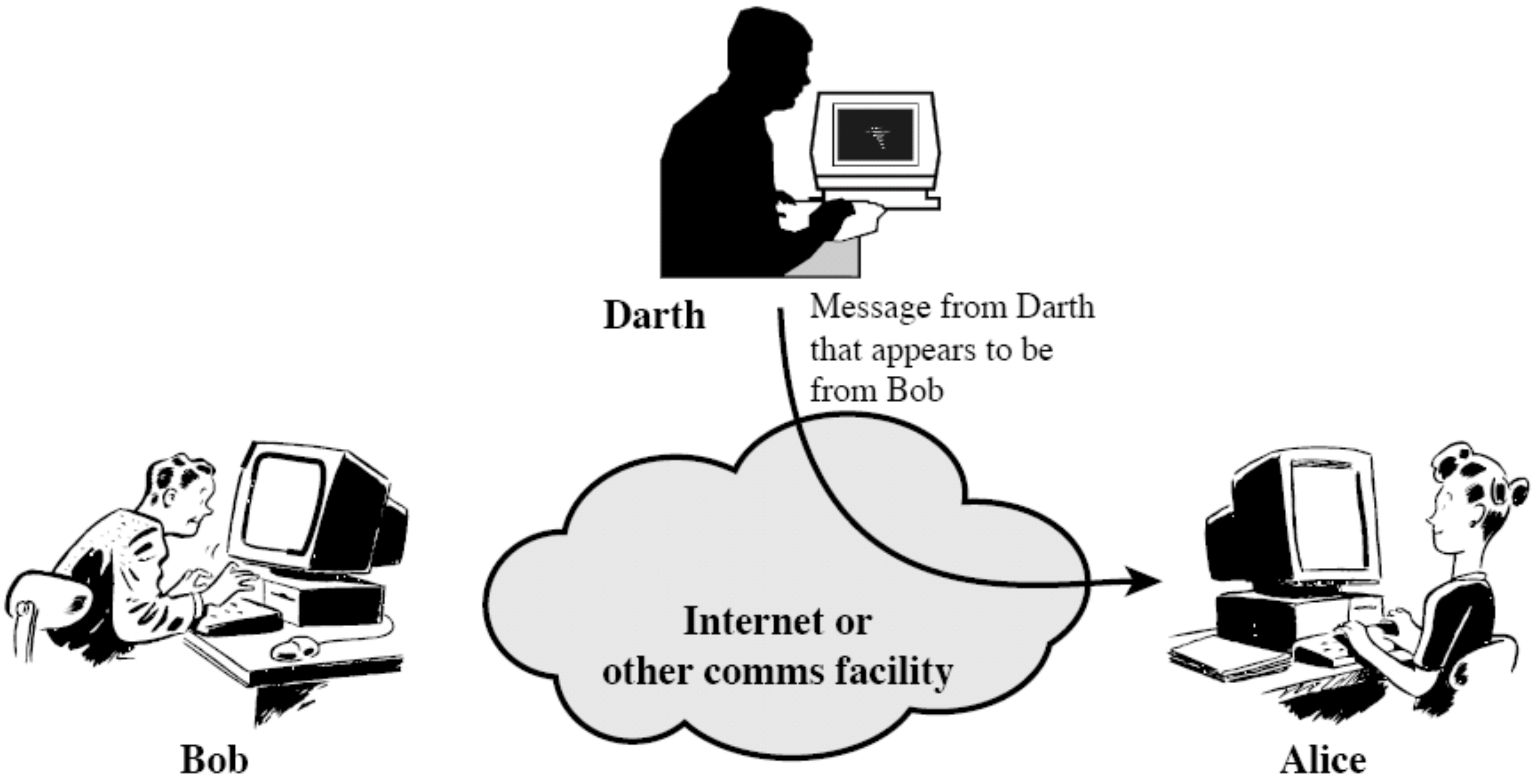
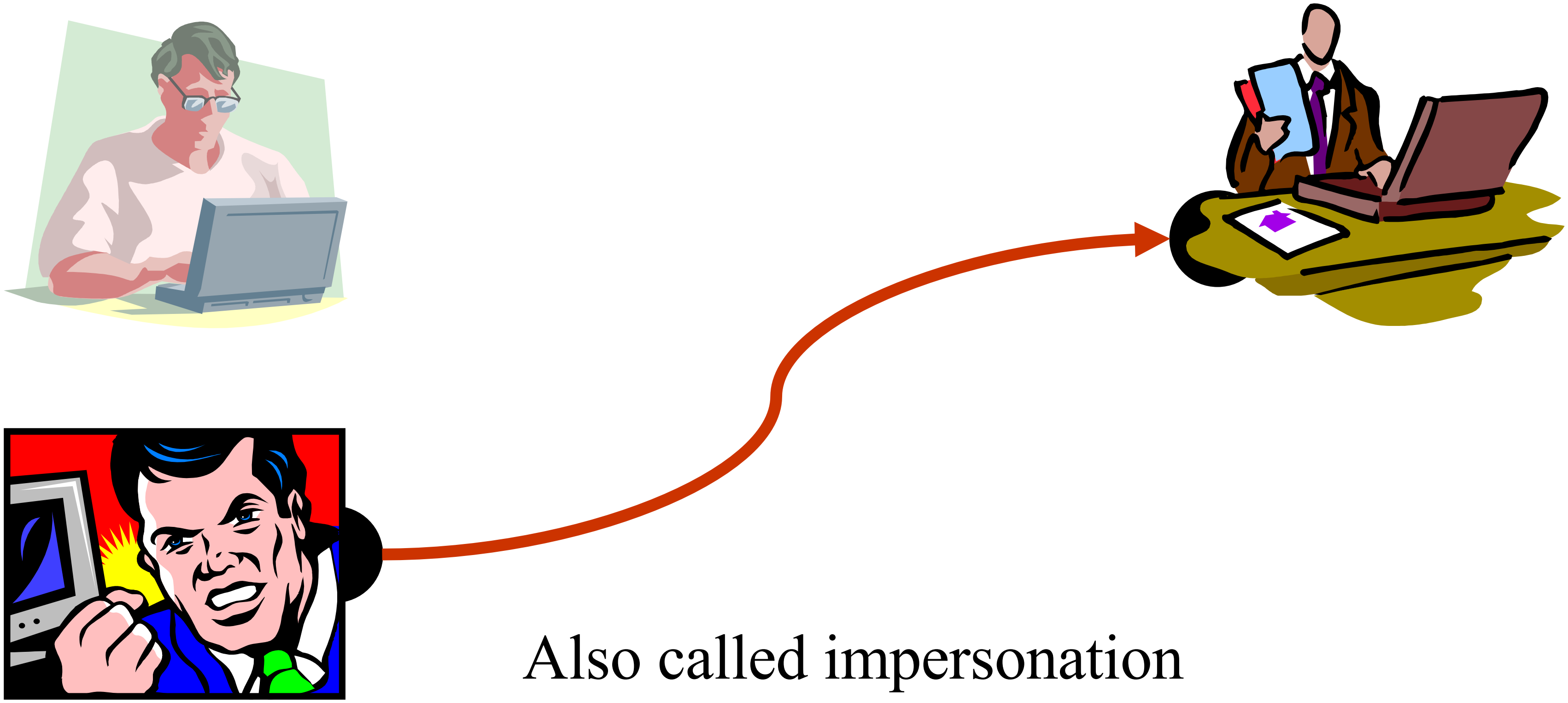
Active Attack: Masquerade

