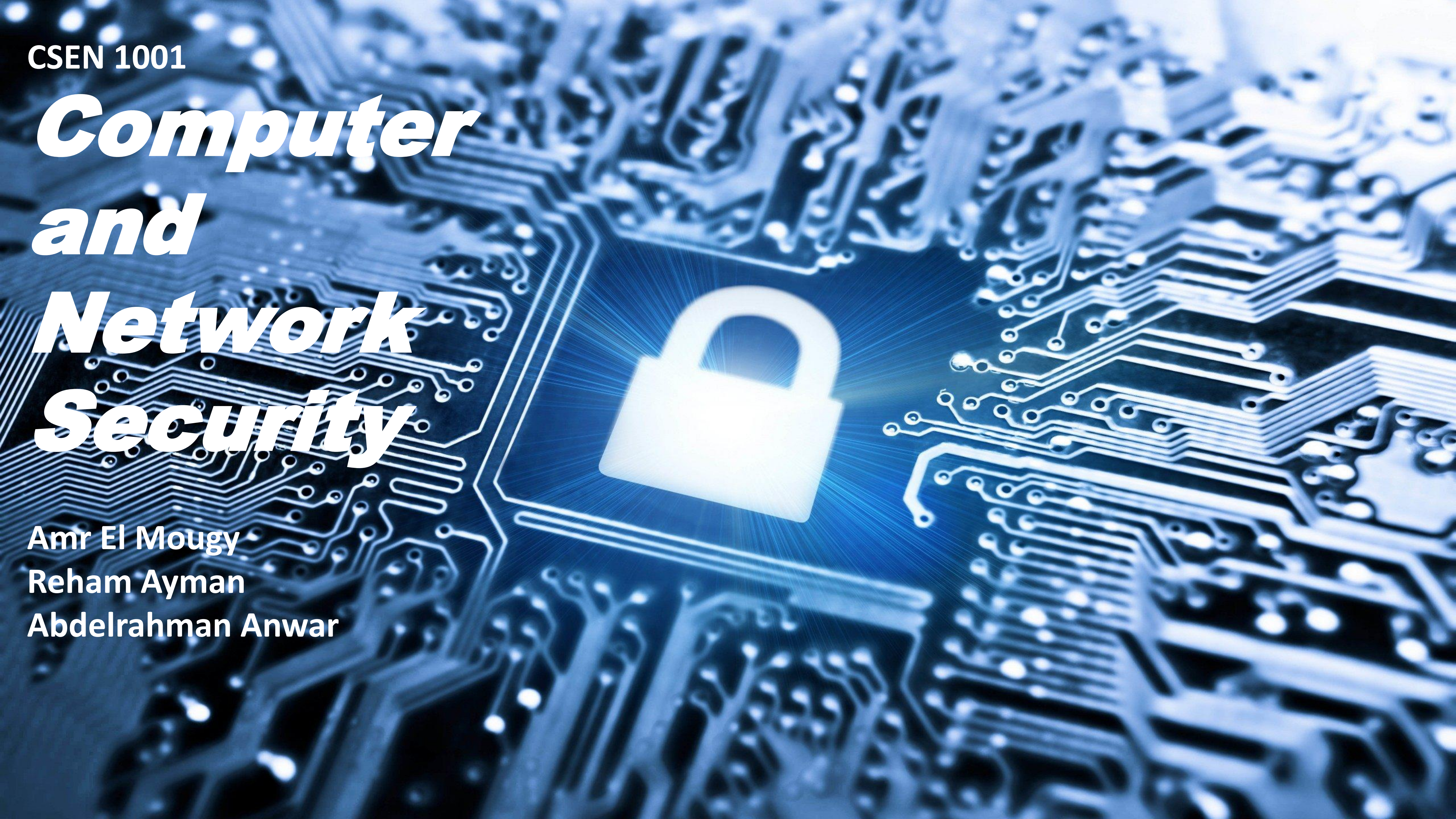
CSEN 1001

Computer and Network Security

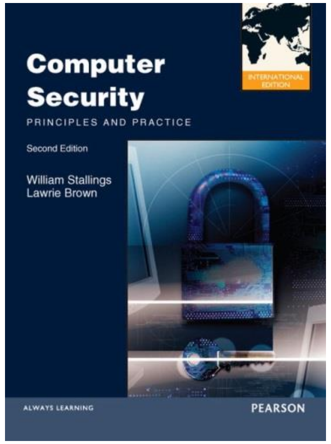


Amr El Mougy
Reham Ayman
Abdelrahman Anwar

Course Details

Week	Lectures	Tutorials
1	Intro + Classical Crypto	
2	Symmetric Encryption AES	PA1 Classical Cryptography
3	Modes of Encryption	Task 1 Classical Cryptanalysis
4	Public Key Cryptography + RSA	Introduction to Euler Sieve
5	Message Authentication – part 1	PA2 RSA
6	Message Authentication – part 2	Task 2 Breaking RSA using Euler Sieve
7	Blockchains	PA3 Authentication
8	Key Management 1	Task 3 Intrusion Detection using ML
