CSEN1001

Computer and Network Security

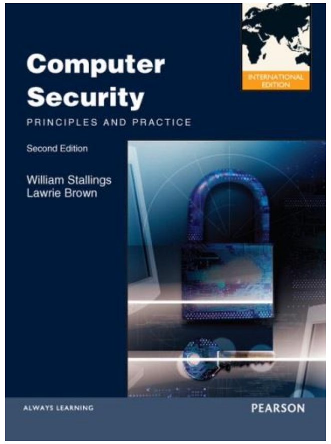
Mervat AbuElkheir (mervat.abuelkheir@guc.edu.eg)
Mohamed Abdelrazik (mohamed.abdelrazik@guc.edu.eg)
Ahmed Helmy (ahmad.helmy@guc.edu.eg)

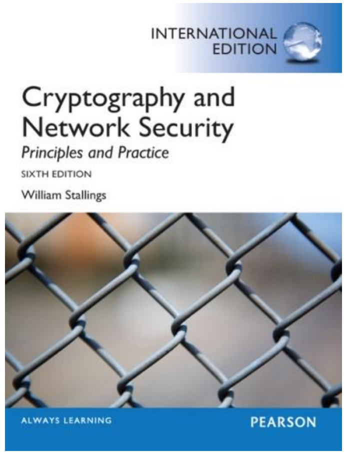
Course Details

- 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

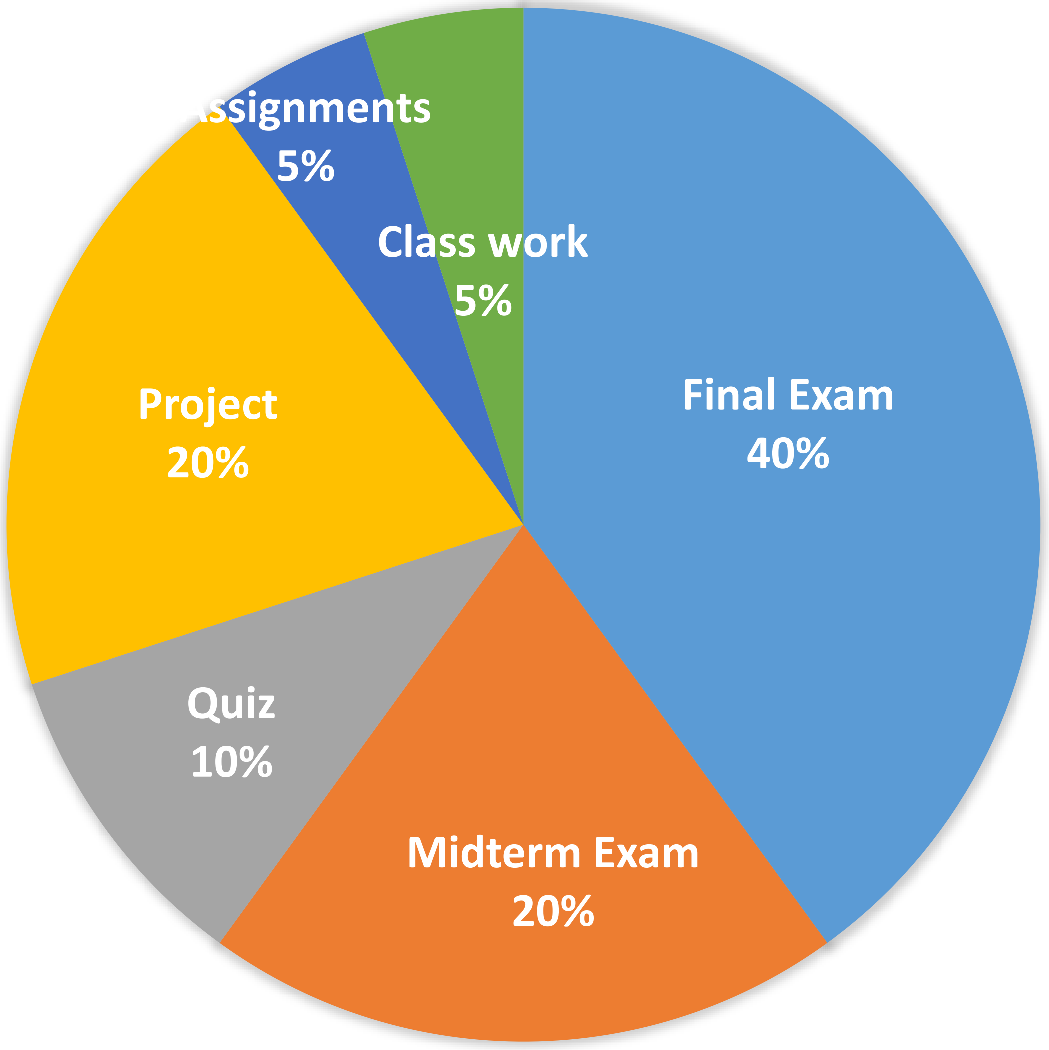




- Note:

  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 Grading



Course Details

Week	Lectures	Tutorials
1	Intro	---
2	Classical Cryptography	Basics and Classical Cryptography
3	Symmetric Encryption and AES	AES and Block Ciphers
4	Asymmetric Encryption and RSA	RSA and Breaking RSA
