COSC 734: Network Security
Chapter 1 - Introduction

Dr. Wei Yu
Dept. of Computer and Information Sciences
Towson University
Email: wyu@towson.edu

- 故用兵之法，无恃其不来，恃吾有以待之; 无恃其不攻，恃吾有所不可攻也。
  - 孙子兵法
- *The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.*
  - The Art of War, Sun Tzu

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

— On War, Carl Von Clausewitz

Outline

- Definition
- Attacks, security mechanisms and services
- Security attacks
- Security services
- Methods of Defense
- A model for Inter-network Security
- Internet standards and RFCs

Definition

- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission over the network
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks

- What about System Security? Examples?

Computer Security

- 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)

(NIST Computer Security Handbook [NIST95])

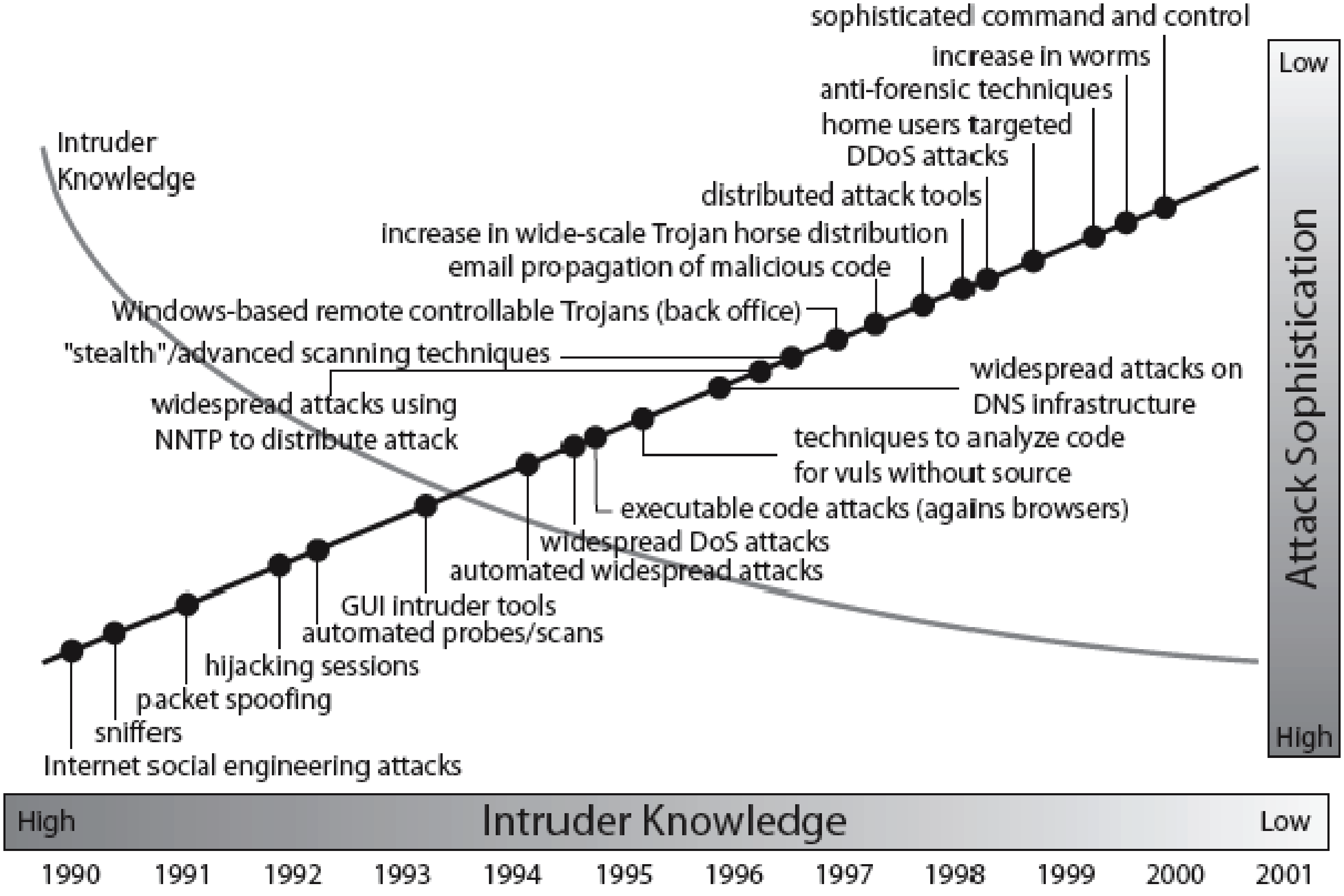
Security Problems

- Public, private, and government networks have been penetrated by unauthorized users and rogue programs
- Increased volume of security breaches attributed Computer Emergency Response Team (CERT) reports a tremendous increase in cracking incidents
- Outsider vs. Insider adversary

Security Concerns

- Distributed Denial of Service (DDoS) attacks
- Malicious code (worm) attacks (e.g., code red) and malwares
- Monitoring and capture of network traffic
  - User IDs, passwords, and other information are often stolen on Internet
  - User's privacy leakage
- Exploitation of software bugs
- Unauthorized access to resources
  - Disclosure, modification, and destruction of resources
- Compromised system used as hostile attack facility (example?)
- Masquerade as authorized user or end system
- Data driven attacks
  - Importation of malicious or infected code
- E-Mail forgery

Security Trend



Source: CERT

Fundamental Issues

- Lack of awareness of threats and risks of networked systems
  - Security measures are often not considered until an enterprise has been penetrated by malicious users
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access
- Vast majority of network traffic is unencrypted
  - Network traffic can be monitored and captured
  - More advanced computation resources for malicious usage

Fundamental Issues (cont.)

- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of security management and administration
- Exploitation of software (e.g., protocol implementation) bugs
  - Example: Sendmail bugs
- Cracker skills keep improving
- More ….

Attacks, Services and Mechanisms

- **Security Attack:** Any action that compromises the security of information.
- **Security Mechanism:** A mechanism that is designed to detect, prevent, or recover from a security attack.
- **Security Service:** A service that enhances the security of data processing systems and information transfers.
  - A security service makes use of one or more security mechanisms.

Security Attacks

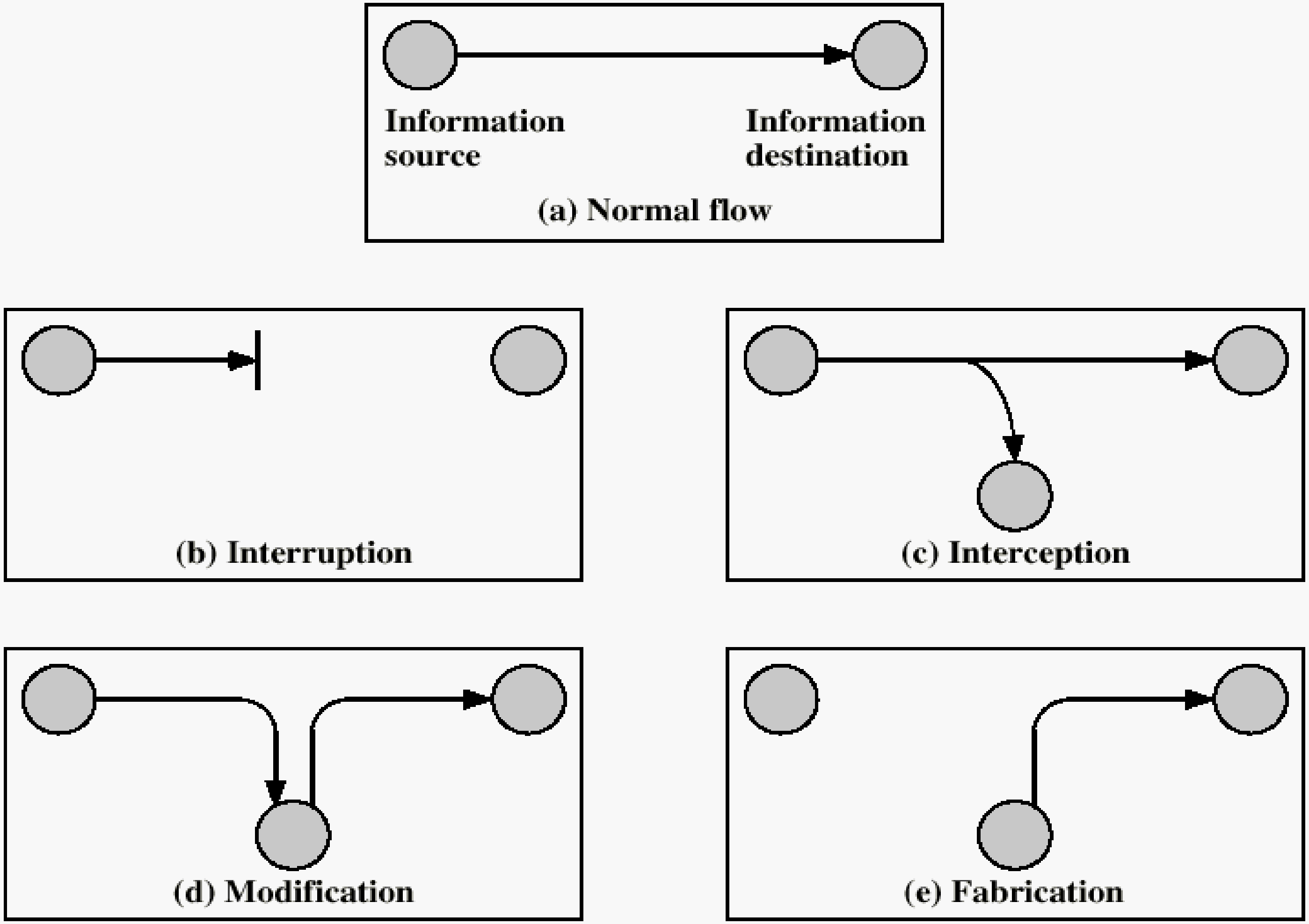
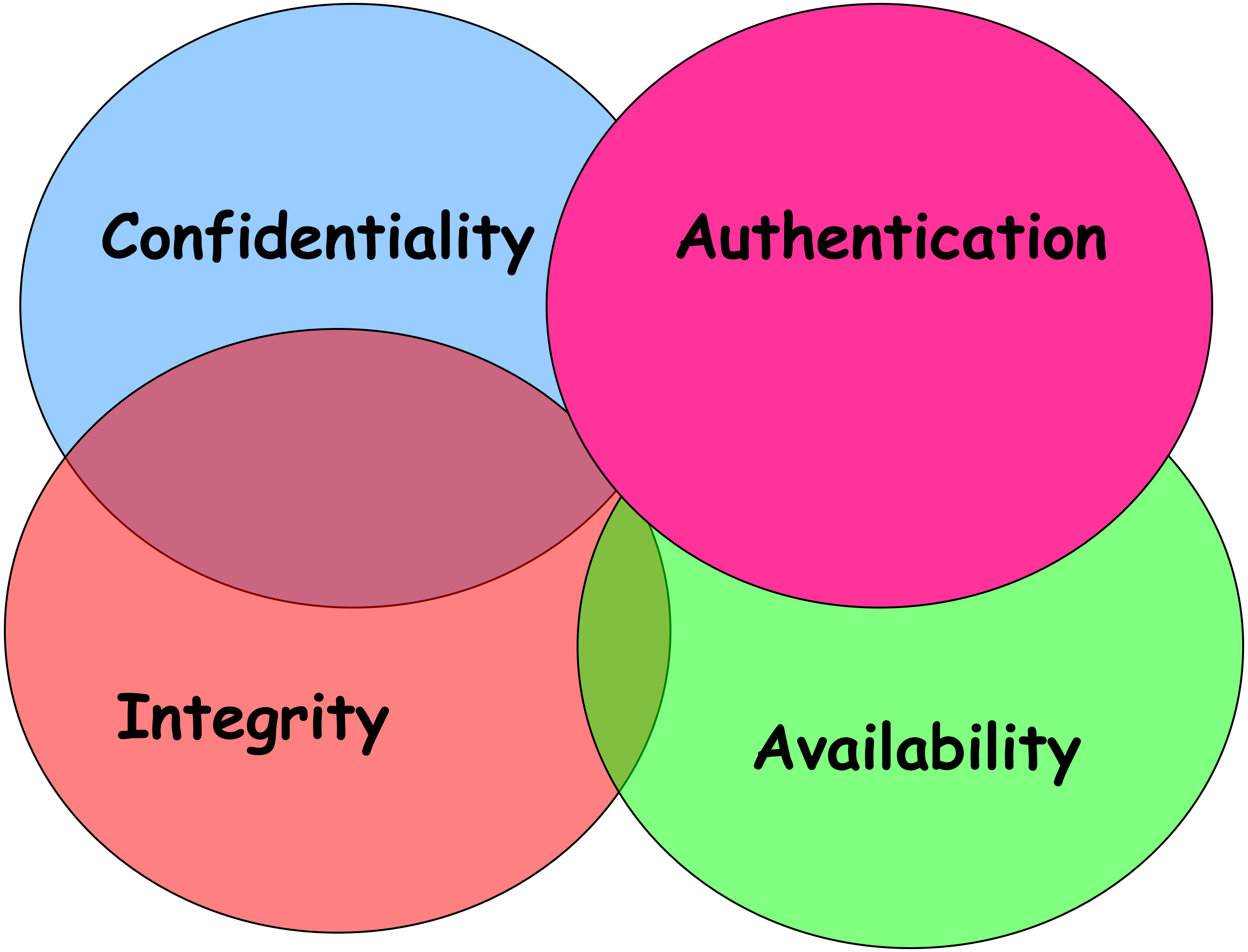