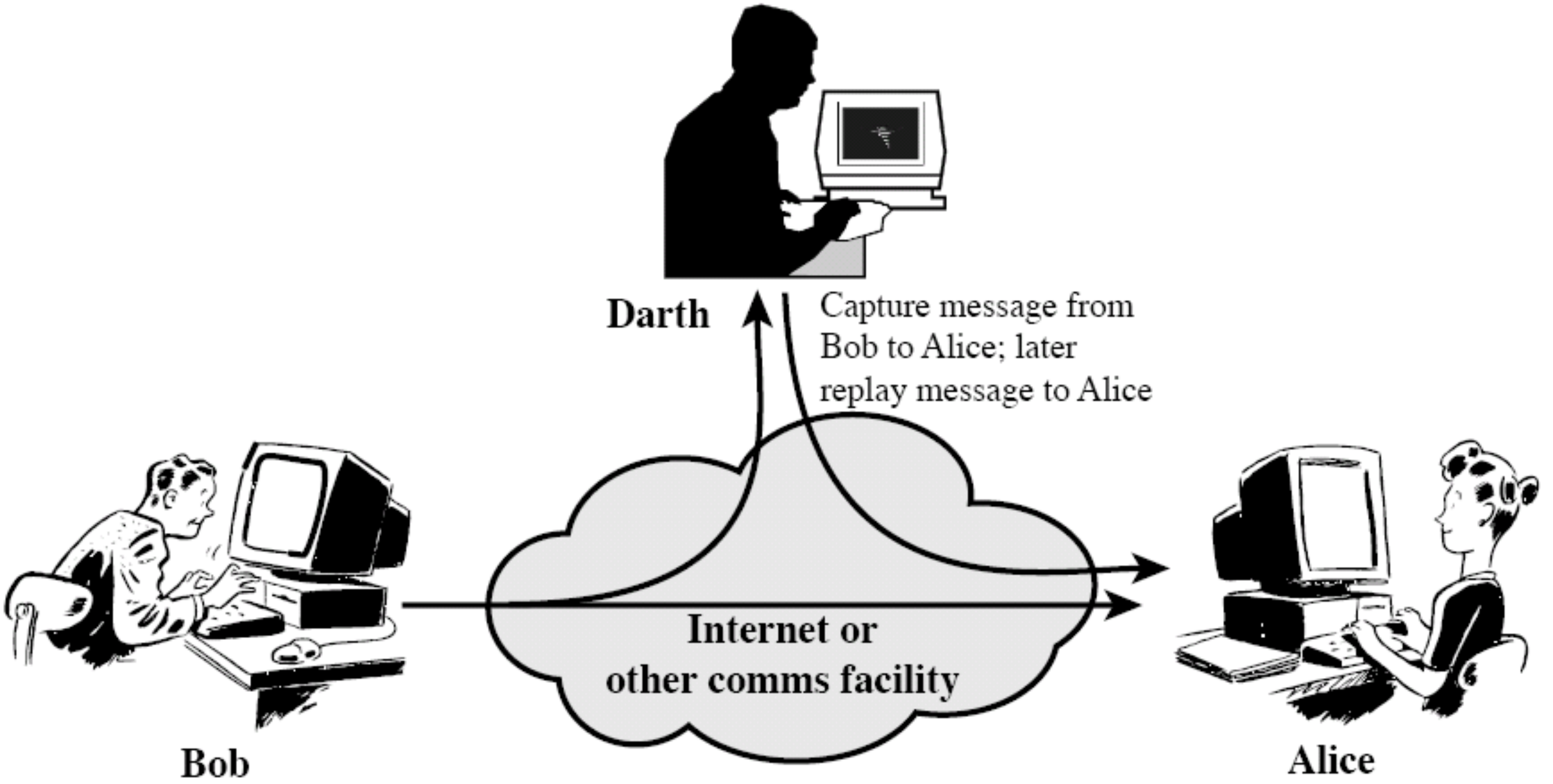

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Also Called: Fabrication (spoofing)

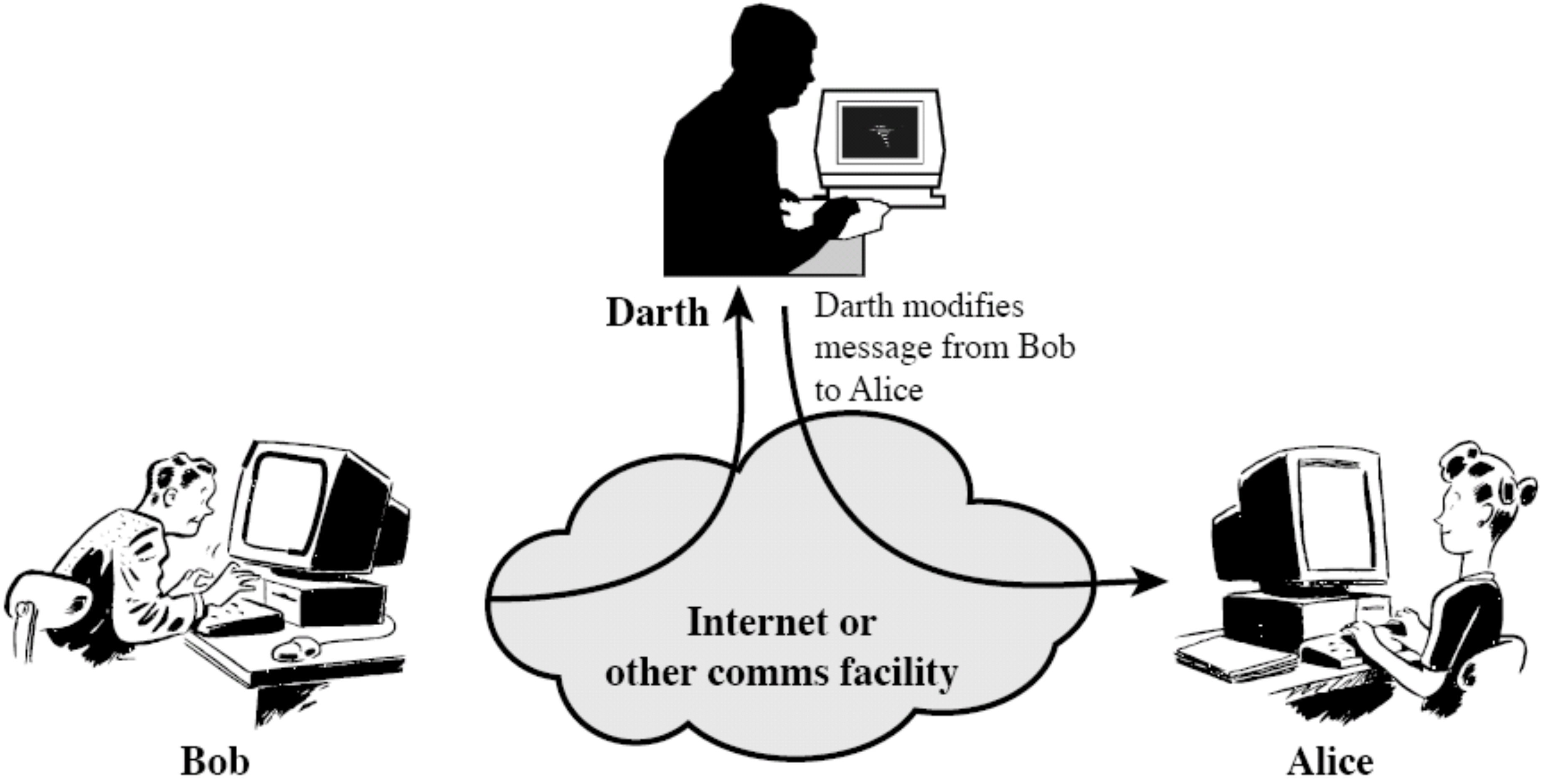


Also called impersonation

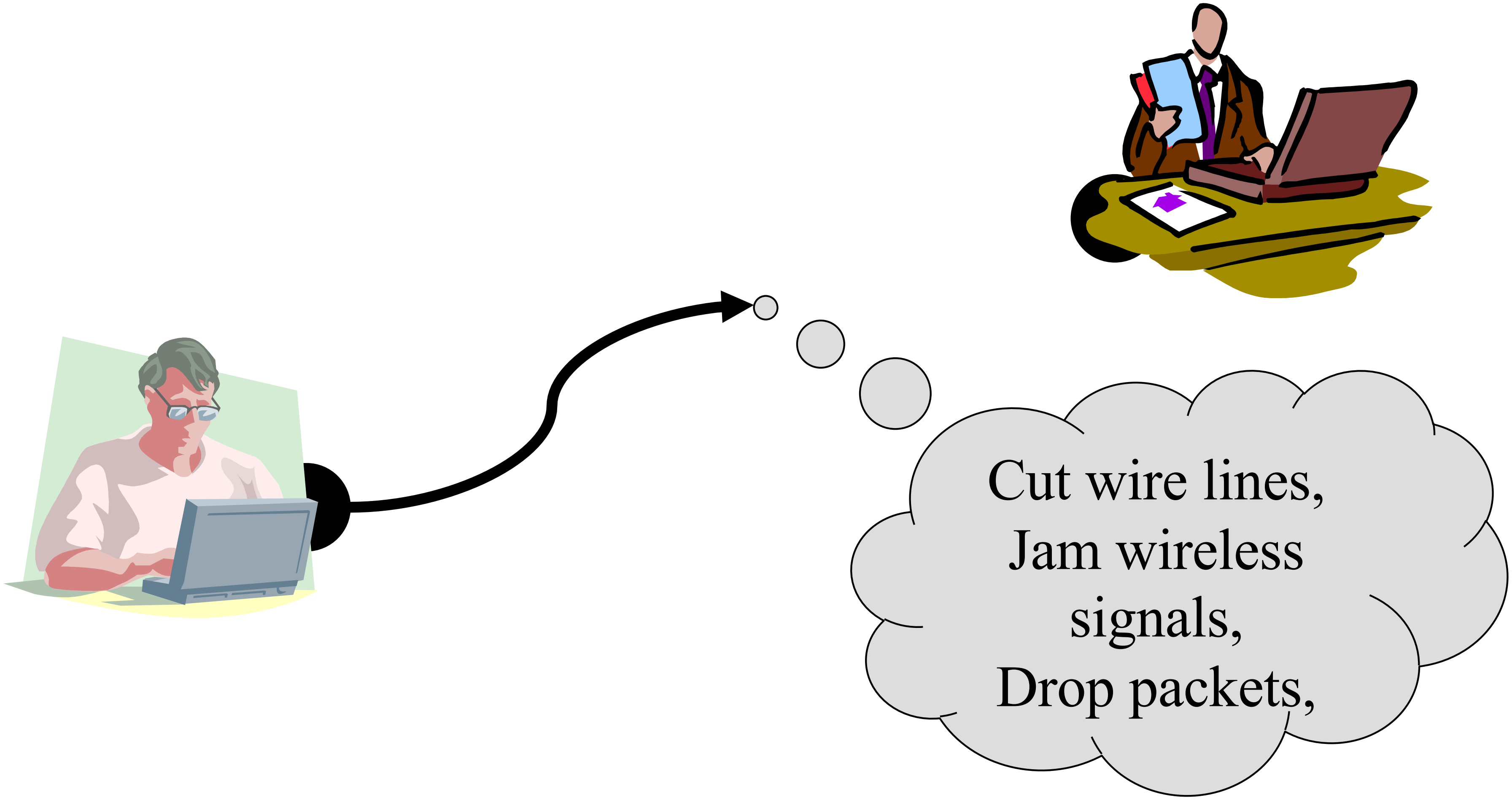
Active Attack: Replay


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attack: Modification of Message