5	Message Authentication and Hash Functions	Hash Functions
6	Key Management and Exchange	Key Management
7	User Authentication Methods	Authentication and Digital Certificates
8	Access Control	Access Control
9	Attacks on Systems and Networks	Malicious Software and Attacks
10	Software Security	Software Security Issues
11	Internet Security Protocols	Security protocols
12	Network Defense Tools (OR Blockchain!)	Project Evaluation

Lecture (1)

Introduction and Key Security Concepts

Definitions

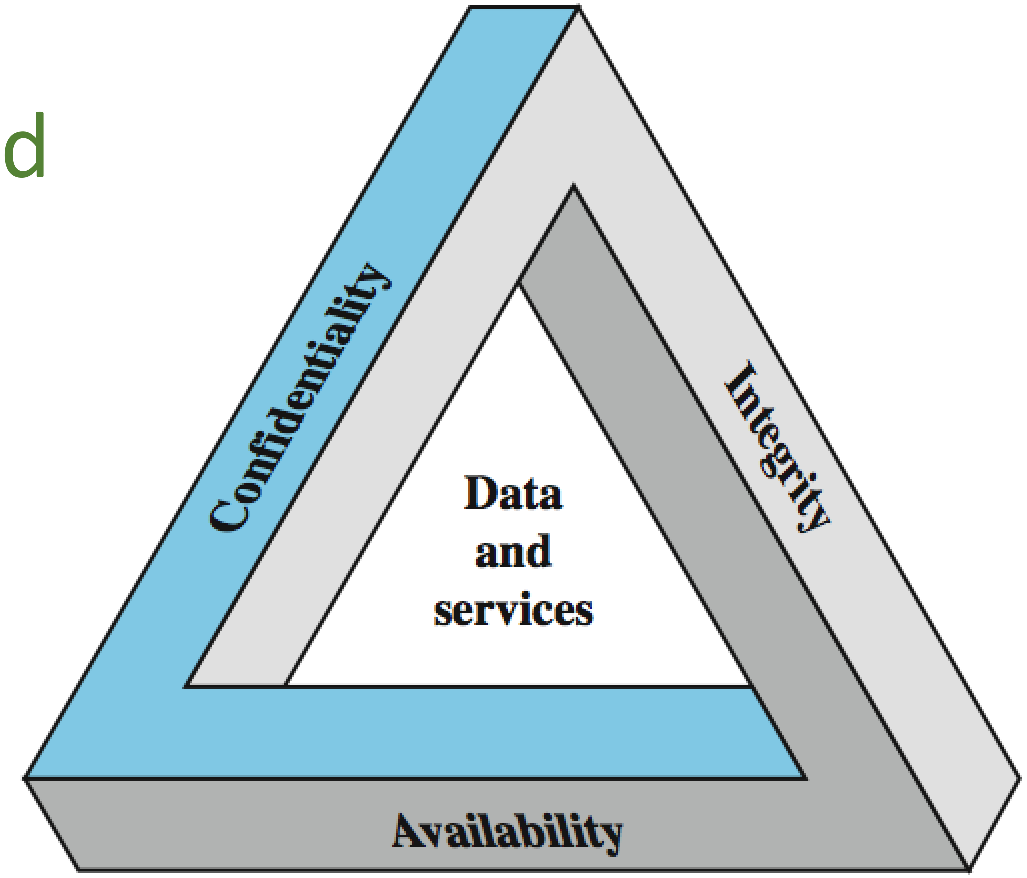
- The US-based National Institute for Standards and Technology (NIST) defines computer security as follows:

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

Confidentiality

Example

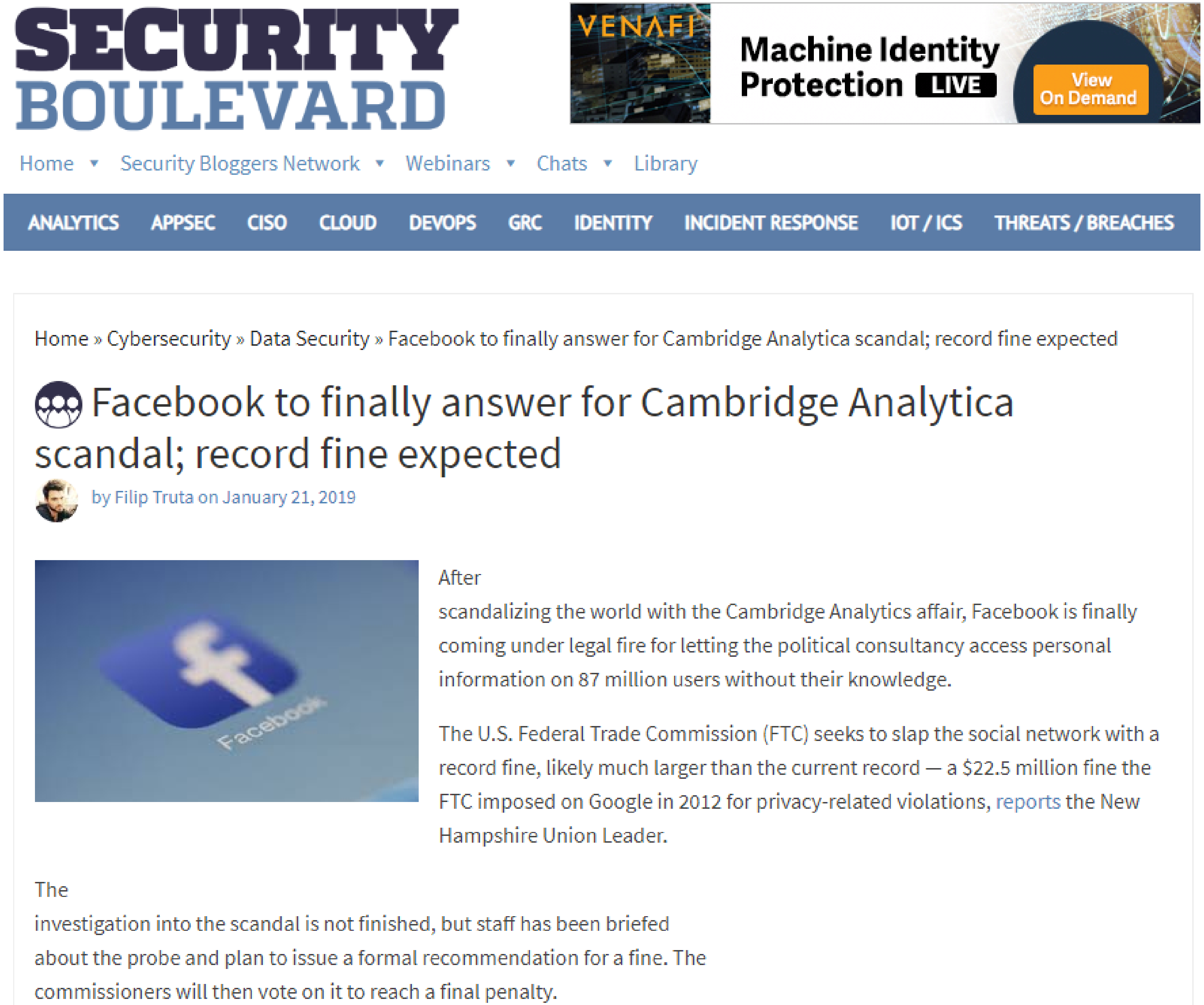
- ❑Student enrollment information
- ❑Student grade information

Which should have a higher level of confidentiality?