Figure 1.1 Security Threats

Security Attacks

- **Interruption:** *An* attack on availability
- **Interception:** *An* attack on confidentiality
- **Modification:** *A*ttack on integrity
- **Fabrication:** *A*ttack on authenticity

Security Goals



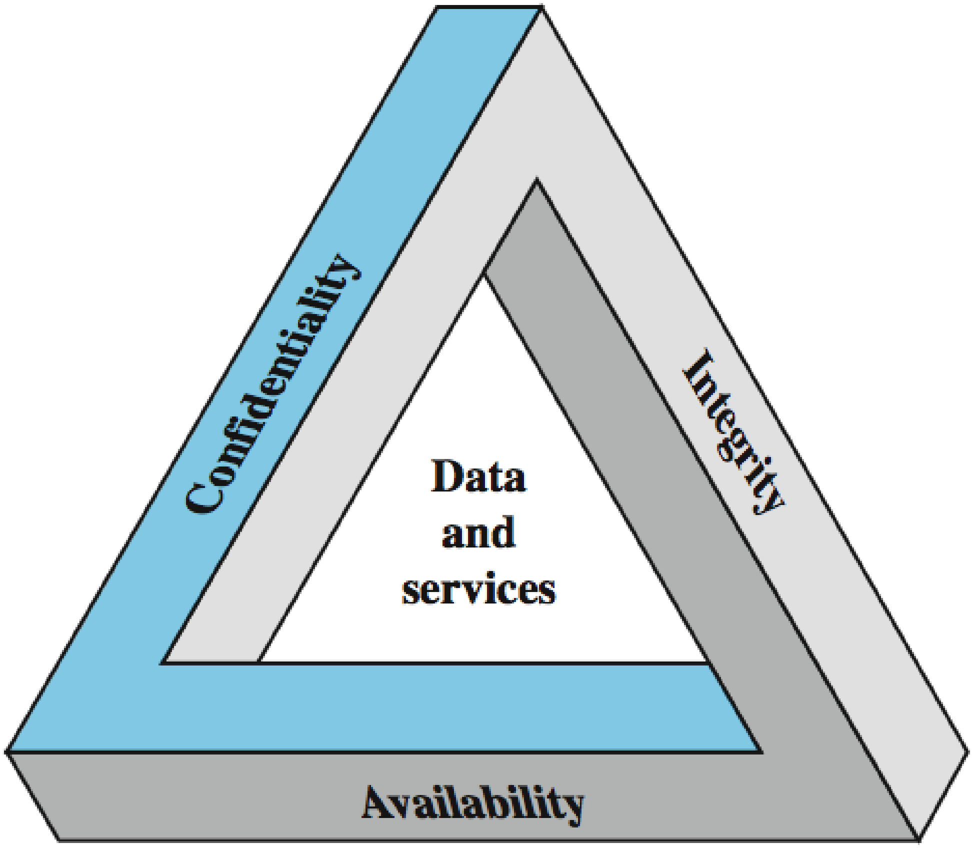
Confidentiality

Authentication

Integrity

Availability

Key Security Concepts (CIA)



Key Components (cont.)

- **Confidentiality (covers both data confidentiality and privacy)**: preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- **Integrity (covers both data and system integrity)**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Key Components (cont.)

- Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture.
- Two of the most commonly mentioned are:
  - **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - **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.

Security Goals: Examples

- Commercial
  - Confidentiality: An employee should not come to know the salary of his manager
  - Integrity: An employee should not be able to modify the employee's own salary
  - Availability: Paychecks should be printed on time as stipulated by law
- Military
  - Confidentiality: The target coordinates of a missile should not be improperly disclosed
  - Integrity :The target coordinates of a missile should not be improperly modified
  - Availability: When the proper command is issued the missile should fire immediately

