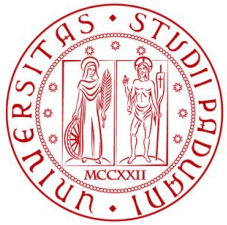
CyberSecurity: Principle and Practice

BSc Degree in Computer Science
2022-2023

Lesson 1: Overview

Prof. Mauro Conti
Department of Mathematics
University of Padua
conti@math.unipd.it
http://www.math.unipd.it/~conti/

Teaching Assistants
Pier Paolo Tricomi
pierpaolo.tricomi@phd.unipd.it
Tommaso Bianchi
tommaso.bianchi@phd.unipd.it



UNIVERSITÀ DEGLI STUDI DI PADOVA

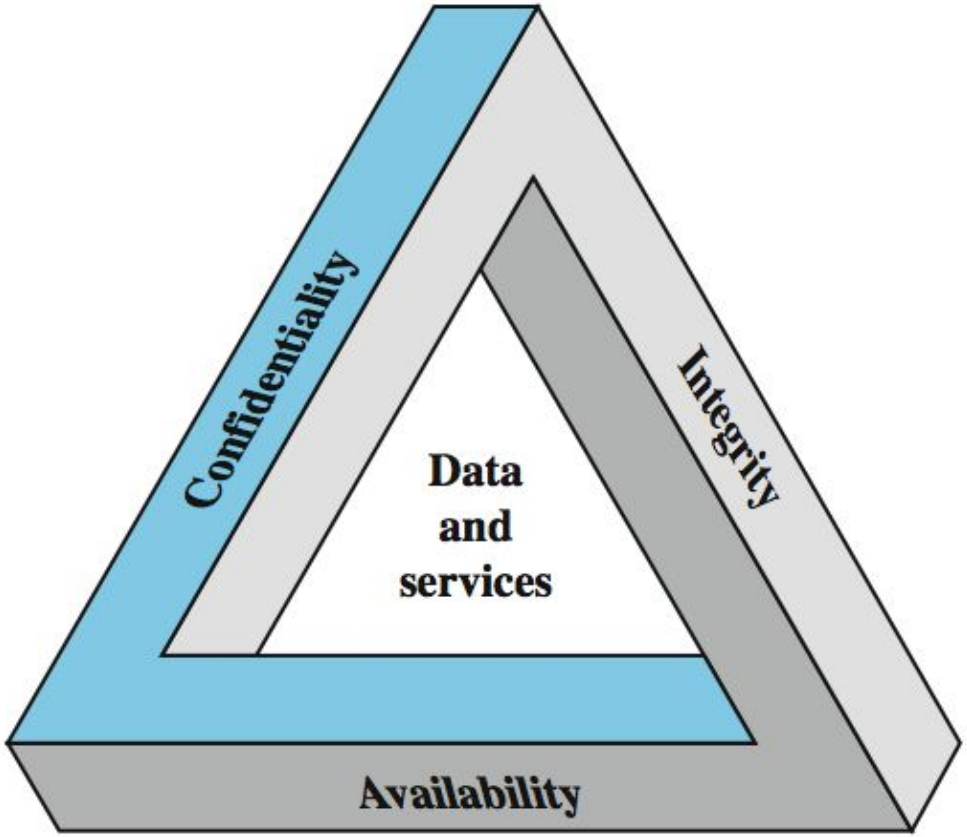
SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

Introduction

Computer Security:
protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Introduction

