

Introduction to Computer Security

Chapter 1: Overview

Chi-Yu Li (2020 Spring)
Computer Science Department
National Chiao Tung University

Focus: Three Fundamental Questions

- What assets do we need to protect?
- How are those assets threatened?
- What can we do to counter those threats?

Outline

- Computer Security Concept
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Computer Security Concepts

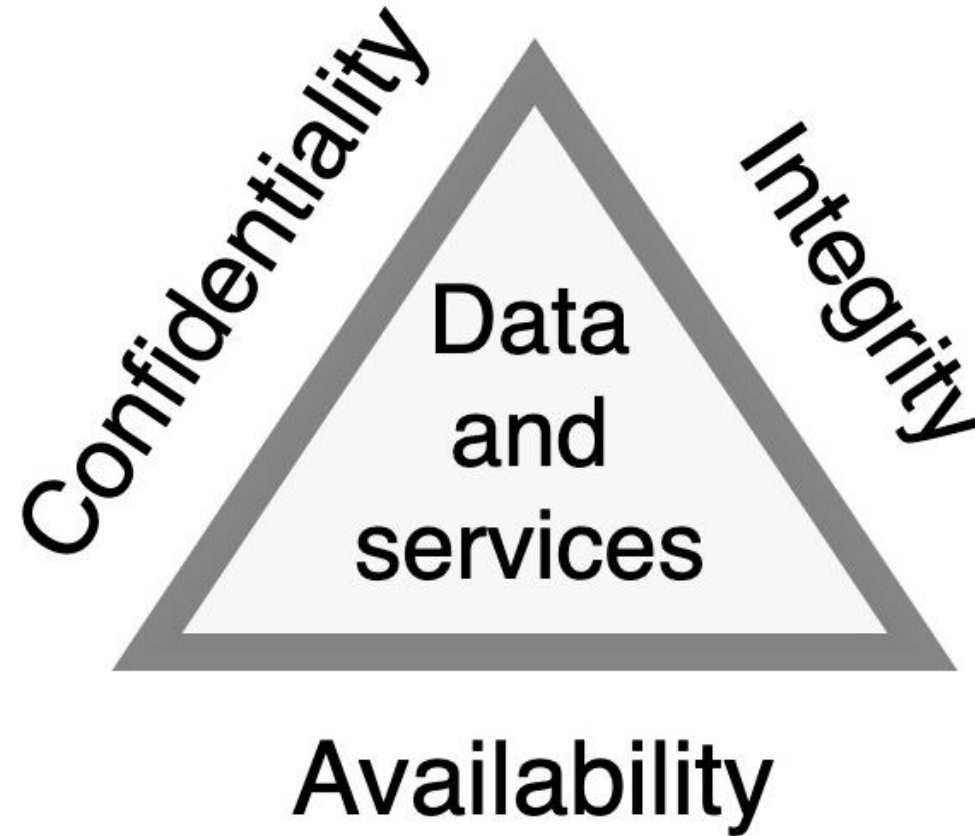
- Definition of Computer Security

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

By the NIST Internal/Interagency Report (NISTIR) 7298
(Glossary of Key Information Security Terms, May 2013)

NIST (National Institute of Standards and Technology): a US federal agency that deals with measurement science, and technology related to US government use.

CIA Triad: Three Key Objectives



Confidentiality

- Assurance

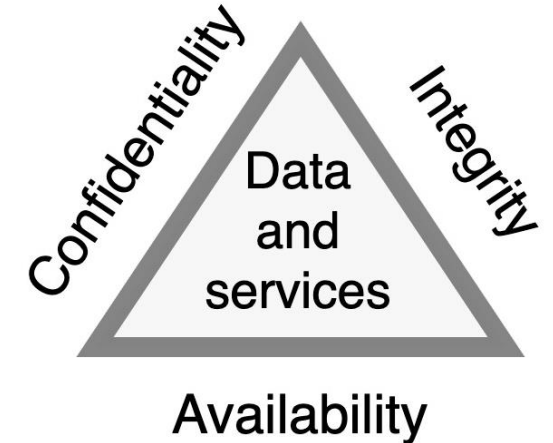
- ❑ **Data confidentiality**: private or confidential info is not disclosed to unauthorized individuals
- ❑ **Privacy**: individuals control or influence what information related to them may be collected and stored

- Requirements

- ❑ Preserving authorized restrictions on information access and disclosure
- ❑ Including means for protecting personal privacy and proprietary info

- Definition of loss

- ❑ Unauthorized disclosure of information



Integrity

- Assurance

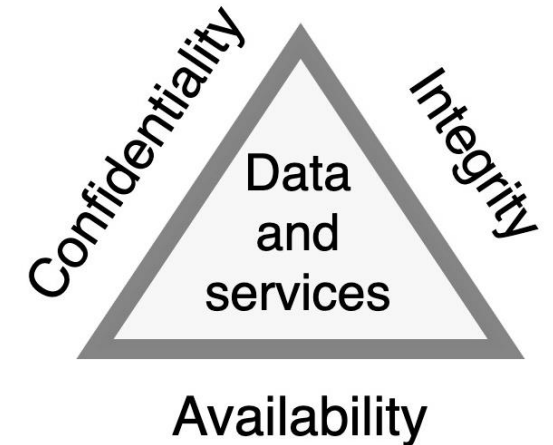
- **Data integrity**: information and programs are changed only in a specified and authorized manner
- **System integrity**: a system performs its intended function in an unimpaired manner