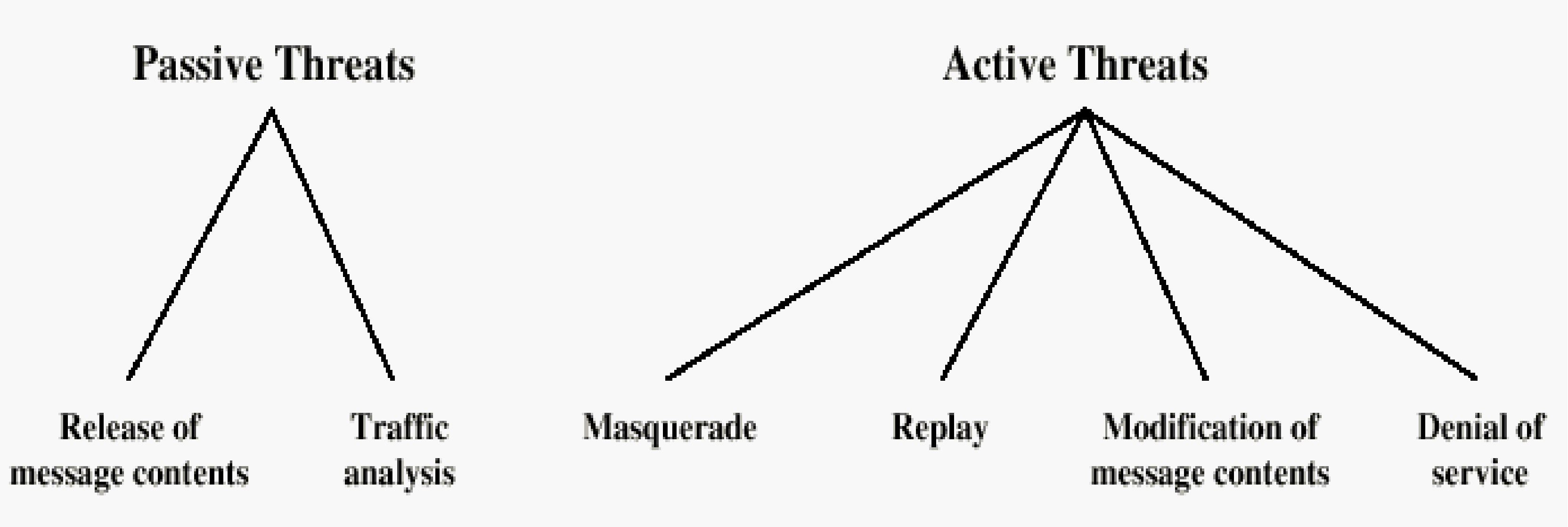
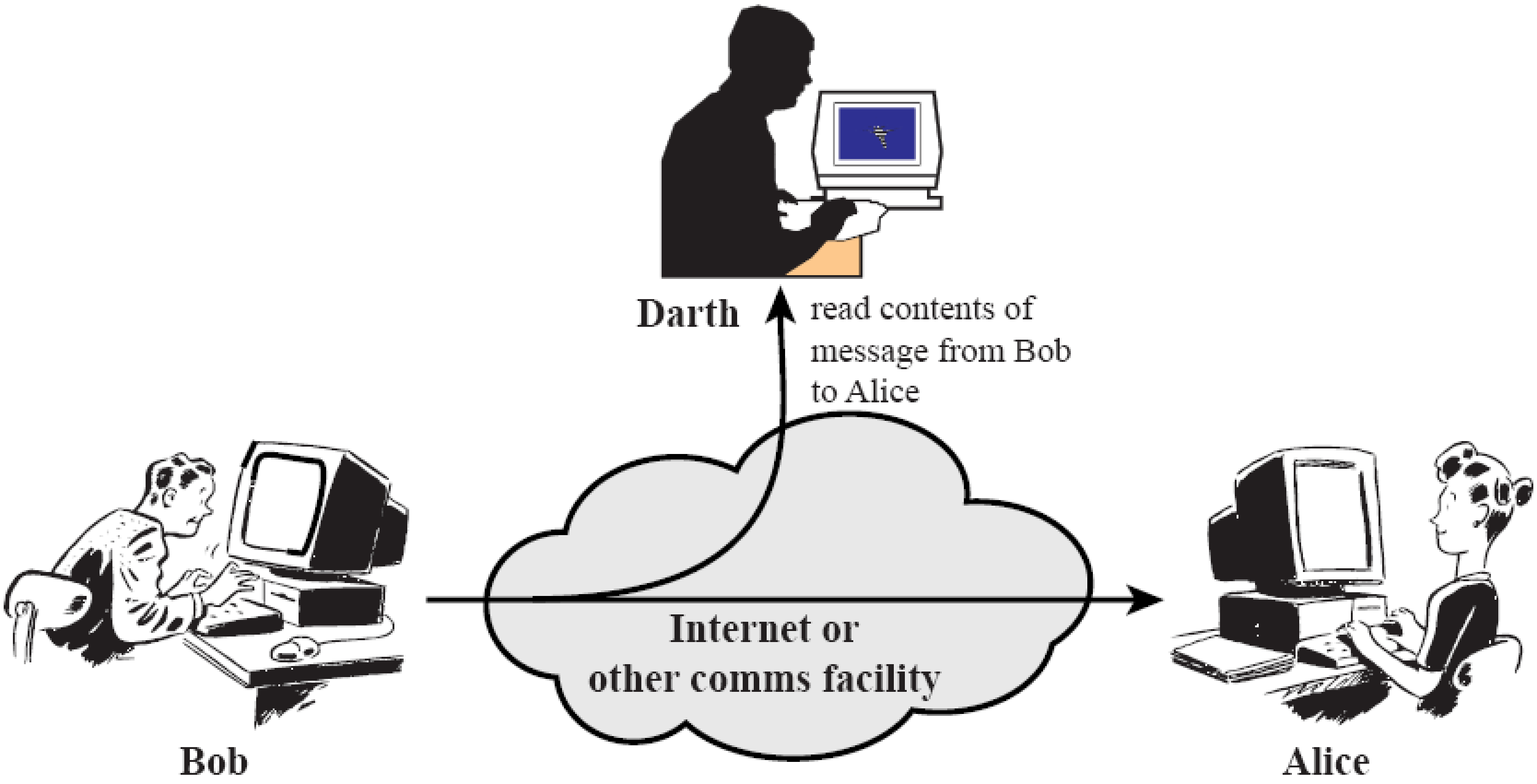
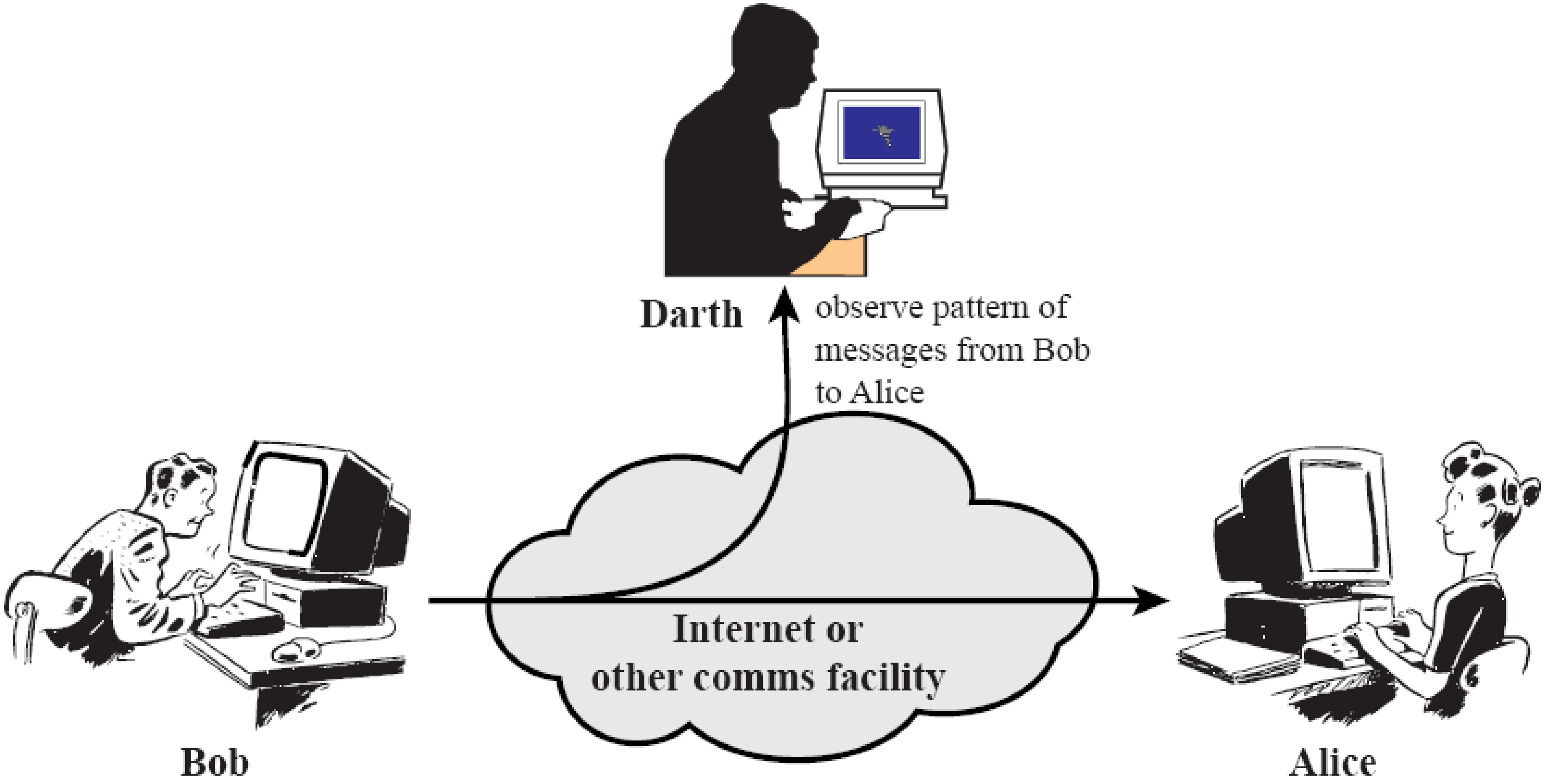


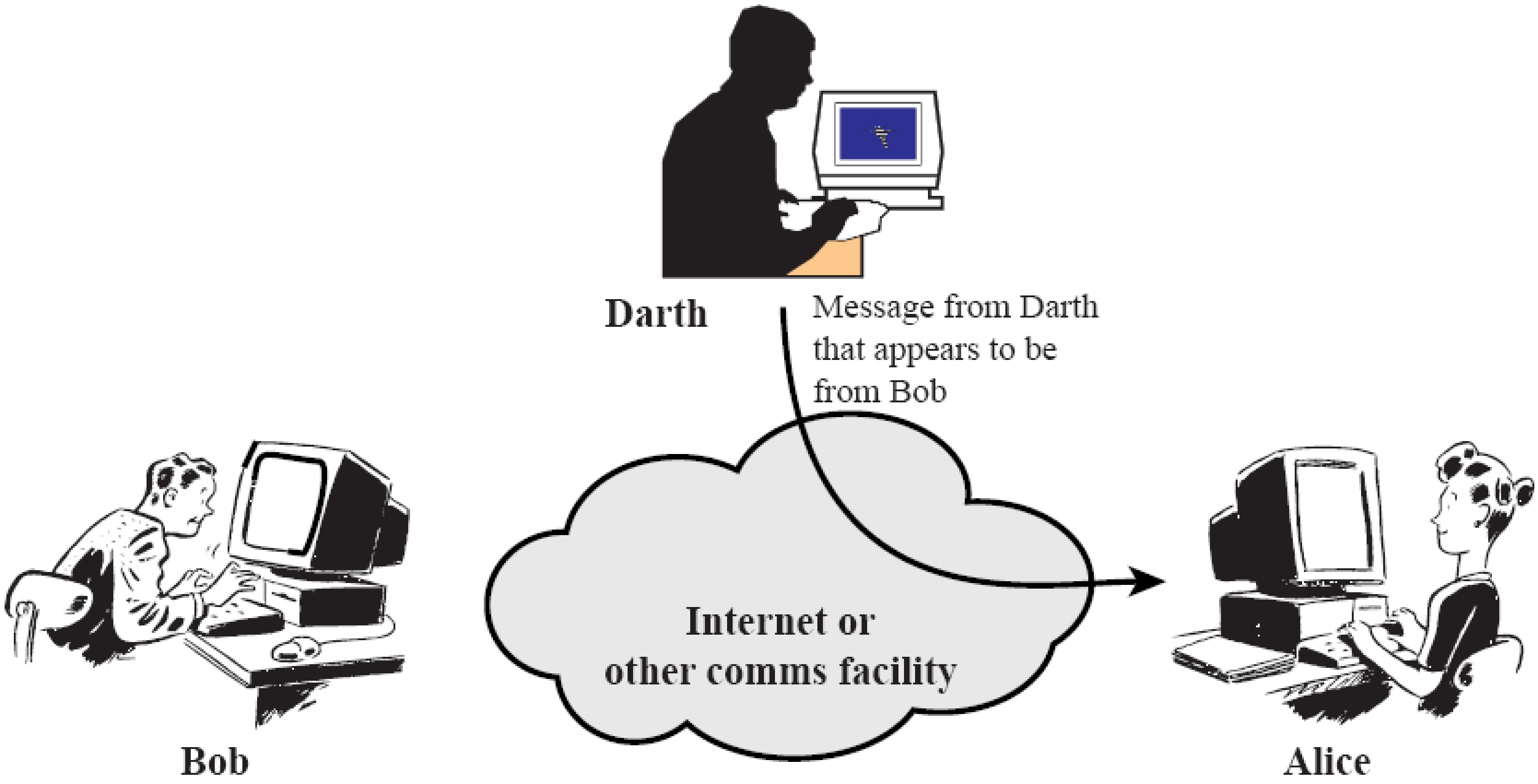
Figure 1.2 Active and Passive Security Threats