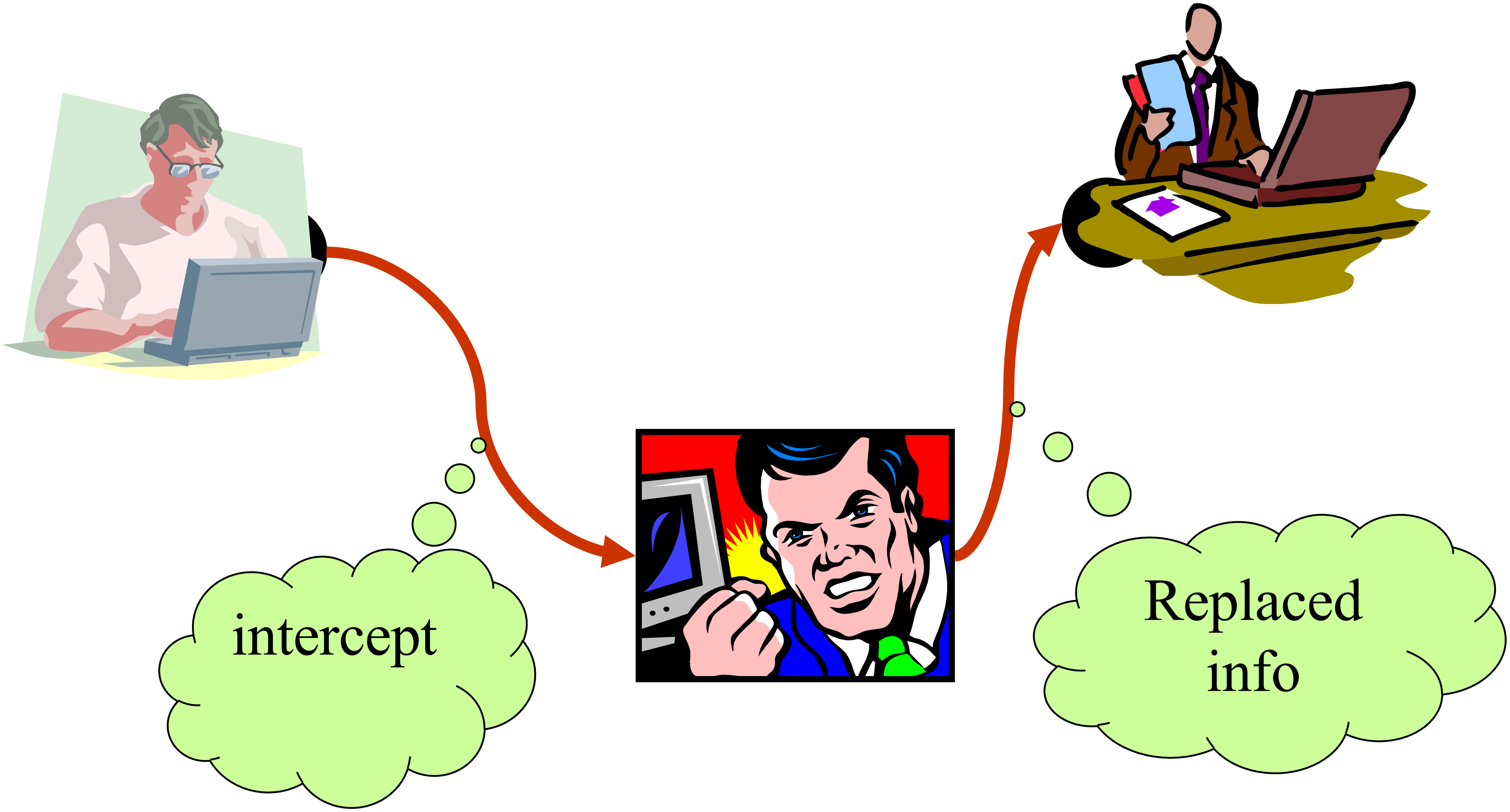

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

Attack: Interruption



Cut wire lines,
Jam wireless
signals,
Drop packets,

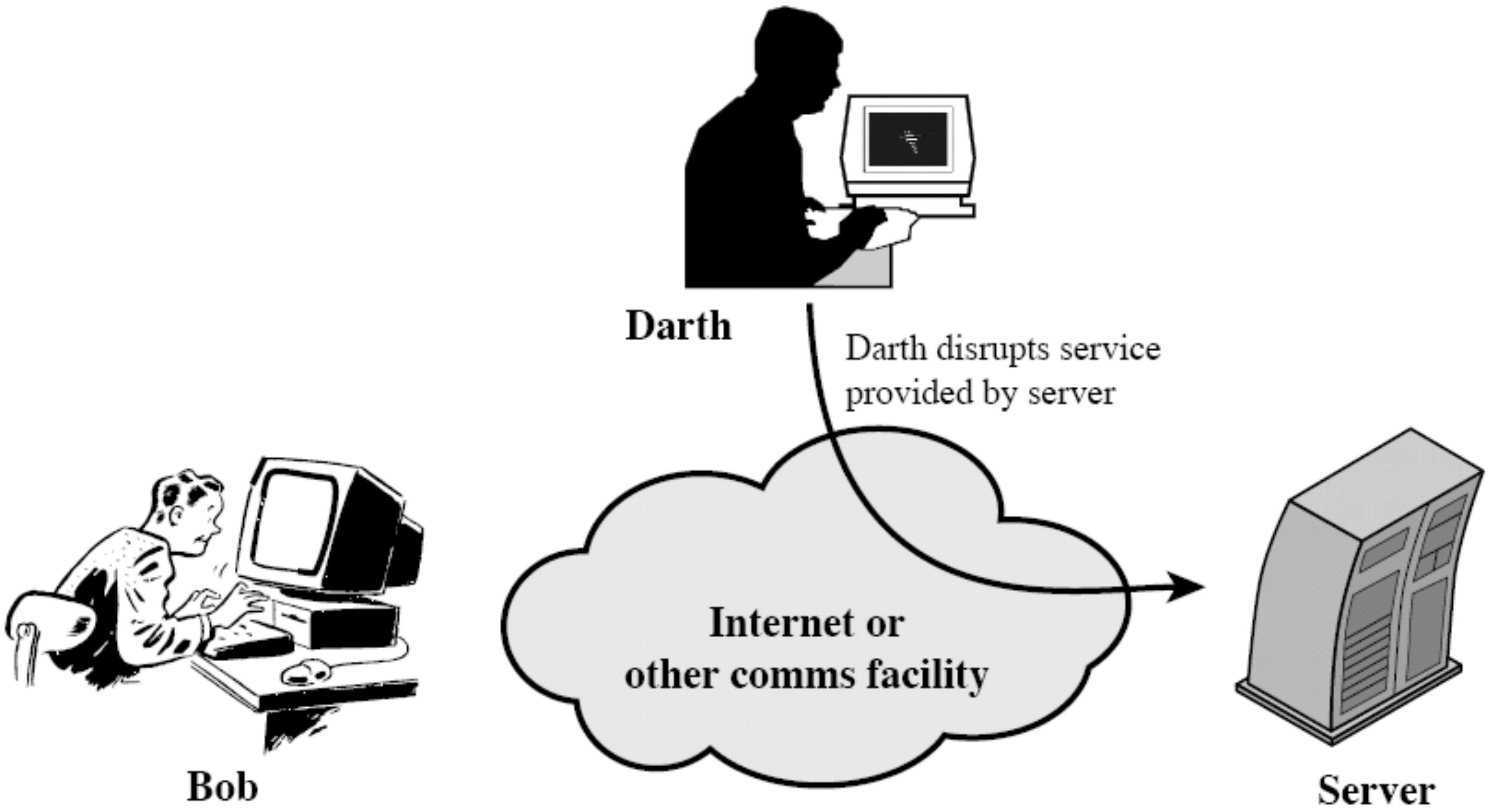
Attack: Modification (tampering)



intercept

Replaced info

Active Attack: Denial of Service


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

Threat Consequence

--> security violation resulting from threat action

Possible Threat Consequences

disclosure

entity gains access to data for which it is not authorized

deception

authorized entity receives false data and believes it to be true

disruption

interruption or prevention of correct operation of system services and functions

usurpation

control of system services or functions by an unauthorized entity

Security Attacks

- **Interruption:** This is an attack on **availability**
- **Interception:** This is an attack on **confidentiality**
- **Modification:** This is an attack on **integrity**
- **Fabrication:** This is an attack on **authenticity**

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

Some Background Information

ISO: International Organization for Standardization (greek: isos, “equal”)

-> network of international standards institutes

ITU: International Telecommunication Union

-> specialized agency of the United Nations (UN)

-> ITU-T: standardizations body of the ITU, used to be CCITT (Comité Consultatif International Téléphonique et Télégraphique)

OSI: Open Systems Interconnection

-> concerted effort of ISO and ITU-T

-> reference model for network protocol implementation (complex!)