- Requirements

- Guarding against improper info modification or destruction
- Including ensuring info non-repudiation and authenticity

- Definition of loss

- Unauthorized modification or destruction of information



Availability

- Assurance

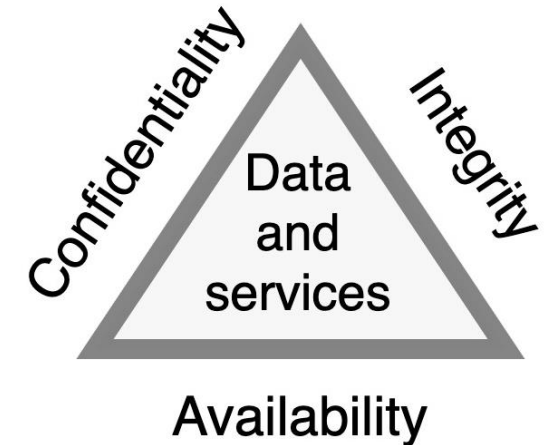
- ❑ Systems work promptly and service is not denied to authorized users

- Requirement

- ❑ Ensuring timely and reliable access to and use of info

- Definition of loss

- ❑ Disruption of access to or use of info or an info system



Other Two Concepts to a Complete Security Picture

● Authenticity

- ❑ Property is genuine and able to be verified and trusted
- ❑ Confident in the validity of a transmission, or a message, or **its originator**

● Accountability

- ❑ Requirement for actions of an entity to be traced uniquely to that entity
- ❑ Be able to trace a security breach to a responsible party

Three levels of Security Impact

- Defined in FIPS 199

- ❑ Low: limited adverse effect (minor)
- ❑ Moderate: serious adverse effect (significant)
- ❑ High: catastrophic adverse effect (catastrophic)

- Confidentiality

- ❑ Low: directory information of departments
- ❑ Moderate: student enrollment information (covered by FERPA)
- ❑ High: student grade information (covered by FERPA)

FIPS: Federal Information Processing System

FERPA: Family Educational Rights and Privacy Act

Three Levels of Security Impact (Cont.)

● Integrity

- ❑ Low: anonymous online poll
- ❑ Moderate: articles in a discussion forum
- ❑ High: patient allergy information

● Availability

- ❑ Low: online telephone directory lookup application
- ❑ Moderate: a public website for a university
- ❑ High: authentication services for critical systems

Challenges of Computer Security

- Computer security is not simple
 - ❑ Requirements seem to be straightforward
 - ❑ Mechanisms can be quite complex
- One must consider potential (unexpected) attacks
 - ❑ Successful attacks look at the problem in a completely different way
 - ❑ Exploiting an unexpected weakness
- Procedures are usually counterintuitive
 - ❑ Typically, a security mechanism is complex
 - ❑ Make sense only when the various aspects of the threat are considered

Challenges of Computer Security (Cont.)

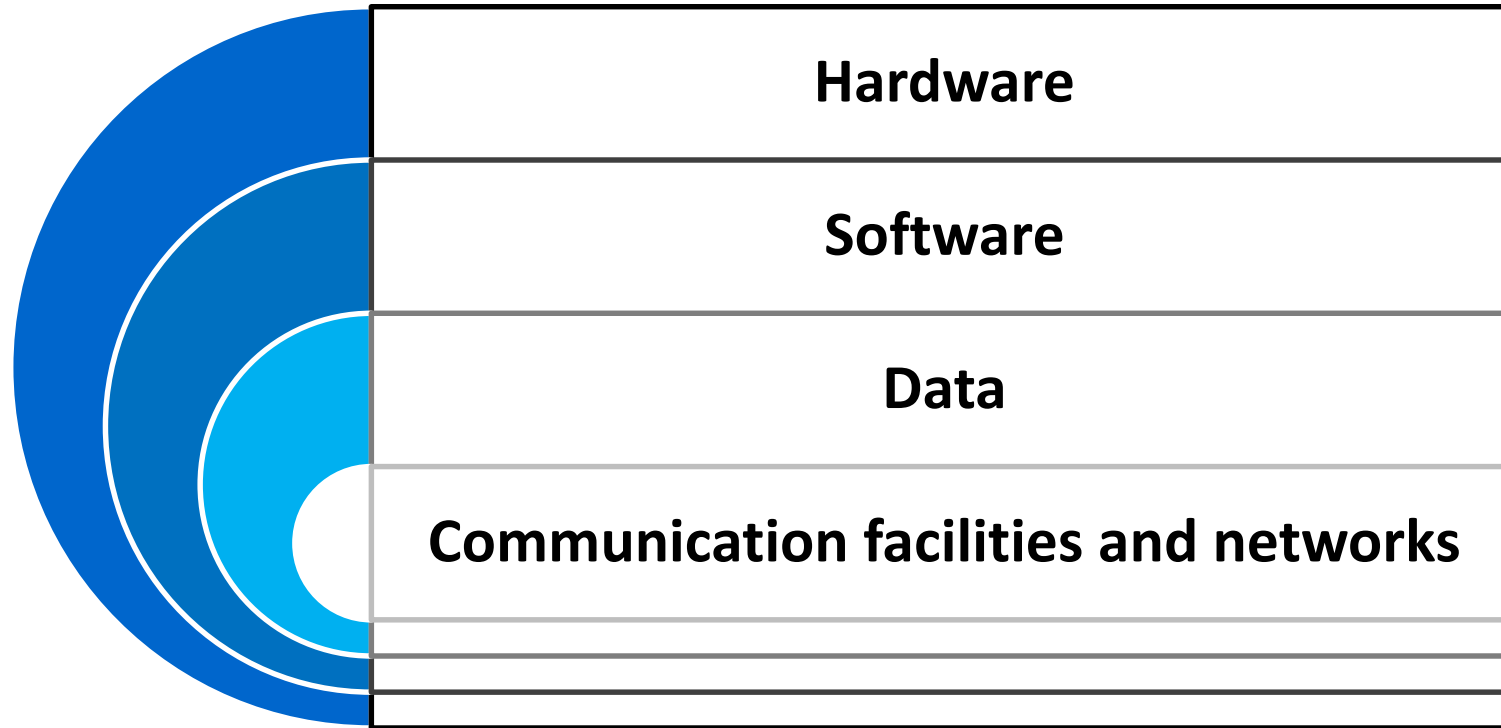
- Must decide where to deploy mechanisms
 - At what points in a network
 - At what layer of an architecture
- Involve algorithms and secret info (keys)
 - How to create, distribute, and protect secret info?
 - Relying on underlying protocols may complicate the development
- A battle of wits between attacker and admin
 - Attacker: find holes, need only find a single weakness
 - Designer: Close holes, eliminate all weaknesses