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

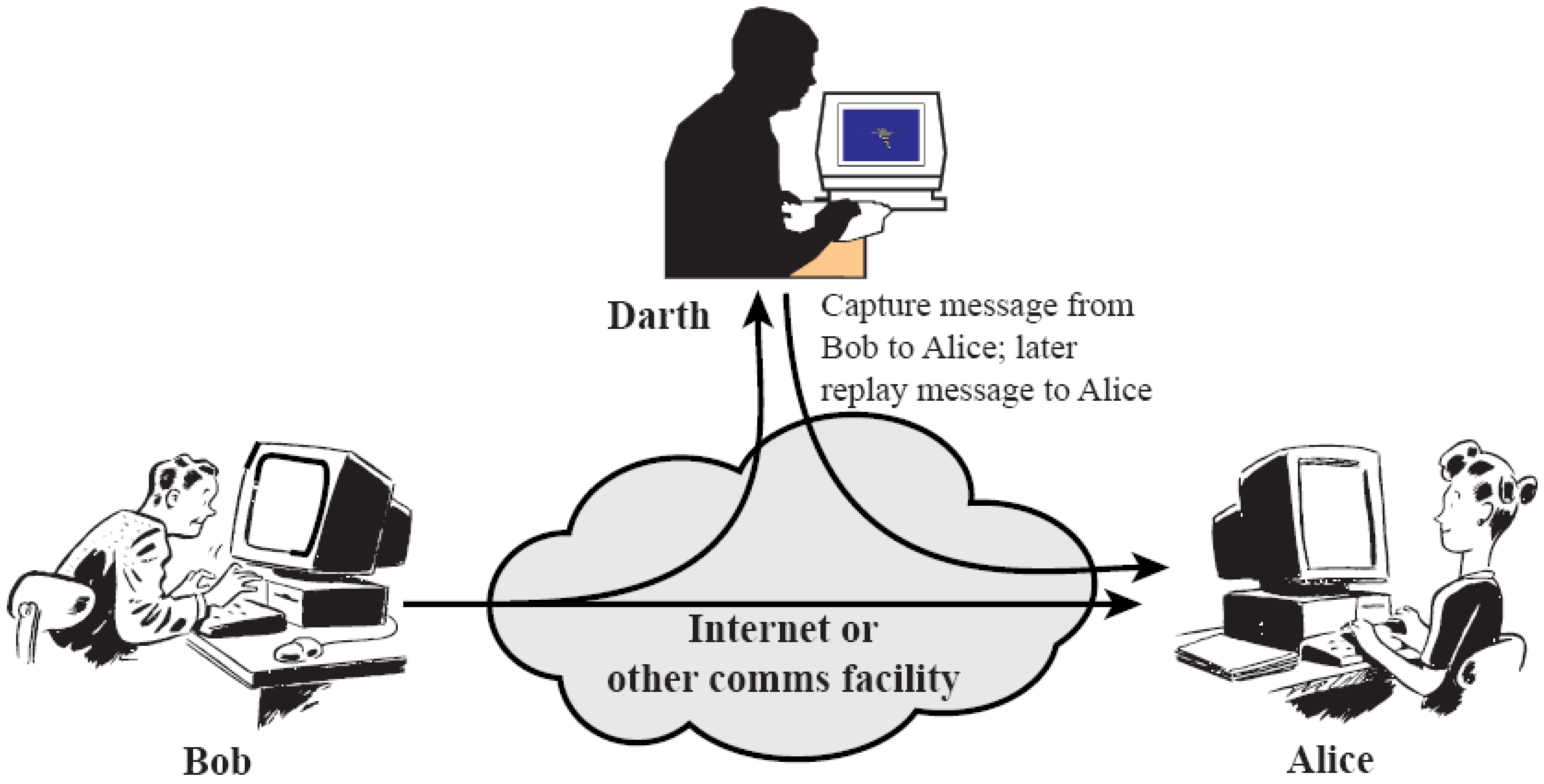
(a) Release of message contents


Darth
observe pattern of messages from Bob to Alice
Internet or other comms facility
Bob
Alice

(b) Traffic analysis

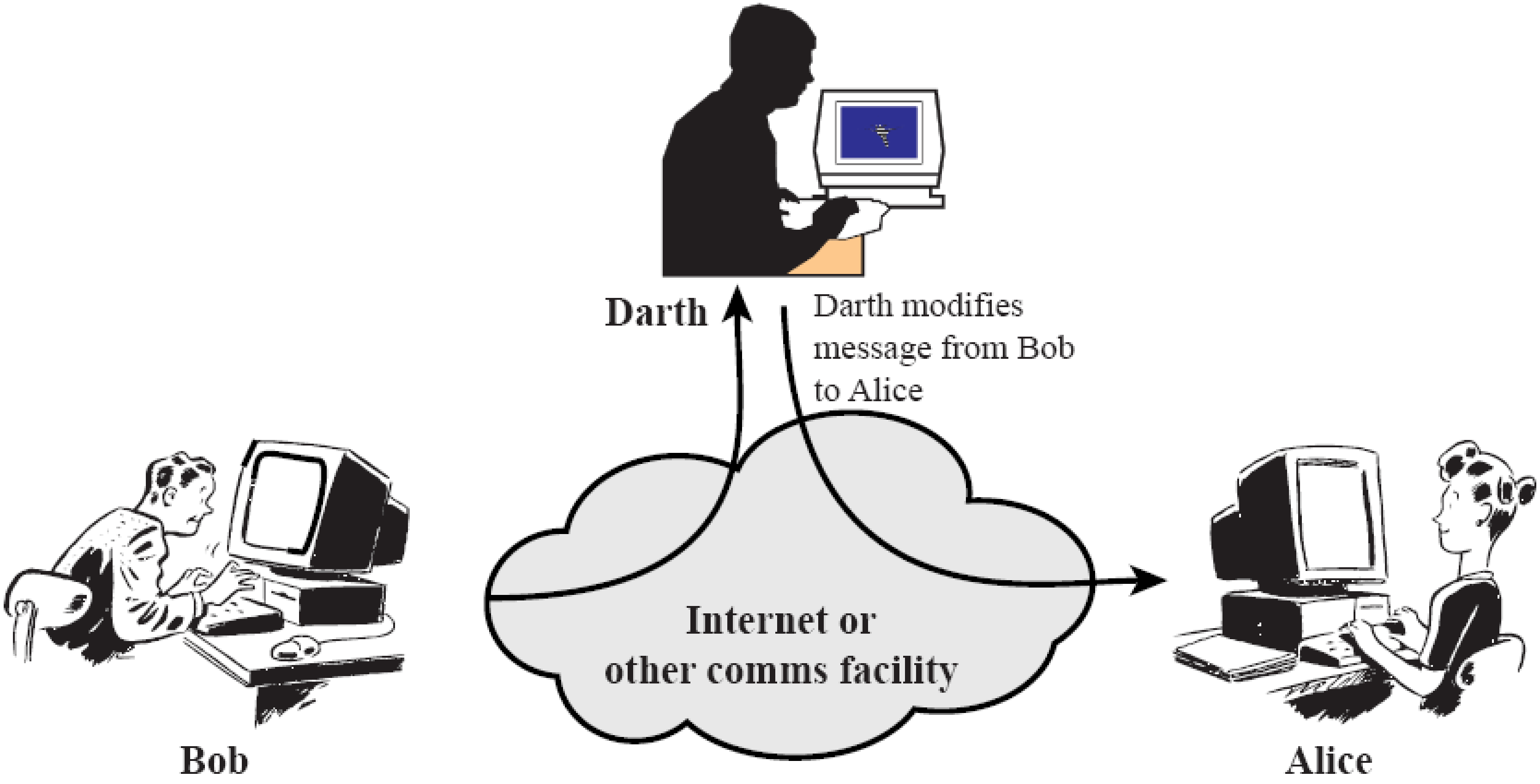


(a) Masquerade

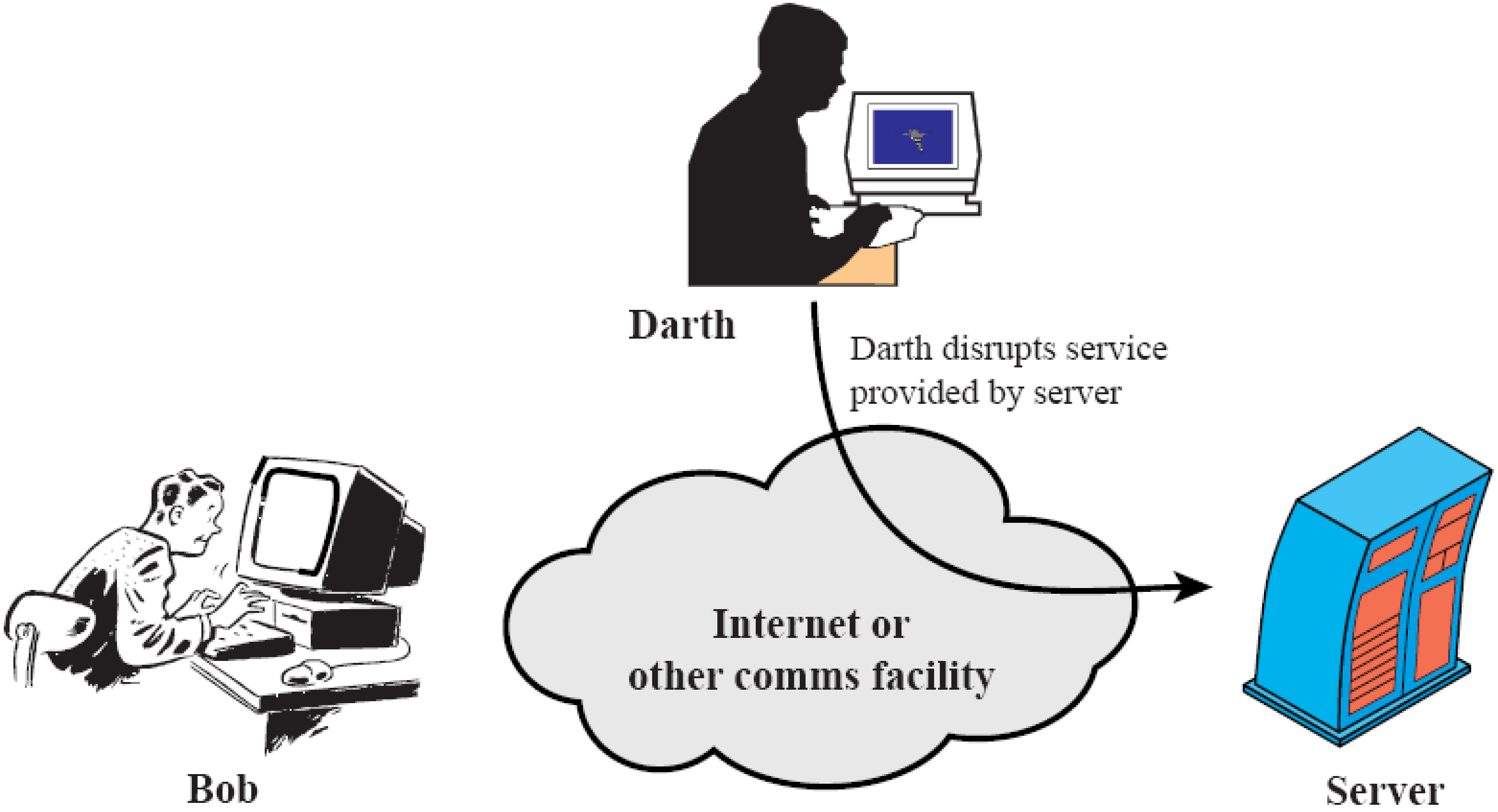

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

(b) Replay

Figure 1.2 Active Attacks (page 1 of 2)



(c) Modification of messages


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

(d) Denial of service

Figure 1.2 Active Attacks (page 2 of 2)