Who should have access?

Who is allowed to disclose the data? To whom?

Confidentiality



SECURITY BOULEVARD

Home » Cybersecurity » Data Security » Facebook to finally answer for Cambridge Analytica scandal; record fine expected

Facebook to finally answer for Cambridge Analytica scandal; record fine expected

by Filip Truta on January 21, 2019

After scandalizing the world with the Cambridge Analytics affair, Facebook is finally coming under legal fire for letting the political consultancy access personal information on 87 million users without their knowledge.

The U.S. Federal Trade Commission (FTC) seeks to slap the social network with a record fine, likely much larger than the current record — a $22.5 million fine the FTC imposed on Google in 2012 for privacy-related violations, reports the New Hampshire Union Leader.

The investigation into the scandal is not finished, but staff has been briefed about the probe and plan to issue a formal recommendation for a fine. The commissioners will then vote on it to reach a final penalty.

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

Integrity

Example

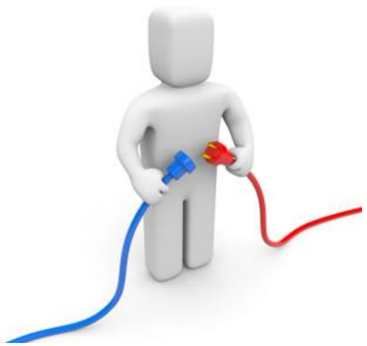
- ❑Bank client’s account information
- ❑Bank client’s transactions history and account balance
- ❑The process through which a bank updates an account

How can a bank accountant trust the balance information?

Who can perform transactions and modify balance amounts?

What to do if power went off during a transaction?

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

Availability

Example

- ❑Web server
- ❑Cloud services

What happens if you can’t access Facebook?

What happens if you can’t access an online exam server?

What happens if you can’t access your online banking portal?

Further Considerations

Some additional aspects are often mentioned:

❑ Authenticity:

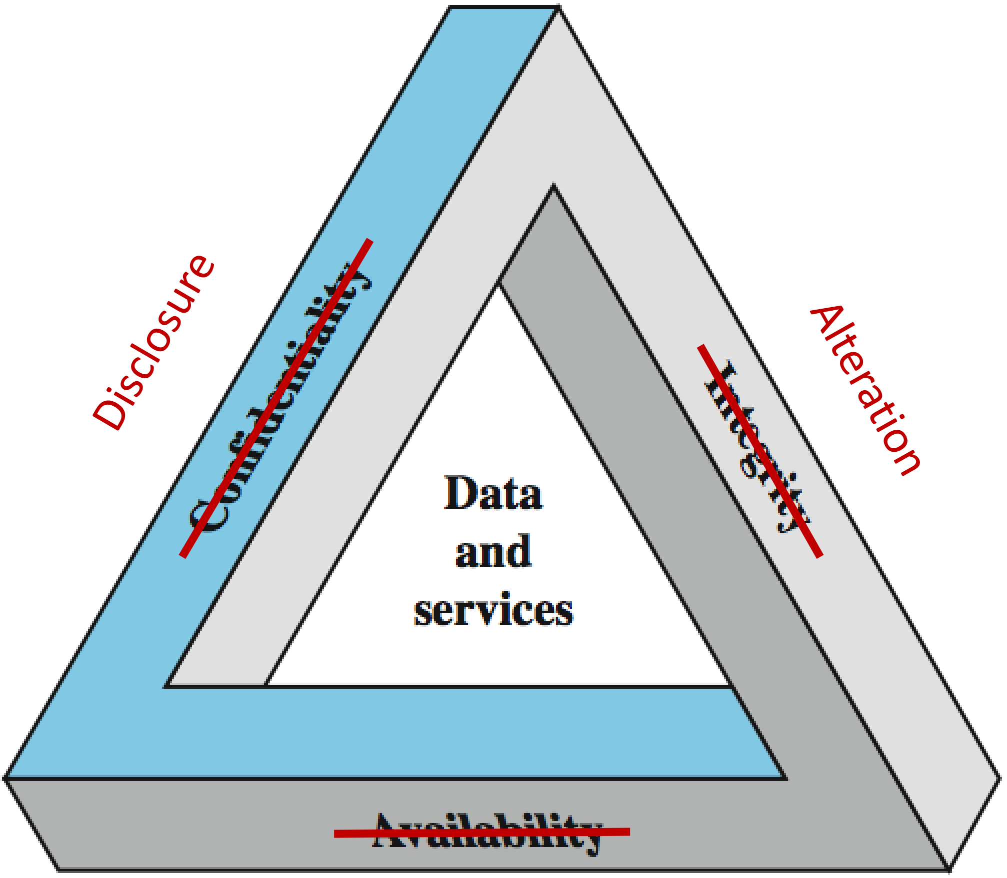
- The property of being genuine and able to be verified
- Confidence in the validity of a transmission, verifiability of a message originator, inputs arriving from trusted sources
- Verifiability of a user’s identity