Challenges of Computer Security (Cont.)

- Users: not perceived on benefits until a security failure
- Requires constant monitoring
 - ▣ Difficult in today's short-term, overloaded environment
- Too often an after-thought (not integral)
 - ▣ Not an integral part of the design process
- Strong security is regarded as an impediment to use of system

A Model for Computer Security

- Assets of a computer system (or system resource)



A Model for Computer Security (Cont.)

- Vulnerability: weakness of system resources

- ❑ Corrupted: loss of integrity
- ❑ Leaky: loss of confidentiality
- ❑ Unavailable or very slow: loss of availability

- Threat: capable of exploiting vulnerabilities

- ❑ Potential harm to an asset

A Model for Computer Security (Cont.)

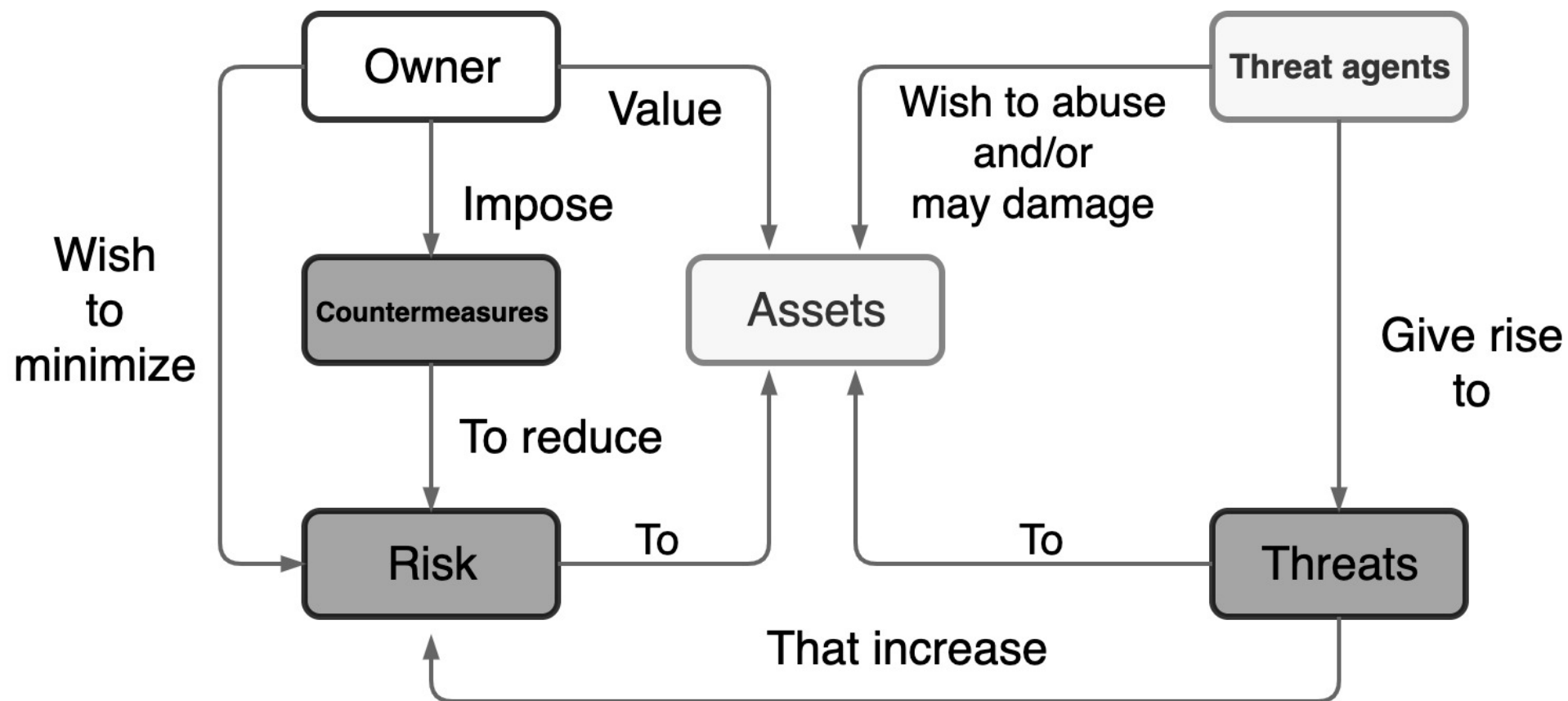
- Attack: a threat that is carried out (threat action)
 - ❑ Passive: learn or make use of info, but doesn't affect system resources
 - ❑ Active: alter system resources or affect their operation
 - ❑ Inside: by an authorized user (using authorized resources in a way not approved)
 - ❑ Outside: by an unauthorized user