-> seven protocol layers (“protocol stack”)

-> was eventually “overtaken” by Internet’s TCP/IP suite (simple!)

OSI Security Architecture

- **ITU-T X.800: “Security Architecture for Open Systems Interconnections for CCITT Applications”, Geneva 1991**
  - RFC 2828
  - Security services implement security policies and are implemented by security mechanisms
- **provides general description of security services and related mechanisms**
- **defines positions within OSI reference model where security services may be provided**
- **thus, provides us with systematic approach to network security**

Security Services (X.800)

Authentication

Access Control

Data Confidentiality

Data Integrity

Non-Repudiation

Security Services (X.800)

Authentication

-> assurance that communicating entity is the one that it claims it is

-> peer entity authentication, data-origin authentication

Access Control

-> prevention of unauthorized use of resources

Data Confidentiality

-> protection of data from unauthorized disclosure

-> per connection, connectionless, selected fields, traffic flow

Data Integrity

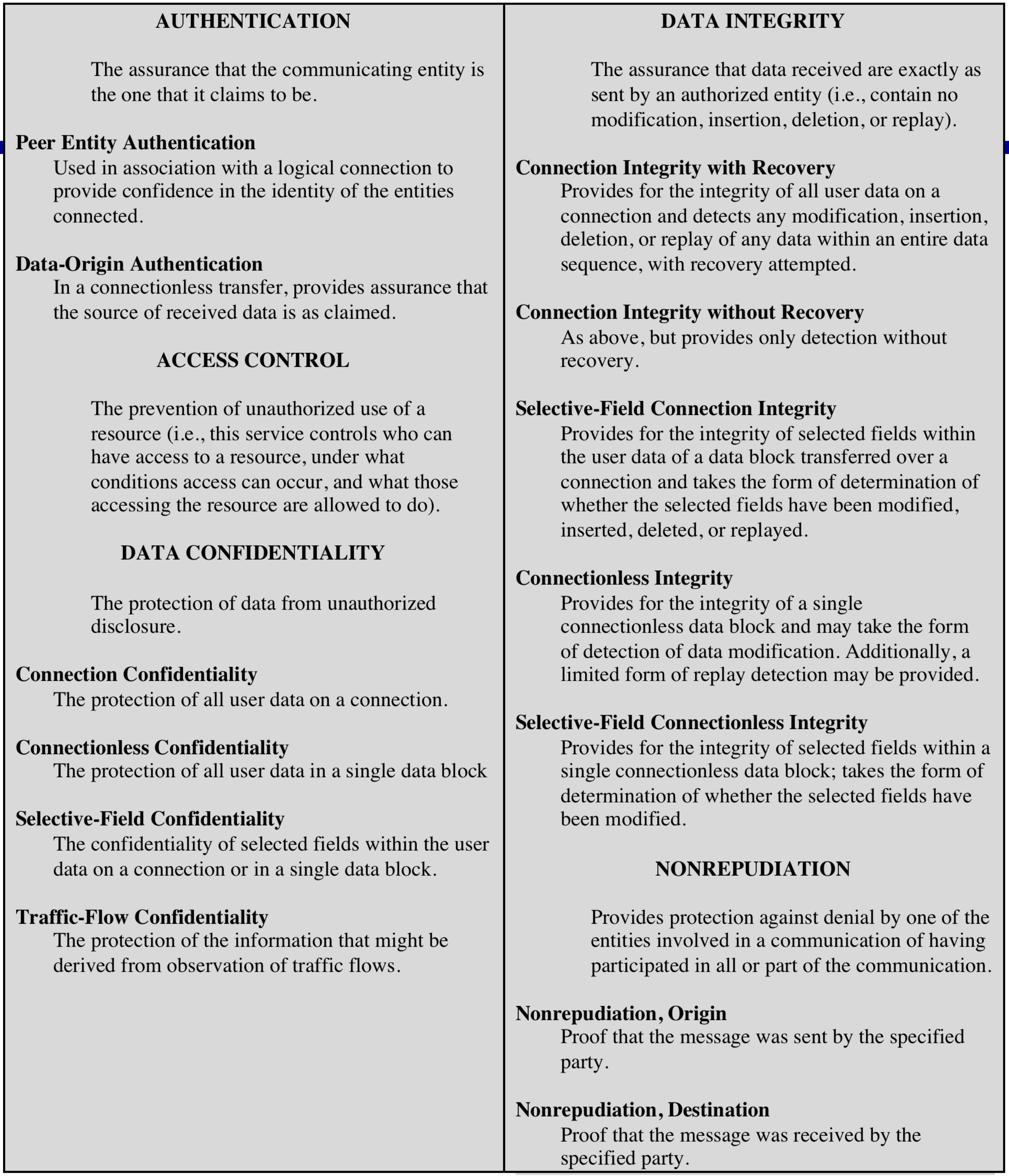
-> assurance that data received = data sent by authorized entity

-> detection with and without recovery

Non-Repudiation

-> protection against denial by one entity involved in communications

-> proof of origin, proof of sending



AUTHENTICATION

The assurance that the communicating entity is the one that it 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).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

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.

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

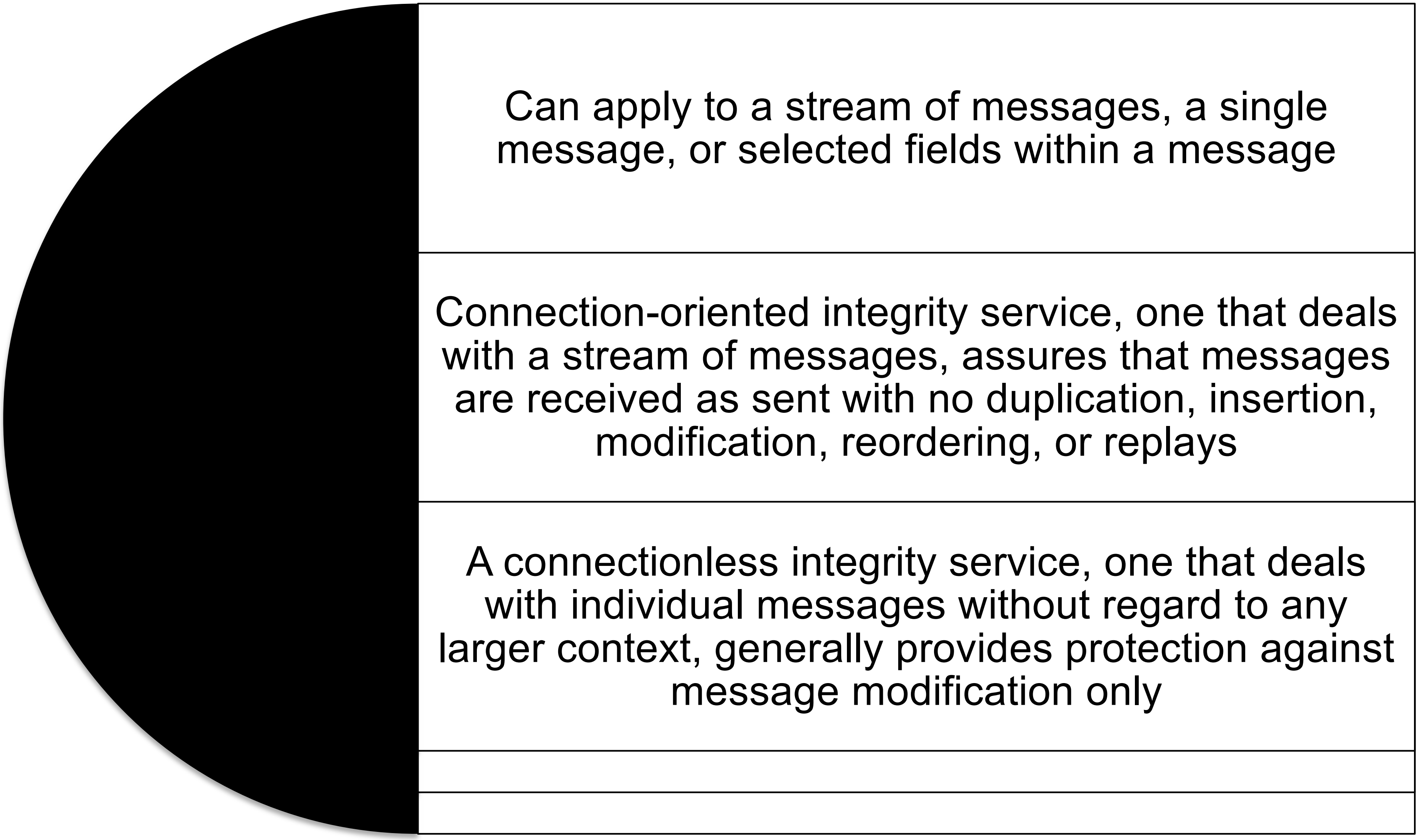
Access Control

- 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

Security Services: don’t forget...