❑ 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

DAD Triad

- The complement of CIA



Unauthorized individuals gain access to confidential information

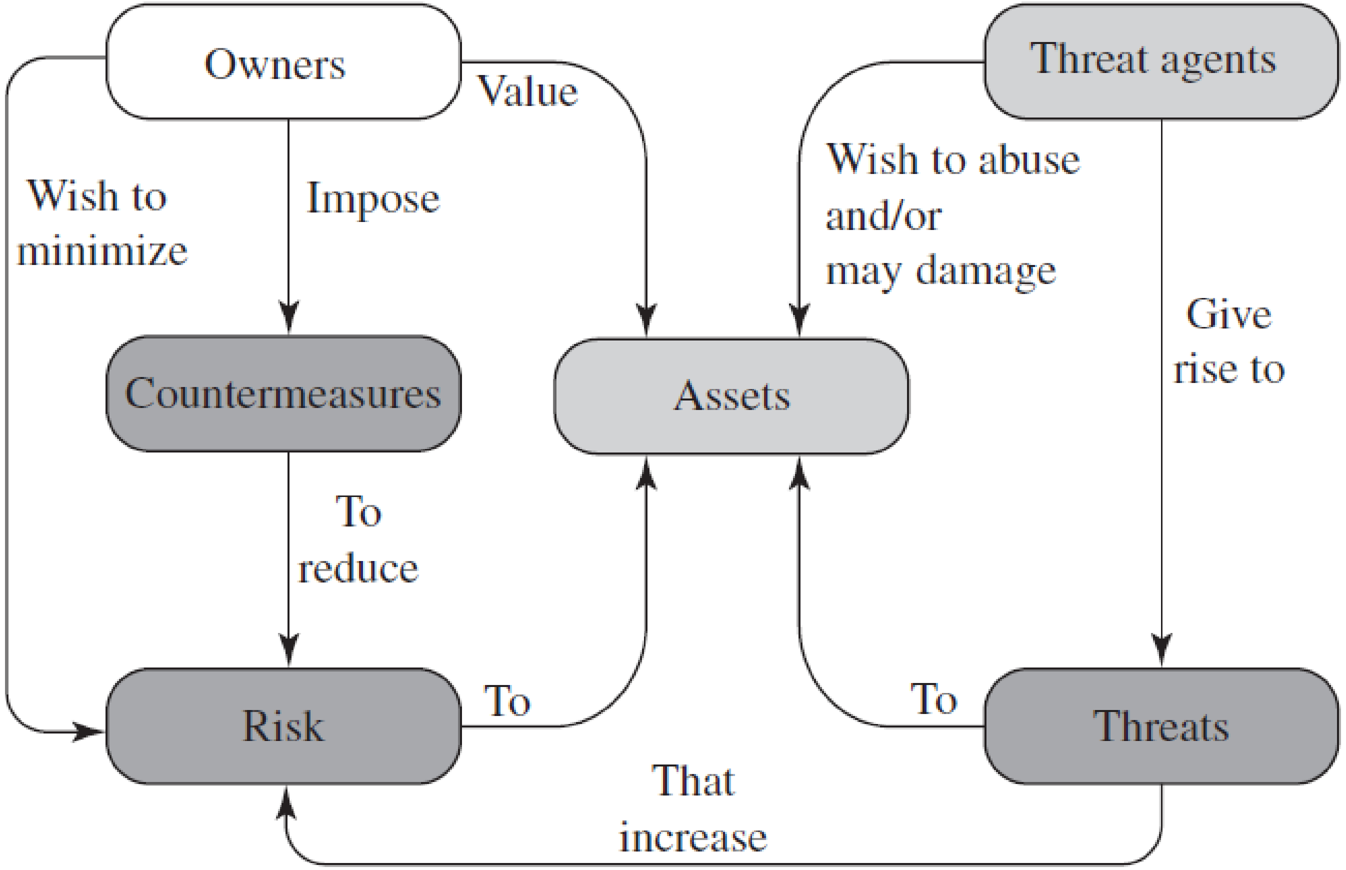
Data is modified or destroyed through some unauthorized mechanism