9	Key Management 2	PA4 Blockchains
10	User Authentication	Task 4 Certificate Authority
11	Elliptic Curve Cryptography	PA5 Key Management
12	Network Security/Software Security	PA6 Elliptic Curve Cryptography

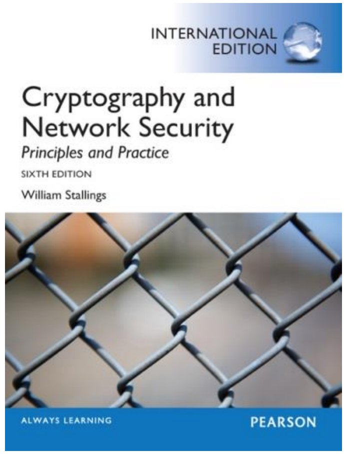
Course Details



- Text books and lecture slides:

  Authors: William Stallings and Lawrie Brown
  Title: Computer Security, Principles and Practice, 2nd Edition
  Publisher: Pearson Education, Inc., 2012

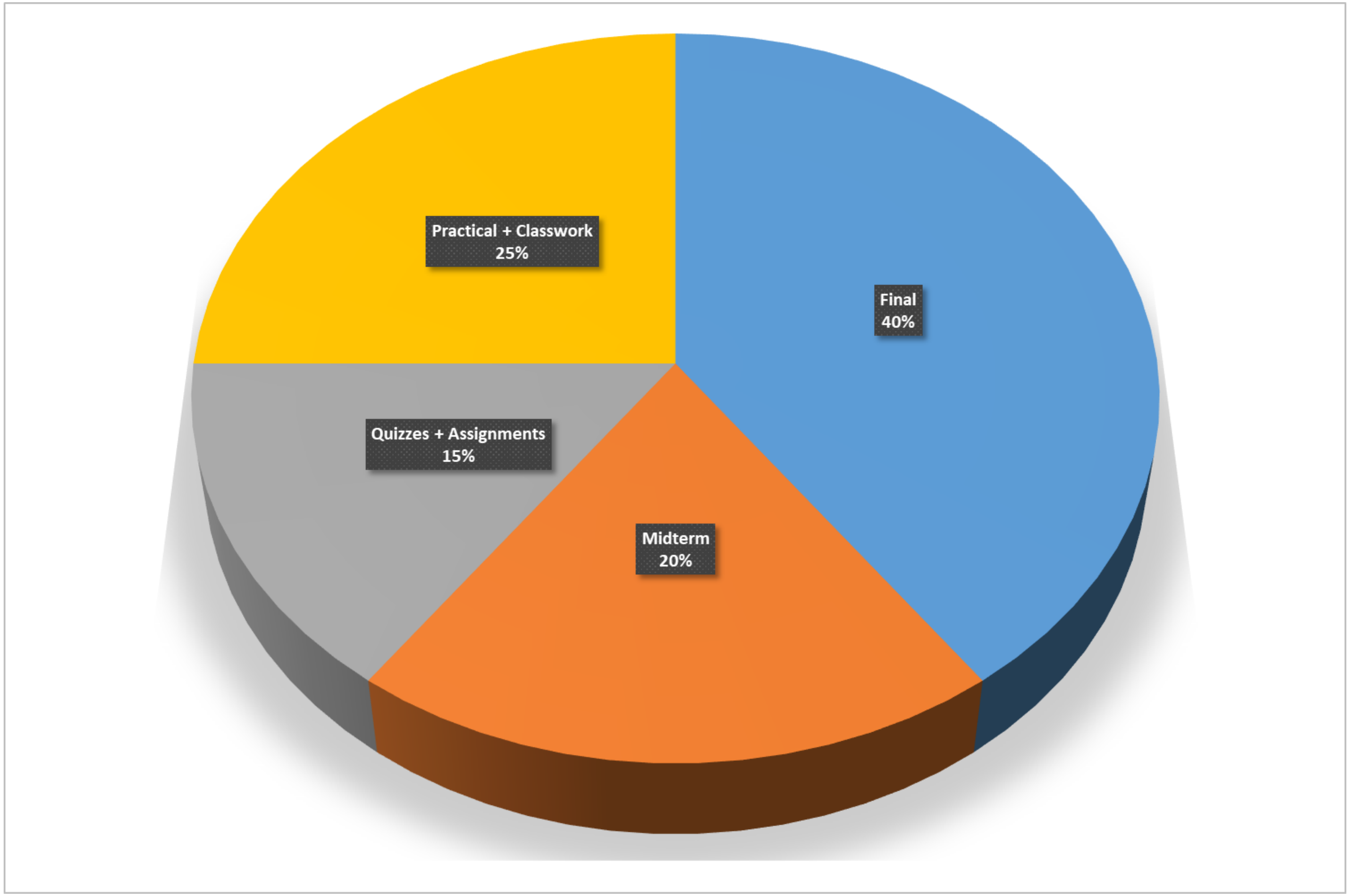
  Author: William Stallings
  Title: Cryptography and Network Security, 6th Edition
  Publisher: Pearson Education, Inc., 2014