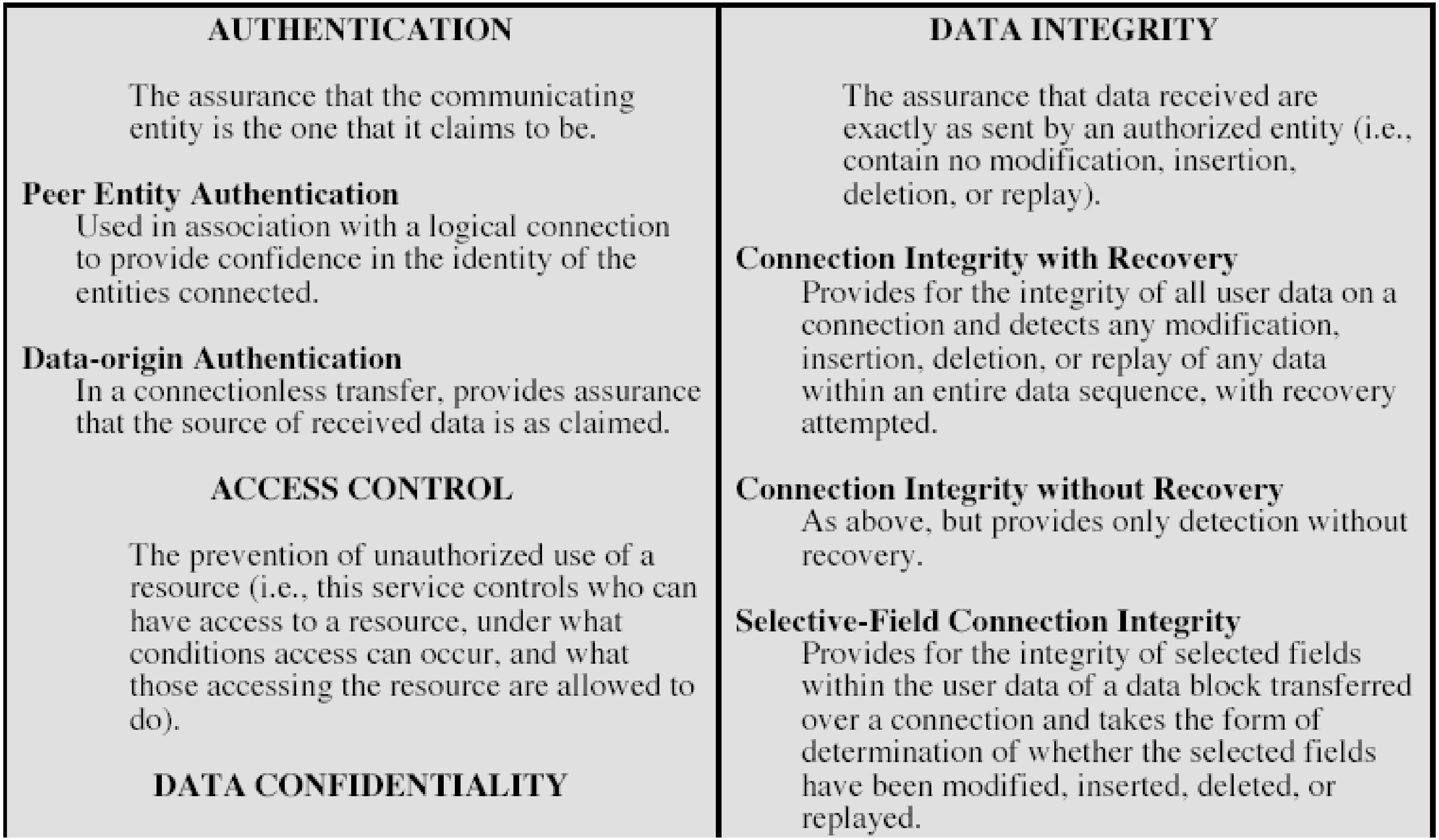
Example of Traffic Analysis Attack

- Passive and Active
- Attack and Defense
- More Discussion?

Security Services

- Confidentiality (privacy/secrecy)
- Authentication (who created or sent the data)
- Integrity (has not been altered)
- Non-repudiation (the order is final)
- Access control (prevent misuse of resources)
- Availability (permanence, non-erasure)
  - Denial of Service Attacks
  - Virus that deletes files

Table 1.2 Security Services (X.800)



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

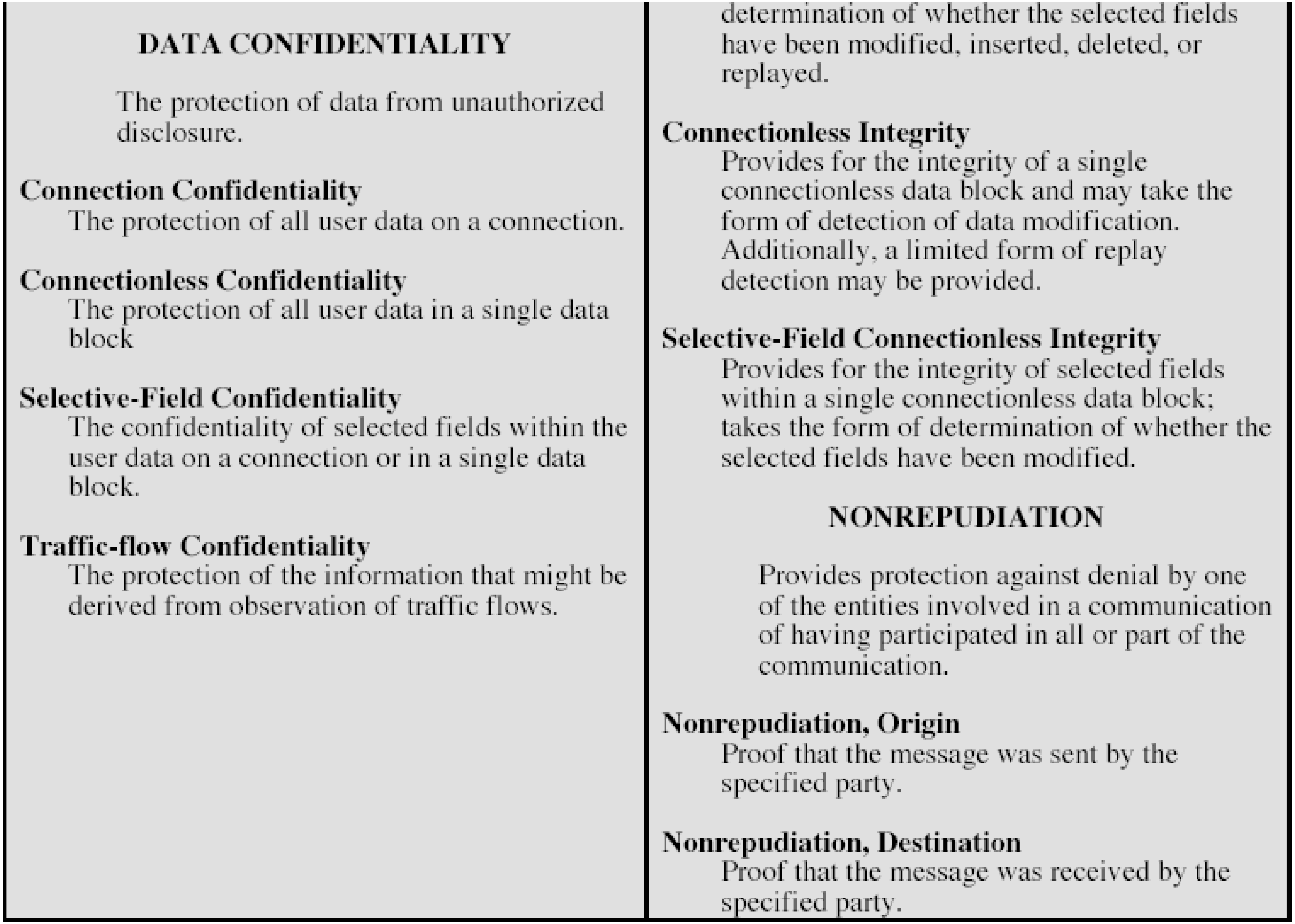
DATA INTEGRITY

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.



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.

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.

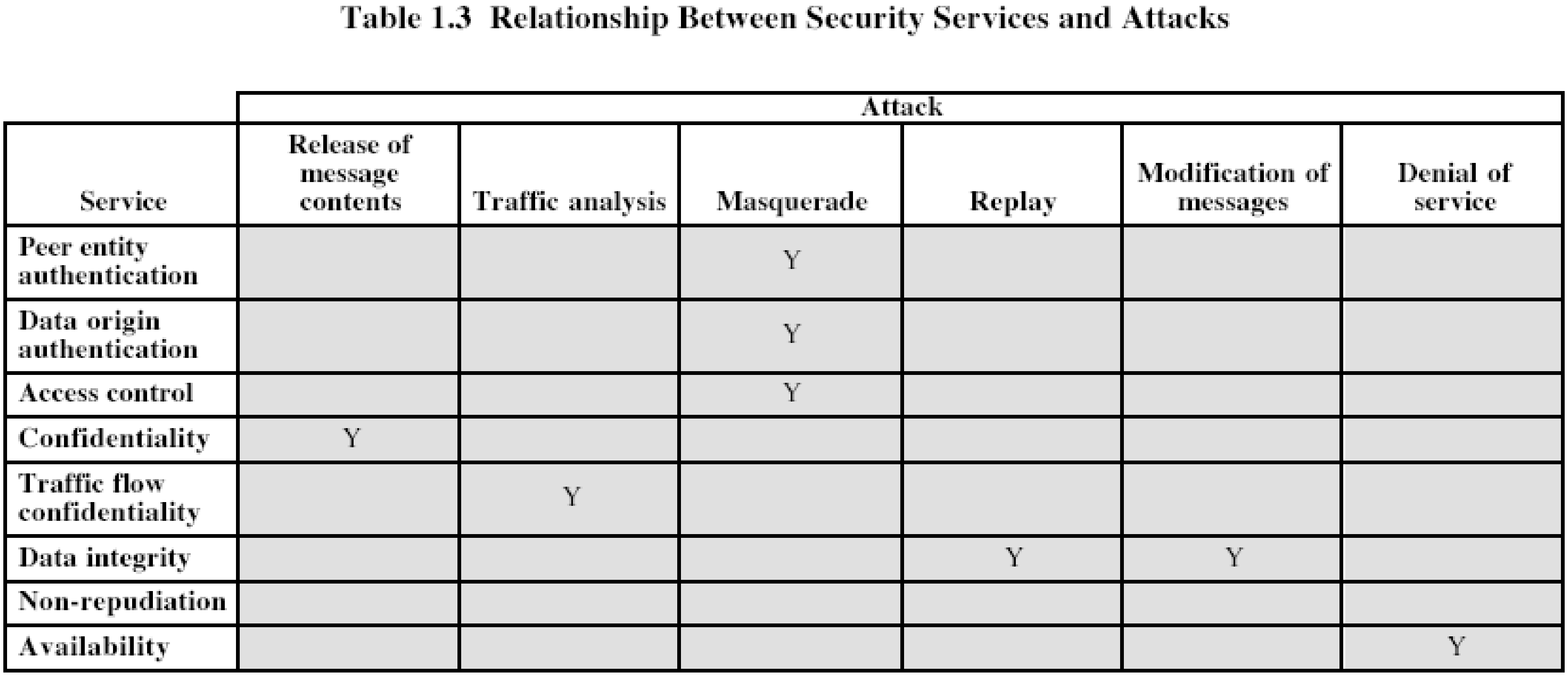


Table 1.3 Relationship Between Security Services and Attacks

	Attack					
Service	Release of message contents	Traffic analysis	Masquerade	Replay	Modification of messages	Denial of service
Peer entity authentication			Y			
Data origin authentication			Y			
Access control			Y			
Confidentiality	Y					
Traffic flow confidentiality		Y				
Data integrity				Y	Y	
Non-repudiation						
Availability						Y

