Sicurezza

CdL in Informatica – L31

Lezione 1

Prof. Emiliano Casalicchio
Department of Computer Science
Sapienza University of Rome

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms* , May 2013) defines the term *computer security* as follows:

Measures and controls that ensure **confidentiality**, **integrity**, and **availability** of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

Domanda

- Quale e' il vostro concetto di **confidenzialita'**, **integrita'** e **Disponibilita'?**

Key objectives/requirements

- Confidentiality
  - Data Confidentiality
  - Privacy
- Integrity
  - Data Integrity
  - System Integrity
- Availability
  - System availability
  - Service availability

The CIA triad (+)

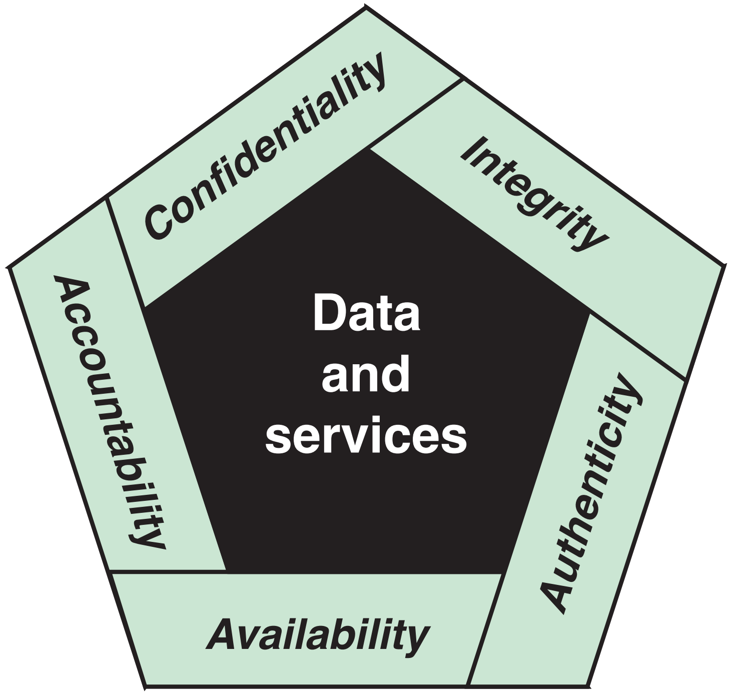


Figure 1.1 Essential Network and Computer Security Requirements

- Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - A loss of confidentiality is the unauthorized disclosure of information

The CIA triad (+)

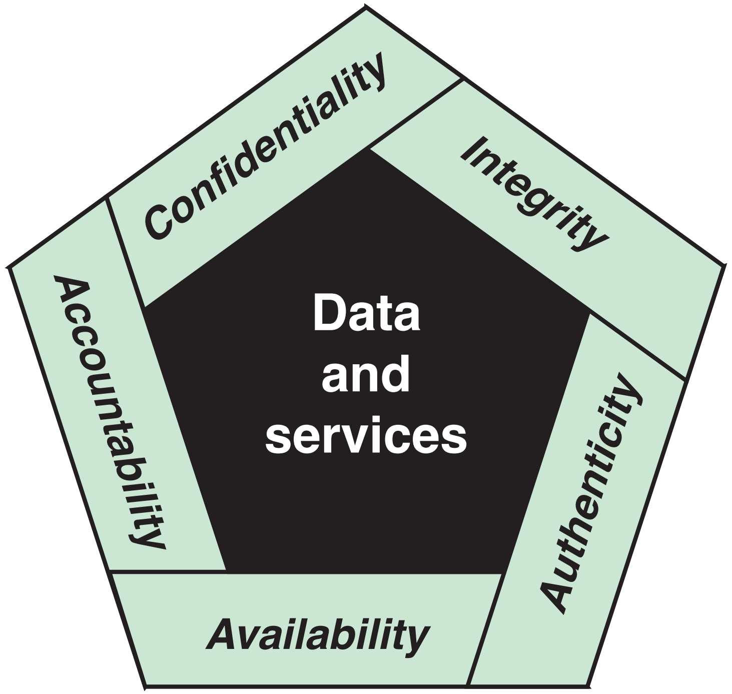


Figure 1.1 Essential Network and Computer Security Requirements

- Integrity - Guarding against improper information modification or destruction, I ncluding ensuring information nonrepudiation and authenticity.
  - A loss of integrity is the unauthorized modification or destruction of information

The CIA triad (+)

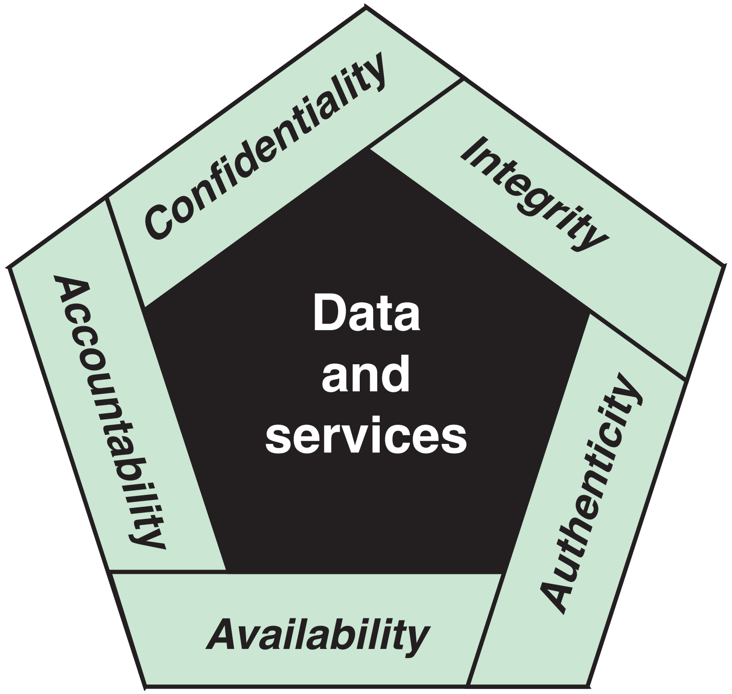


Figure 1.1 Essential Network and Computer Security Requirements

- Availability - Ensuring timely and reliable access to and use of information.
    - A loss of availability is the disruption of access to or use of information or an information system

The CIA triad (+)

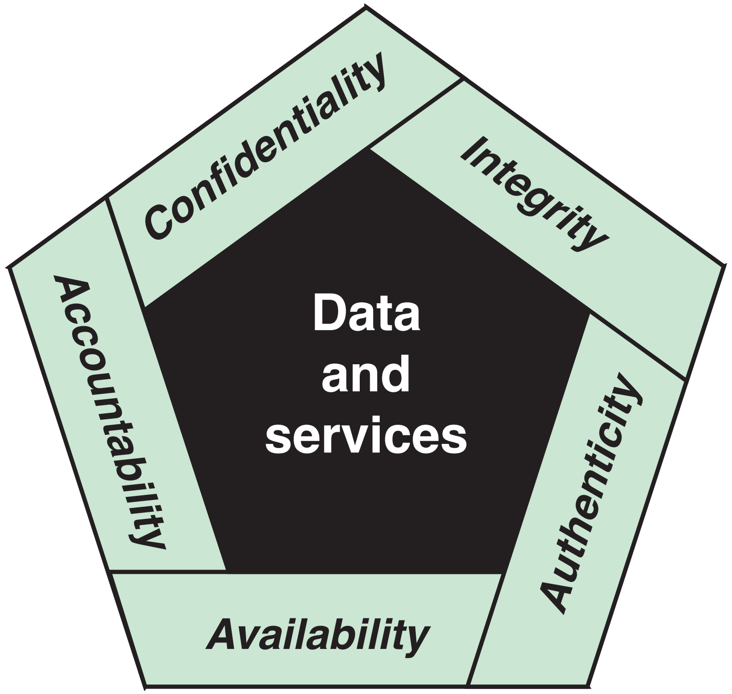


Figure 1.1 Essential Network and Computer Security Requirements

- **Authenticity** - The property of
  - being genuine and being able to be verified and trusted;
  - confidence in the validity of a transmission, a message, or message originator.