- Note:

  These slides are not meant to be comprehensive lecture notes! They are only remarks and pointers. The material presented here is not sufficient for studying for the course. Your main sources for studying are the text and your own lecture notes

Course Details



Lecture (1)

Introduction and Key Security Concepts

Definitions

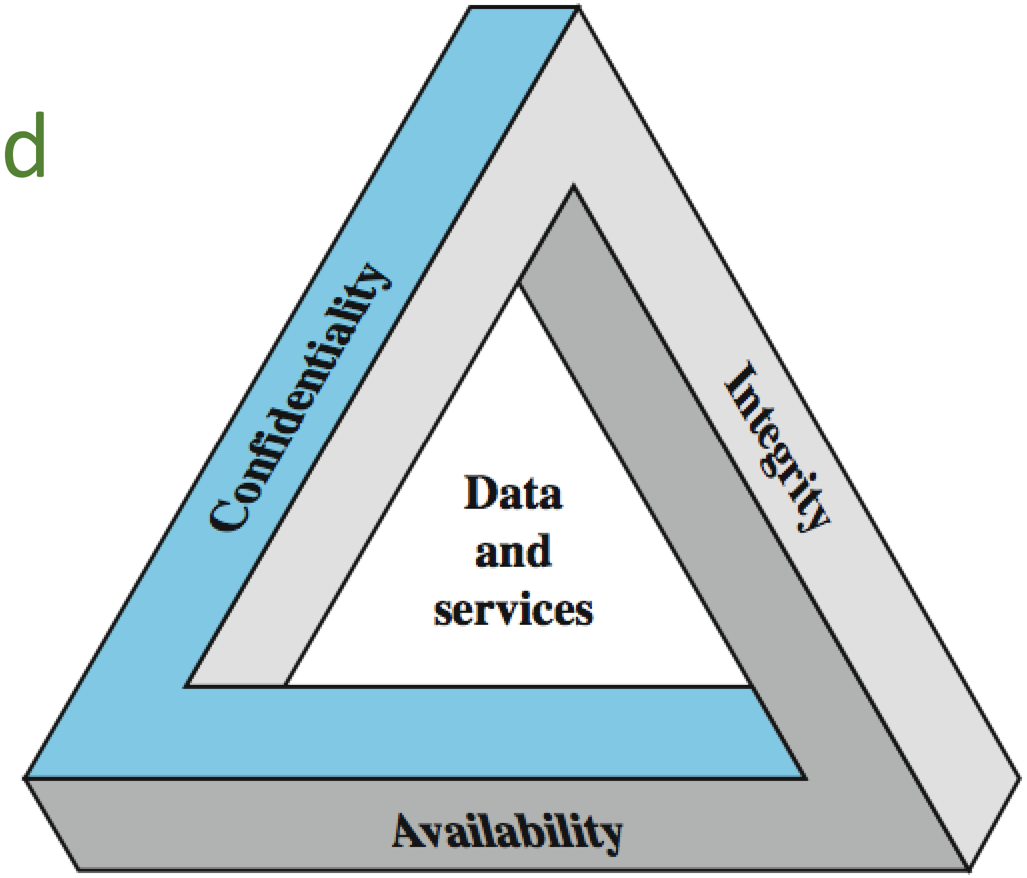
- The US-based National Institute for Standards and Technology (NIST) defines computer security as follows:

Definition (Computer Security)

[Computer security is] the protection afforded to an automated information system in order to attain the applicable objectives of preserving integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

Key Security Concepts

CIA Triad



Confidentiality

Confidentiality covers two 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

Integrity as a security goal also 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

Availability ensures that a system works promptly and service is not denied to authorized users. A loss of availability is the disruption of access to or use of information or an information system

Further Considerations

Some additional aspects are often mentioned:

❑Authenticity:

- The property of being genuine and able to be verified
- Confidence in the validity of a transmission, verifiability of a message originator, inputs arriving from trusted sources
- Verifiability of a user's identity

❑Accountability:

- Actions can be uniquely traced to their originator
- Essential for nonrepudiation, deterrence, fault isolation, intrusion detection, after action recovery, legal action
- Truly secure systems are not achievable, so security breaches must be traceable

Attacks on Communication Networks

We distinguish:

❑ Passive attacks

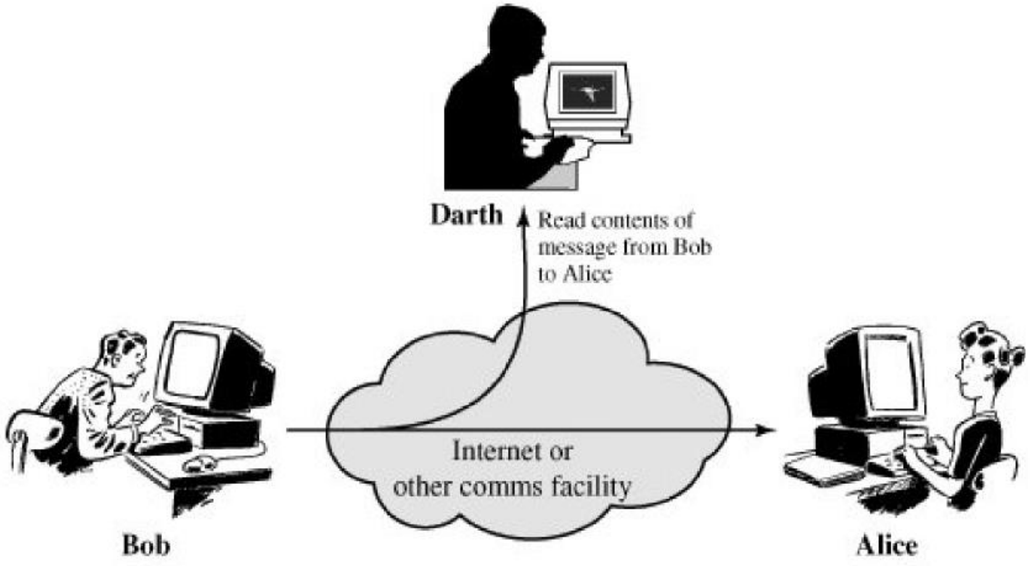
- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping or monitoring of transmissions

❑ Active attacks

- Attempts to alter system resources or affect their operation.

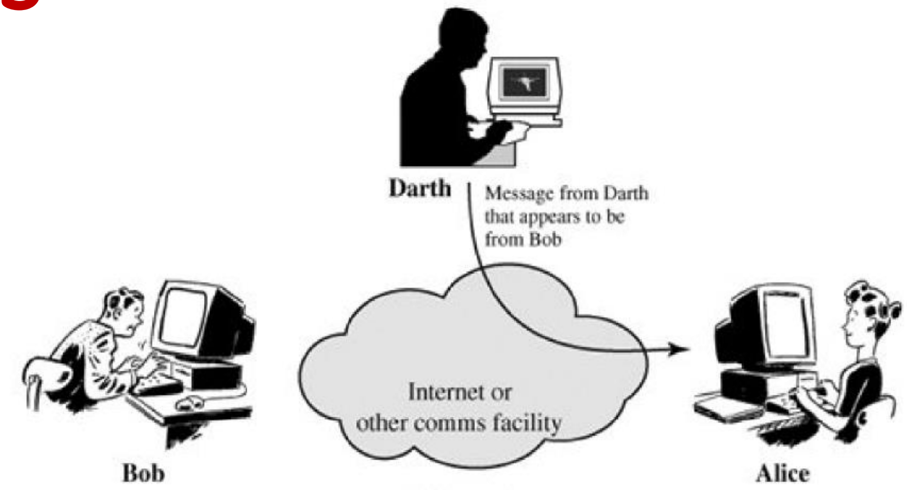
Passive Attacks

- ❑Release of message contents / snooping
- ❑Traffic analysis / spoofing
- ❑Passive attacks are hard to detect!