A Model for Computer Security (Cont.)

● Countermeasures

- Means used to deal with security attacks
 - Prevent attacks
 - Detect them and then recover
- May itself introduce new vulnerabilities
- Residual vulnerabilities may remain
- Goal is to minimize residual level of risk to the assets
 - Residual risk: the amount of risk associated with an action/event remaining, after inherent risks have been reduced by risk controls

Security Concepts and Relationships



Threats and Attacks (RFC 4949)

Threat Consequence	Threat Action (Attack)
<u>Unauthorized Disclosure</u> - Threats to confidentiality	(1) Exposure ; (2) Interception ; (3) Inference : inferring data/info from traffic patterns or repeated queries; (4) Intrusion
<u>Deception</u> - Threats to system/data integrity	(1) Masquerade : an unauthorized user who gains access to a system by posing as an authorized user, or a Trojan horse behaves; (2) Falsification ; (3) Repudiation : falsely denying responsibility for an act

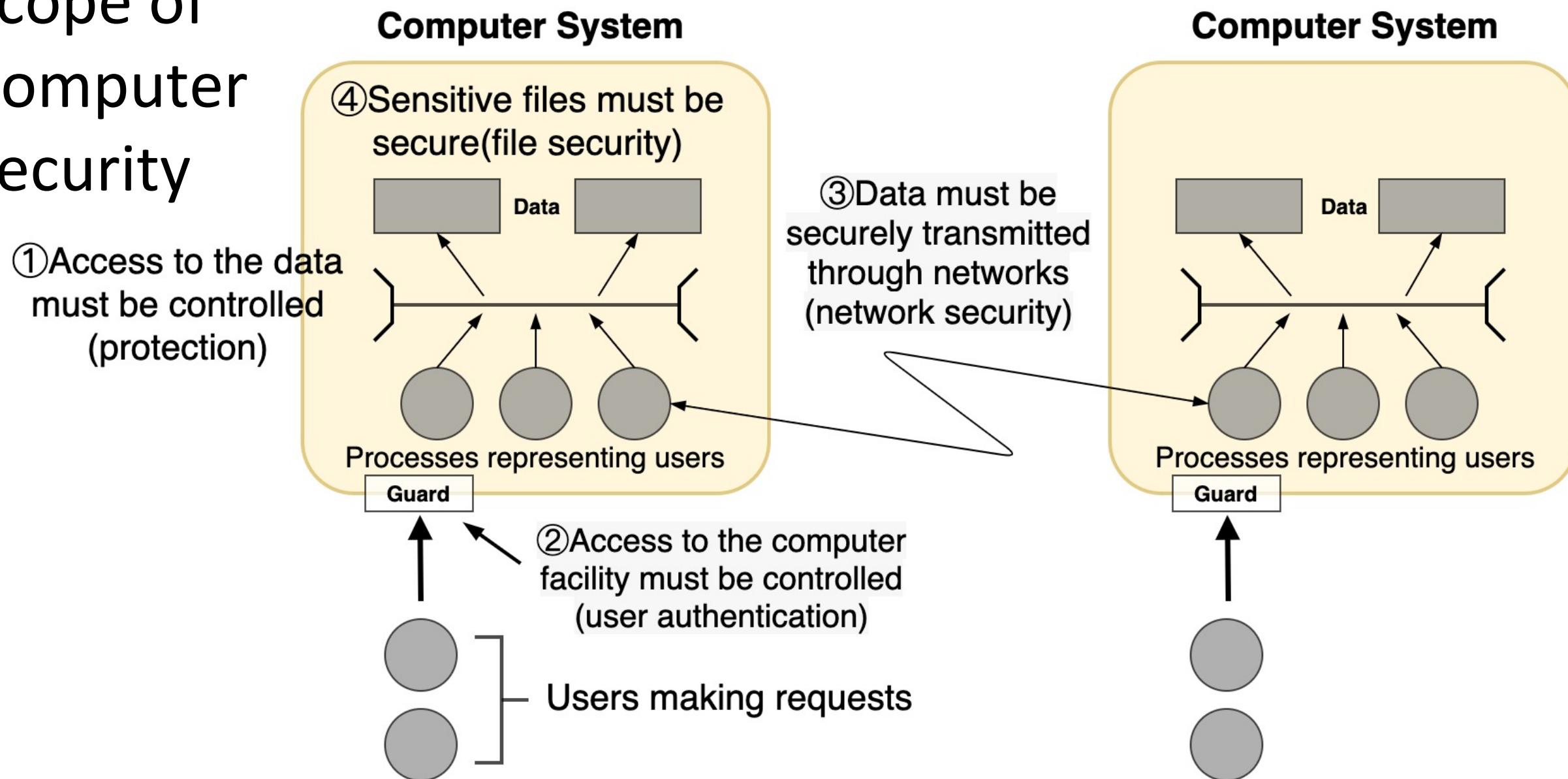
Threats and Attacks (RFC 4949)

