

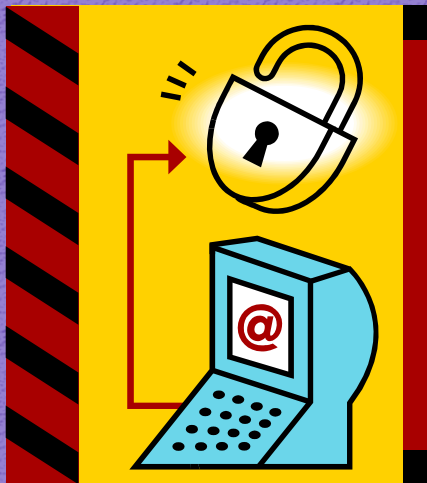
# Computer Networking and Security

Instructor: Dr. Hao Wu

Week 10 Security Basics

# The field of network and Internet security consists of:

---



- measures to deter, prevent, detect, and correct security violations that involve the transmission of information

# Computer Security

---

The NIST *Computer Security Handbook* defines the term computer security as:

“the 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)

# Computer Security Objectives

## • Confidentiality

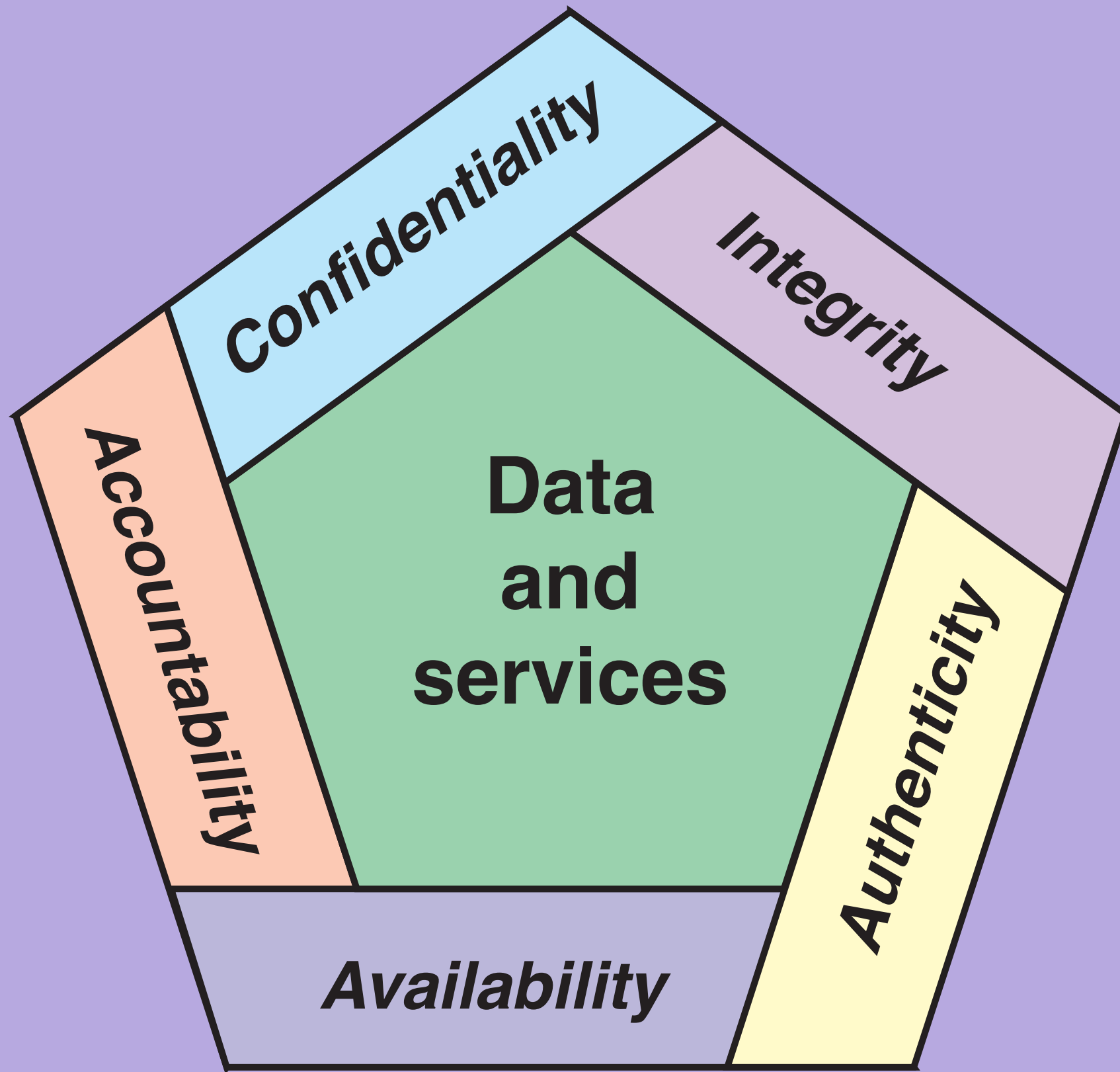
- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