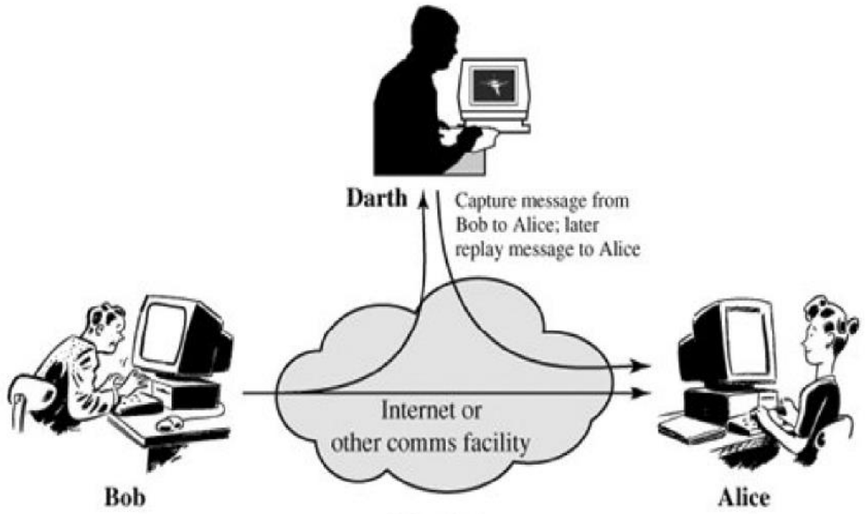

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks

❑ Masquerade: One entity pretends to be a different entity

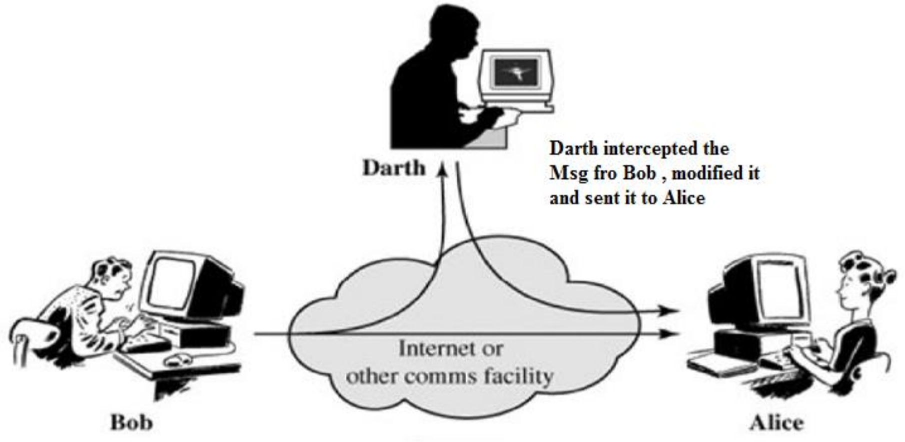

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

❑ Replay attack: Passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

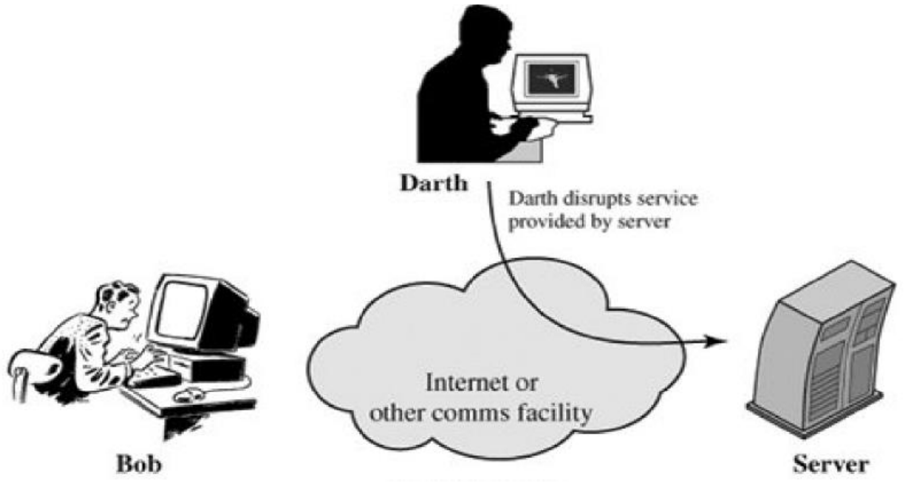