- This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source

The CIA triad (+)

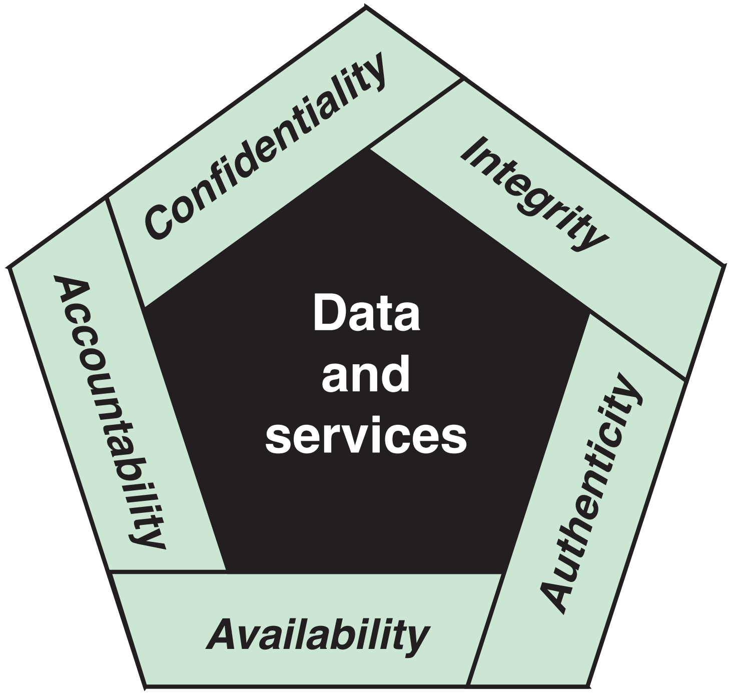
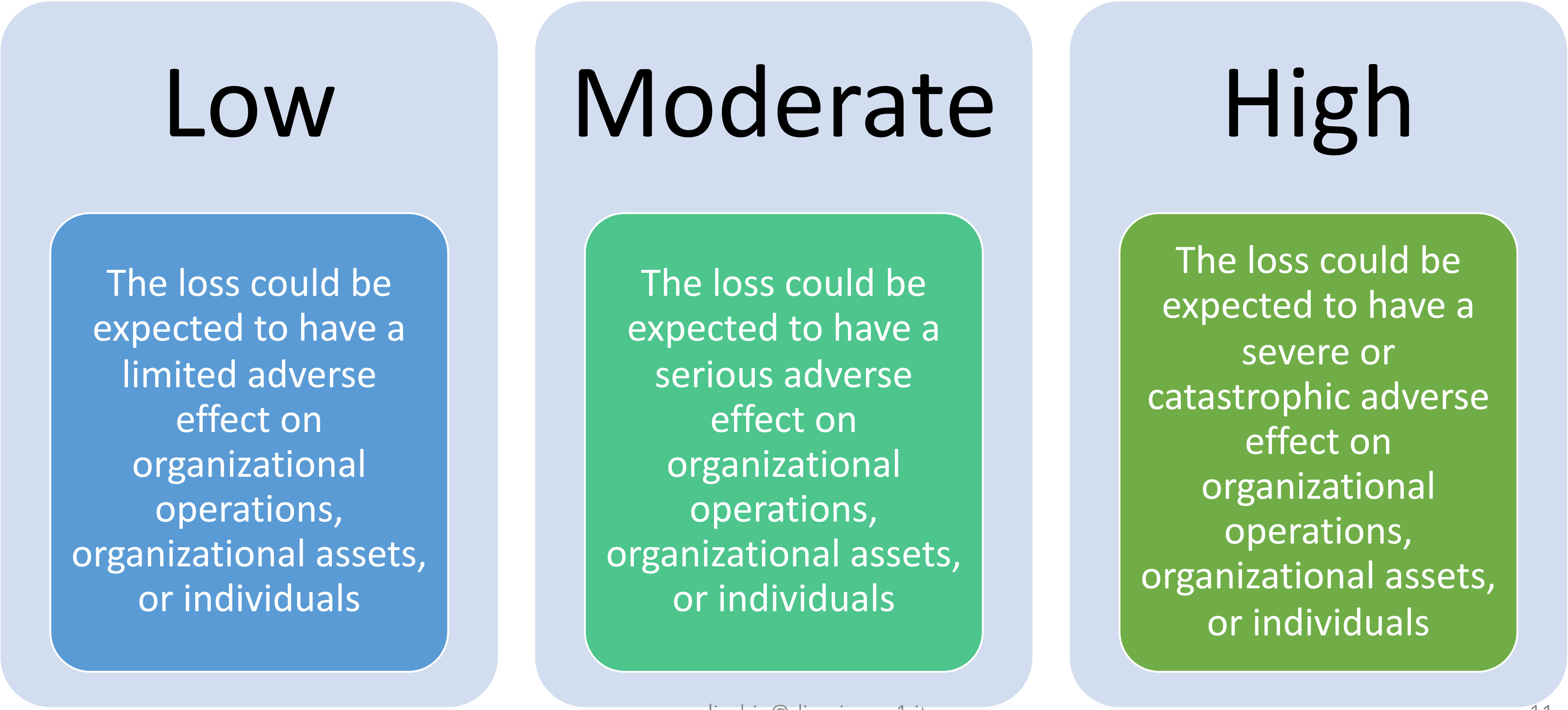


Figure 1.1 Essential Network and Computer Security Requirements

- **Accountability** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
- This supports
  - nonrepudiation,
  - deterrence,
  - fault isolation,
  - intrusion detection and prevention,
  - action recovery and legal action.
- We must be able to trace a security breach to a responsible party.
- Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Levels of Impact



Low

The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Low impact level

- For an organization, the loss of CIA might
  - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is **noticeably reduced**;
  - (ii) result in minor damage to organizational assets;
  - (iii) result in minor financial loss; or
  - (iv) result in minor harm to individuals.

Moderate Impact Level

- For an organization, the loss of CIA might
  - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is **significantly reduced;**
  - (ii) result in significant damage to organizational assets;
  - (iii) result in significant financial loss; or
  - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

High Impact Level

- For an organization, the loss of CIA might
  - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the **organization is not able to perform** one or more of its primary functions;
  - (ii) result in major damage to organizational assets;
  - (iii) result in major financial loss; or
  - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Examples

- Low Impact:
  - Loss of confidentiality for Directory information
  - Loss of integrity of an anonymous online pool
  - Loss of availability for a online telefon directory lookup application
- Moderate Impact:
  - Loss of confidentiality for student enrollment information
  - Loss of Integrity for an online forum
  - Loss of availability for a university web site providing information for current and prospective students and donors.
- High Impact
  - Loss of confidentiality of classified information (industrial/military)
  - Loss of integrity for a Database of medical record
  - Loss of availability of an authentication services for critical systems, applications, and devices

Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice

2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features

3. Procedures used to provide particular services are often counterintuitive

Computer Security Challenges

4. Physical and logical placement needs to be determined

5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information

Computer Security Challenges

6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security

7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process

8. Security requires regular and constant monitoring

Computer Security Challenges

9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs

10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Un modello per la Computer Security

