COMPUTER SECURITY: PRINCIPLES AND PRACTICE

WILLIAM STALLINGS AND LAWRIE BROWN

Institute of Information Technology
Noakhali Science & Technology University

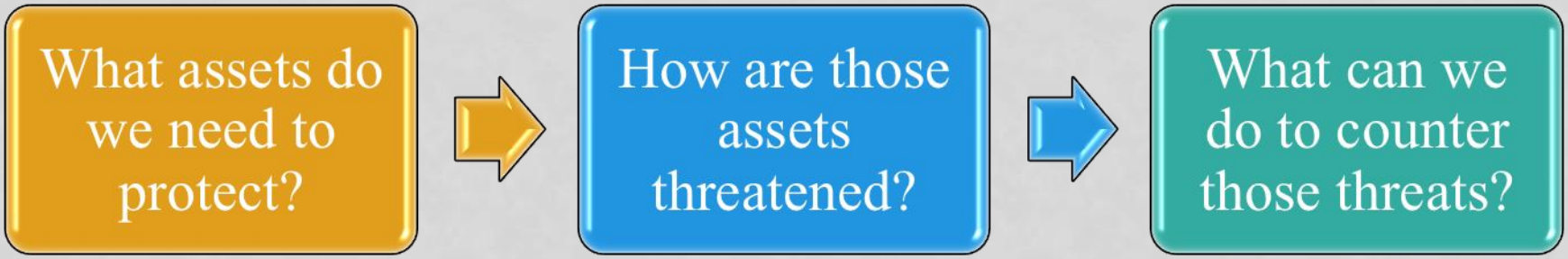
LEARNING OBJECTIVES

- Describe the key security requirements of confidentiality, integrity, and availability
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets
- Summarize the functional requirements for computer security
- Explain the fundamental security design principles
- Discuss the use of attack surfaces and attack trees
- Understand the principle aspects of a comprehensive security strategy

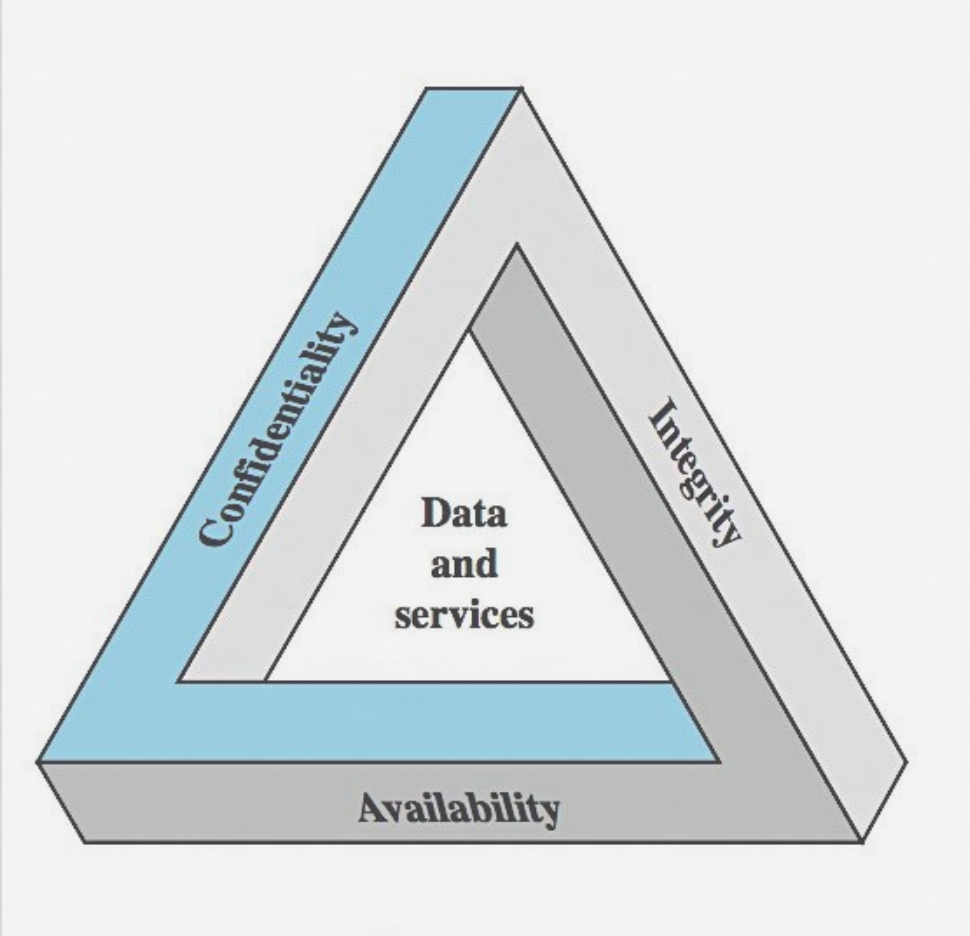
OVERVIEW

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).

3 FUNDAMENTAL QUESTIONS



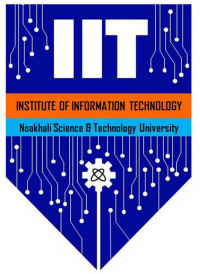
KEY SECURITY CONCEPTS



COMPUTER SECURITY CONCEPTS

- **Confidentiality:** This term covers two related concepts:
  - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals
  - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed
- **Integrity:** This term covers two related concepts:
  - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner
  - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- **Availability:** Assures that systems work promptly and service is not denied to authorized users

ADDITION TO CIA



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.