## • Integrity

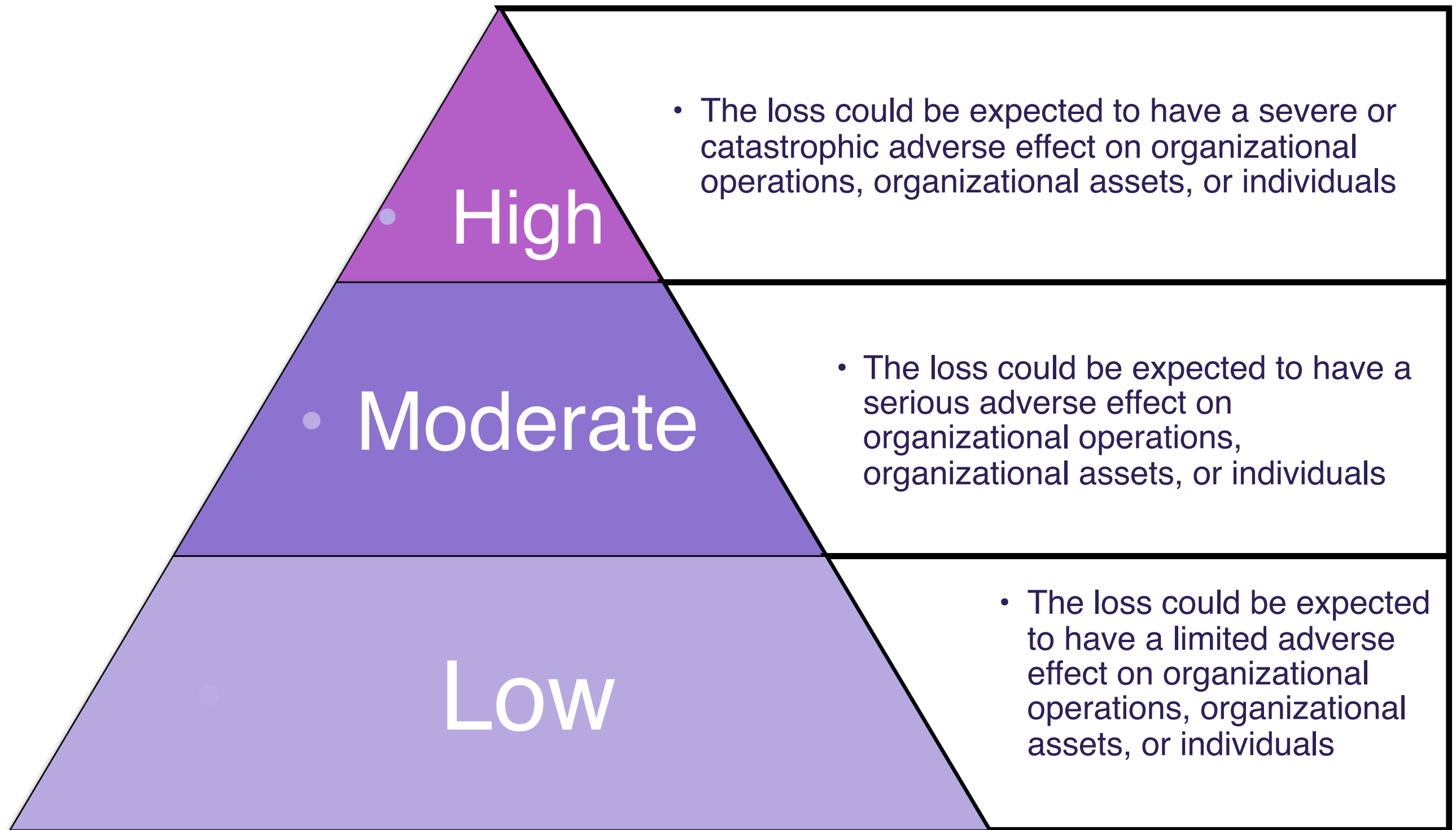
- Data integrity
  - Assures that information and programs are changed only in a specified and authorized manner
- System integrity
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

## • Availability

- Assures that systems work promptly and service is not denied to authorized users



# Breach of Security Levels of Impact



# Computer Security Challenges

---

1. Security is not simple
2. Potential attacks on the security features need to be considered
3. Procedures used to provide particular services are often counter-intuitive
4. It is necessary to decide where to use the various security mechanisms
5. Security mechanisms typically involve more than a particular algorithm or protocol
6. Security is essentially a battle of wits between a perpetrator and the designer
7. Little benefit from security investment is perceived until a security failure occurs
8. Requires constant monitoring
9. Is too often an afterthought
10. Strong security is often viewed as an impediment to efficient and user-friendly operation

# OSI Security Architecture

---

- Security attack
  - Any action that compromises the security of information owned by an organization
- Security mechanism
  - A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack
- Security service
  - A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization
  - Intended to counter security attacks, and they make use of one or more security mechanisms to provide the service