Threat Consequence	Threat Action (Attack)
<u>Disruption</u> <ul style="list-style-type: none">- Threats to availability or system integrity	(1) Incapacitation: prevents or interrupts system operation; (2) Corruption: undesirably alters system operation; (3) Obstruction: interrupts delivery of system services
<u>Usurpation</u> <ul style="list-style-type: none">- Threats to system integrity	(1) Misappropriation: unauthorized logical or physical control of a system resource (e.g., DDoS attacks) (2) Misuse: gaining unauthorized access to a system

Threats and Assets

- Assets: hardware, software, data, and communication lines and networks
 - Threats: breaches of availability, confidentiality, and integrity
- Network security attacks
 - Passive attacks
 - Eavesdropping on, or monitoring of, transmissions
 - Goal: to obtain info that is being transmitted
 - Two types: release of message content, and traffic analysis
 - Active attacks
 - Involving some modification of the data stream or the creation of a false stream
 - Four types: replay, masquerade, modification of messages, and DoS

Scope of Computer Security



Security Functional Requirements

- One computer security expert, Bruce Schneier, observed

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

- Why?

Security Functional Requirements (FIPS 200)

- 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

Outline

- Computer Security Concept
- Threats, Attacks, and Assets
- Security Functional Requirements
- Fundamental Security Design Principles
- Attack Surfaces and Attack Trees
- Computer Security Strategy

Fundamental Security Design Principles

- Why do we need principles?

- ❑ No security design and implementation techniques that can **systematically** exclude security flaws and prevent all unauthorized actions
- ❑ But, good practices for good design have been documented

Fundamental Security Design Principles

- Economy of mechanism

- Design should be as simple and small as possible

- Fail-safe defaults

- Access decisions should be based on permission rather than exclusion

- Complete mediation

- Every access must be checked against the access control mechanism

- Open design

- Design should be open rather than secret
(e.g., widespread adoption of NIST-approved algorithms)

Fundamental Security Design Principles (Cont.)

- Separation of privilege

- Separate users and processes based on different levels of trust, needs, and privilege requirements

- Least privilege

- Every process and every user of the system should operate using the least set of privileges necessary to perform the task

- Least common mechanism

- Design should minimize the functions shared by different users for mutual security

Fundamental Security Design Principles (Cont.)

- Psychological acceptability

- ❑ Should not interfere unduly with the work of users or hinder the usability or accessibility of resources

- Isolation

- ❑ Resources at public access systems
 - ❑ Processes and files of individual users
 - ❑ Security mechanisms

- Encapsulation

- ❑ A specific form of isolation based on object-oriented functionality

Fundamental Security Design Principles (Cont.)

- Modularity

- Development of security functions as separate, protected modules
- Use of a modular architecture for mechanism design and implementation