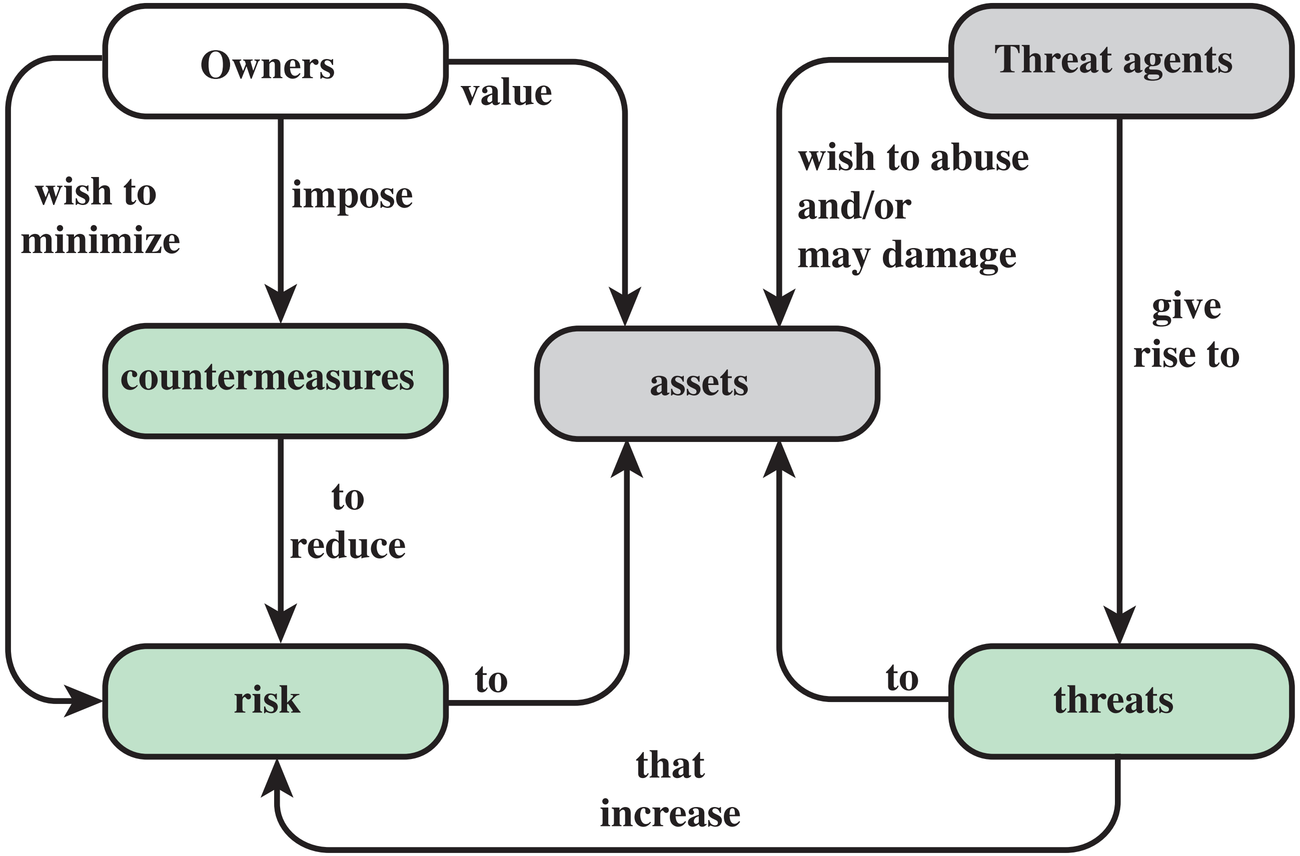
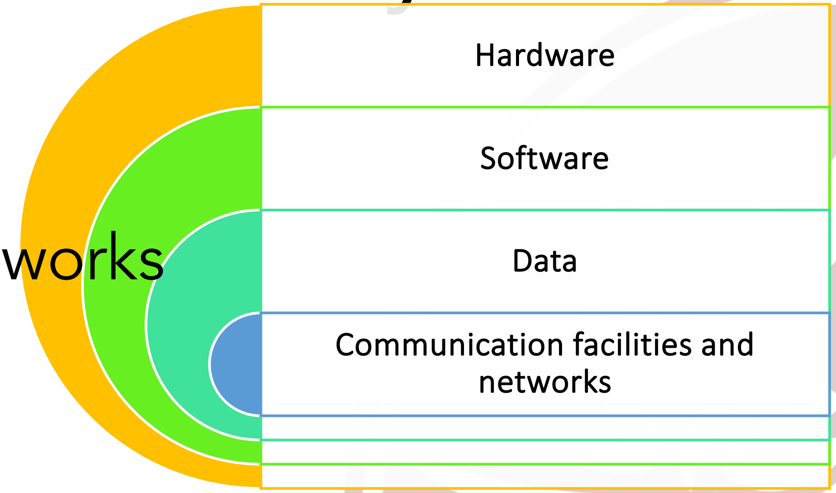


Figure 1.2 Security Concepts and Relationships

Un modello per la Computer Security

- System Resource (Asset)
  - HW, SW, Data, Communication facilities and networks
- Vulnerability (of an Asset)
  - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source
  - General categories of vulnerabilities. A system could be
    - Corrupted
    - Leaky
    - Unavailable



Un modello per la Computer Security (cont'd)

- Threat
  - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- Adversary (threat agent)
  - Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Un modello per la Computer Security (cont’d)

- Attack
  - Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- Countermeasure
  - A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Un modello per la Computer Security (cont'd)

- Risk
  - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of
    - 1) the adverse impacts that would arise if the circumstance or event occurs; and
    - 2) the likelihood of occurrence.
  - **R = P x D**
- Security Policy
  - A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