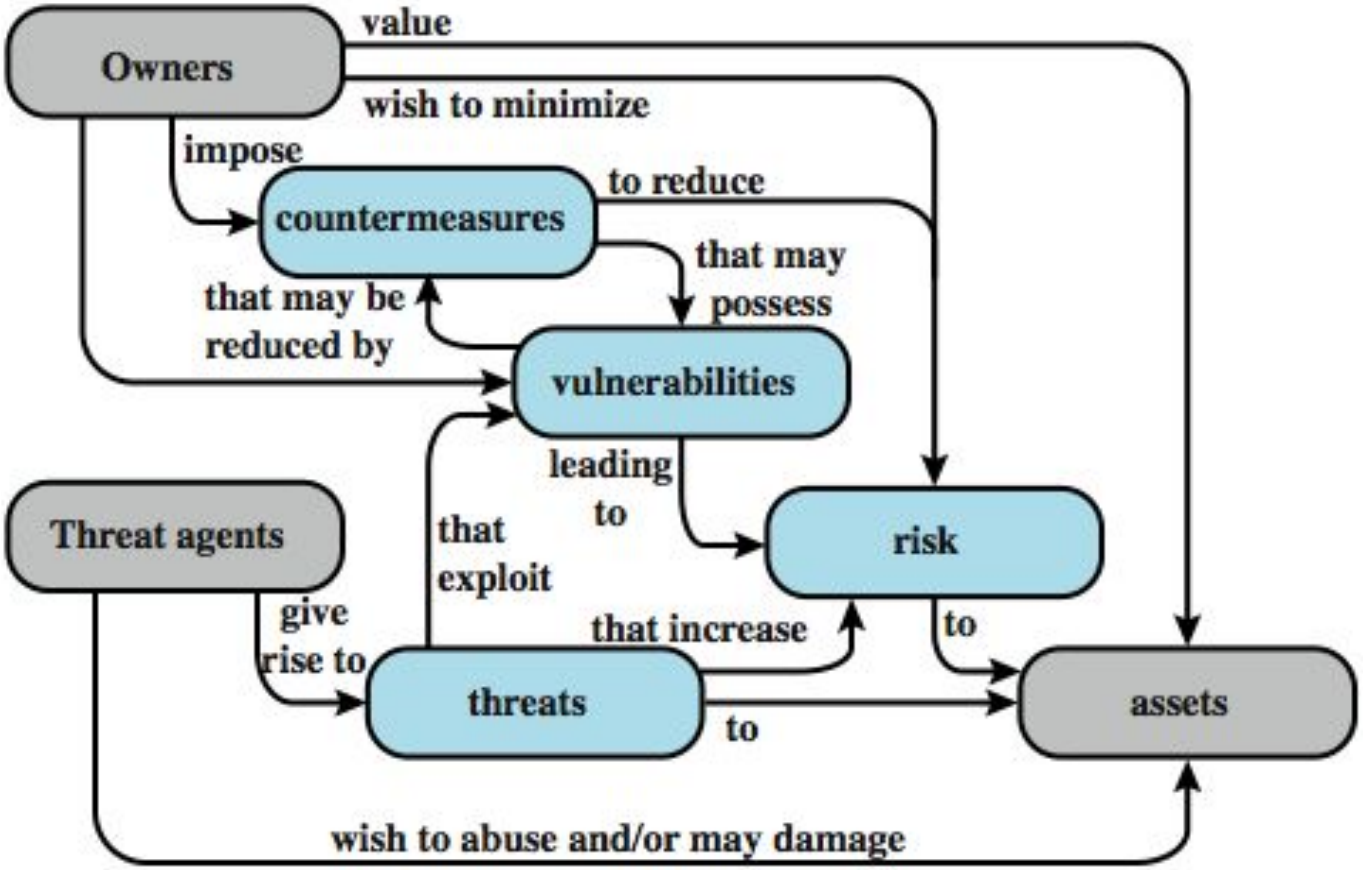


Introduction

Challenges:

1. not simple
2. must consider potential attacks
3. procedures used counter-intuitive
4. involve algorithms and secret info
5. must decide where to deploy mechanisms
6. battle of wits between attacker / admin
7. not perceived on benefit until fails
8. requires regular monitoring
9. too often an after-thought
10. regarded as impediment to using system

Introduction



Vulnerabilities and Attacks

- system resource: with vulnerabilities may
  - be corrupted (loss of integrity)
  - become leaky (loss of confidentiality)
  - become unavailable (loss of availability)
- attacks are threats carried out and may be
  - passive
  - active
  - insider
  - outsider