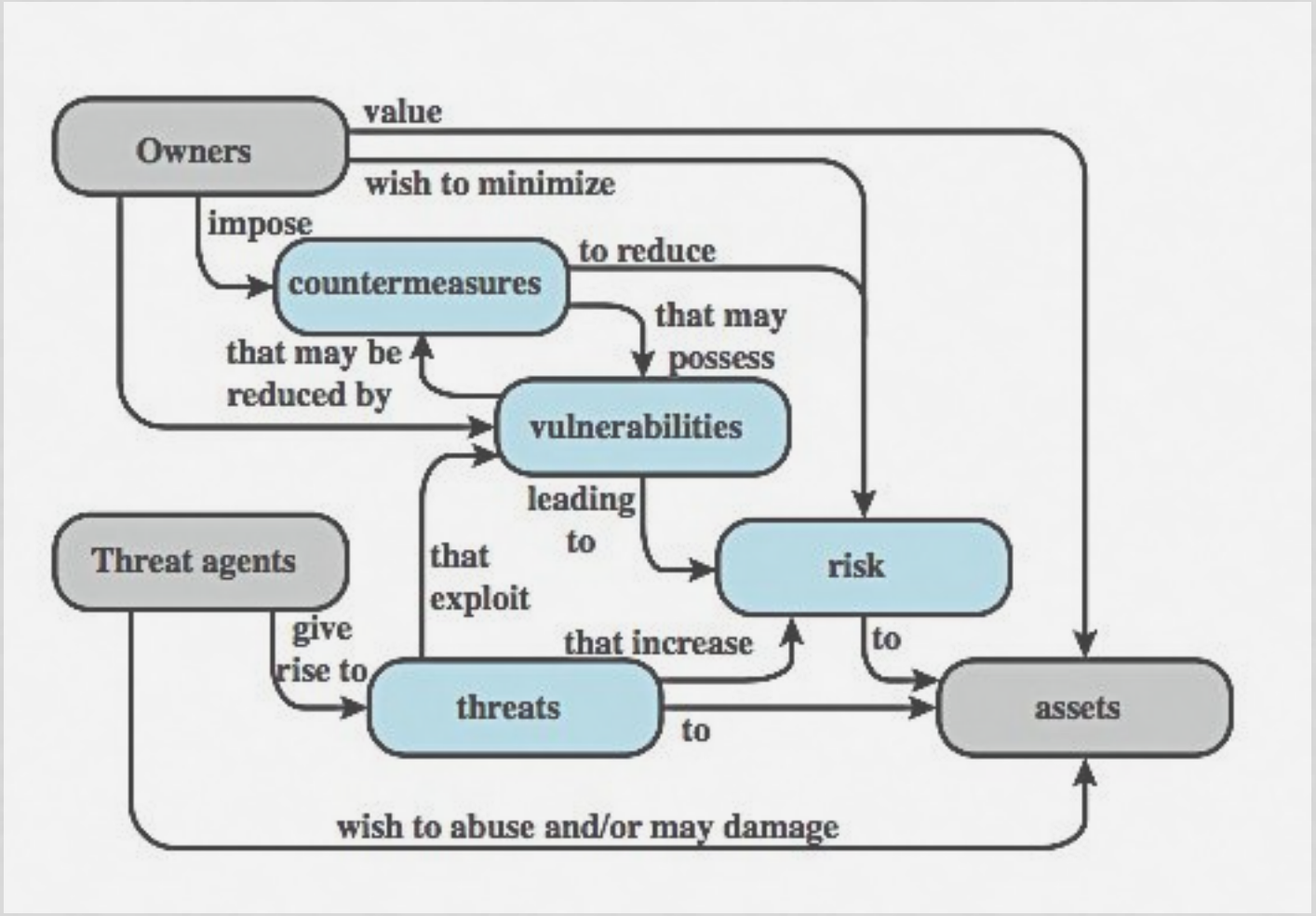
Accountability

- 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, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, 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.