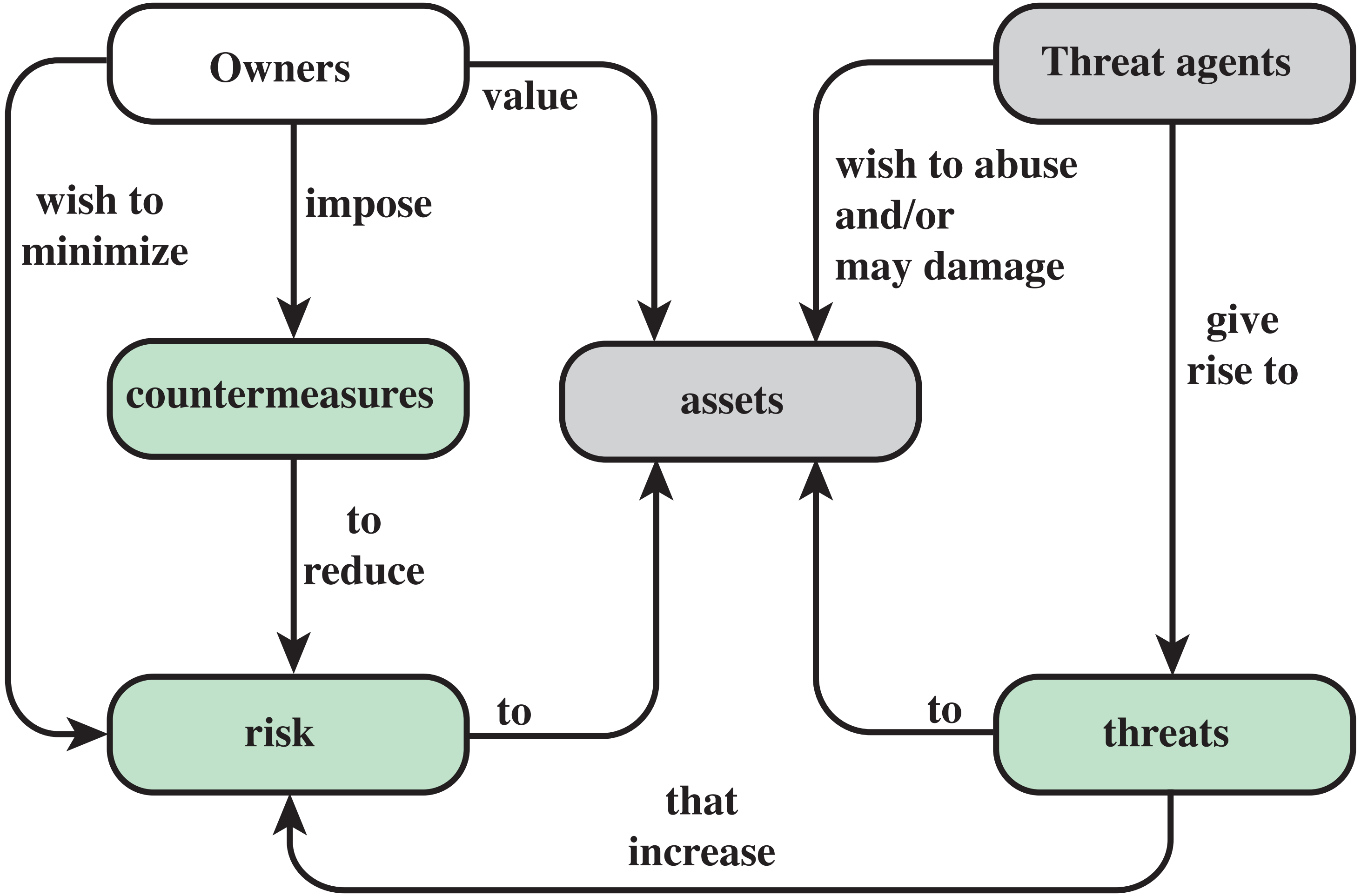
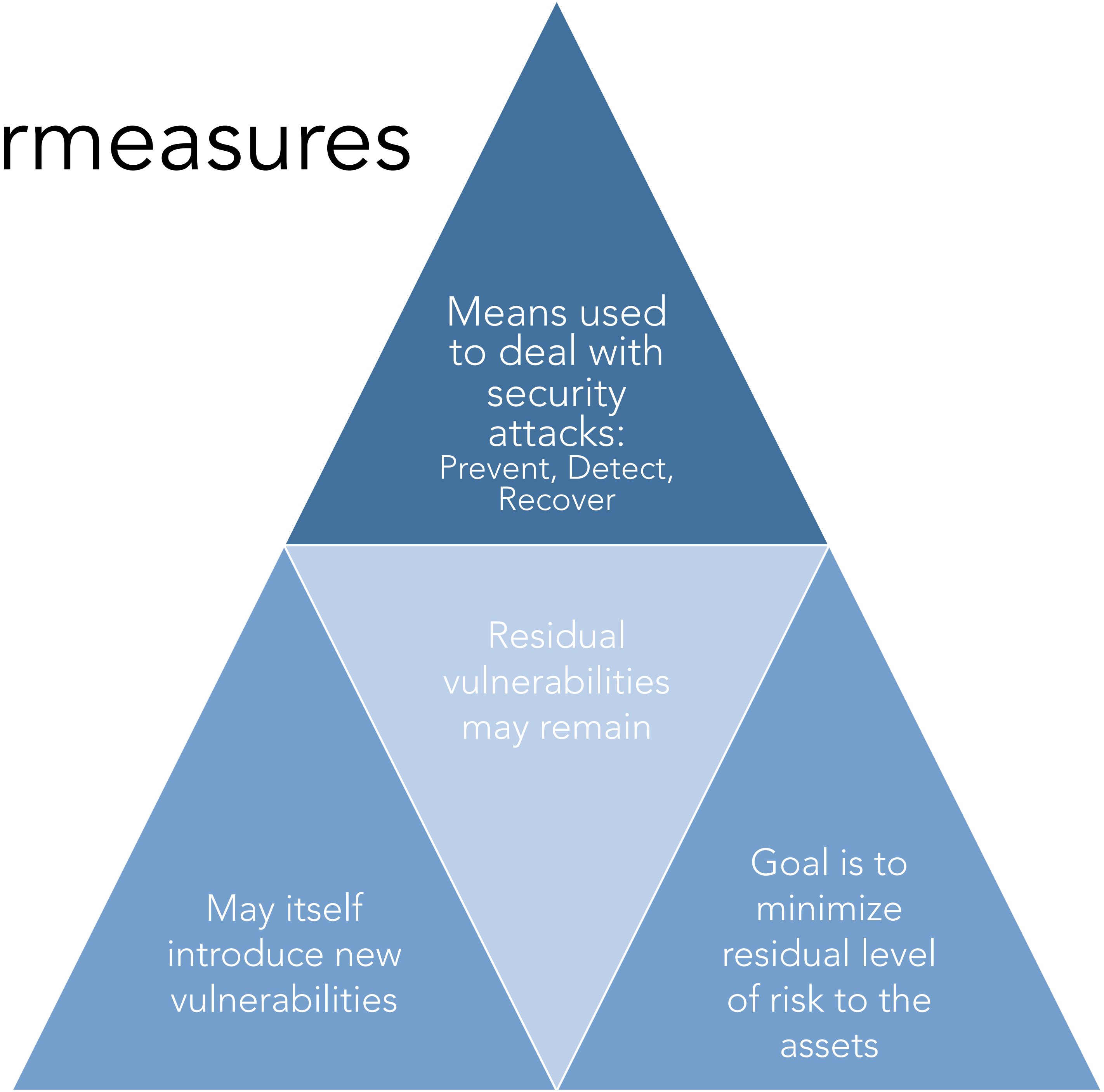


Figure 1.2 Security Concepts and Relationships

Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
  - Corrupted (loss of integrity)
  - Leaky (loss of confidentiality)
  - Unavailable or very slow (loss of availability)
- Threats
  - Capable of exploiting vulnerabilities
  - Represent potential security harm to an asset
- Attacks (threats carried out)
  - Passive – attempt to learn or make use of information from the system that does not affect system resources
  - Active – attempt to alter system resources or affect their operation
  - Insider – initiated by an entity inside the security perimeter
  - Outsider – initiated from outside the perimeter