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attacks

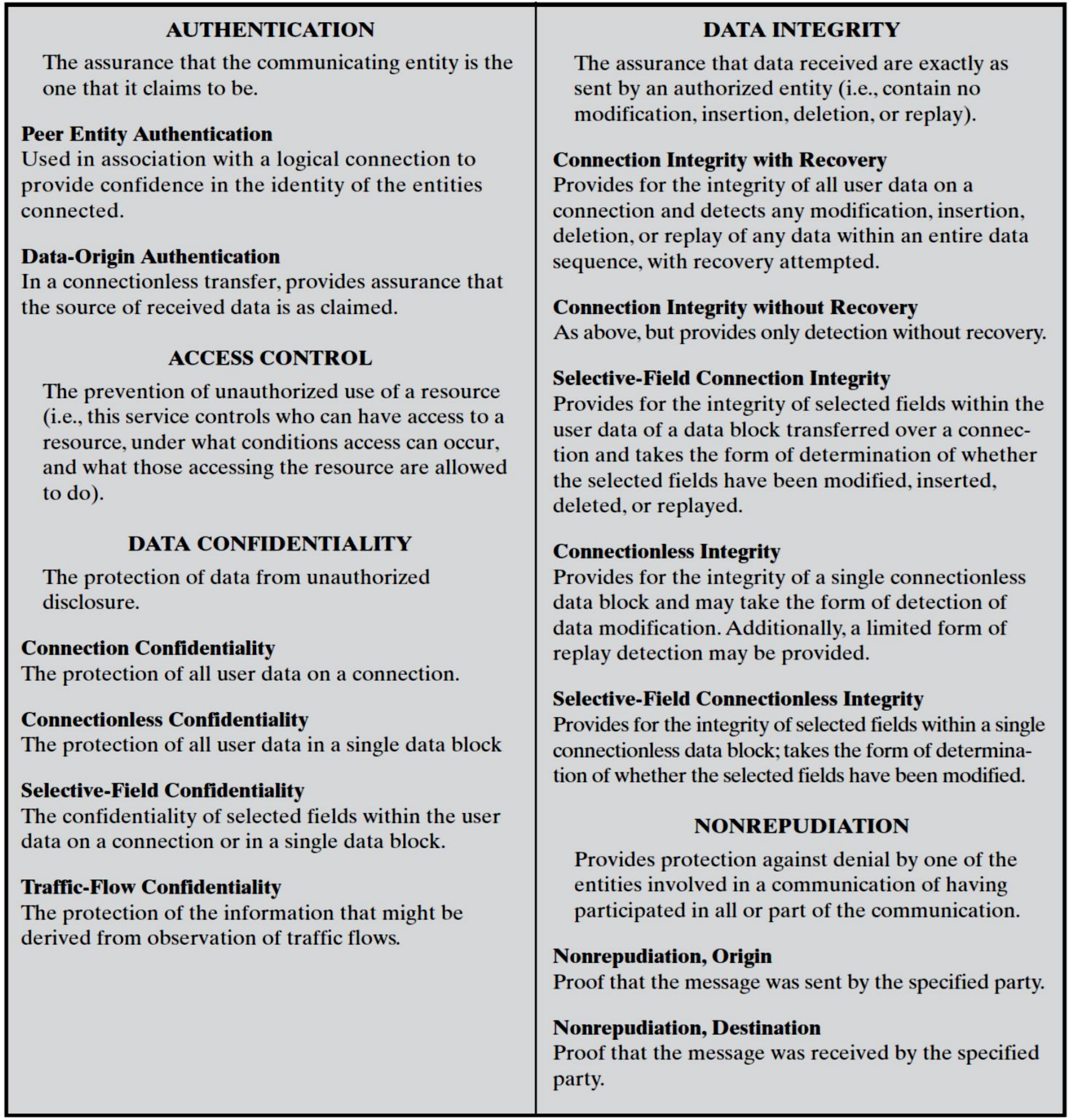
- Modification attack: Some portion of a legitimate message is altered or messages are reordered to produce an unauthorized effect



- Denial of service: Prevents or inhibits the normal use or management of communications facilities



Security Services



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.