COMPUTER SECURITY 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

SECURITY CONCEPTS AND RELATIONSHIPS



VULNERABILITIES AND ATTACKS

- system resource 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

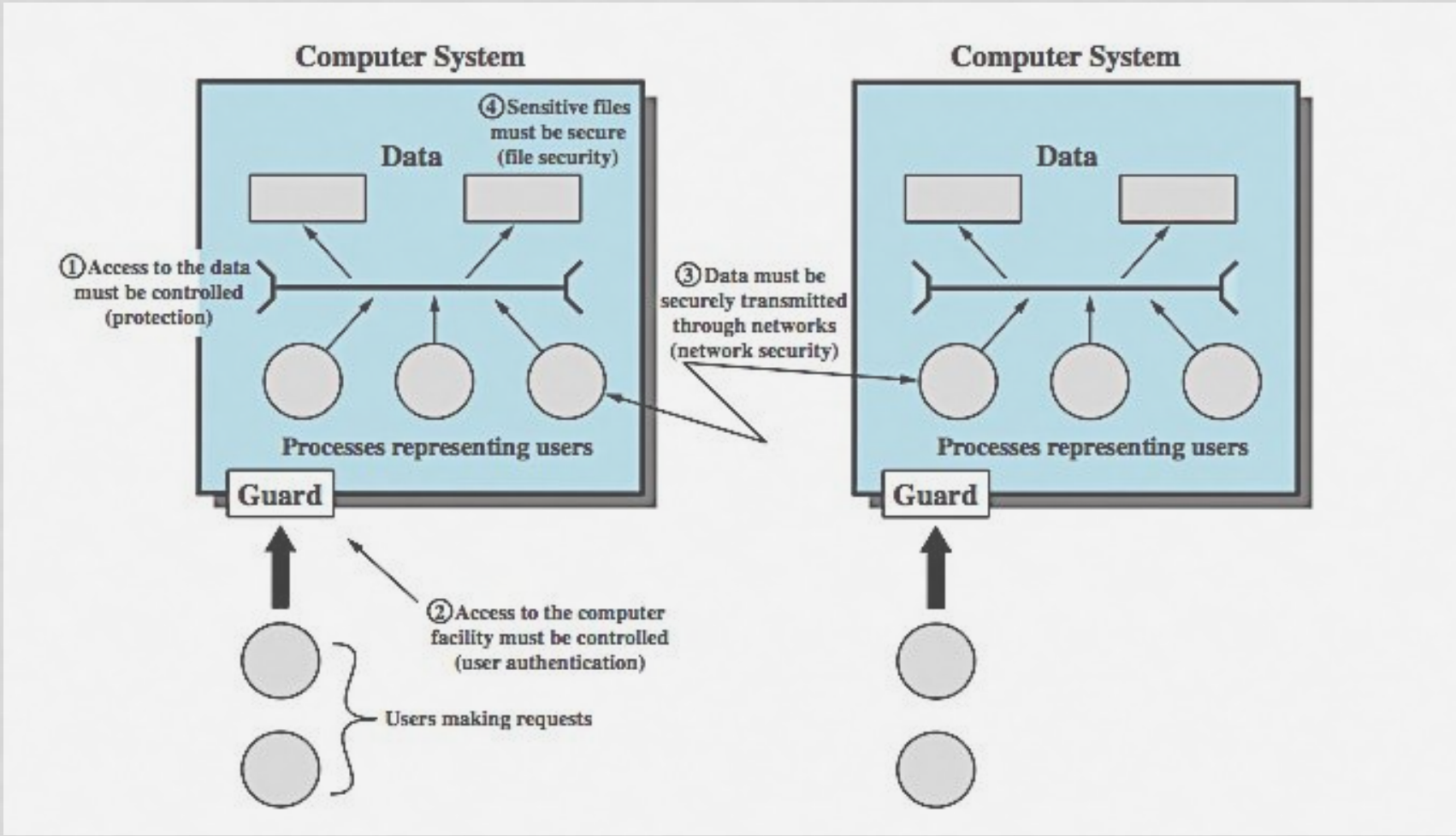
THREAT CONSEQUENCES

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

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

SCOPE OF COMPUTER SECURITY



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.

SECURITY FUNCTIONAL REQUIREMENTS

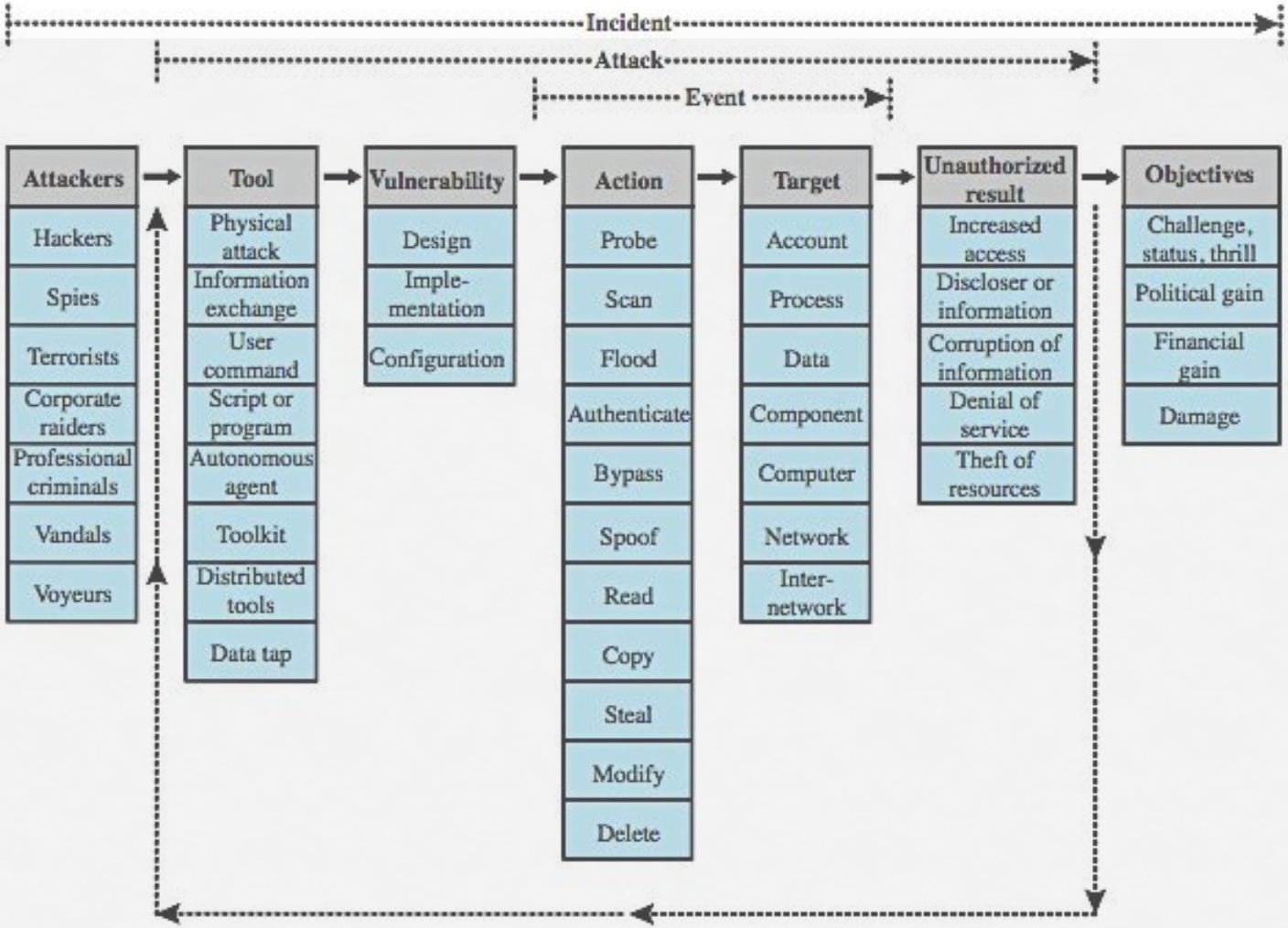
- Technical Measures:
  - access control; identification & authentication; system & communication protection; system & information integrity
- Management Controls and Procedures:
  - awareness & training; audit & accountability; certification, accreditation & security assessments; contingency planning; maintenance; physical & environmental protection; planning; personnel security; risk assessment; systems & services acquisition
- Overlapping Technical and Management:
  - configuration management; incident response; media protection