Countermeasures



Means used to deal with security attacks:
Prevent, Detect, Recover

Residual vulnerabilities may remain

May itself introduce new vulnerabilities

Goal is to minimize residual level of risk to the assets

Minacce e attacchi

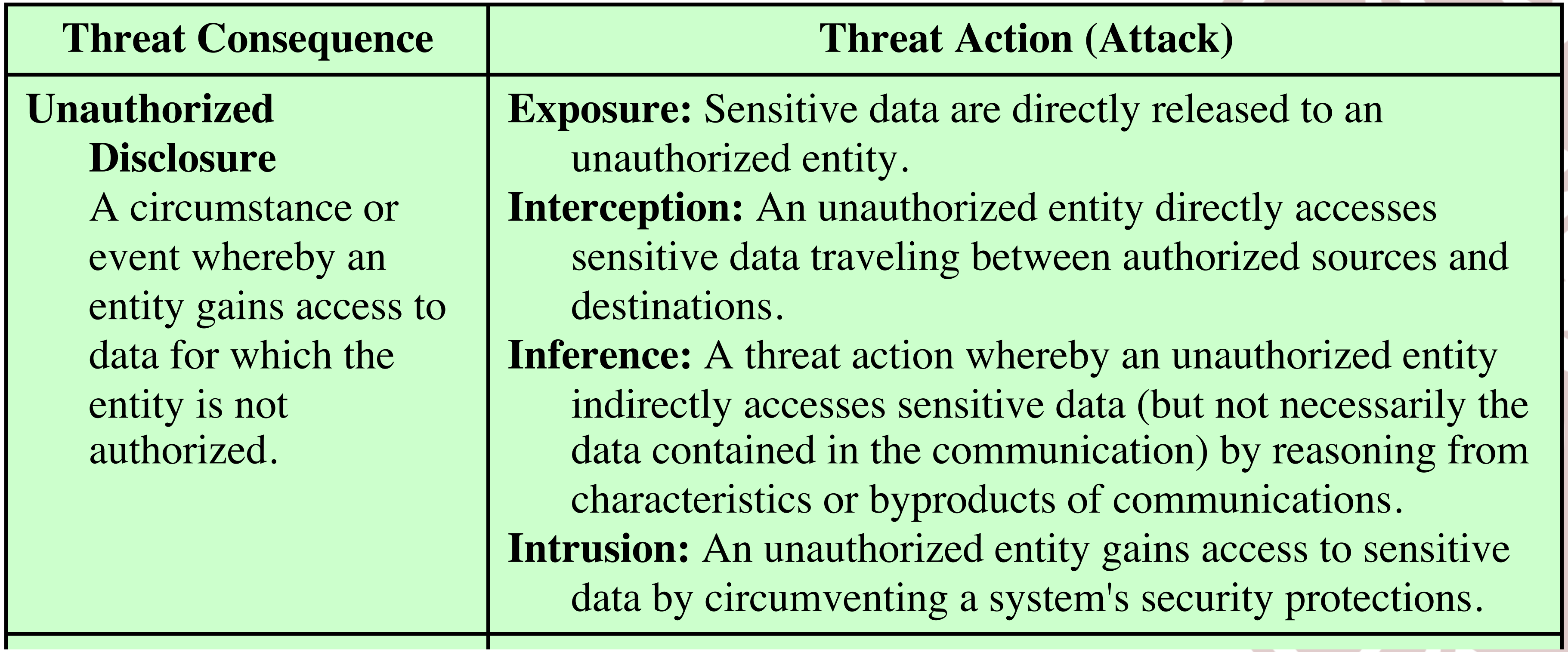
Conseguenze di minacce e tipi di attacco che producono tali conseguenze (RFC4949)

Threat consequenses

- Unauthorized disclosure
- Deception
- Disruption
- Usurpation

Minacce e attacchi

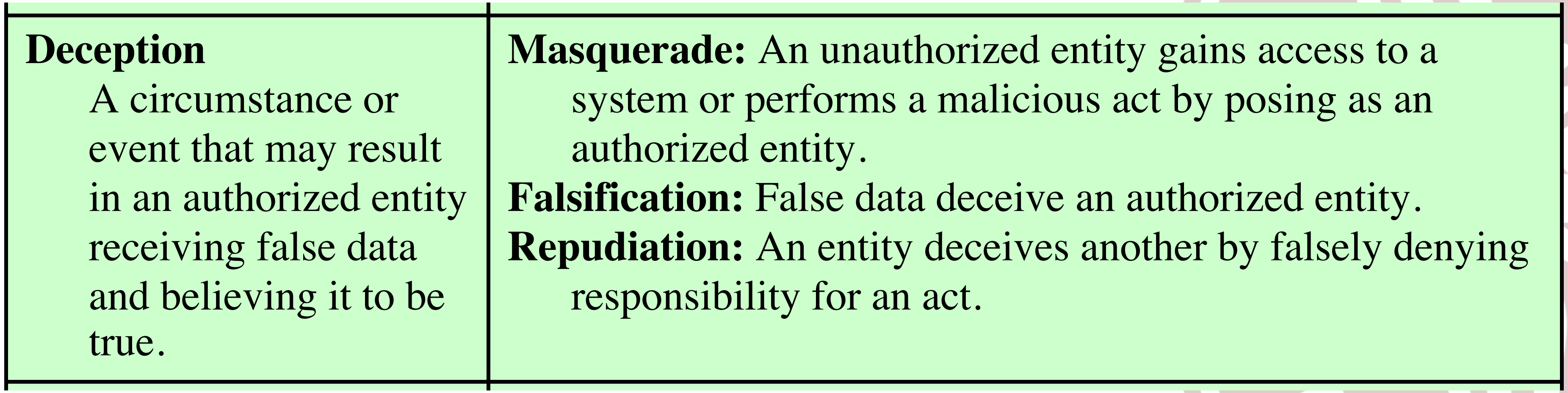
Conseguenze di minacce e tipi di attacco che producono tali conseguenze (RFC4949)



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.

Minacce e attacchi

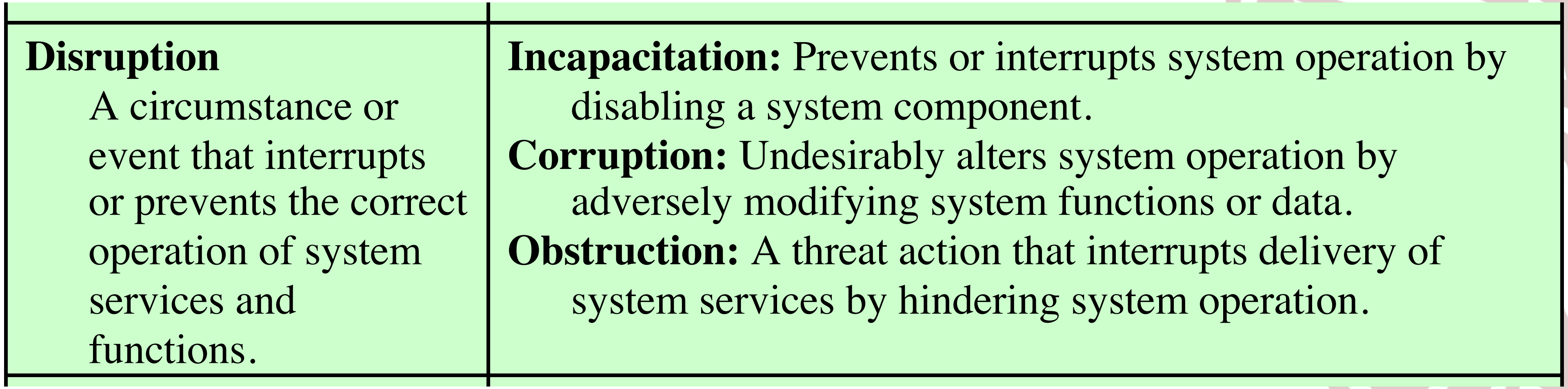
Conseguenze di minacce e tipi di attacco che producono tali conseguenze (RFC4949)



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.