# Table 1.1 Threats and Attacks (RFC 4949)

---



## 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.

## 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.

# Security Attacks

- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation

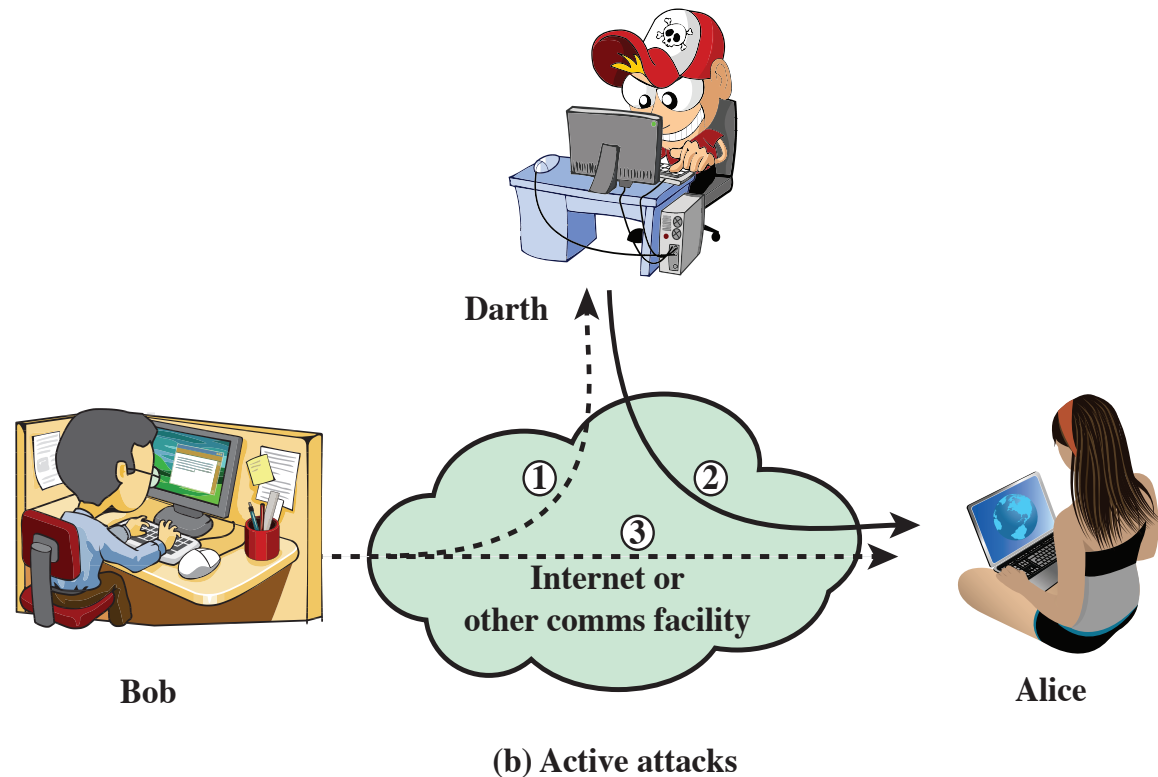
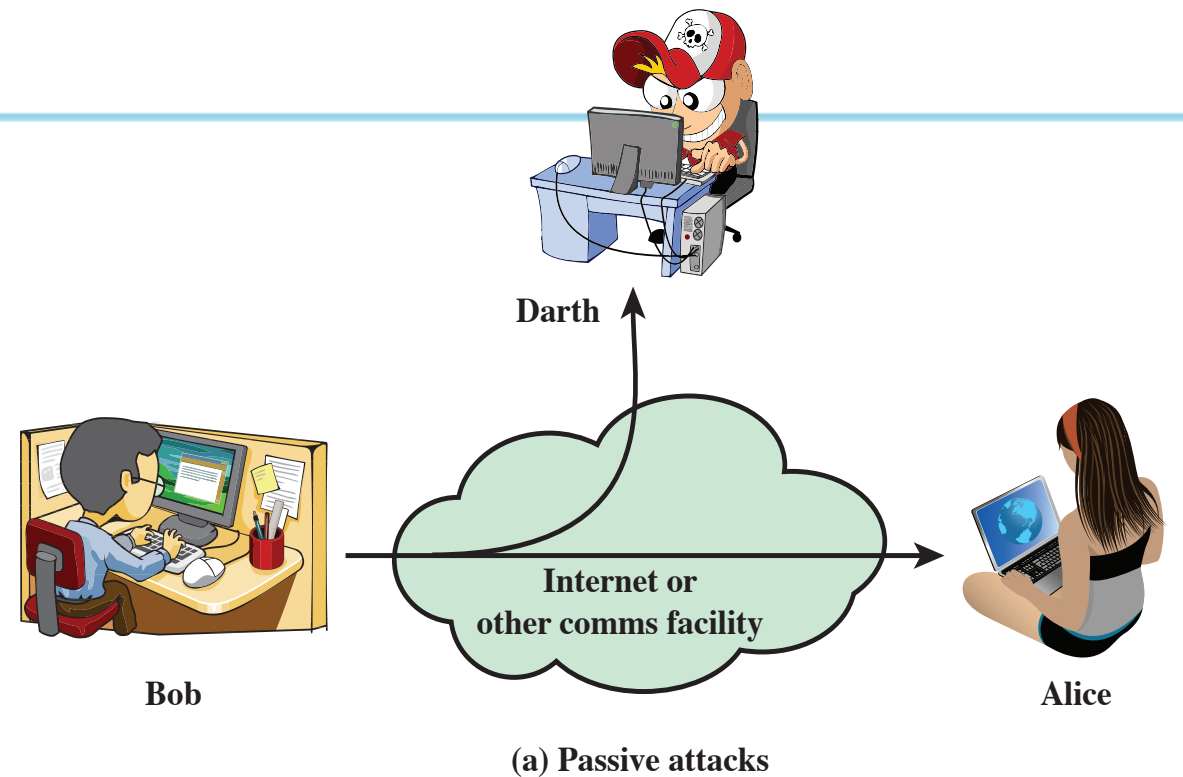


Figure 1.2 Security Attacks

# Passive Attacks

---

- Two types of passive attacks are:
  - The release of message contents
  - Traffic analysis



# Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them



## Masquerade

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms

## Replay

- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

## Modification of messages

- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized

## Denial of service

- Prevents or inhibits the normal use or management of communications facilities

# Security Services

---

- Defined by X.800 as:
  - A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers
- Defined by RFC 4949 as:
  - A processing or communication service provided by a system to give a specific kind of protection to system resources

# Security Services (X.800)

---

- **Authentication:** The assurance that the communicating entity is the one that is claims to be.
  - **Peer Entity Authentication:** Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - **Data-Origin Authentication:** In a connectionless transfer, provides assurance that the source of received data is as claimed.
- **Access control:** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).
  - **Connection Confidentiality:** The protection of all user data on a connection.
  - **Connectionless Confidentiality:** The protection of all user data in a single data block.
  - **Selective-Field Confidentiality:** The confidentiality of selected fields within the user data on a connection or in a single data block.
  - **Traffic-Flow Confidentiality:** The protection of the information that might be derived from observation of traffic flows.