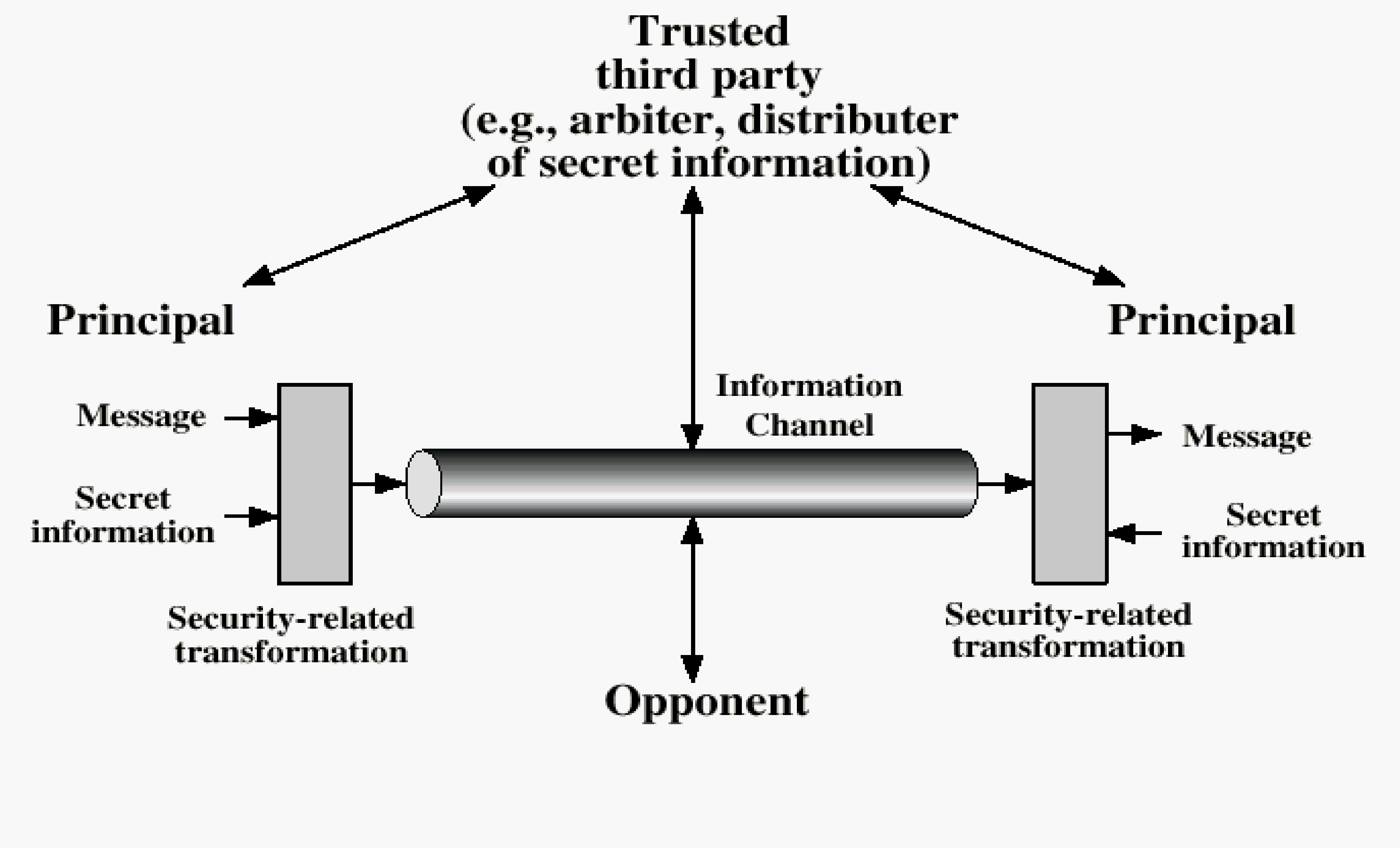


Figure 1.3 Model for Network Security

Model of Network Security

- Using this model requires us to:
  - Design a suitable algorithm for the security transformation
  - Generate the secret information (keys) used by the algorithm
  - Develop methods to distribute and share the secret information
  - Specify a protocol enabling the principals to use the transformation and secret information for a security service

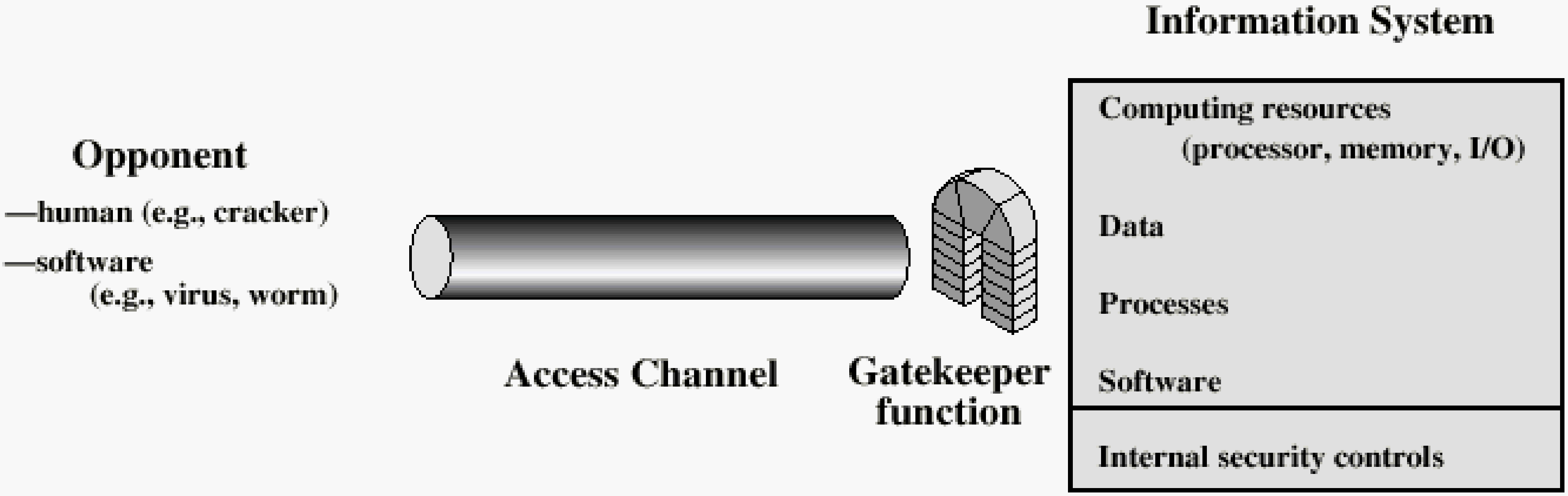
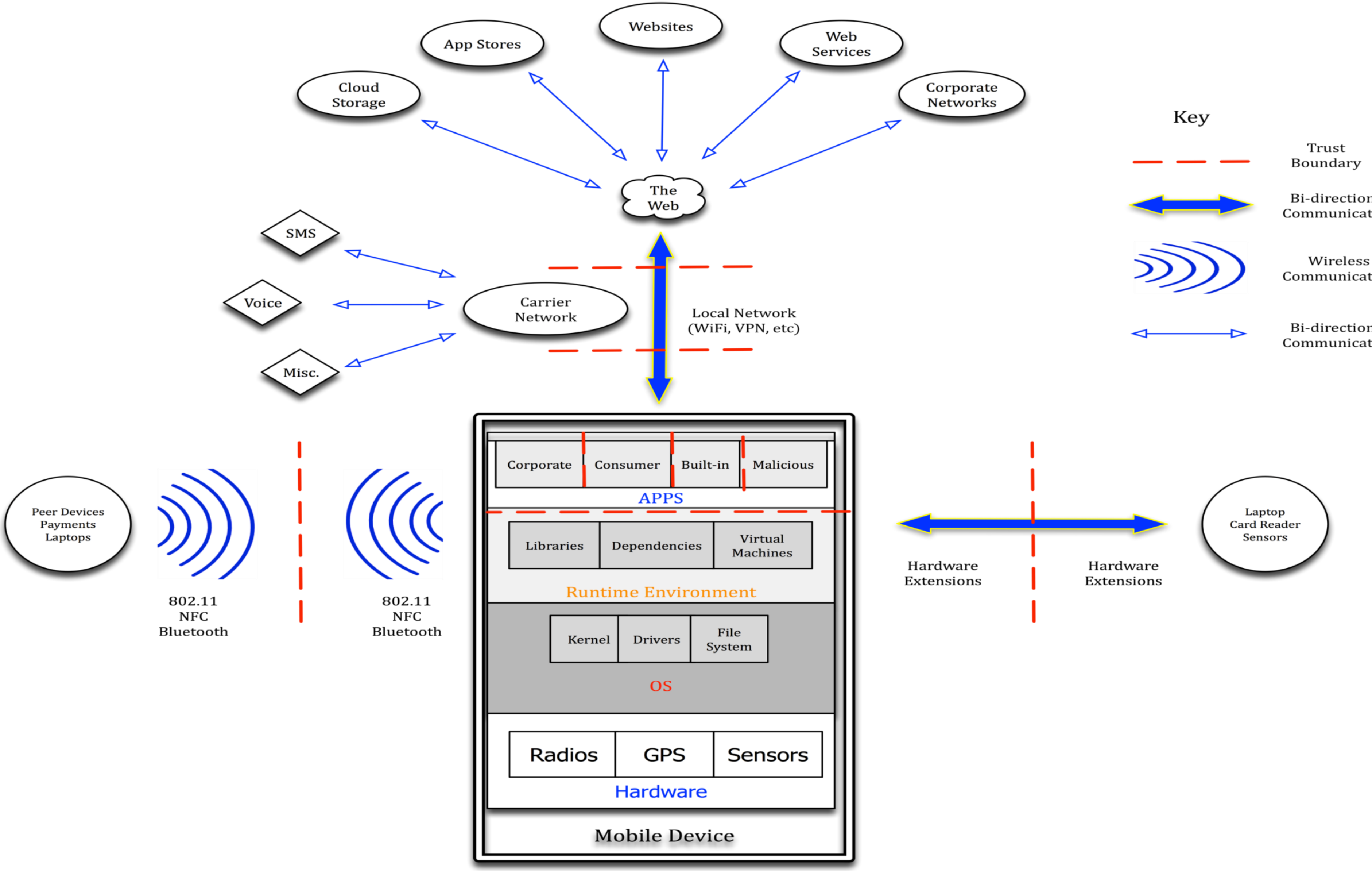