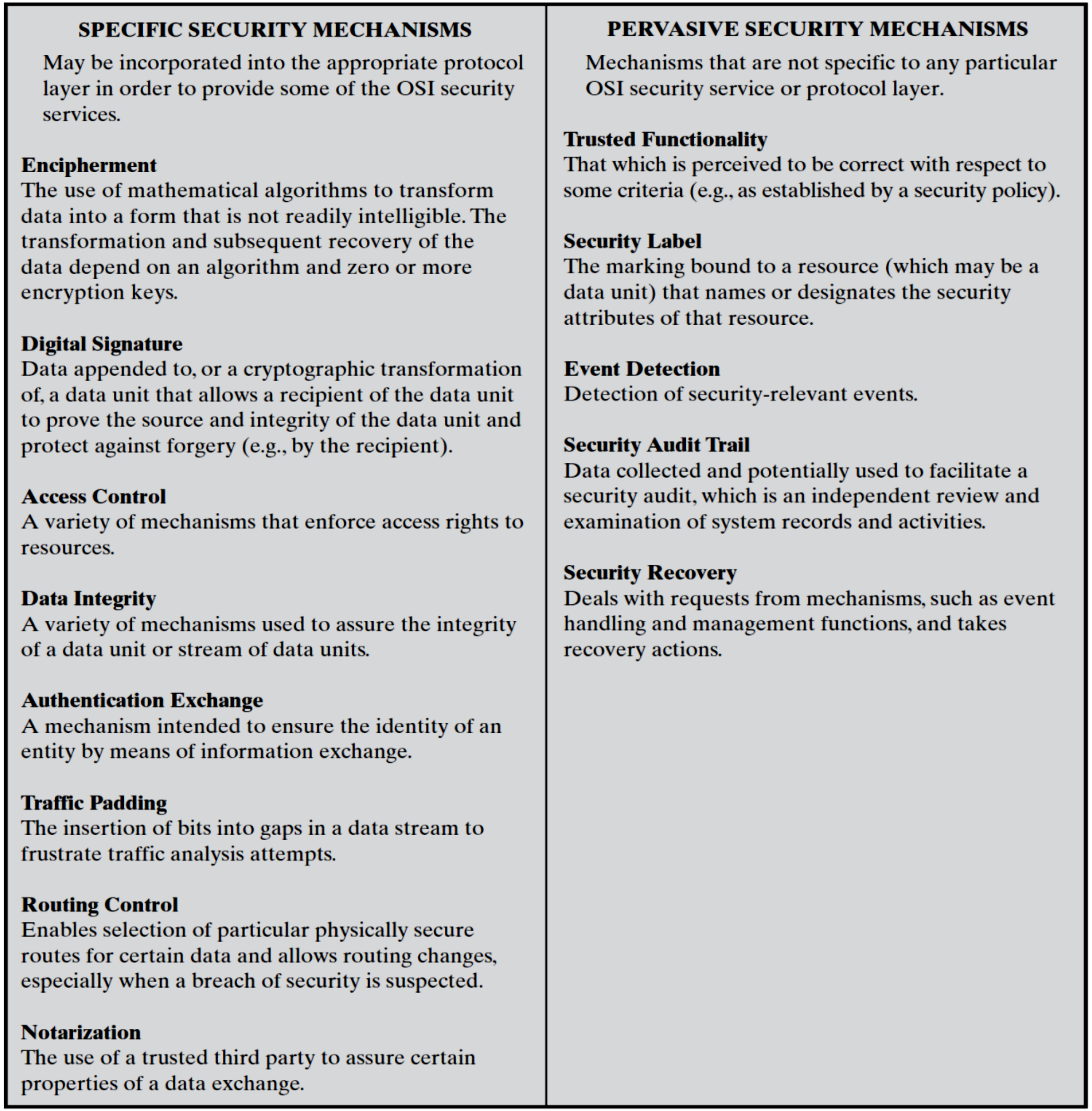
NONREPUDIATION

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.

Security Mechanisms



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.