# Security Services (X.800) (Cont.)

---

- **Data integrity:** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - **Connection Integrity with Recovery:** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.
  - **Connection Integrity without Recovery:** As above, but provides only detection without recovery.
  - **Selective-Field Connection Integrity:** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.
  - **Connectionless Integrity:** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
  - **Selective Field Connectionless Integrity:** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.
- **Nonrepudiation:** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
  - **Nonrepudiation, Origin:** Proof that the message was sent by the specified party.
  - **Nonrepudiation, Destination:** Proof that the message was received by the specified party.

# Authentication

---

- Concerned with assuring that a communication is authentic
  - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
  - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication



# Access Control

---

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual



# Data Confidentiality

---

- The protection of transmitted data from passive attacks
  - Broadest service protects all user data transmitted between two users over a period of time
  - Narrower forms of service includes the protection of a single message or even specific fields within a message
- The protection of traffic flow from analysis
  - This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

# Data Integrity

---

Can apply to a stream of messages, a single message, or selected fields within a message

Connection-oriented integrity service, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, generally provides protection against message modification only

# Nonrepudiation

---

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message



# Availability Service

---

- Protects a system to ensure its availability
- This service addresses the security concerns raised by denial-of-service attacks
- It depends on proper management and control of system resources and thus depends on access control service and other security services

# Security Mechanisms (X.800)

---

## Specific Security Mechanisms

- Encipherment
- Digital signatures
- Access controls
- Data integrity
- Authentication exchange
- Traffic padding
- Routing control
- Notarization

## Pervasive Security Mechanisms

- Trusted functionality
- Security labels
- Event detection
- Security audit trails
- Security recovery

# 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

# Fundamental Security Design Principles

---

- **Economy of mechanism**

- Means that the design of security measures embodied in both hardware and software should be as simple and small as possible
- Relatively simple, small design is easier to test and verify thoroughly
- With a complex design, there are many more opportunities for an adversary to discover subtle weaknesses to exploit that may be difficult to spot ahead of time



# Fundamental Security Design Principles

---

- **Fail-safe defaults**

- Means that access decisions should be based on permission rather than exclusion
- The default situation is lack of access, and the protection scheme identifies conditions under which access is permitted
- Most file access systems and virtually all protected services on client/server use fail-safe defaults

# Fundamental Security Design Principles

---

- **Complete mediation**

- Means that every access must be checked against the access control mechanism
- Systems should not rely on access decisions retrieved from a cache
- To fully implement this, every time a user reads a field or record in a file, or a data item in a database, the system must exercise access control
- This resource-intensive approach is rarely used

# Fundamental Security Design Principles

---

- **Open Design**

- Means that the design of a security mechanism should be open rather than secret
- Although encryption keys must be secret, encryption algorithms should be open to public scrutiny
- Is the philosophy behind the NIST program of standardizing encryption and hash algorithms

# Fundamental Security Design Principles

---

- **Separation of privilege**

- Defined as a practice in which multiple privilege attributes are required to achieve access to a restricted resource
- Multifactor user authentication is an example which requires the use of multiple techniques, such as a password and a smart card, to authorize a user

# Fundamental Security Design Principles

---

- **Least of privilege**

- Means that every process and every user of the system should operate using the least set of privileges necessary to perform the task
- An example of the use of this principle is role-based access control; the system security policy can identify and define the various roles of users or processes and each role is assigned only those permissions needed to perform its functions

# Fundamental Security Design Principles

---

- **Least common mechanism**
  - Means that the design should minimize the functions shared by different users, providing mutual security
  - This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications

# Fundamental Security Design Principles

---

- **Psychological acceptability**

- Implies that the security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access
- Where possible, security mechanisms should be transparent to the users of the system or, at most, introduce minimal obstruction
- In addition to not being intrusive or burdensome, security procedures must reflect the user's mental model of protection

# Fundamental Security Design Principles

---

- **Isolation**

- Applies in three contexts:
  - Public access systems should be isolated from critical resources to prevent disclosure or tampering
  - Processes and files of individual users should be isolated from one another except where it is explicitly desired
  - Security mechanisms should be isolated in the sense of preventing access to those mechanisms



# Fundamental Security Design Principles

---

- **Encapsulation**

- Can be viewed as a specific form of isolation based on object-oriented functionality
- Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem, and the procedures may be called only at designated domain entry points

# Fundamental Security Design Principles

---

- **Modularity**

- Refers both to the development of security functions as separate, protected modules and to the use of a modular architecture for mechanism design and implementation

# Fundamental Security Design Principles

---

- **Layering**

- Refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems
- The failure or circumvention of any individual protection approach will not leave the system unprotected

# Fundamental Security Design Principles

---

- **Least astonishment**

- Means that a program or user interface should always respond in the way that is least likely to astonish the user
- The mechanism for authorization should be transparent enough to a user that the user has a good intuitive understanding of how the security goals map to the provided security mechanism