Minacce e attacchi

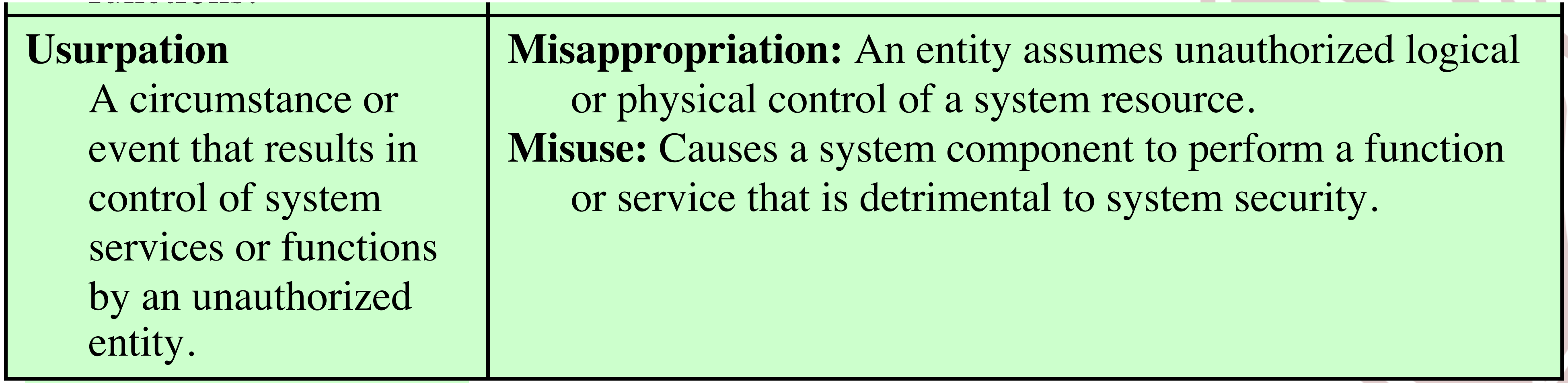
Conseguenze di minacce e tipi di attacco che producono tali conseguenze (RFC4949)



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.

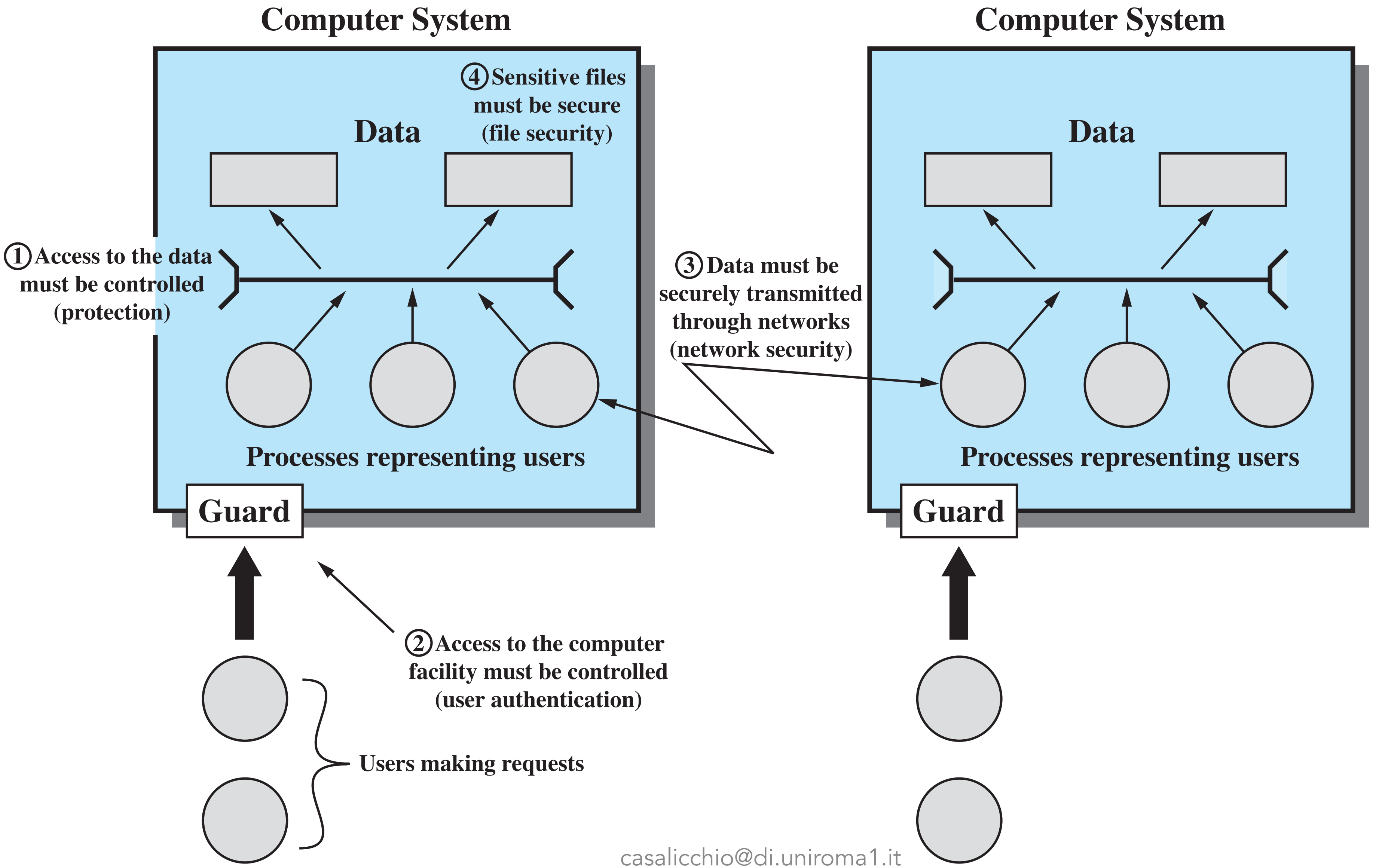
Minacce e attacchi

Conseguenze di minacce e tipi di attacco che producono tali conseguenze (RFC4949)



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.

Minacce e Risorse (threats and assets)


Computer System
Data
④ Sensitive files must be secure (file security)
① Access to the data must be controlled (protection)
Processes representing users
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests
③ Data must be securely transmitted through networks (network security)
Computer System
Data
Processes representing users
Guard

Computer and Network Assets, with Ex. of Threats

	Availability	Confidentiality	Integrity
Hardware	1	2	
Software	3	4	5 task.
Data	6	7	8
Communication Lines and Networks	9	10	11

Table 1.3

Computer and Network Assets, with Examples of Threats

	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.

Passive and Active Attacks

Passive attacks

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
  - Release of message contents
  - Traffic analysis

Active attacks

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
  - Replay
  - Masquerade
  - Modification of messages
  - Denial of service

Requisiti di sicurezza (Security requirements)

- Contromisure alle vulnerabilità e minacce possono essere classificate e categorizzate in differenti modi
- Un approccio e' classificare le contromisure in funzione dei requisiti funzionali (*FIPS 200 - Minimum Security Requirements for Federal Information and Information Systems*)
  - 17 aree di contromisure per protezione CIA
  - Contromisure tecniche
  - Contromisure funzionali (gestione della sicurezza)
  - Insieme di contromisure Tecniche e funzionali

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" [SCHN00]

Requisiti di sicurezza tecnici

- Controllo degli accessi (access control)
- Identificazione e autenticazione (Identification and Authentication)
- Protezione dei sistemi e delle comunicazioni (Systems and Communication Protection)
- Integrita del sistema e delle informazioni (Systems and Information Integrity)

Requisiti di sicurezza funzionali

- Consapevolezza e formazione (Awareness and Training)
- Controllo e responsabilizzazione (Audit and Accountability)
- Certificazione, accreditamento e valutazione di sicurezza (Cartification, Accreditation and Security Assessment)
- Pianificazione dell'emergenza (Contingency Planning)
- Manutenzione (Maintenance)
- Protezione fisica e ambientale (Physical and Environmental protection)
- Pianificazione (Planning)
- Sicurezza del personale (Personnel Security)
- Valutazione dei rischi (Risk Assessment)
- Acquisizione dei sistemi e servizi (Systems and Service Acquisition)

Requisiti di sicurezza funzionali+tecnici (overlap)

