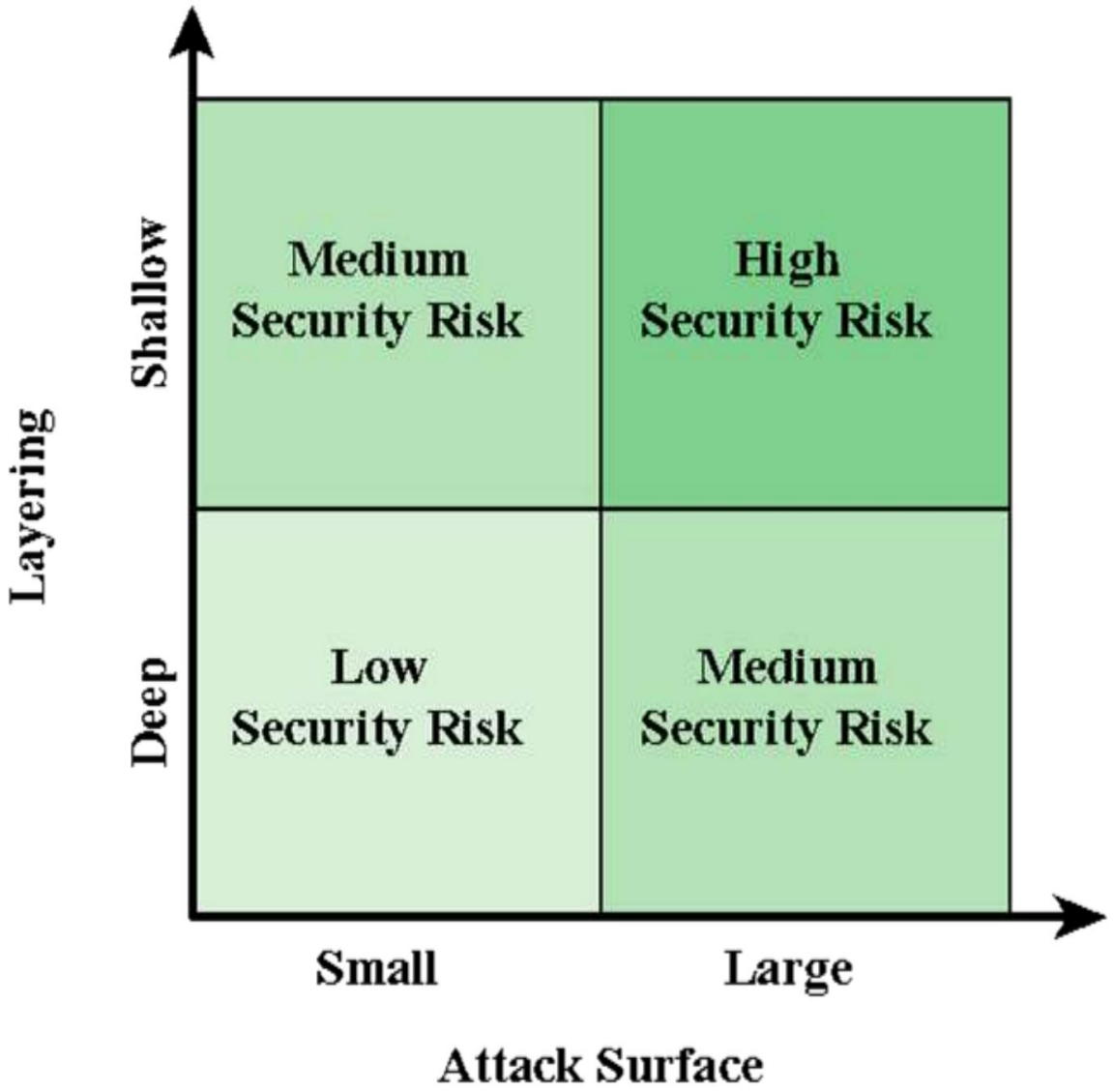


Figure 1.3 Defense in Depth and Attack Surface

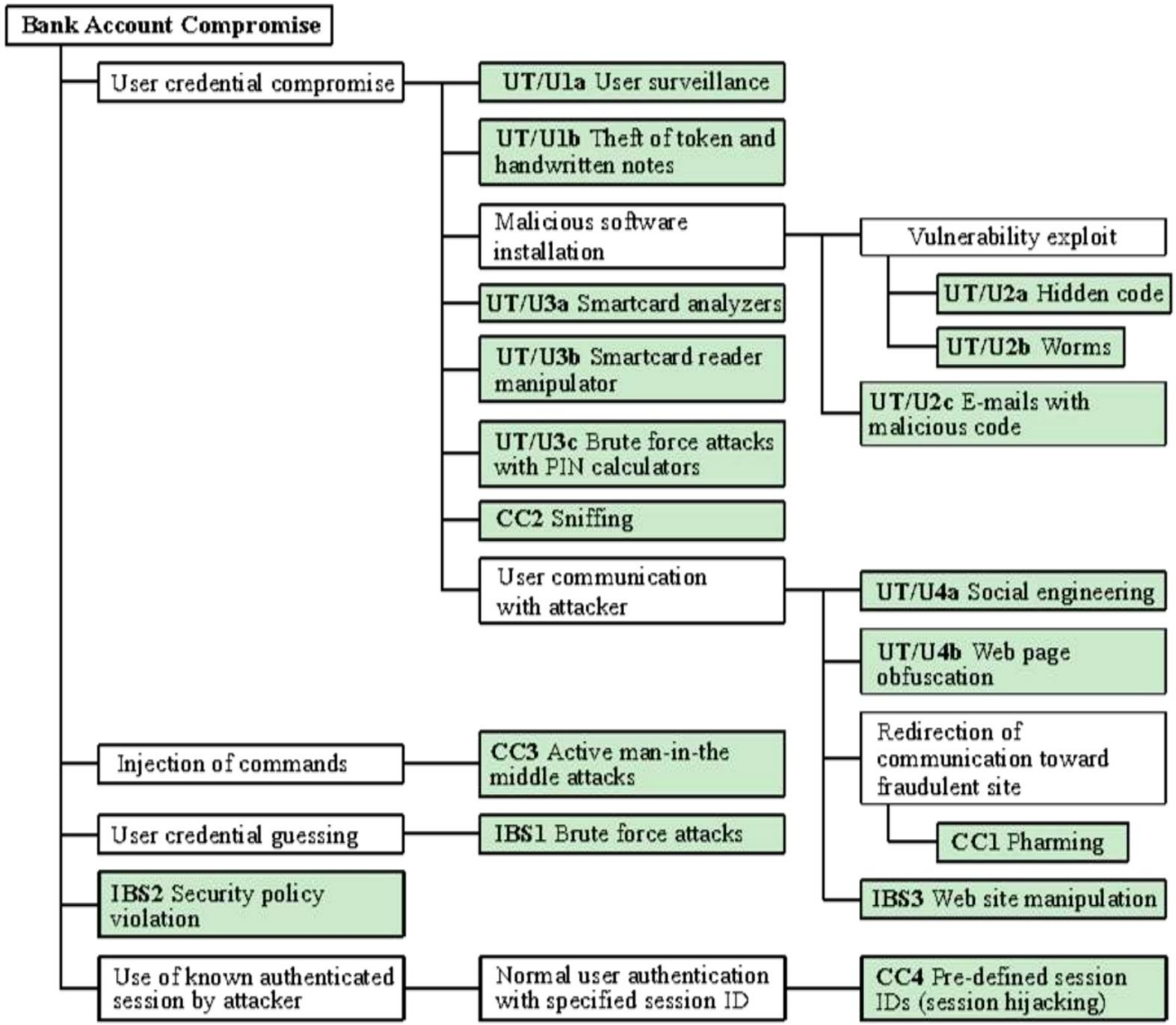


Figure 1.4 An Attack Tree for Internet Banking Authentication

Estrategia de seguridad informática

Política de seguridad

- Declaración formal de reglas y prácticas que especifican o regulan cómo un sistema u organización proporciona servicios de seguridad para proteger recursos críticos y sensibles del sistema

Seguridad Implementación

- Implica cuatro líneas de acción complementarias:
  - Prevención
  - Detección
  - Respuesta
  - Recuperación

Garantía

- El grado de confianza que uno tiene en que las medidas de seguridad, tanto técnicas como operativas, funcionan como se pretende para proteger el sistema y la información que procesa.

Evaluación

- Proceso de examinar un producto o sistema informático con respecto a ciertos criterios

Resumen

- Conceptos de seguridad informática
  - o Definición o Desafíos
  - o Modelo
- Amenazas, ataques y activos
  - o Amenazas y ataques
  - o Amenazas y activos
- Requisitos funcionales de seguridad

- Fundamental principios de diseño de seguridad
- Superficies de ataque y atacar árboles
  - o Superficies de ataque
  - o Ataque de árboles
- Estrategia de seguridad informática
  - o Política de seguridad
  - o Implementación de seguridad
  - o Aseguramiento y evaluación