# Attack Surfaces

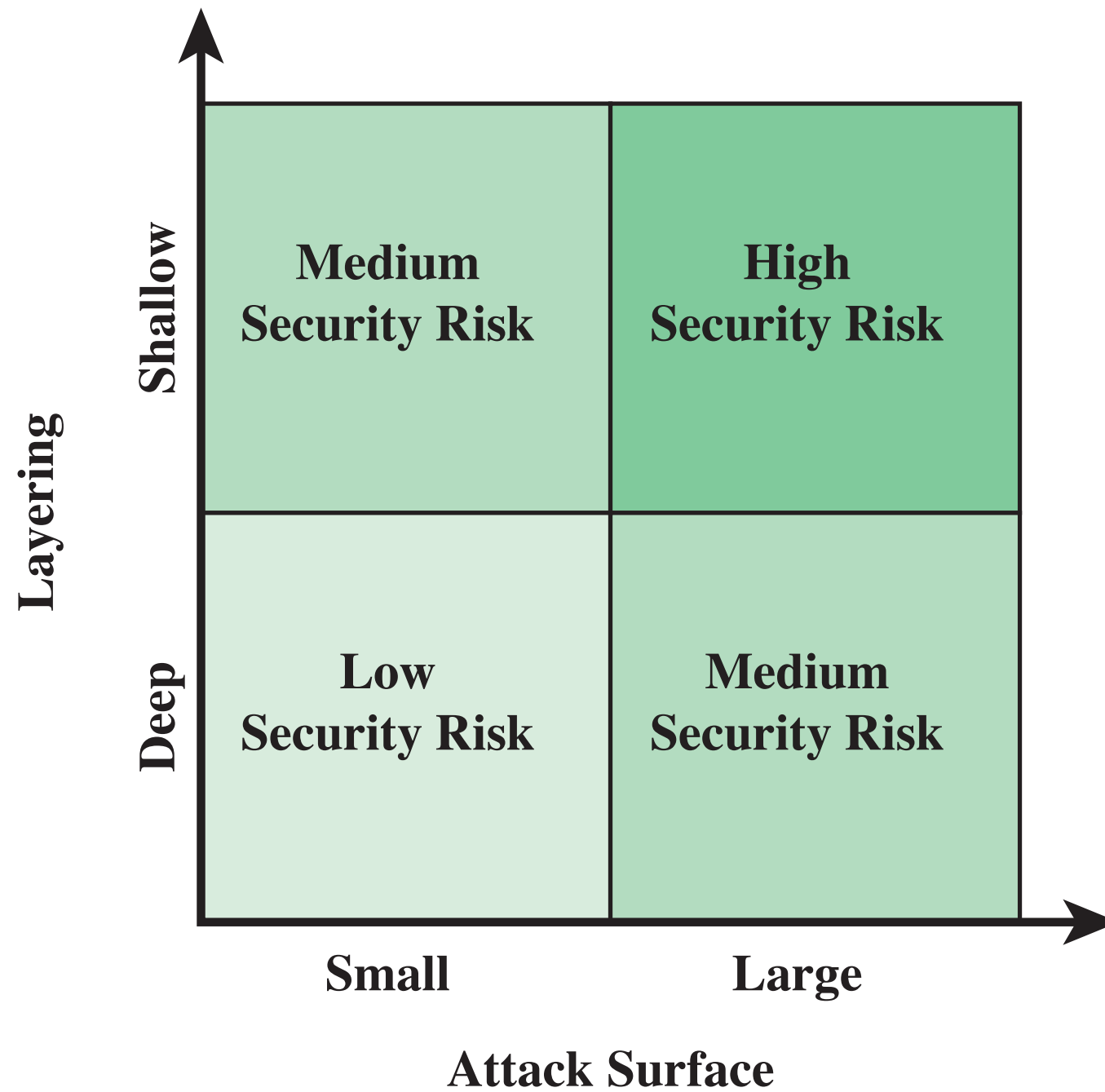
---

- An attack surface consists 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
  - Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
- Software attack surface
  - Refers to vulnerabilities in application, utility, or operating system code
- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders

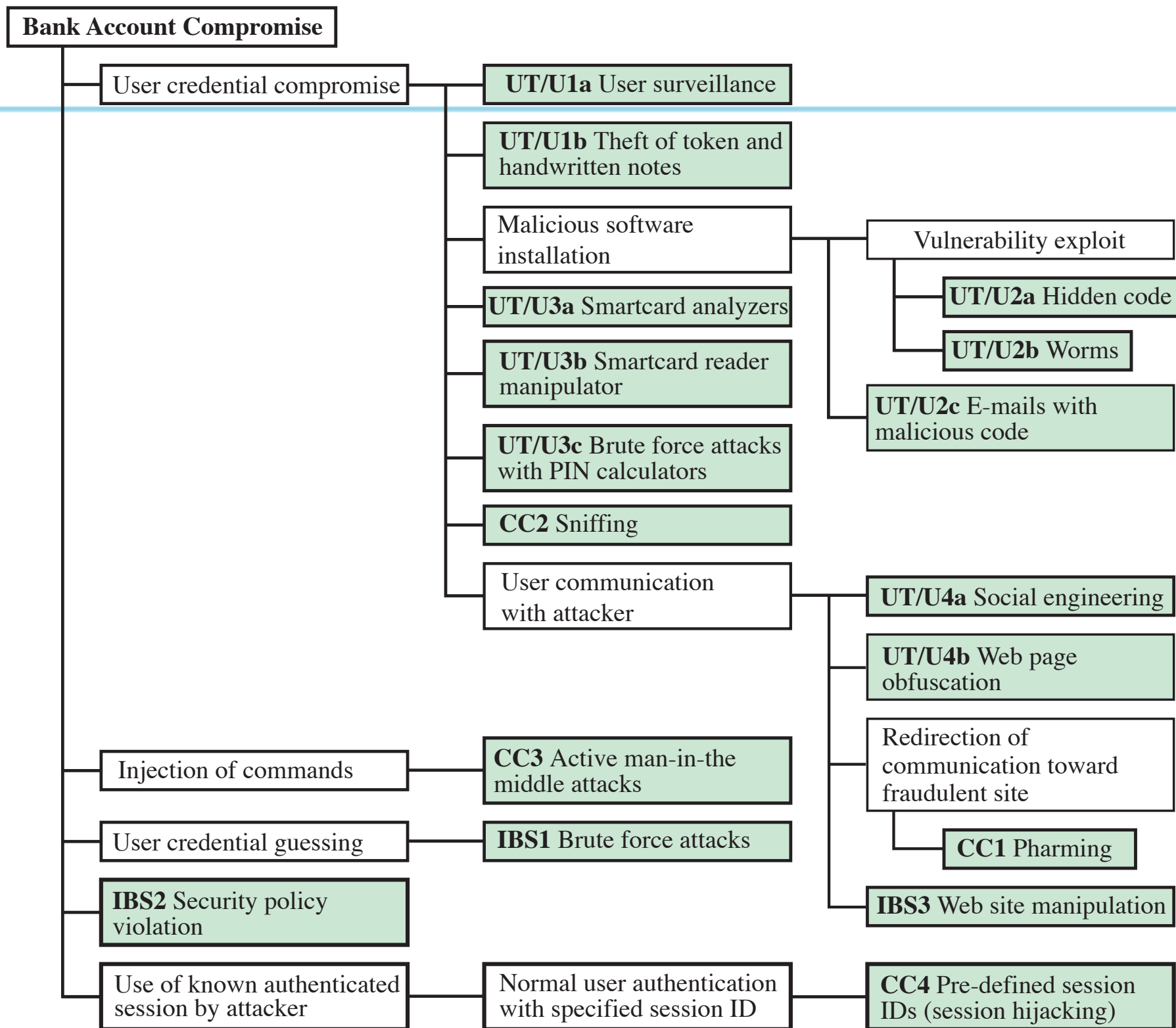


# Attack Tree

---

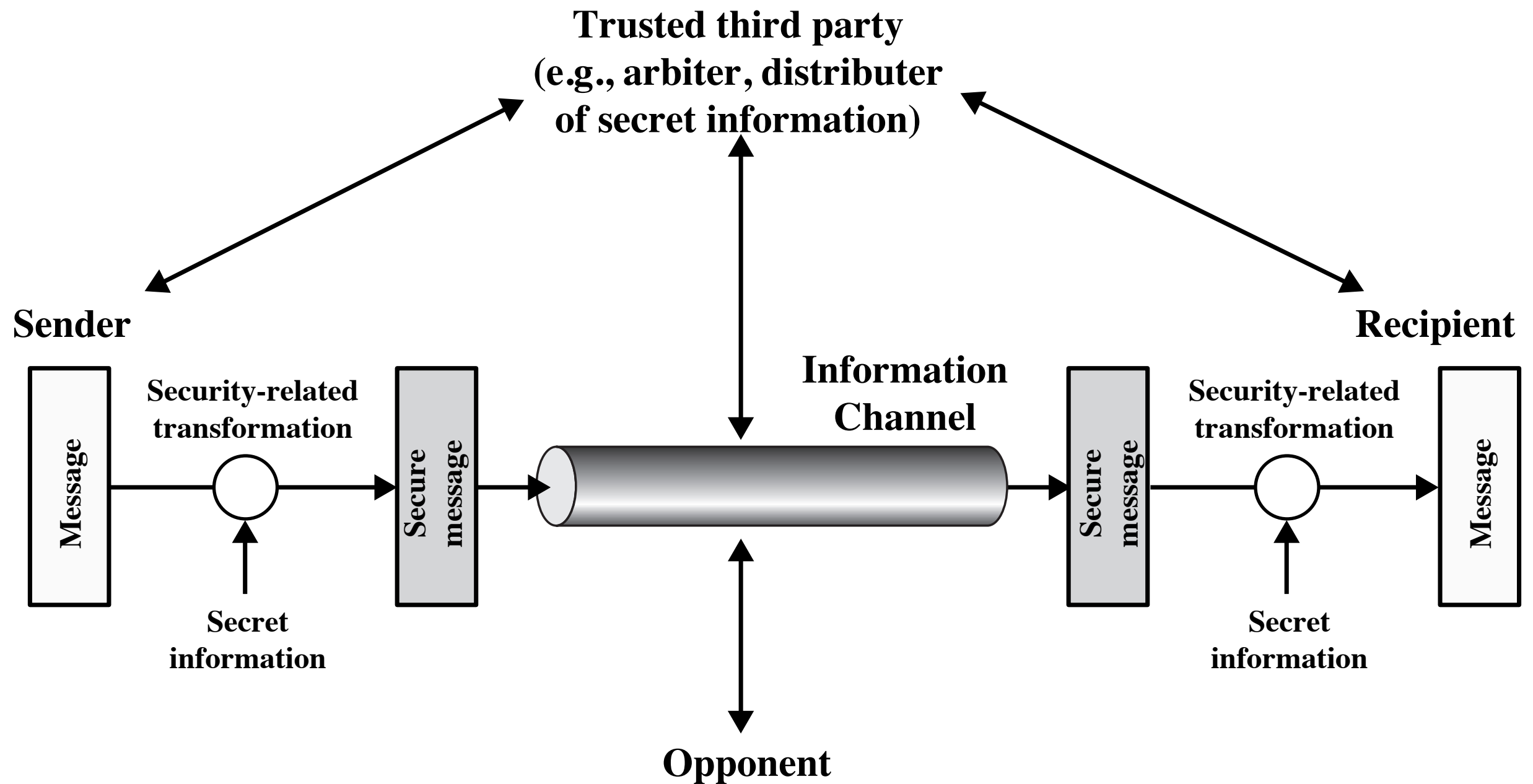
- A branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities
- The security incident that is the goal of the attack is represented as the root node of the tree, and the ways that an attacker could reach that goal are represented as branches and subnodes of the tree
- The final nodes on the paths outward from the root, (leaf nodes), represent different ways to initiate an attack
- The motivation for the use of attack trees is to effectively exploit the information available on attack patterns