... Availability

-> not a service in X.800, however very important!

Definition of “Availability” according [RFC 2828]

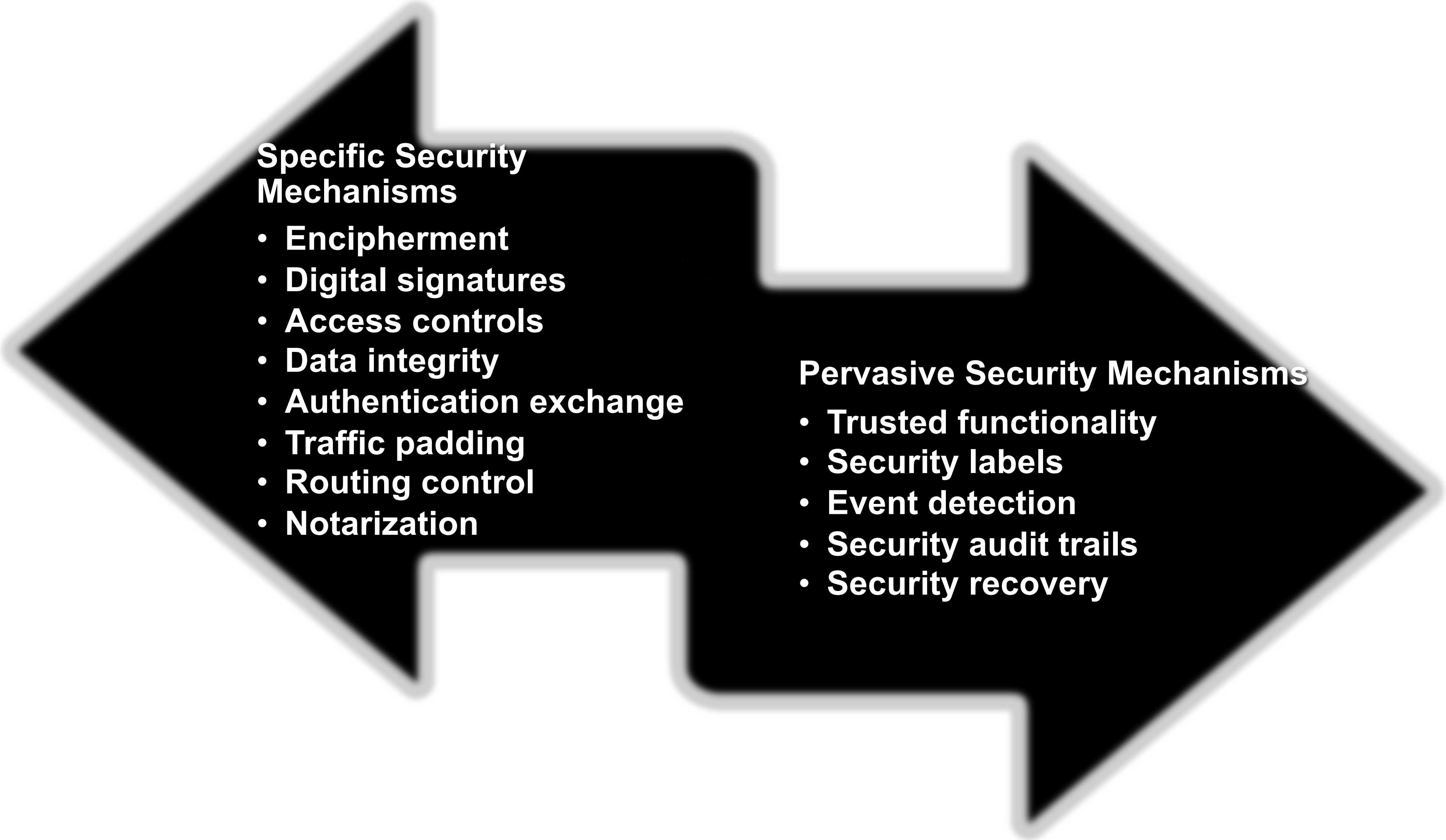
Property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

- 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

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

Specific Security Mechanisms (X.800)

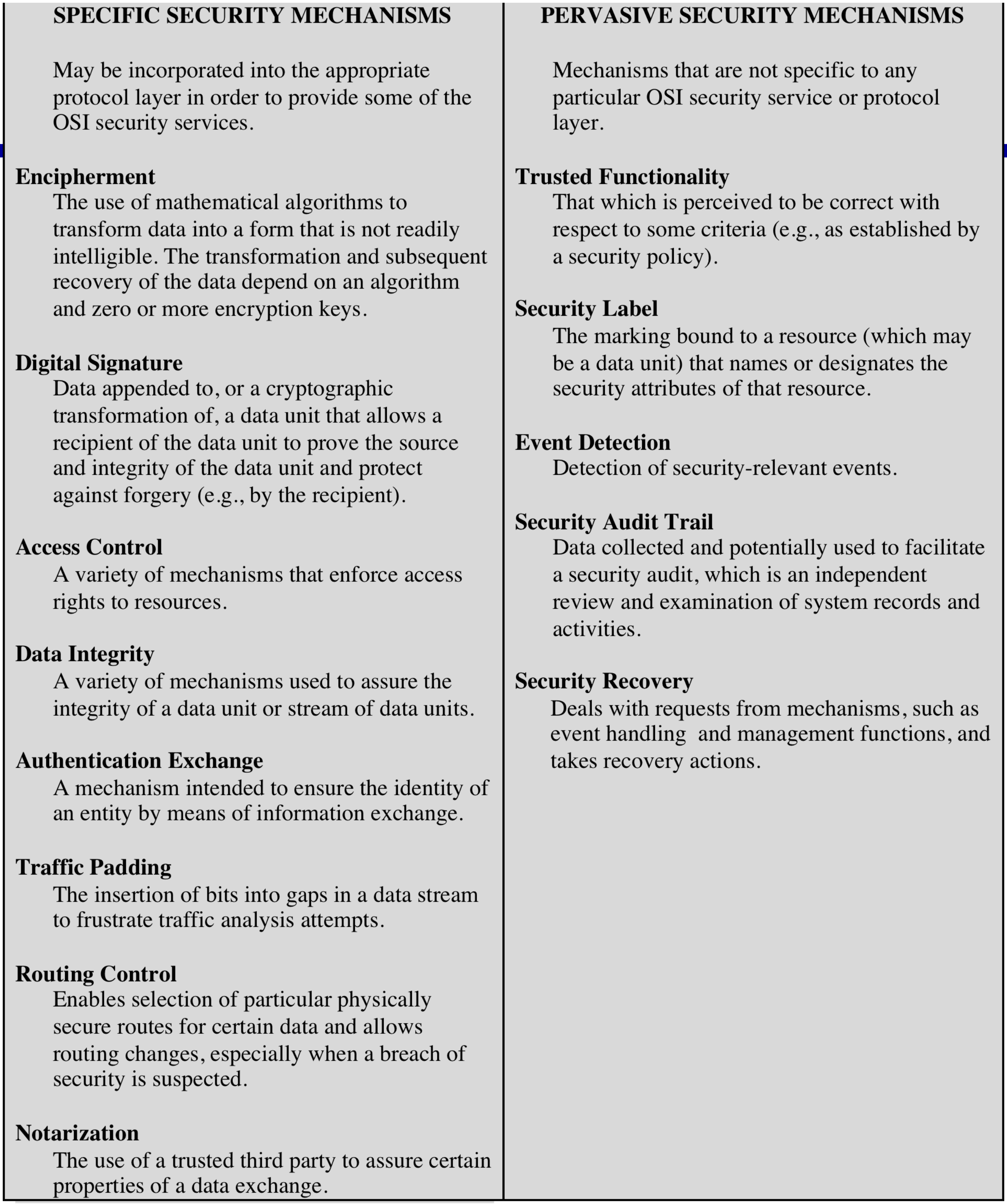


Specific Security Mechanisms

- 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



SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

Access Control
A variety of mechanisms that enforce access rights to resources.