Figure 1.4 Network Access Security Model

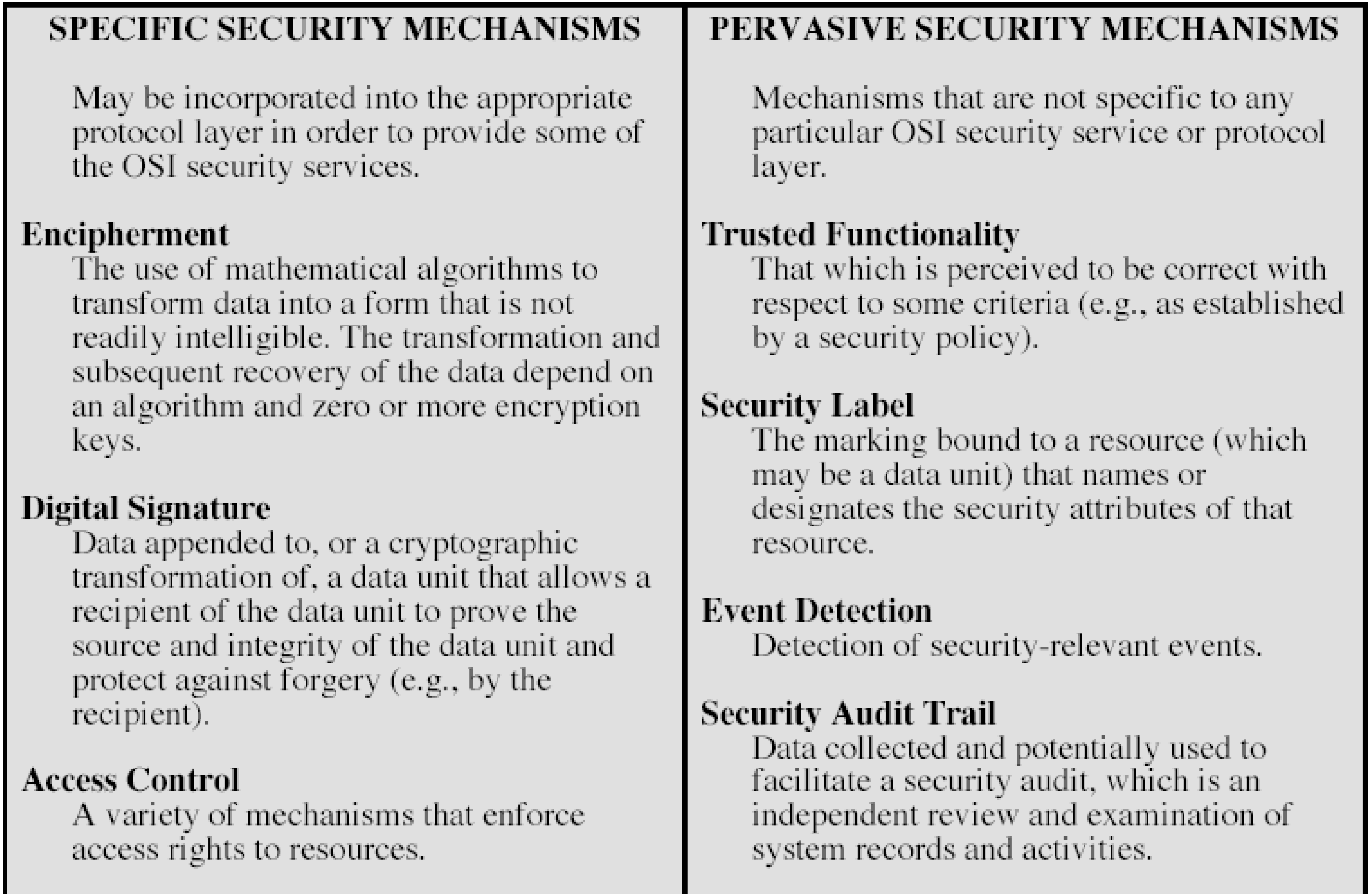
Example: A Mobile Threat Model



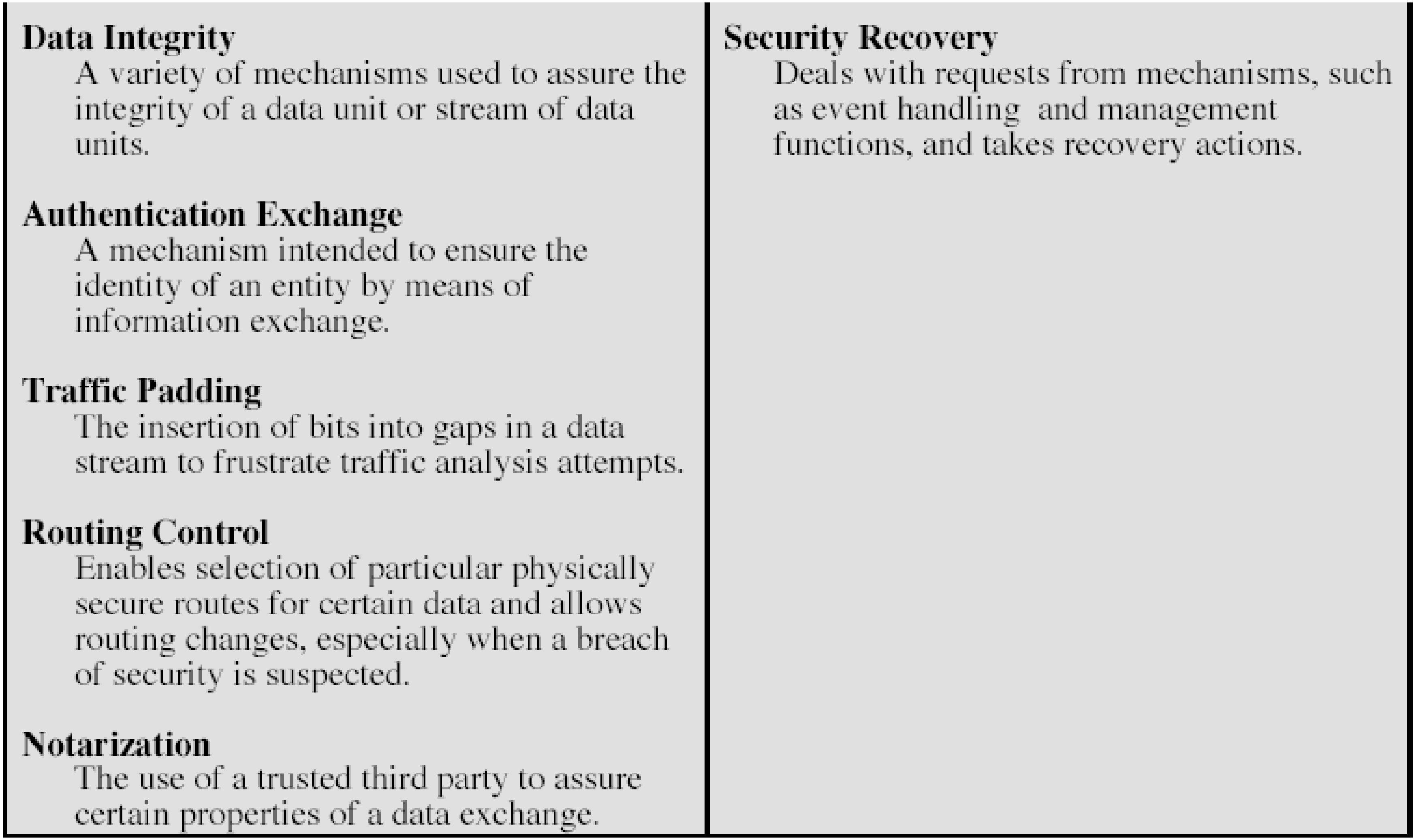
Methods of Defense

- Encryption
- Software Controls (access limitations in a data base, in operating system protect each user from other users)
- Hardware Controls (smartcard)
- Policies (frequent changes of passwords, firewall allow/deny rules)
- Physical Controls

Table 1.4 Security Mechanisms (X.800)



SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
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.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
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).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**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.



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.

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

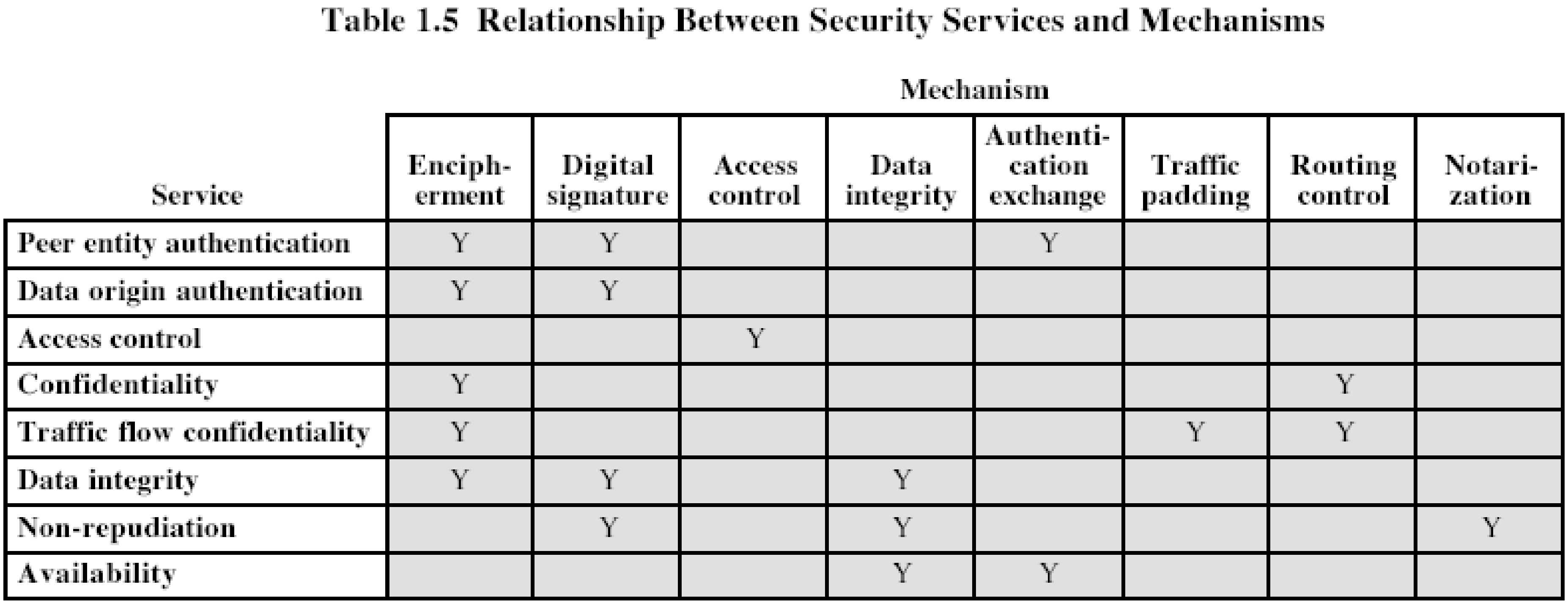


Table 1.5 Relationship Between Security Services and Mechanisms

	Mechanism							
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				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