- Layering

- Use of multiple, overlapping protection approaches

- Least astonishment

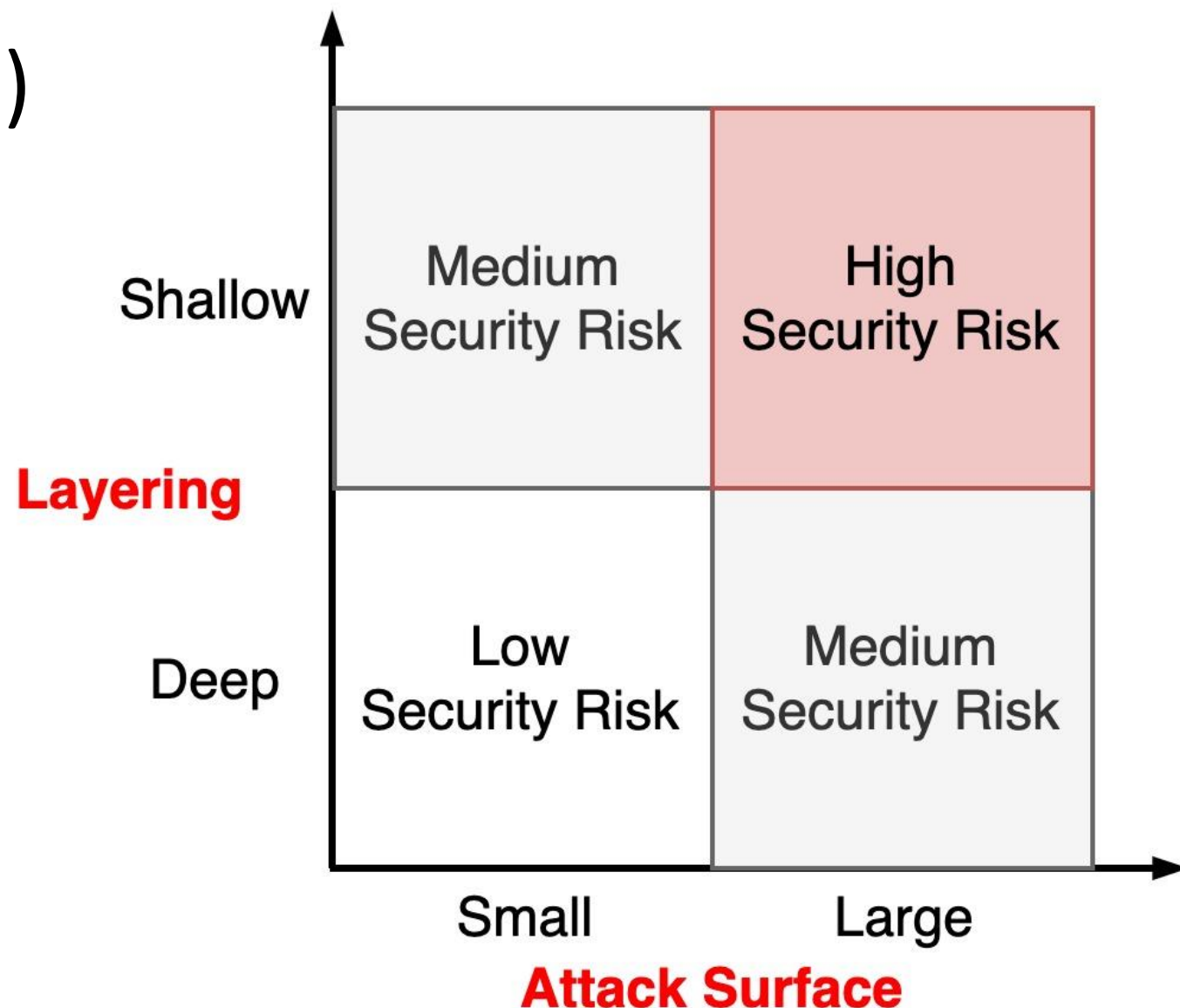
- A program or user interface should always respond in the way that is least likely to astonish the user

Attack Surfaces

- Consist of the reachable and exploitable vulnerabilities in a system
 - Network attack surface
 - Network protocol vulnerabilities
 - e.g., open ports on outward facing Web and other servers
 - Software attack surface
 - Vulnerabilities in application, utility, or operating system code
 - e.g., interfaces, SQL, and web forms
 - Human attack surface
 - Vulnerabilities created by personnel
 - e.g., an employee with access to sensitive info vulnerable to a social engineering attack

Attack Surfaces (Cont.)

- Why is an attack surface analysis useful?
 - Assess the scale and severity of threats to a system
 - Make developers aware of where security mechanisms are required