SECURITY DESIGN PRINCIPLES

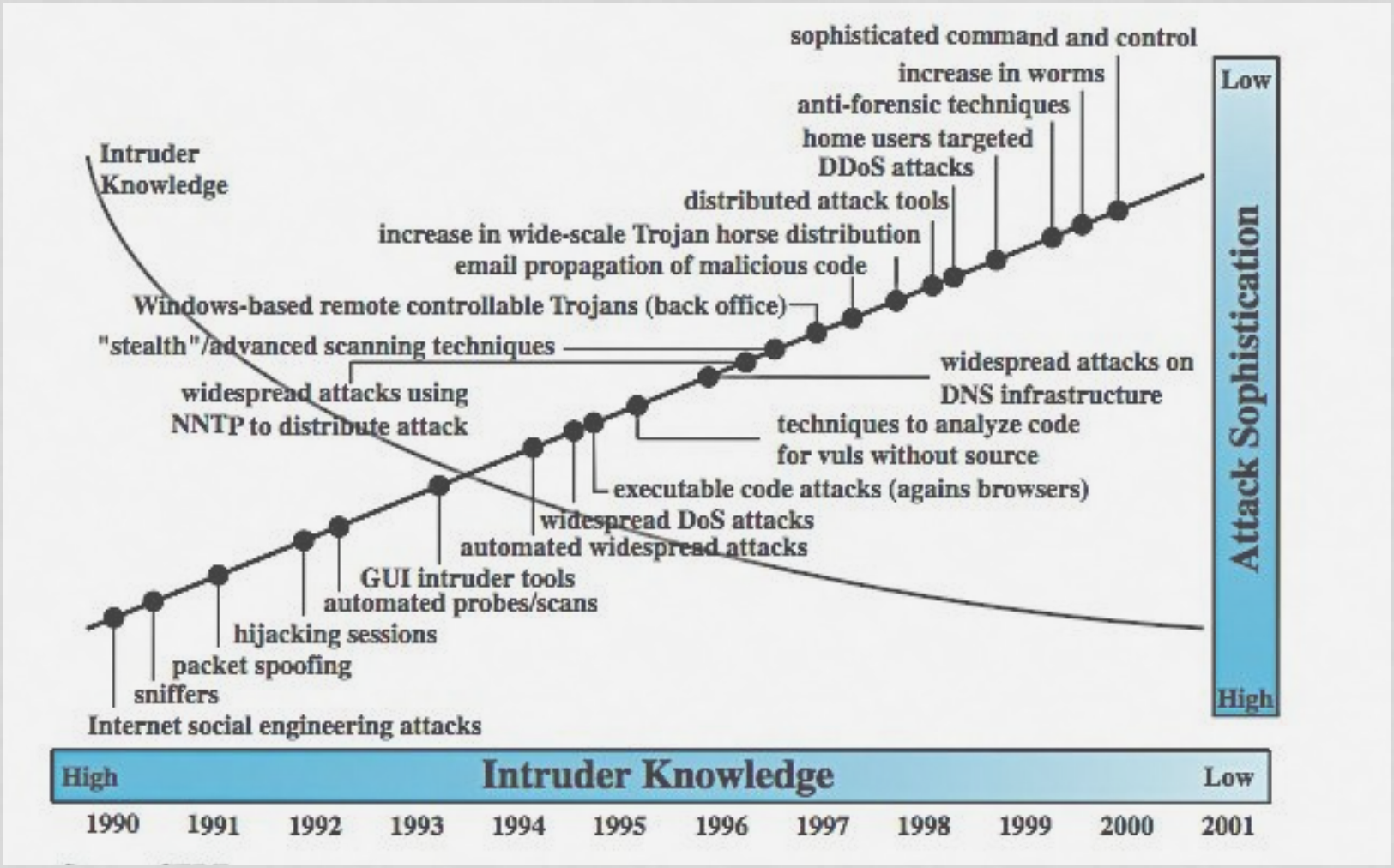
The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security, list the following as fundamental security design principles:

- 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

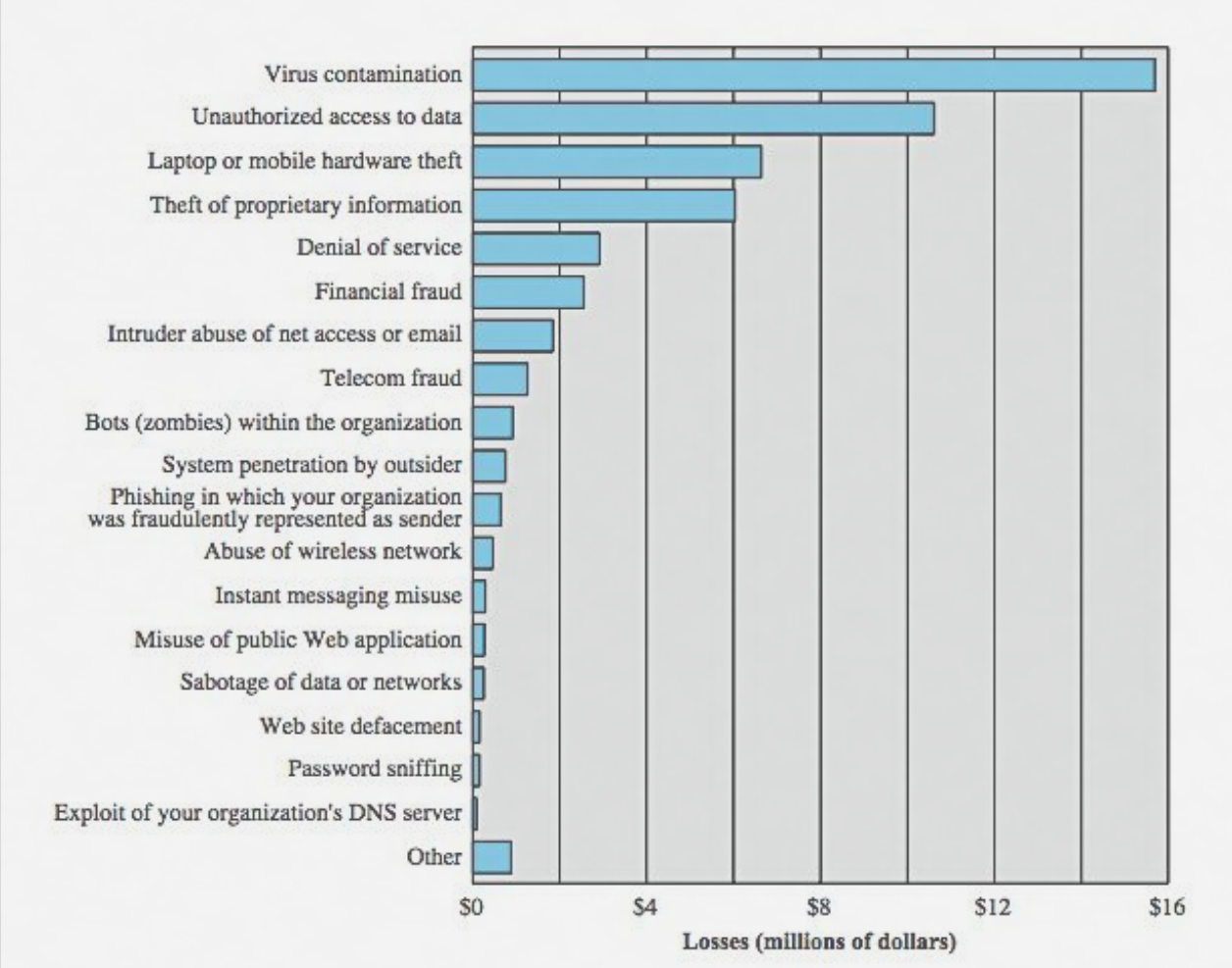
SECURITY TAXONOMY



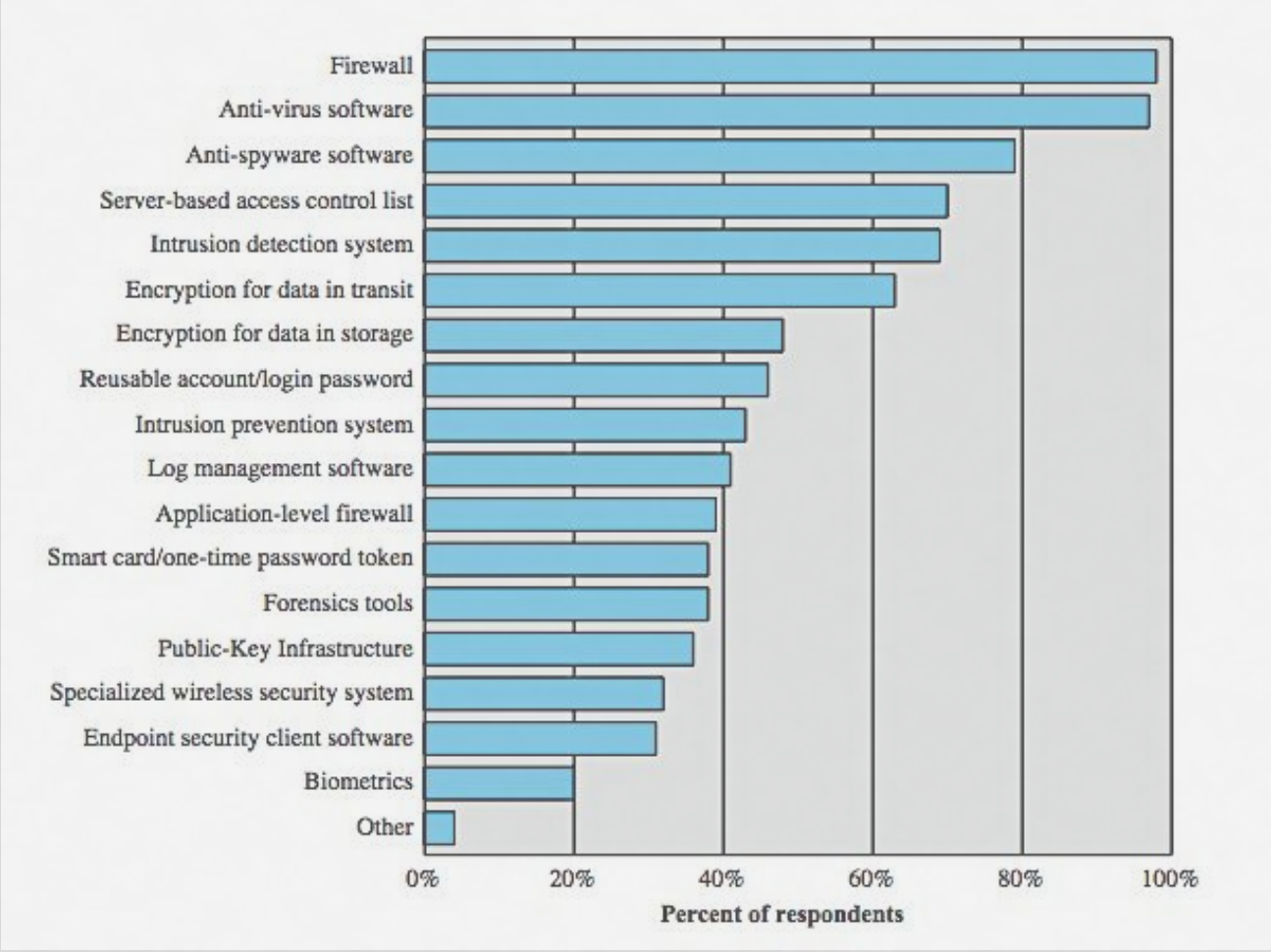
SECURITY TRENDS



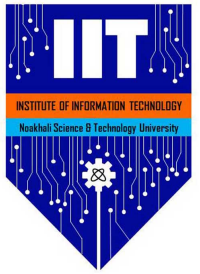
COMPUTER SECURITY LOSSES