Data Integrity
A variety of mechanisms used to assure the integrity of a data unit or stream of data units.

Authentication Exchange
A mechanism intended to ensure the identity of an entity by means of information exchange.

Traffic Padding
The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.

Routing Control
Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

Trusted Functionality
That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

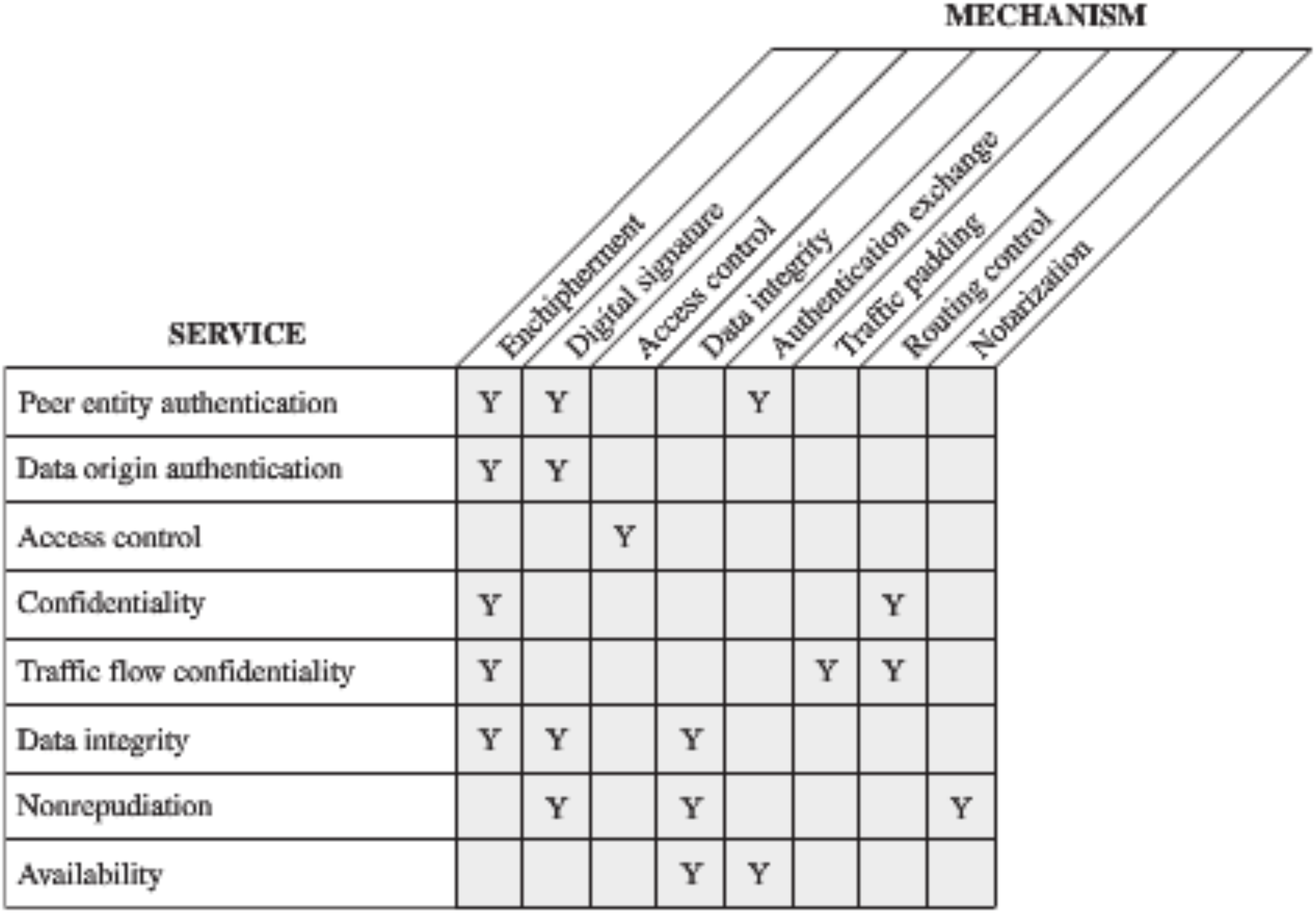
Security Label
The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.

Event Detection
Detection of security-relevant events.

Security Audit Trail
Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.

Security Recovery
Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Relationship between Security Services and Mechanisms



SERVICE	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ **Fundamental Security Design Principles**
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete meditation
- 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

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

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

Least 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

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

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

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

Outline

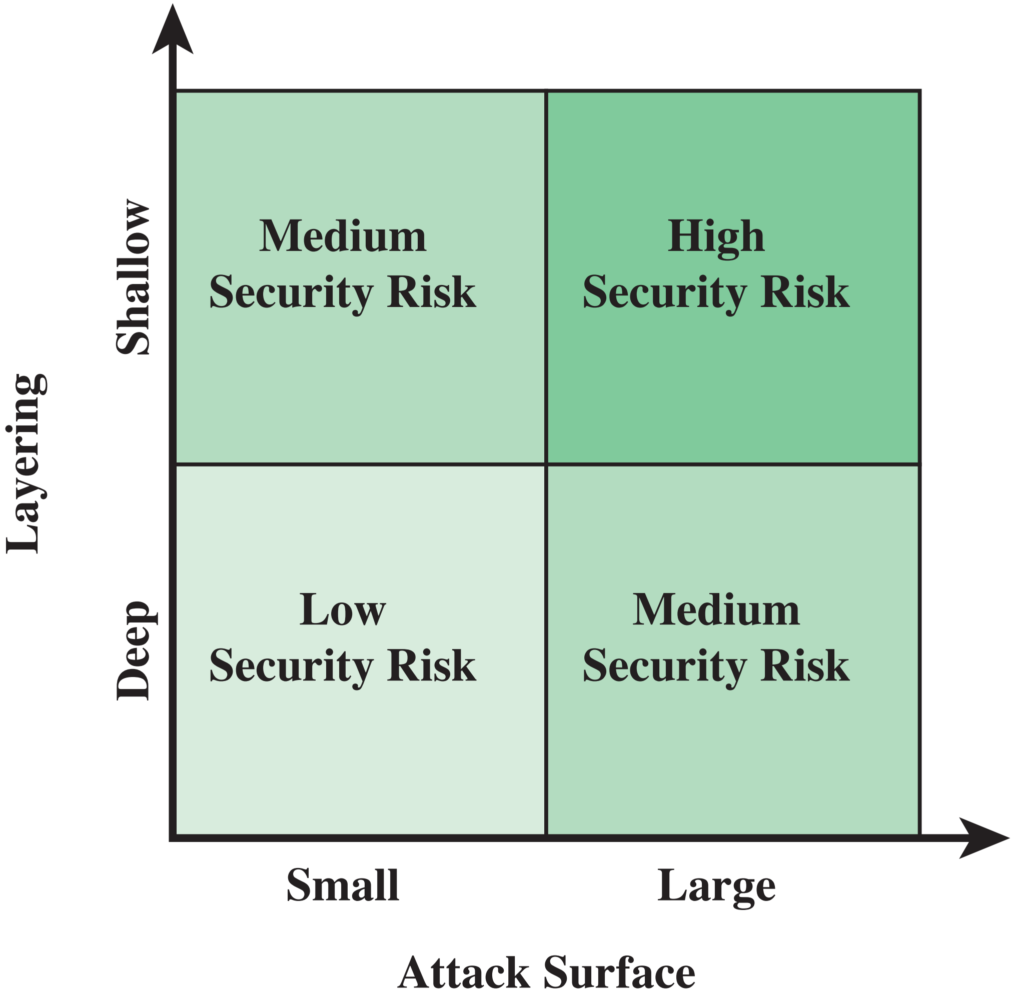
- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ Standards