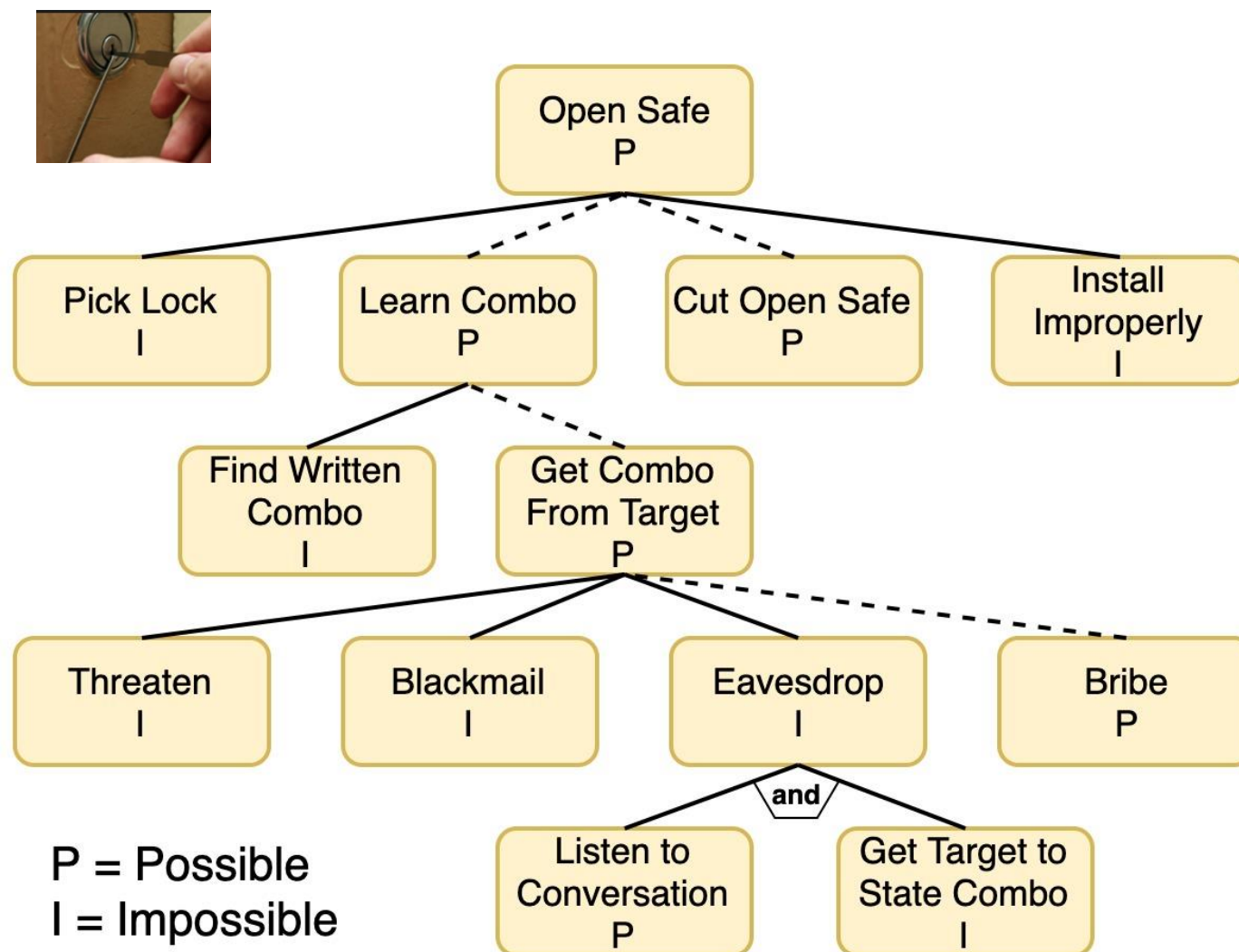


Attack Trees

- A branching, hierarchical data structure: a set of potential techniques for exploiting security vulnerabilities

- ❑ Root: the attack goal
- ❑ Leaf: different ways to initiate an attack
- ❑ Each node (other than a leaf) is either an AND-node or an OR-node

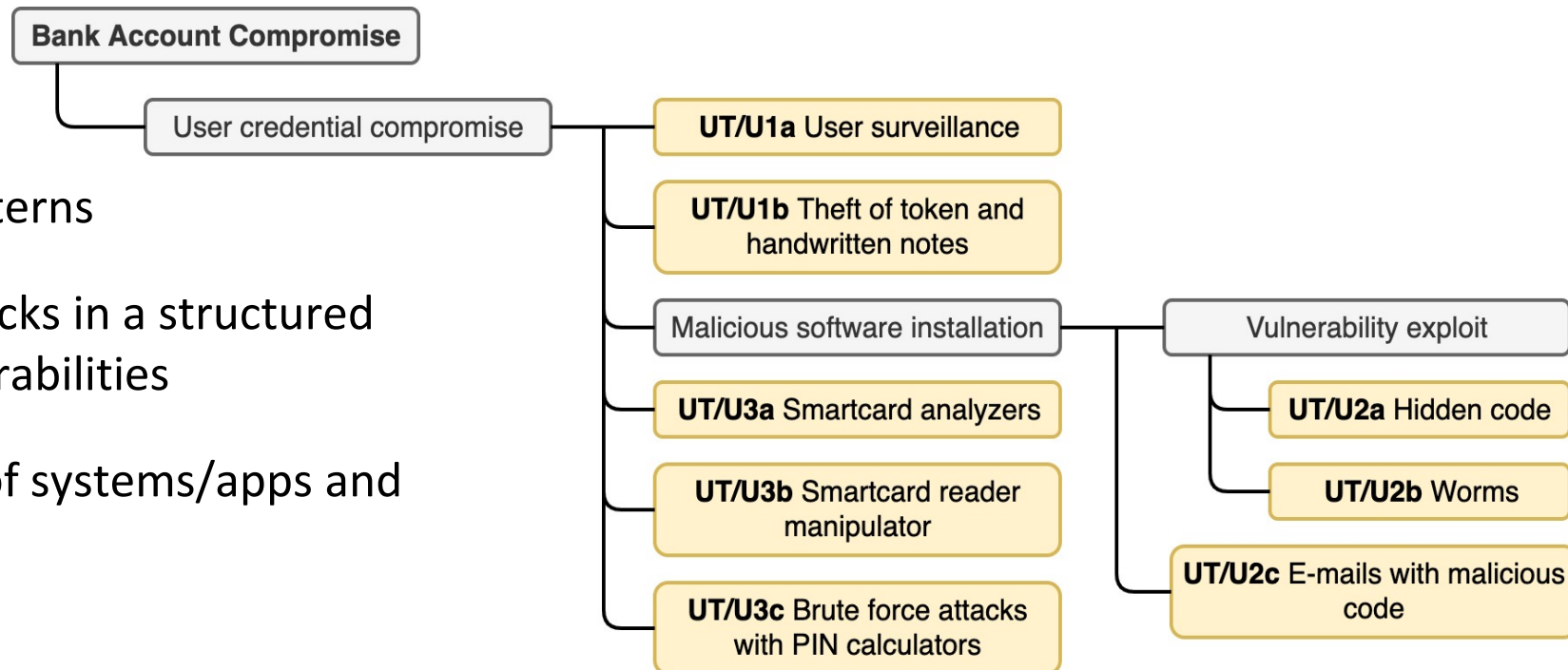
- Why are attack trees needed?



Attack Trees (Cont.)