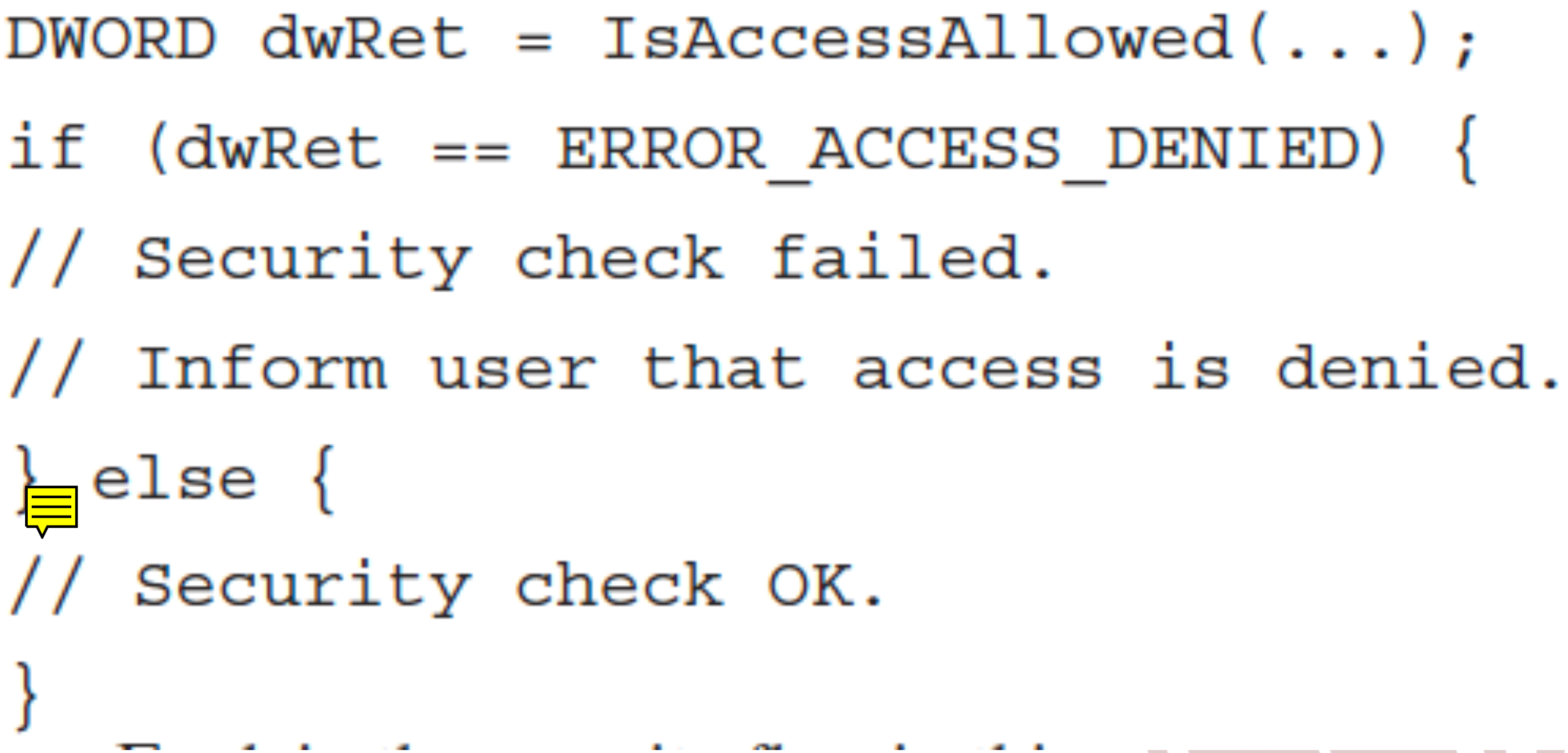
- Gestione della configurazione (Configuration management)
- Risposta agli incidenti (Incident Response)
- Protezione dei media (Media Protection)

Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Esercizio

- Consideriamo il seguente frammento di codice per controllare l’accesso ad una risorsa
- Individuare e spiegare la falla di sicurezza
- Riscrivere il codice per rimuovere la vulberabilita’



```
DWORD dwRet = IsAccessAllowed(...);
if (dwRet == ERROR_ACCESS_DENIED) {
// Security check failed.
// Inform user that access is denied.
} else {
// Security check OK.
}
```

Attack Surfaces

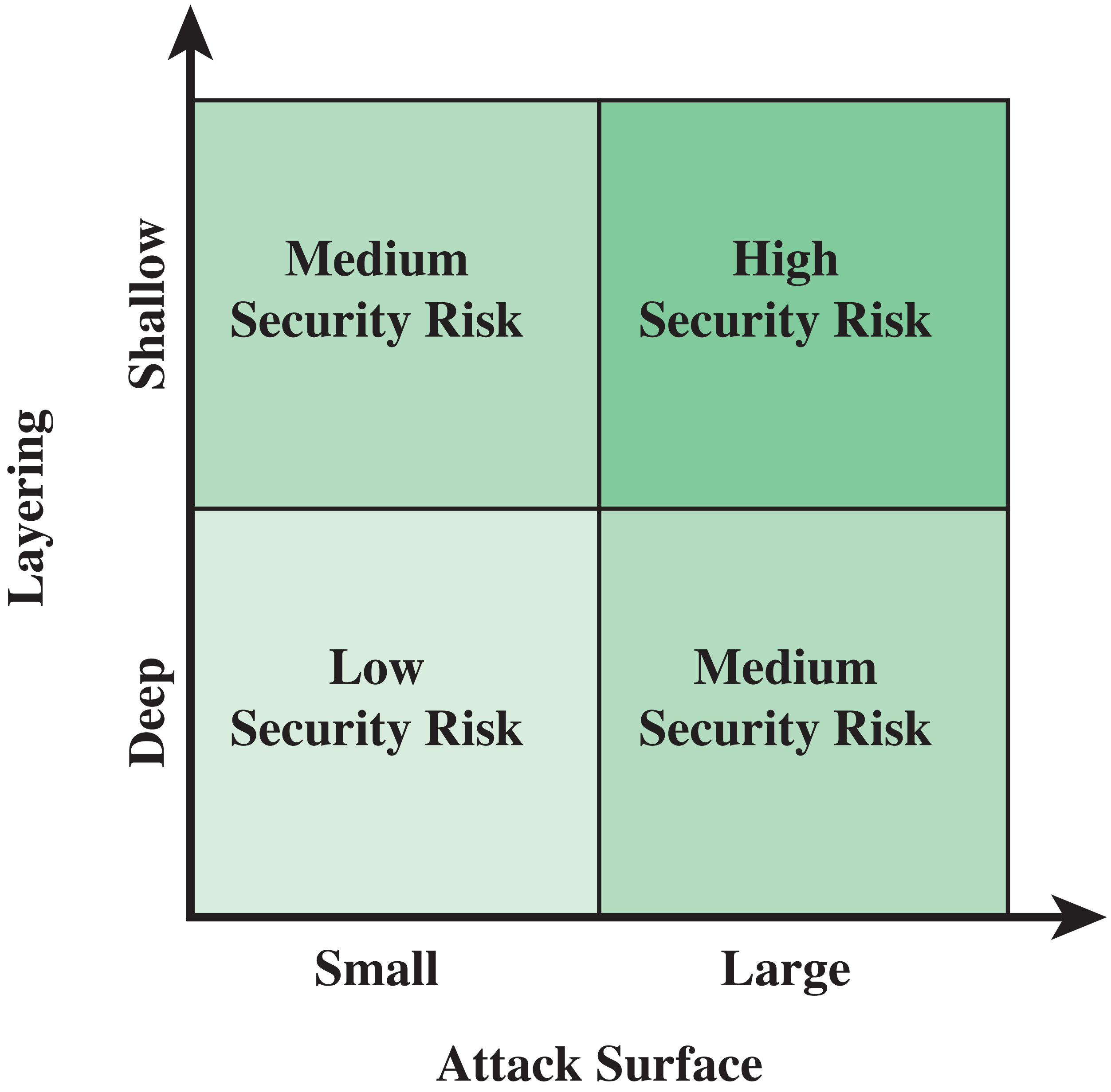
Consist of the reachable and exploitable vulnerabilities in a system