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



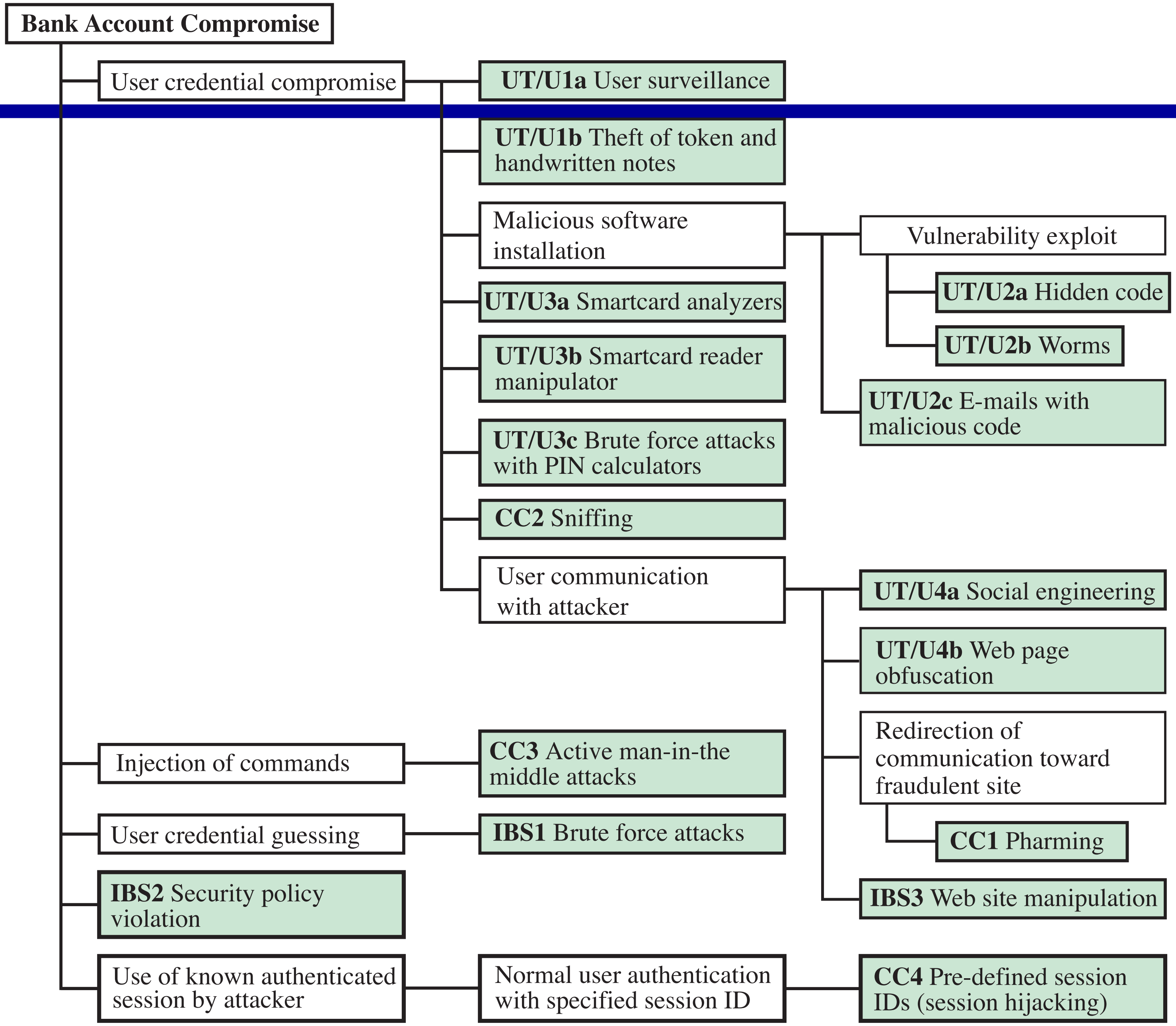
Layering	Small	Large
Shallow	Medium Security Risk	High Security Risk
Deep	Low Security Risk	Medium Security Risk

Attack Surface

Figure 1.3 Defense in Depth and Attack Surface

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

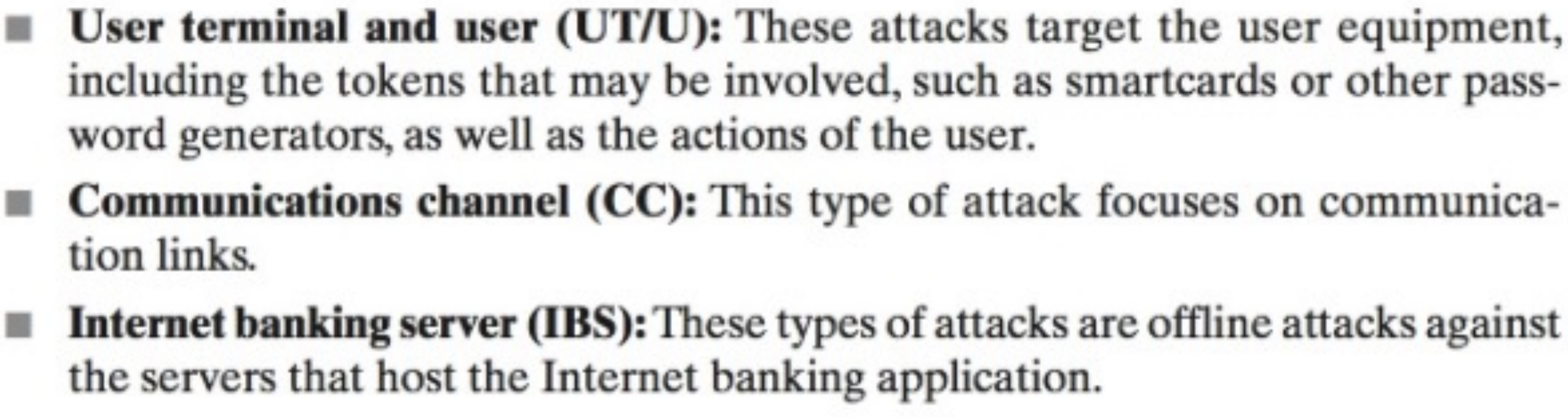


Bank Account Compromise

- 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)

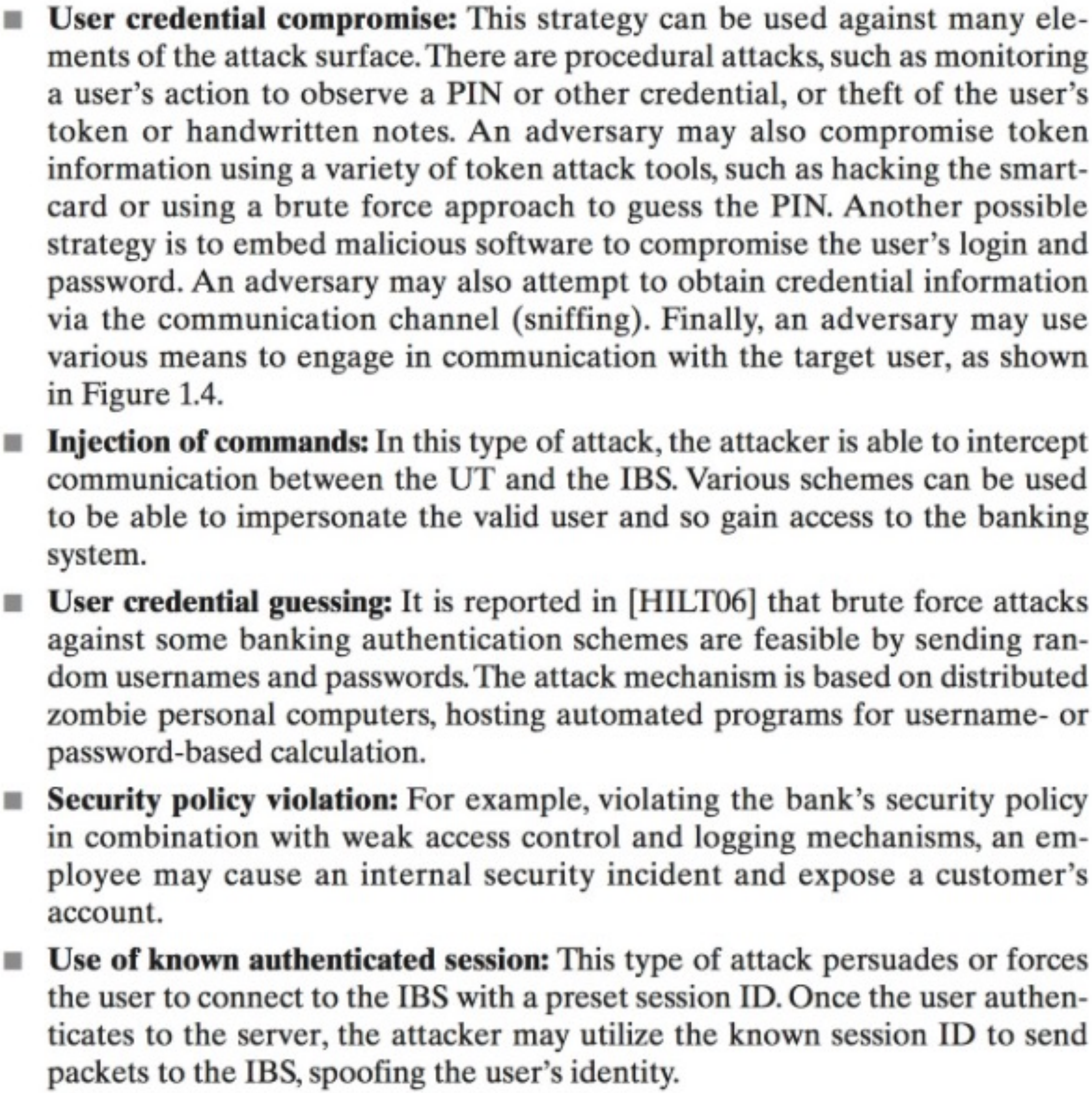
Figure 1.4 An Attack Tree for Internet Banking Authentication

Three Components in Authentication



- **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 attacks against the servers that host the Internet banking application.