● Using attack trees

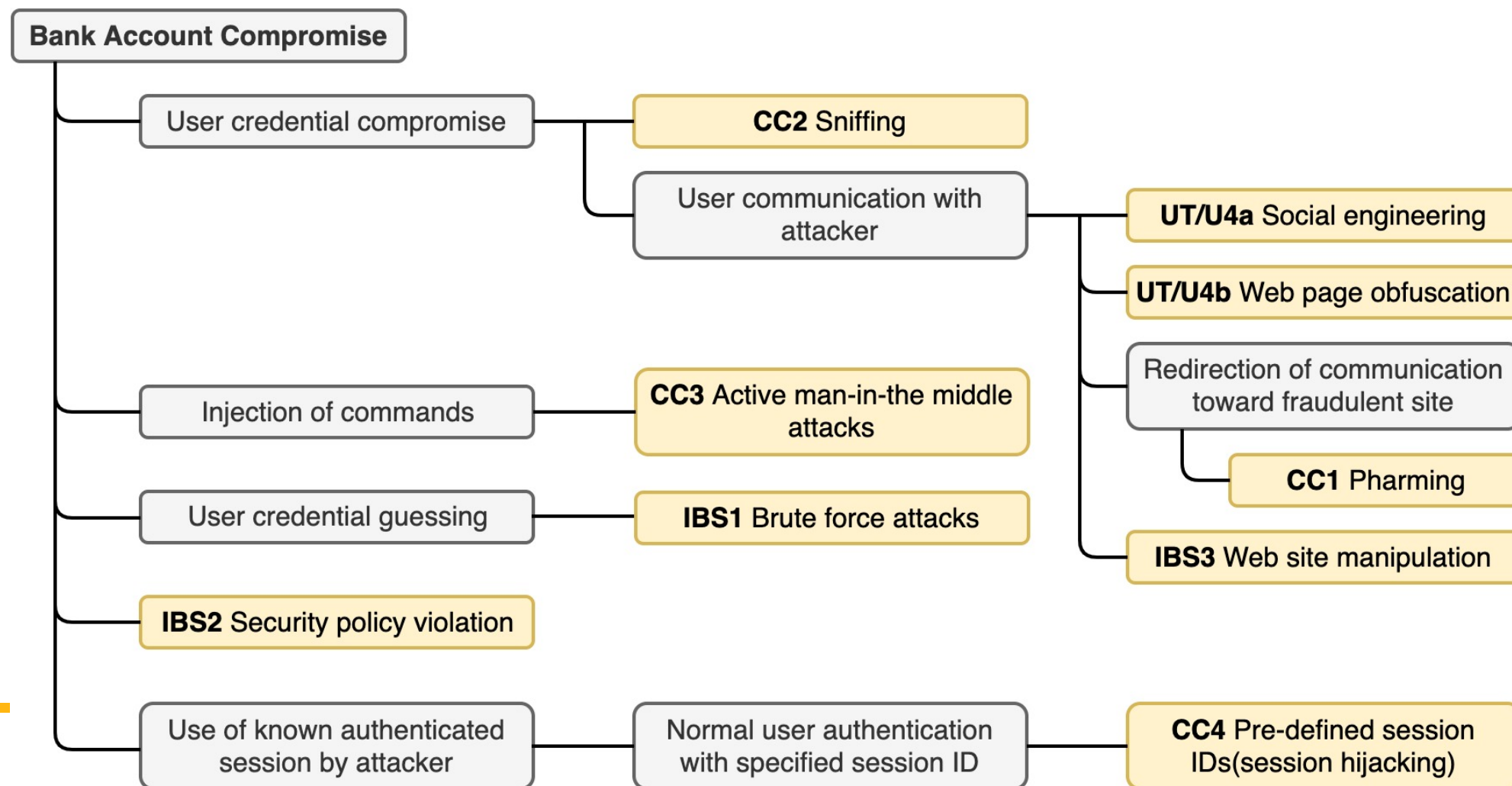
- ❑ To effectively exploit the info available on attack patterns
- ❑ To document security attacks in a structured form that reveals key vulnerabilities
- ❑ To guide both the design of systems/apps and countermeasures



An Internet banking authentication app

UT/U: User terminal and user
CC: Communications channel
IBS: Internet banking server

Attack Trees (Cont.)



Computer Security Strategy

- Involves three aspects

- ❑ Specification/policy: What is the security scheme supposed to do?
- ❑ Implementation/mechanisms: How does it do it?
- ❑ Correctness/assurance: Does it really work?

Security Policy

- A formal statement of rules and practices
 - that specify (or regulate) how a system (or organization) provides security services to protect critical system resources (RFC 4949)
- A security manager needs to consider:
 - The value of the assets being protected (e.g., critical files)
 - The vulnerabilities of the system (e.g., the system is open to guests)
 - Potential threats and the likelihood of attacks (e.g., data leakage)
 - Trade-off: ease of use vs. security (e.g., remember and type two passwords?)
 - Trade-off: cost of security vs. cost of failure and recovery

Security policy: a business decision, possibly influenced by legal requirements

Security Implementation and Assurance

- Security implementation
 - Prevention, detection, response, recovery
- Assurance: provides grounds for having confidence that the system operates such that the system's security policy is enforced
 - expressed as a degree of confidence
 - based on formal models
- Evaluation: examines a computer product or system w.r.t. certain criteria

Questions?