SECURITY TECHNOLOGIES USED



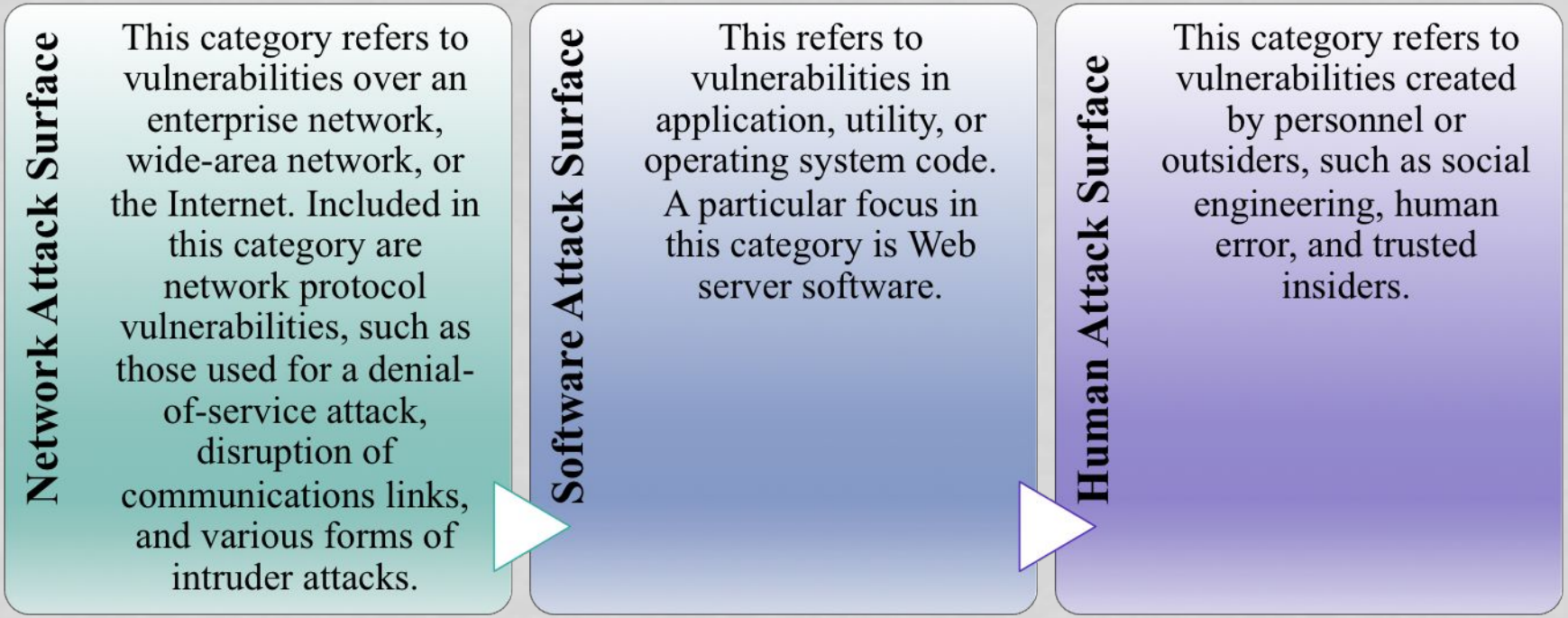
ATTACK SURFACES



An attack surface consists of the reachable and exploitable vulnerabilities in a system. Examples of attack surfaces are the following:

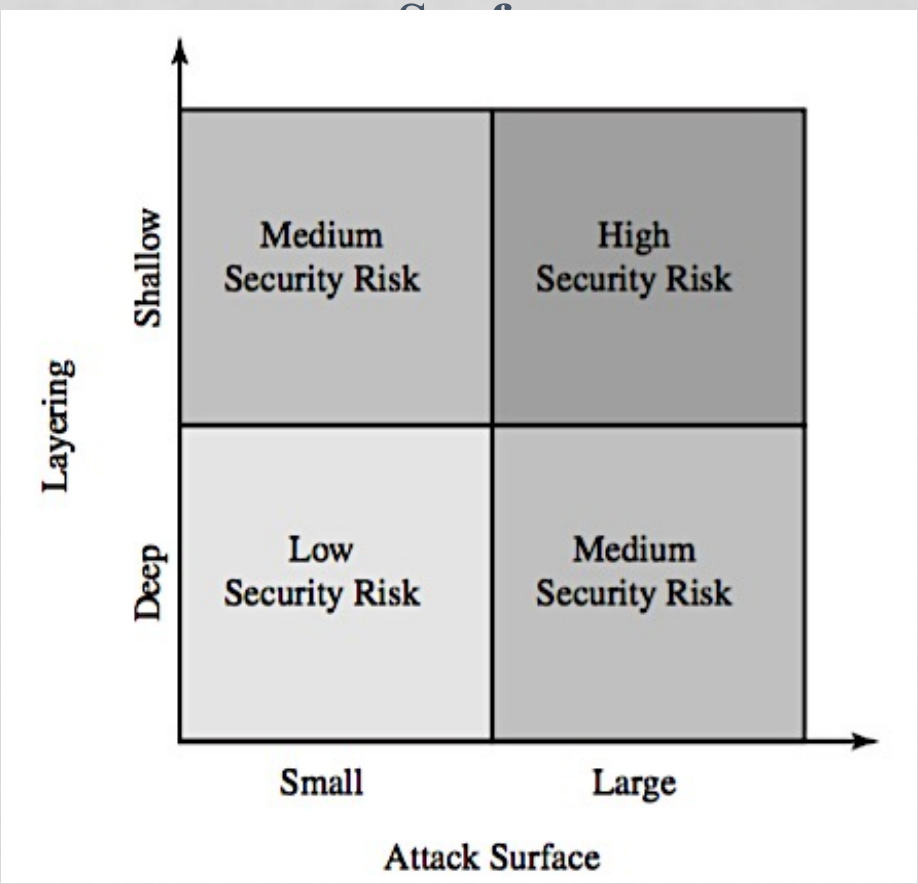
- Open ports on outward facing Web and other servers, and code listening on those ports
- Services available on the inside of a firewall
- Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and Web forms
- An employee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