Examples:

- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack surface categories

- Network attack surface
- Software attack surface
- Human attack surface



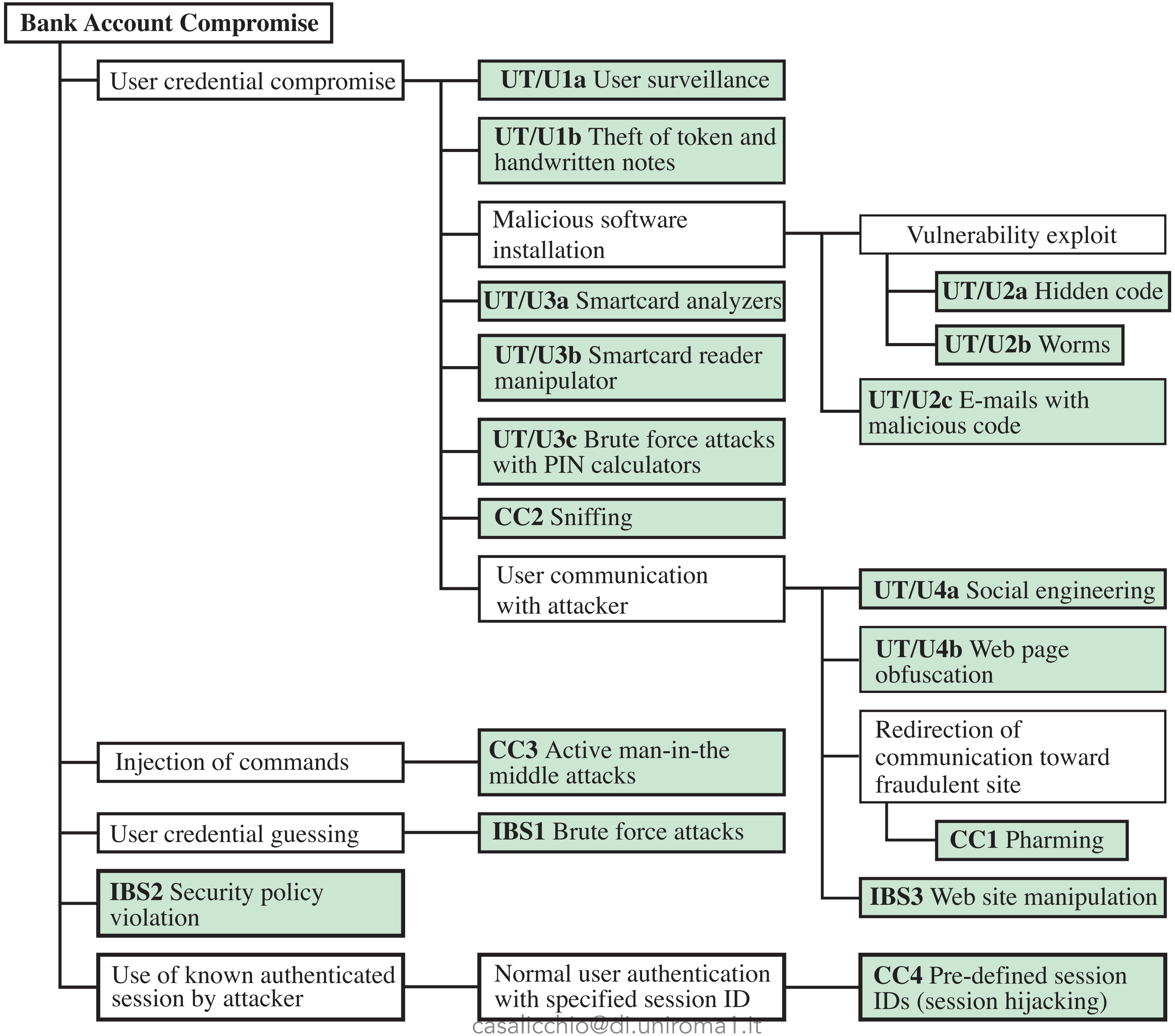
Layering	Small	Large
Shallow	Medium Security Risk	High Security Risk
Deep	Low Security Risk	Medium Security Risk

Attack Surface

Alberi di attacco

- Struttura dati gerarchica e ramificata che rappresenta un insieme di tecniche per sfruttura le vulnerabilità di sicurezza

- Radice = Obiettivo dell'attacco / incidente di sicurezza
- Nodi intermedi = sotto-obiettivi
  - AND
  - OR
- Foglie = diversi modi per iniziare l'attacco



- **Bank Account Compromise**
  - User credential compromise
    - **UT/U1a** User surveillance
    - **UT/U1b** Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - **UT/U2a** Hidden code
        - **UT/U2b** Worms
      - **UT/U2c** E-mails with malicious code
    - **UT/U3a** Smartcard analyzers
    - **UT/U3b** Smartcard reader manipulator
    - **UT/U3c** Brute force attacks with PIN calculators
    - **CC2** Sniffing
    - User communication with attacker
      - **UT/U4a** Social engineering
      - **UT/U4b** Web page obfuscation
      - Redirection of communication toward fraudulent site
        - **CC1** Pharming
      - **IBS3** Web site manipulation
  - Injection of commands
    - **CC3** Active man-in-the middle attacks
  - User credential guessing
    - **IBS1** Brute force attacks
  - **IBS2** Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - **CC4** Pre-defined session IDs (session hijacking)

Sicurezza delle reti

- Sicurezza della comunicazione
- Sicurezza dei dispositivi

Sicurezza della comunicazione

- Protocolli di rete (Protocollo di sicurezza)
  - Parte di un protocollo esistente
    - Ipsec
  - Protocollo autonomo
    - TLS
    - SSH
    - HTTPS
    - …

Sicurezza dei dispositivi

- Firewall
  - Filtro
- Rilevamento delle intrusioni (Intrusion detection)
  - Genera allarme
- Prevenzione delle intrusioni (Intrusion prevention)
  - Rileva e “blocca”

Computer Security Strategy

Security Policy

- Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources

Security Implementation

- Involves four complementary courses of action:
  - Prevention
  - Detection
  - Response
  - Recovery

Assurance

- Encompassing both system design and system implementation, assurance is an attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced

Evaluation

- Process of examining a computer product or system with respect to certain criteria
- Involves testing and may also involve formal analytic or mathematical techniques

Security policy

- In developing a security policy, a security manager needs to consider the following factors:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks

and trade-off

  - Ease of use versus security
  - Cost of security versus cost of failure and recovery

Assurance

- Assurance deals with the questions
  - “Does the security system design meet its requirements?”
  - “Does the security system implementation meet its specifications?”
- Assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct

Summary

- Computer security concepts
  - Definition
  - Challenges
  - Model
- Threats, attacks, and assets
  - Threats and attacks
  - Threats and assets
- Security functional requirements

- Fundamental security design principles
- Attack surfaces and attack trees
  - Attack surfaces
  - Attack trees
- Computer security strategy
  - Security policy
  - Security implementation
  - Assurance and evaluation