Five Attack Strategies

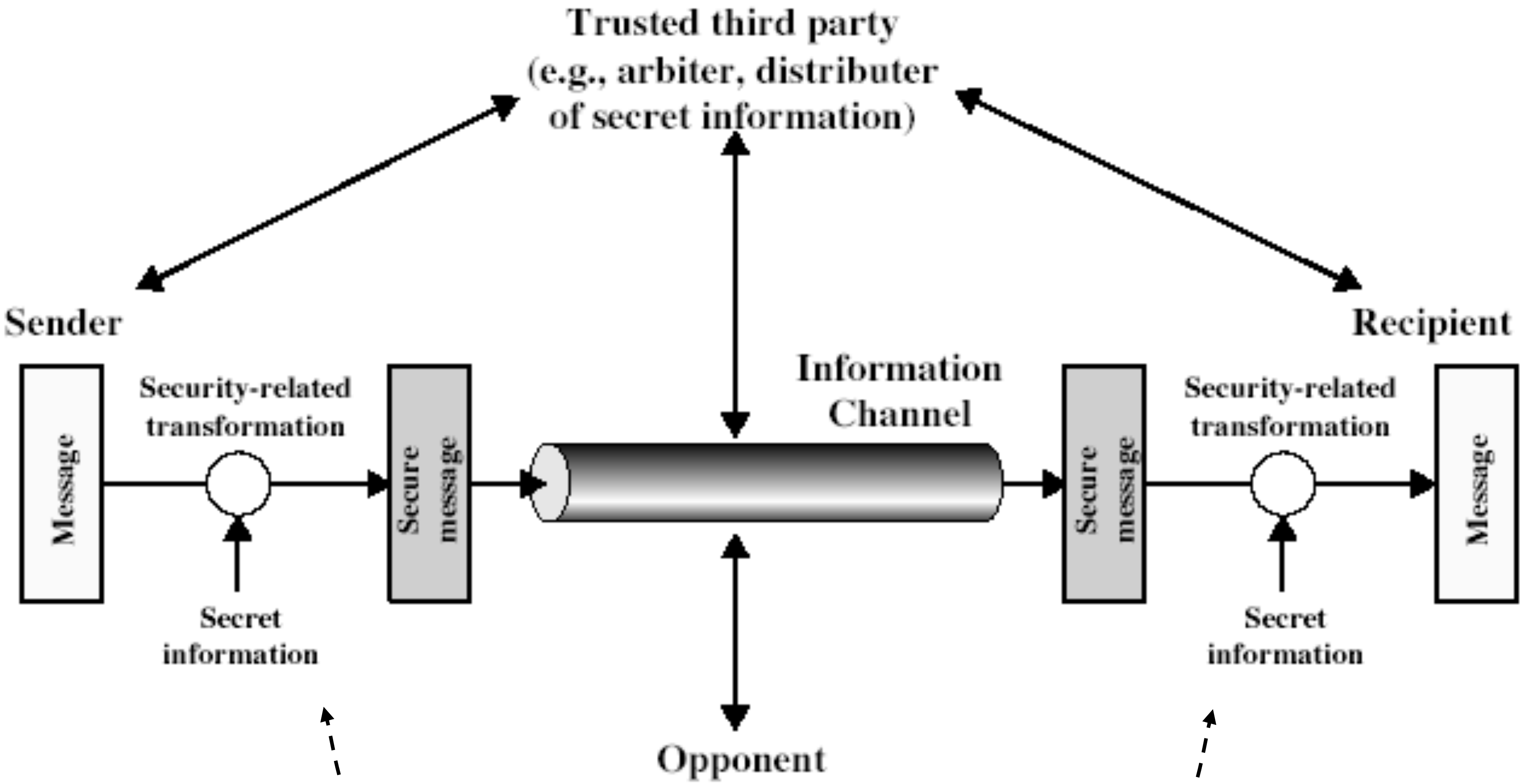


- **User credential compromise:** This strategy can be used against many elements of the attack surface. There are procedural attacks, such as monitoring a user's action to observe a PIN or other credential, or theft of the user's token or handwritten notes. An adversary may also compromise token information using a variety of token attack tools, such as hacking the smartcard or using a brute force approach to guess the PIN. Another possible strategy is to embed malicious software to compromise the user's login and password. An adversary may also attempt to obtain credential information via the communication channel (sniffing). Finally, an adversary may use various means to engage in communication with the target user, as shown in Figure 1.4.
- **Injection of commands:** In this type of attack, the attacker is able to intercept communication between the UT and the IBS. Various schemes can be used to be able to impersonate the valid user and so gain access to the banking system.
- **User credential guessing:** It is reported in [HILT06] that brute force attacks against some banking authentication schemes are feasible by sending random usernames and passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username- or password-based calculation.
- **Security policy violation:** For example, violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.
- **Use of known authenticated session:** This type of attack persuades or forces the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity.

Outline

- ❑ **Computer Security Concepts**
- ❑ **The OSI Security Architecture**
- ❑ **Security Attacks**
- ❑ **Security Services**
- ❑ **Security Mechanisms**
- ❑ **Fundamental Security Design Principles**
- ❑ **Attack Surfaces and Attack Trees**
- ❑ **A model for Network Security**
- ❑ **Standards**

Model for Network Security



not always the same

Necessary Tasks

1. **Design appropriate algorithm for security-related transformation**
2. **Generate secret information to be used with the algorithm**
3. **Develop methods to distribute and share secret information**
4. **Specify protocol that makes use of security algorithm and secret information to achieve particular security service**

Model for Network Access Security

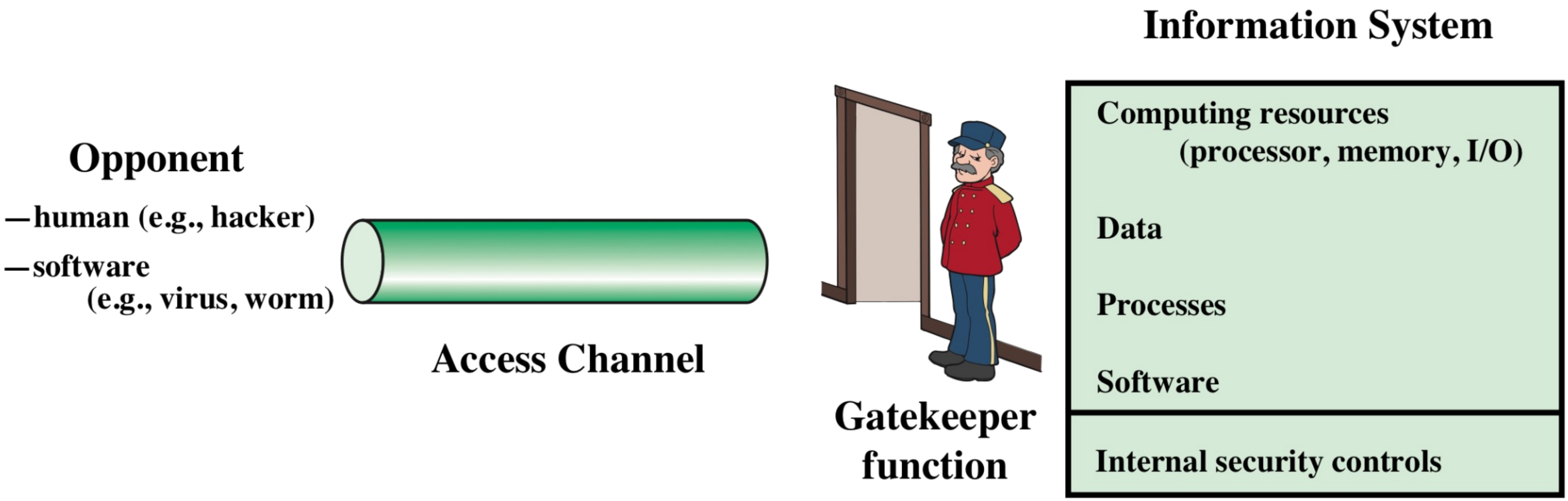


Figure 1.3 Network Access Security Model

Necessary Tasks

1. **Select appropriate gatekeeper functions to identify users**
2. **Implement internal security controls to ensure that authorized users can only access dedicated information and resources**

- **trusted computer systems can be used to implement this 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 inhi legitimate users

Outline

- ❑ Computer Security Concepts
- ❑ The OSI Security Architecture
- ❑ Security Attacks
- ❑ Security Services
- ❑ Security Mechanisms
- ❑ Fundamental Security Design Principles
- ❑ Attack Surfaces and Attack Trees
- ❑ A model for Network Security
- ❑ **Standards**

Standards

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

Summary

- **Computer security concepts**
  - Definition
  - Examples
  - Challenges
- **The OSI security architecture**
- **Security attacks**
  - Passive attacks
  - Active attacks

– Attack surfaces and attack trees

- **Security services**
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- **Security mechanisms**
- **Fundamental security design principles**
- **Network security model**
- **Standards**