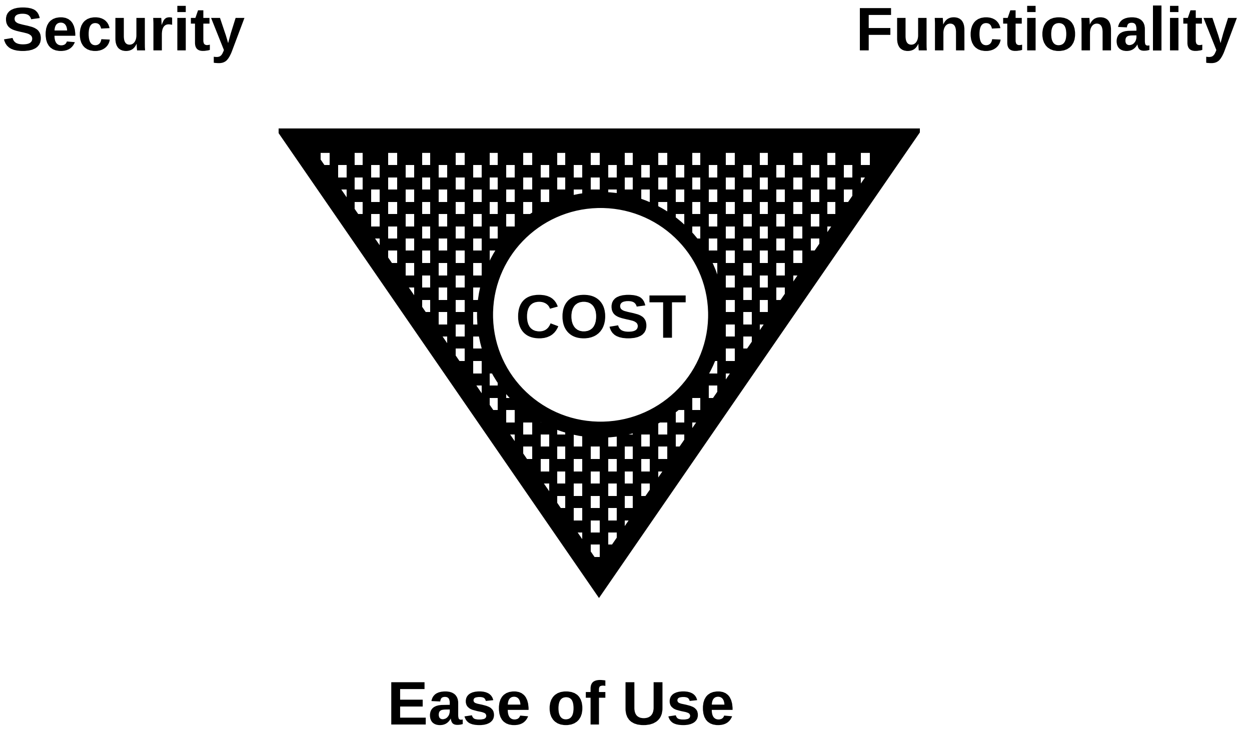
Security by Obscurity

- Security by obscurity says that if we hide the inner workings of a system it will be secure
- It is a bad idea.
- Why?
  - Less and less applicable in the emerging world of vendor-independent open standards
  - Less and less applicable in a world of widespread computer knowledge and expertise

Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- It is a bad idea
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder
- User awareness and cooperation is important, but cannot be the principal focus for achieving security

Security Tradeoffs



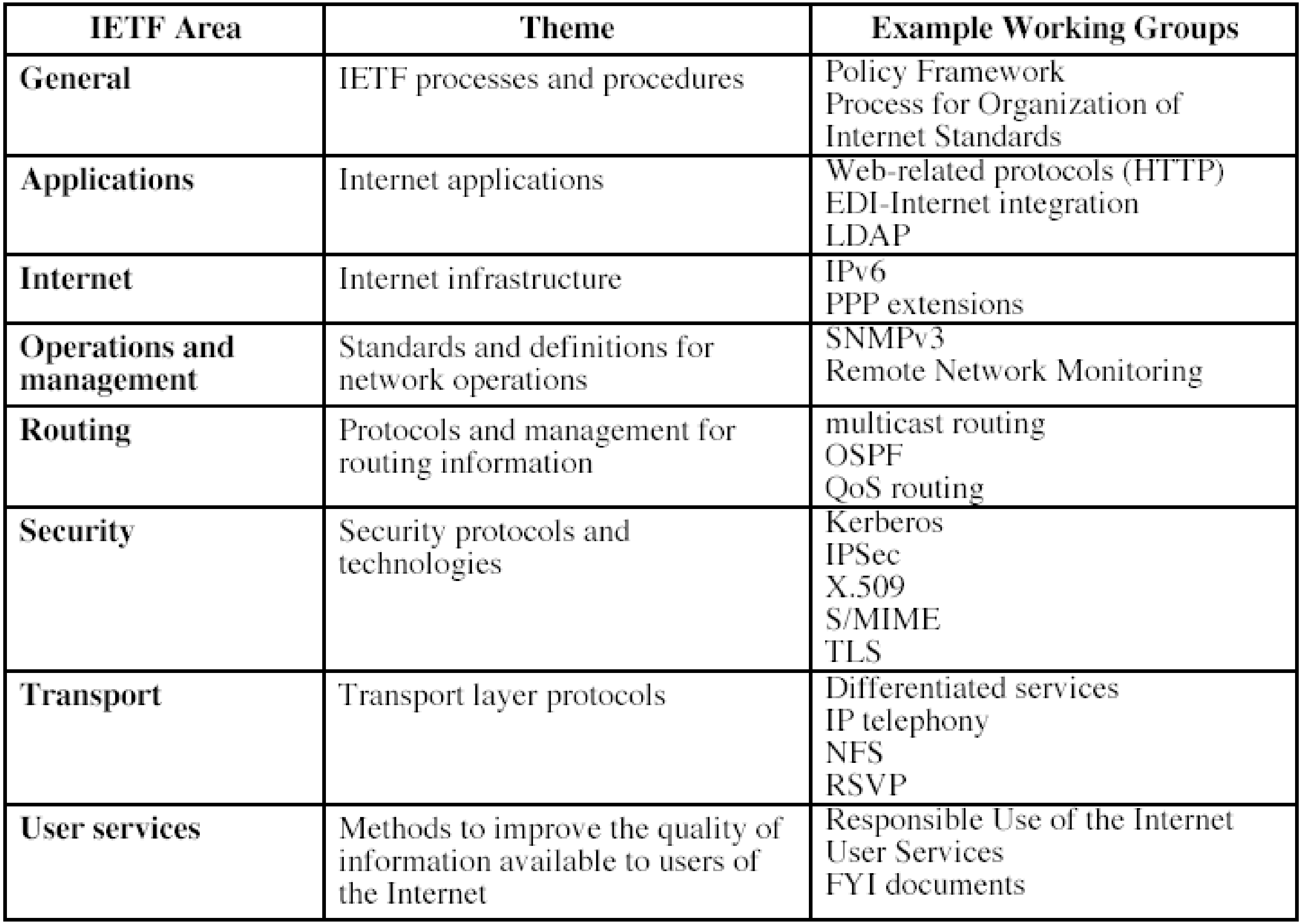
Threat-Vulnerability-Risk

- Threats — Possible attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm
- Risk — A measure of the possibility of security breaches and severity of the ensuing damage
- Requires assessment of threats and vulnerabilities
- Risk analysis
  - Mathematical formulae and computer models can be developed, but the underlying parameters are difficult to estimate.

Internet standards and RFCs

- The Internet society
  - Internet Architecture Board (IAB)
  - Internet Engineering Task Force (IETF)
  - Internet Engineering Steering Group (IESG)

Table 1.6 IETF Areas



IETF Area	Theme	Example Working Groups
General	IETF processes and procedures	Policy Framework Process for Organization of Internet Standards
Applications	Internet applications	Web-related protocols (HTTP) EDI-Internet integration LDAP
Internet	Internet infrastructure	IPv6 PPP extensions
Operations and management	Standards and definitions for network operations	SNMPv3 Remote Network Monitoring
Routing	Protocols and management for routing information	multicast routing OSPF QoS routing
Security	Security protocols and technologies	Kerberos IPSec X.509 S/MIME TLS
Transport	Transport layer protocols	Differentiated services IP telephony NFS RSVP
User services	Methods to improve the quality of information available to users of the Internet	Responsible Use of the Internet User Services FYI documents

Internet RFC Publication Process

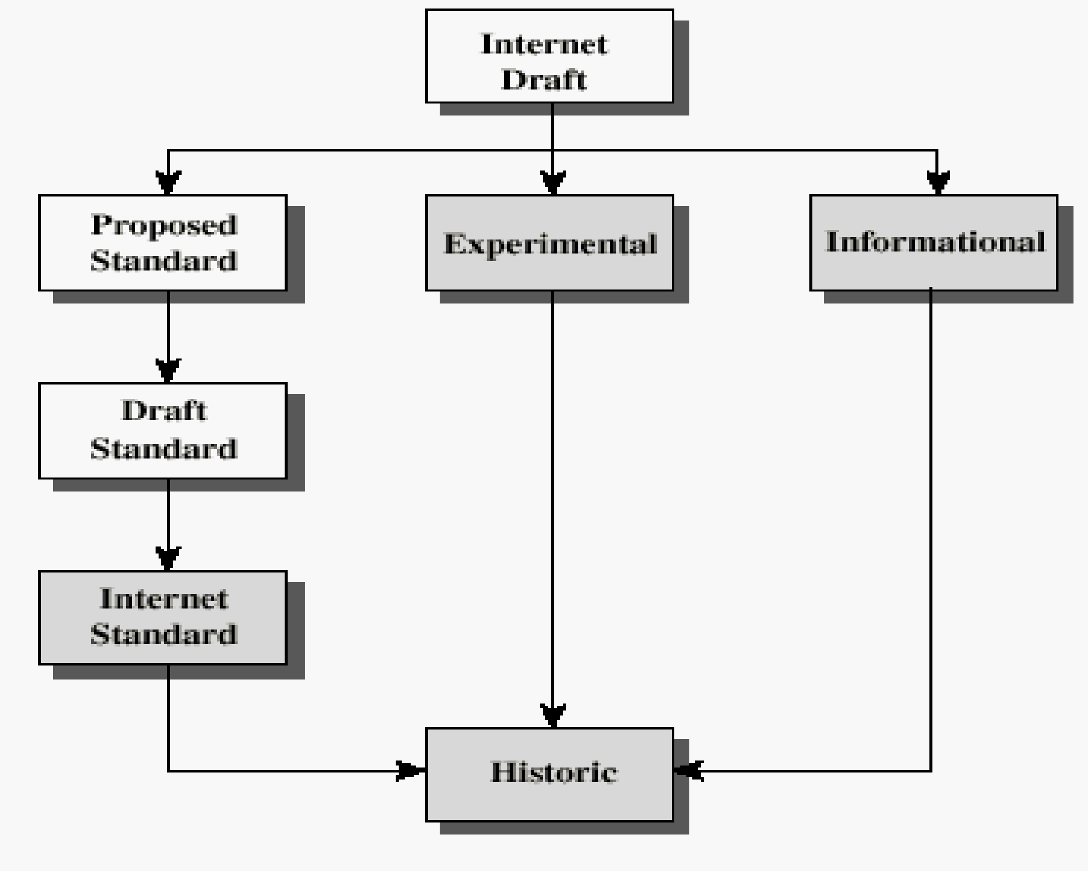


Figure 1.5 Internet RFC Publication Process

Recommended Reading

- Pfleeger, C. *Security in Computing.* Prentice Hall, 1997.
- Mel, H.X. Baker, D. *Cryptography Decrypted*. Addison Wesley, 2001.