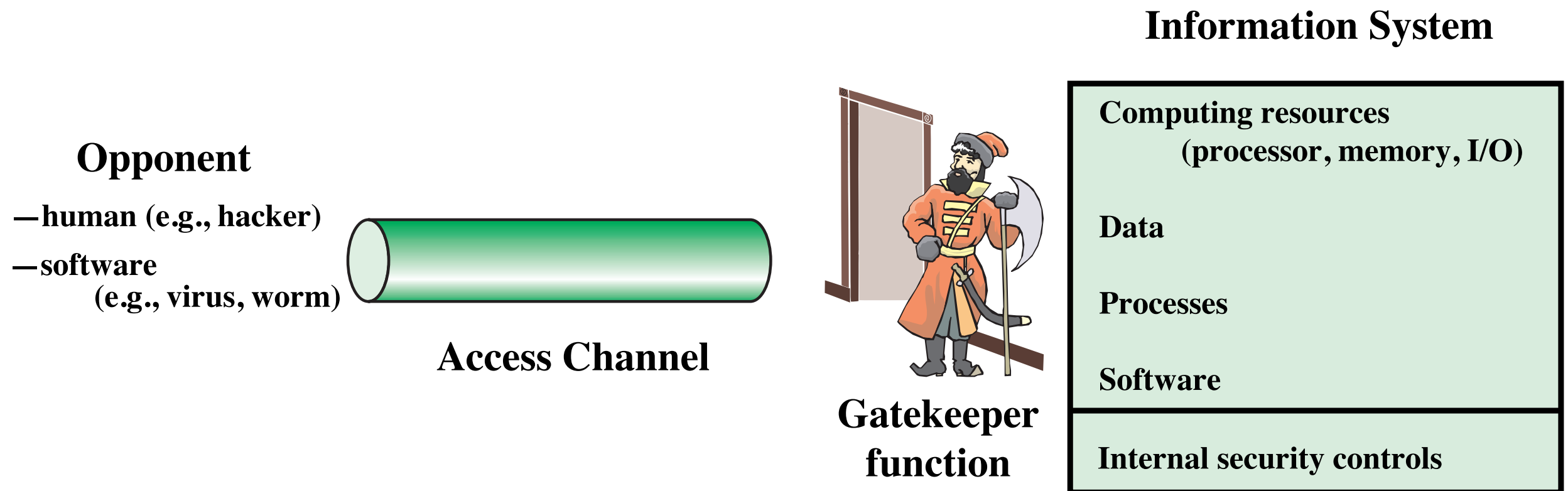
## An Attack Tree for Internet Banking Authentication

# Model for Network Security



Model for Network Security

# Network Access Security Model



## Network Access Security Model

# Unwanted Access

---

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs such as editors and compilers
- Programs can present two kinds of threats:
  - Information access threats
    - Intercept or modify data on behalf of users who should not have access to that data
  - Service threats
    - Exploit service flaws in computers to inhibit use by legitimate users



## **National Institute of Standards and Technology**

- NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation
- Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

## **Internet Society**

- ISOC is a professional membership society with world-wide organizational and individual membership
- Provides leadership in addressing issues that confront the future of the Internet and is the organization home for the groups responsible for Internet infrastructure standards

## **ITU-T**

- The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services
- The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU and whose mission is the development of technical standards covering all fields of telecommunications

## **ISO**

- The International Organization for Standardization is a world-wide federation of national standards bodies from more than 140 countries
- ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity

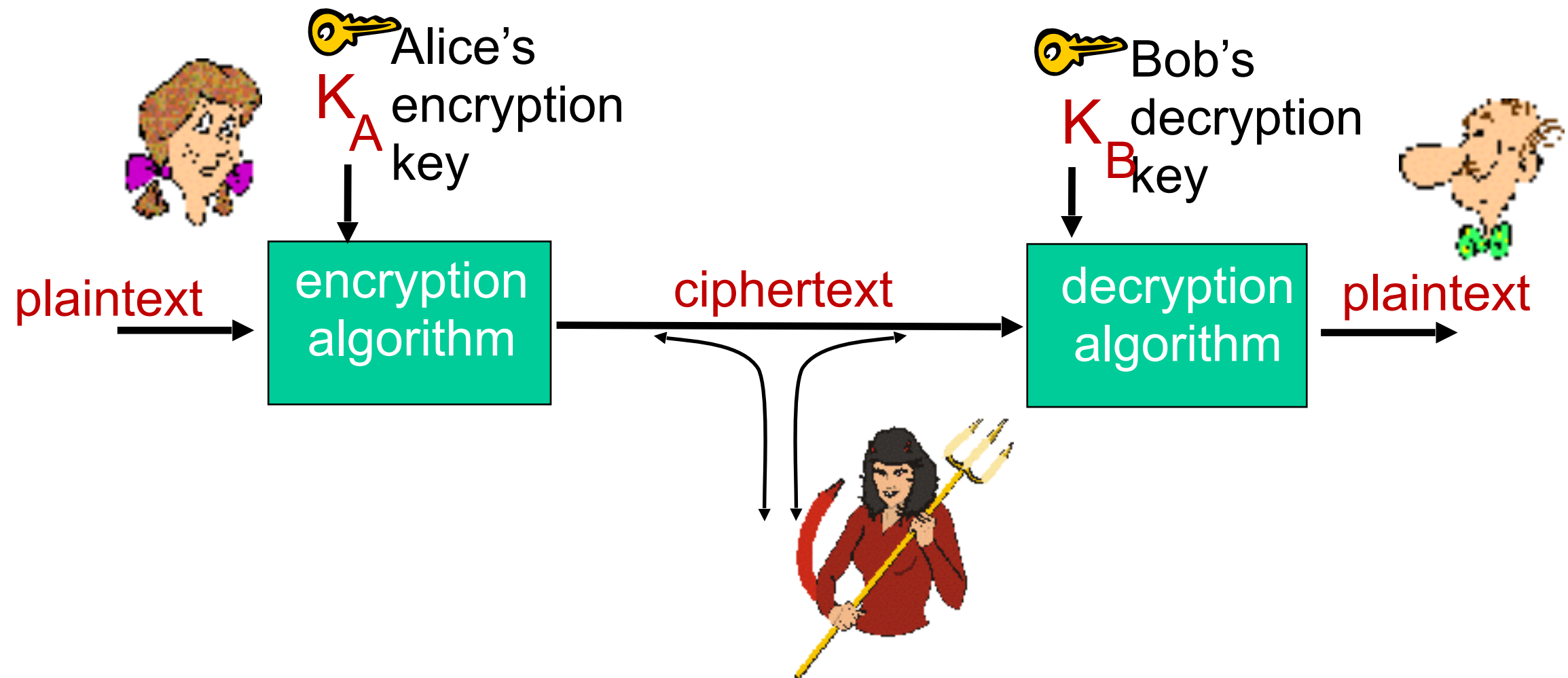
# Introduction to Cryptography

# The language of cryptography

$m$  plaintext message

$K_A(m)$  ciphertext, encrypted with key  $K_A$

$m = K_B(K_A(m))$





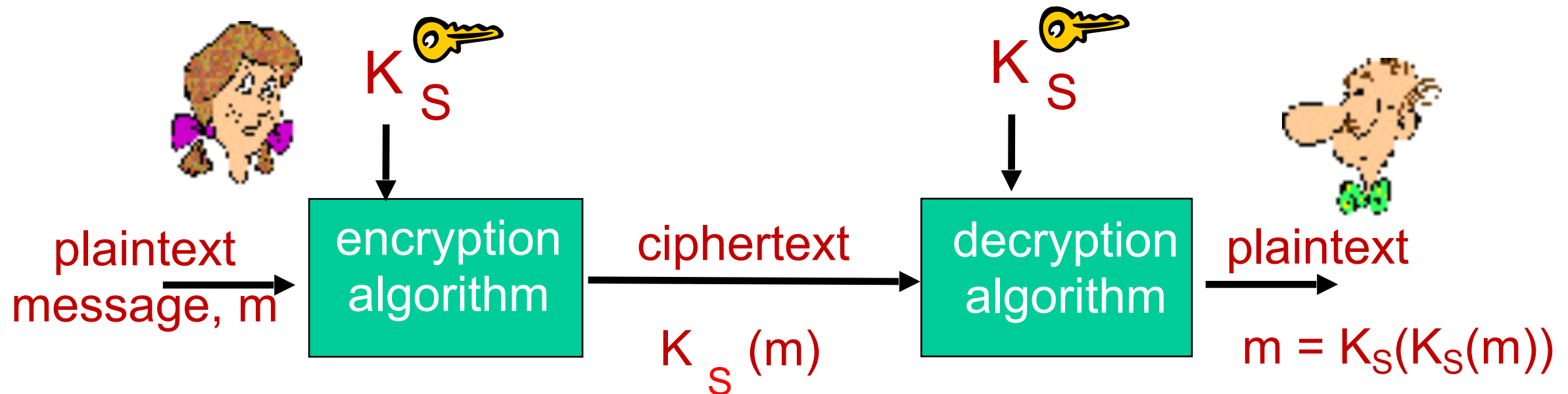
# Breaking an encryption scheme

---

- **cipher-text only attack:**  
Trudy has ciphertext she can analyze
- **two approaches:**
  - brute force: search through all keys
  - statistical analysis
- **known-plaintext attack:**  
Trudy has plaintext corresponding to ciphertext
  - e.g., in monoalphabetic cipher, Trudy determines pairings for a,l,i,c,e,b,o,
- **chosen-plaintext attack:**  
Trudy can get ciphertext for chosen plaintext



# Symmetric key cryptography



**symmetric key crypto:** Bob and Alice share same (symmetric) key:  $K_S$

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher

**Q:** how do Bob and Alice agree on key value?

# Public Key Cryptography

## *symmetric key crypto*

- requires sender, receiver know shared secret key
- Q: how to agree on key in first place (particularly if never “met”)?

## *public key crypto*

- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver



# Public key cryptography