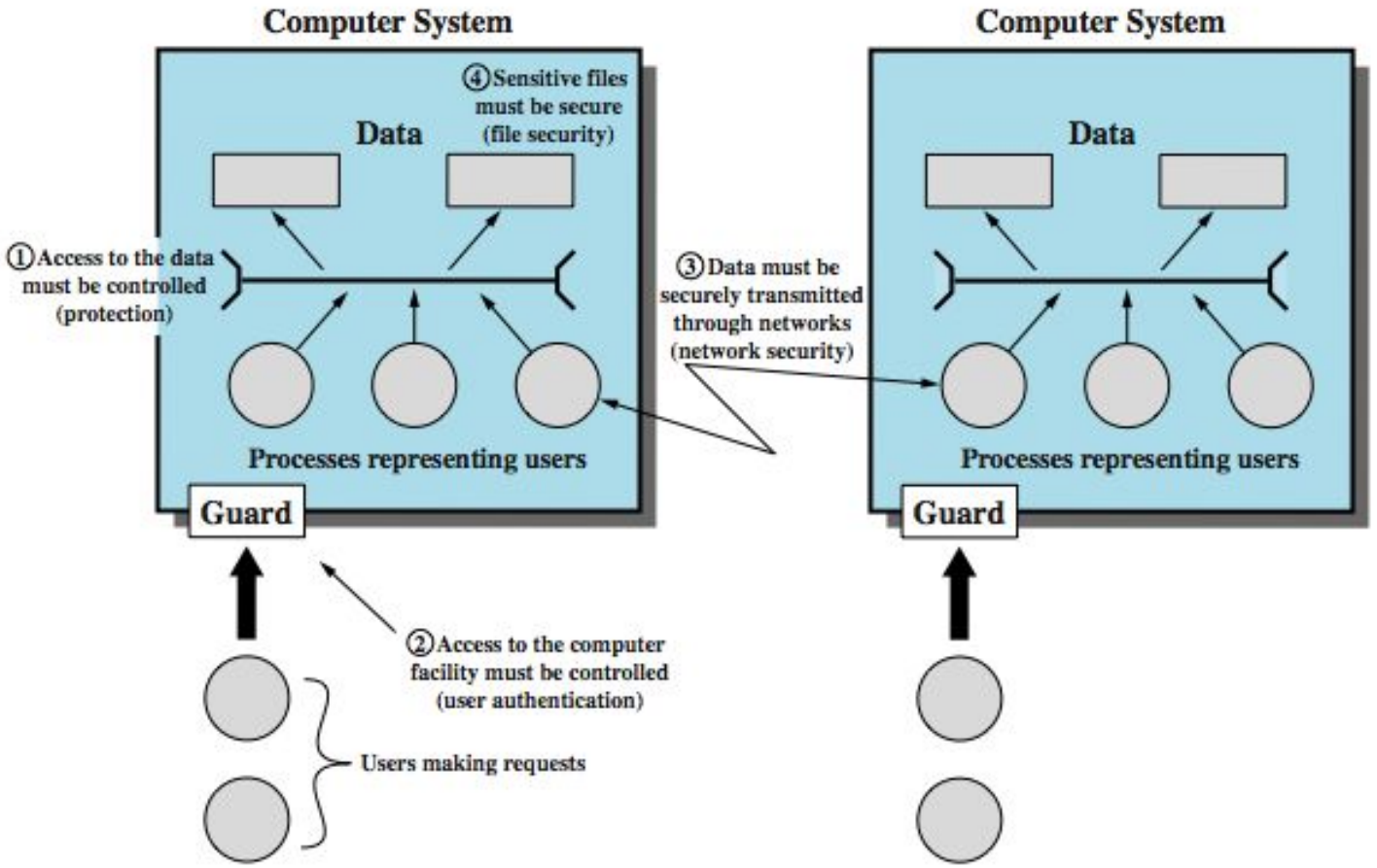
Countermeasures

- means used to deal with security attacks
  - prevent
  - detect
  - recover
- may result in new vulnerabilities
- will have residual vulnerability
- goal is to minimize risk, given constraints

Threat Consequences

- unauthorized disclosure
  - exposure, interception, inference, intrusion
- deception
  - masquerade, falsification, repudiation
- disruption
  - incapacitation, corruption, obstruction
- usurpation
  - misappropriation, misuse

Scope of Computer Security



Network Security Attacks

- classify as passive or active
- passive attacks are eavesdropping
  - release of message contents
  - traffic analysis
  - are hard to detect so aim to prevent
- active attacks modify/fake data
  - masquerade
  - replay
  - modification
  - denial of service
  - hard to prevent so aim to detect

Security Functional Requirements

- technical measures:
  - access control; identification & authentication; system & communication protection; system & information integrity
- management controls and procedures
  - awareness & training; audit & accountability; certification, accreditation, & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- overlapping technical and management:
  - configuration management; incident response; media protection

Computer Security Strategy

- specification/policy
  - what is the security scheme supposed to do?
  - codify in policy and procedures
- implementation/mechanisms
  - how does it do it?
  - prevention, detection, response, recovery
- correctness/assurance
  - does it really work?
  - assurance, evaluation

Questions? Feedback? Suggestions?