ATTACK SURFACES CATEGORY



ATTACK TREES

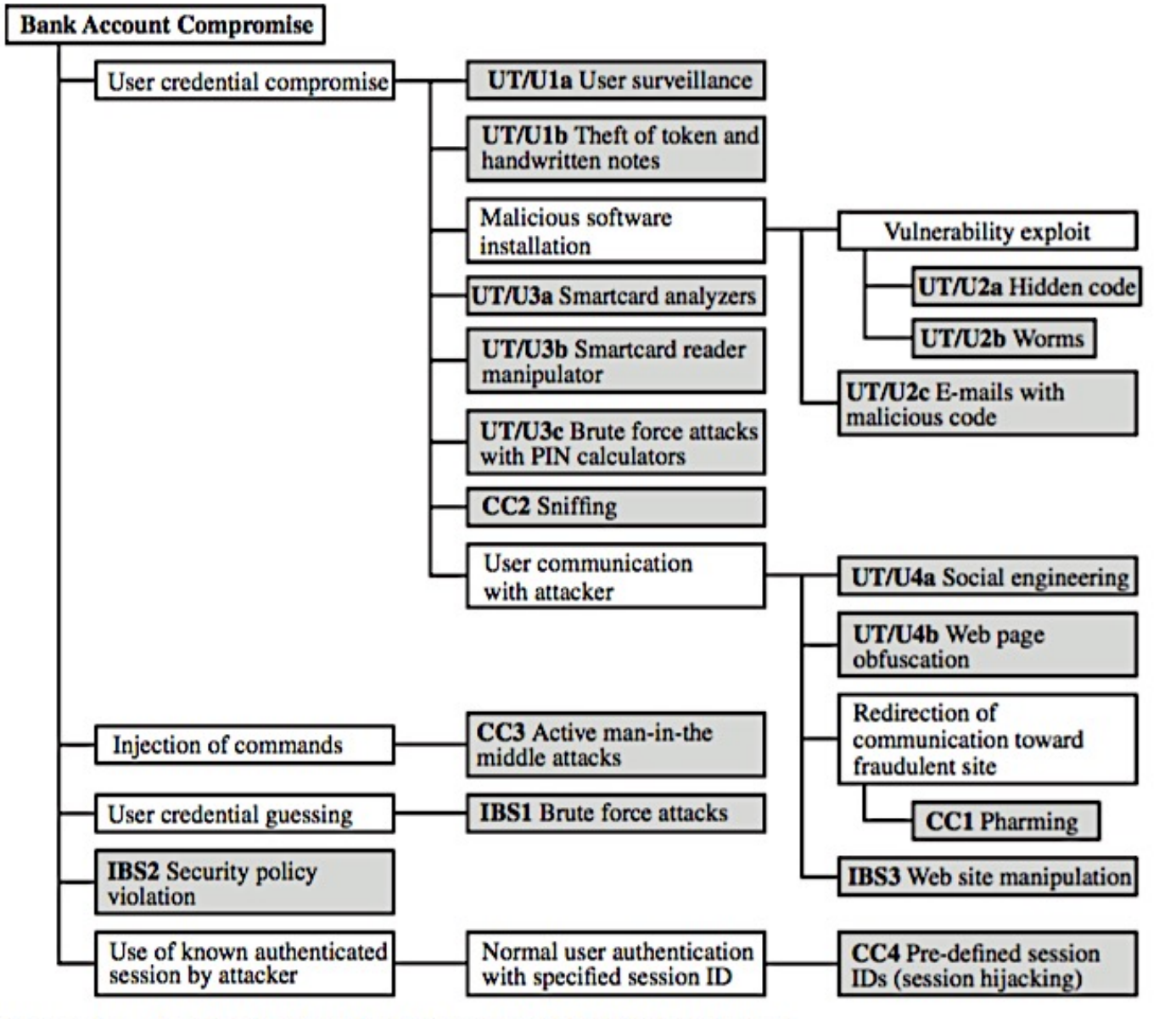
Defense in Depth and Attack



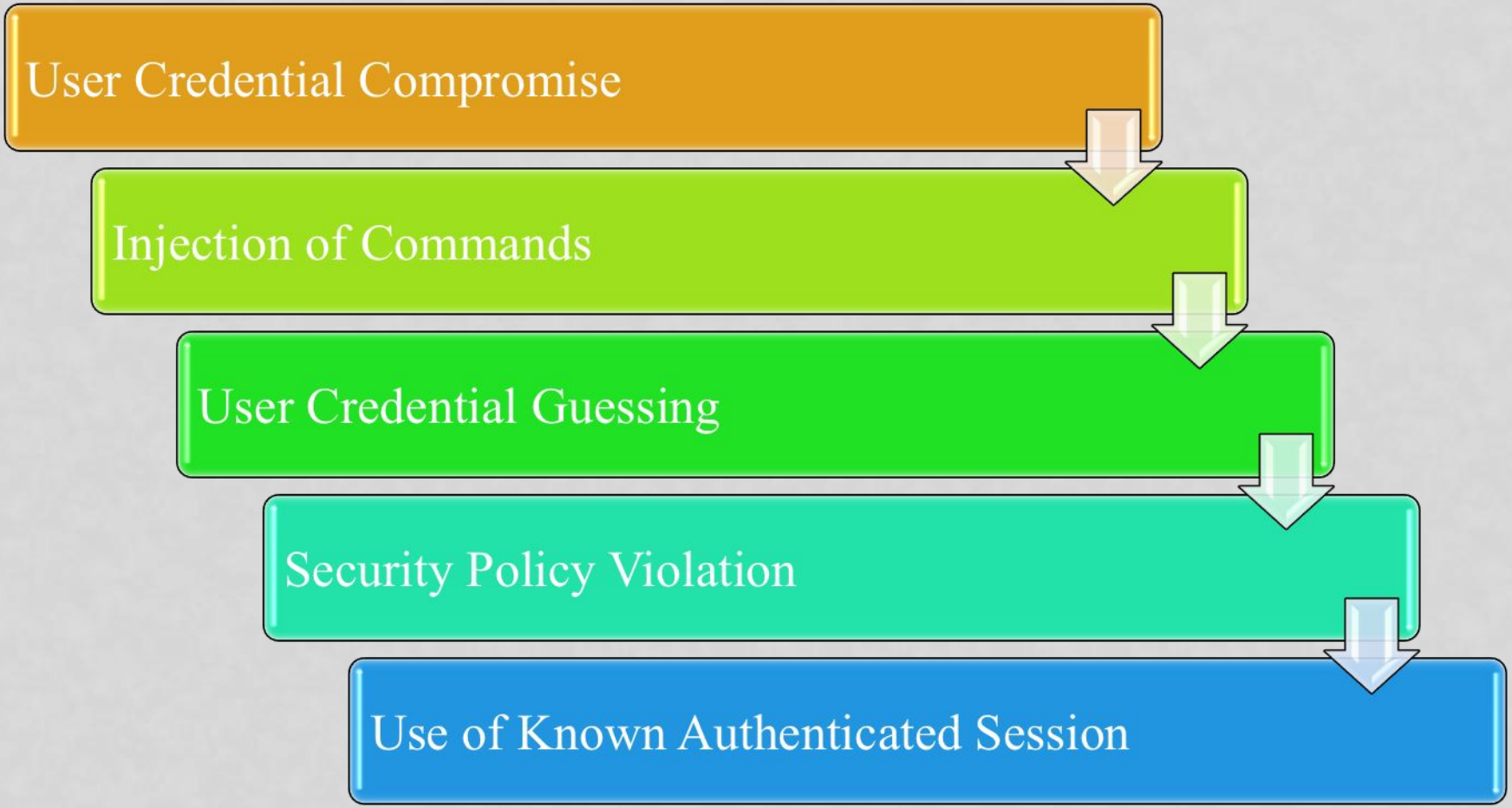
Attack Tree Generation

- **User Terminal and User (UT/U):** These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user.
- **Communications Channel (CC):** This type of attack focuses on communication links.
- **Internet Banking Server (IBS):** These types of attacks are offline attack against the servers that host the Internet banking application.

AN ATTACK TREE FOR INTERNET BANKING AUTHENTICATION



ATTACK STRATEGIES



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

SUMMARY

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