Denial

Authorized users can not gain access to a system for legitimate purposes

DAD activities may be malicious or accidental

Security Concepts and Relationships



Assets

Hardware → availability and confidentiality threats

- Equipment damage
- Stolen hard drives or other storage media

Software → availability and integrity threats

- Deleted software
- Code alteration
- Software piracy

Data → availability, integrity, and confidentiality threats

- Destruction of files
- Modification of data
- Exposure of data

Communication Lines→ availability, integrity, and confidentiality threats

- DOS attacks
- Message modification
- Traffic analysis

Layered Security Aspects

Security considerations include:

❑ Physical security

❑ Operating system security

Windows, Mac OS, Unix/Linux (Sun OS, Solaris, Open BSD, . . .)

❑ Application layer security

Browser, e-mail client, . . .

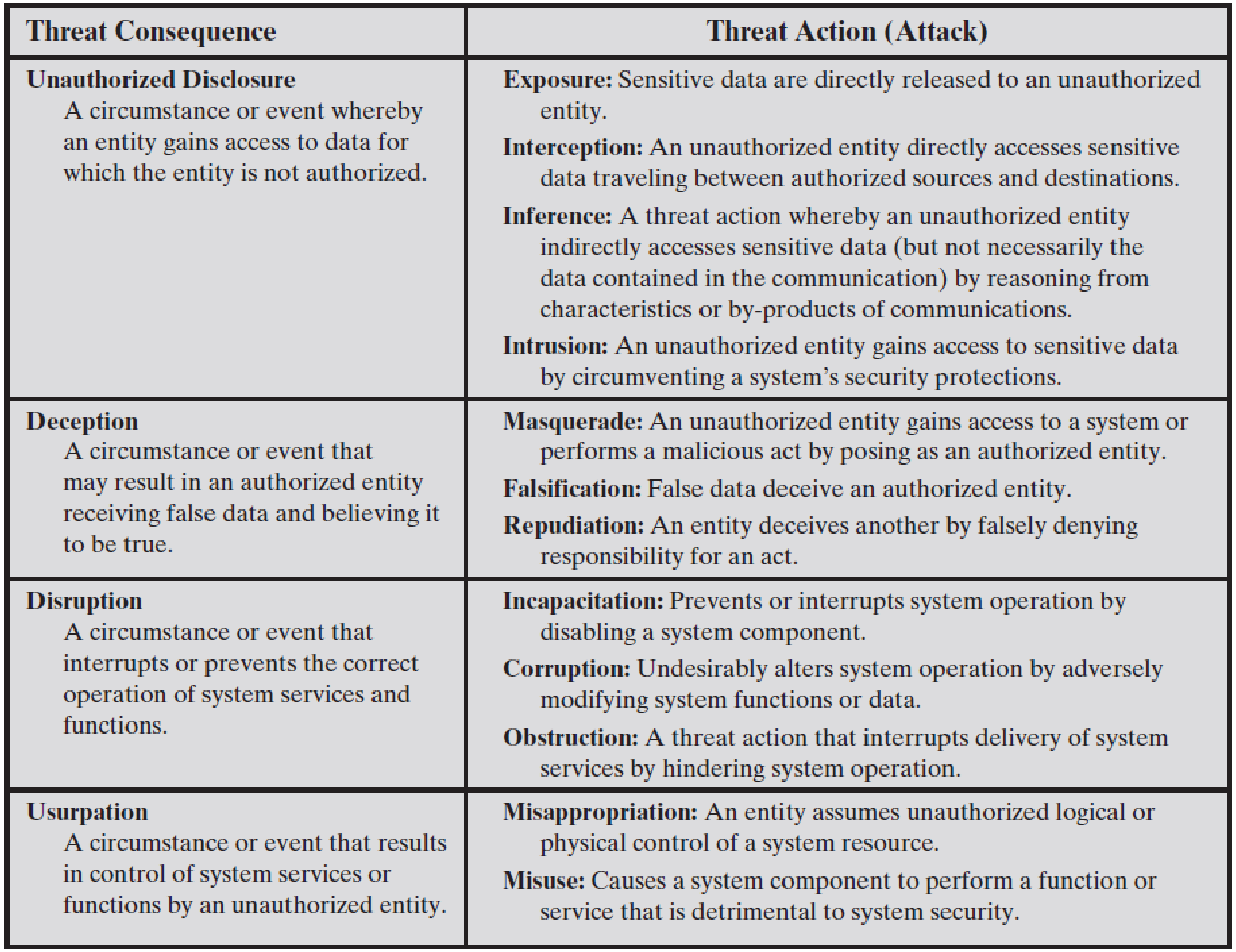
❑ Communication security

- Encryption
- Firewalls
- Intrusion detection systems

Vulnerabilities and Attacks

- Vulnerability is a flaw in a system's design, implementation, or operation and management that could be exploited to make system resources:
  - corrupted (loss of integrity)
  - leaky (loss of confidentiality)
  - unavailable (loss of availability)
- Threat is potential of exploiting vulnerability
- Risk is probability of threat exploiting vulnerability
- Attack is a threat carried out and may be
  - passive
  - active
  - inside
  - outside

Threats and Attacks



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Source: Based on RFC 4949

Typical Attackers

❑Hacker

- Anyone who attempts to penetrate the security of an information system, regardless of intent
- Early definition included anyone very proficient in computer use

❑Malicious insider

- Someone from within the organization that attempts to go beyond the rights and permissions that they legitimately hold
- Security professionals and system administrators are particularly dangerous

Typical Attacks on Software

Malicious code object

- ❑Virus:

  A program that attaches itself to a program or file so it can spread from one computer to another, leaving infections as it travels

- ❑Worm:

  A program that takes advantage of file or information transport features on your system, which allows it to travel unaided. The biggest danger with a worm is its capability to replicate itself on your system (e.g., sending itself to all of the e-mail list in your computer)

- ❑Trojan horse:

  A program that at first glance will appear to be useful software but will actually do damage once installed or run on your computer. It usually appears that is coming from a trusted source

Attacks on Communication Networks

We distinguish:

❑ Passive attacks

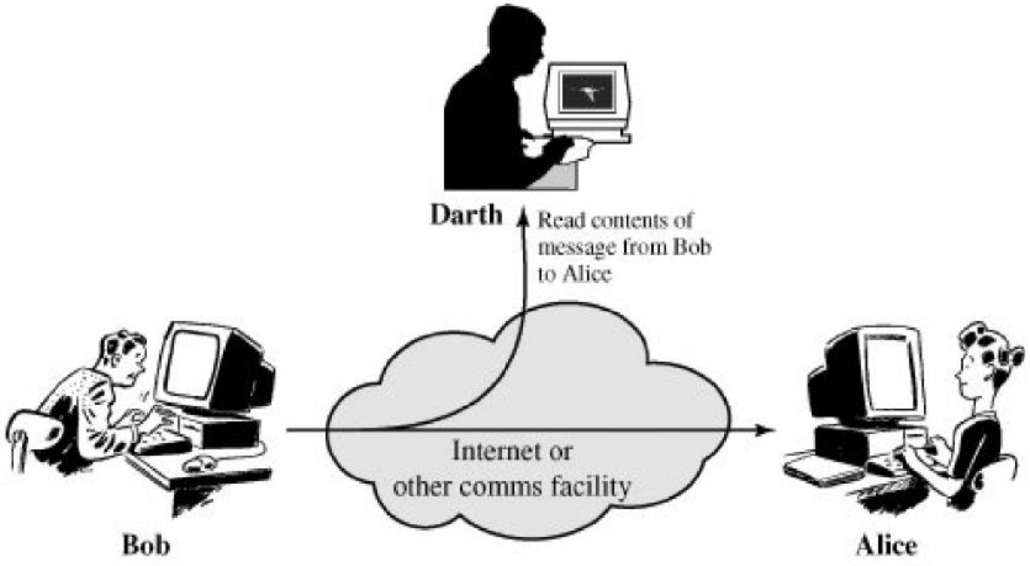
- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping or monitoring of transmissions

❑ Active attacks

- Attempts to alter system resources or affect their operation.

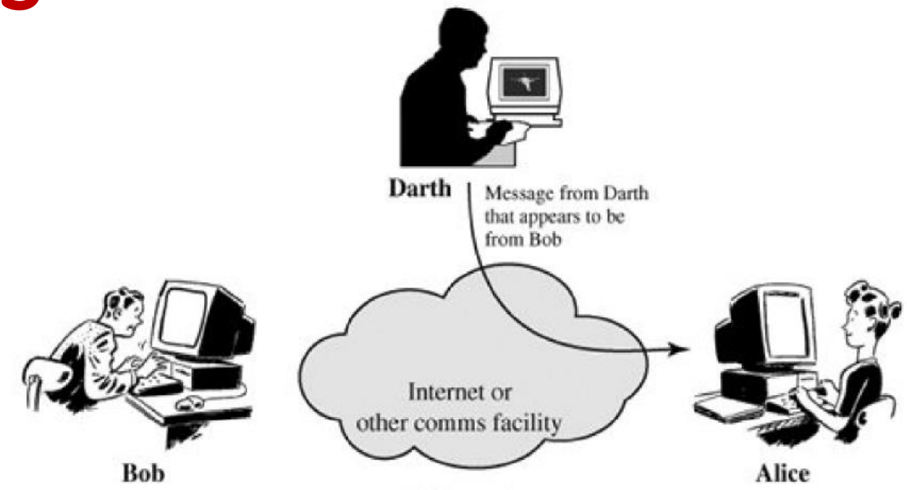
Passive Attacks

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

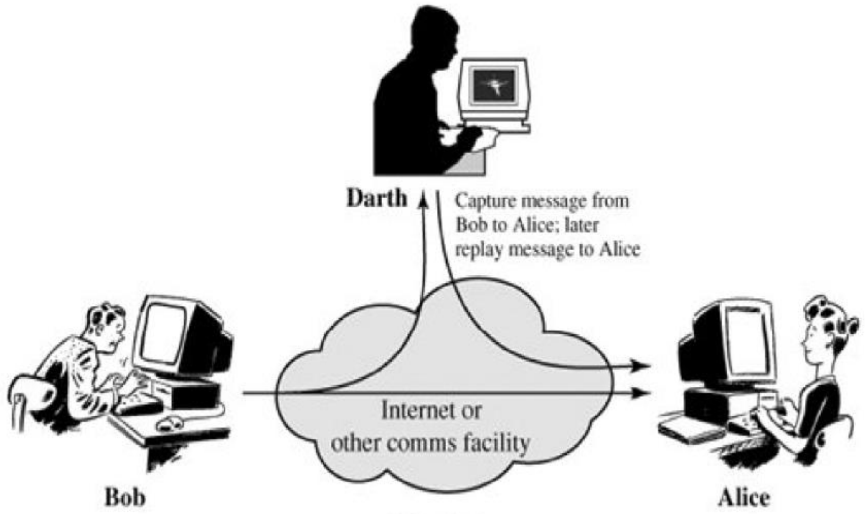

Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Attacks

❑Masquerade: One entity pretends to be a different entity

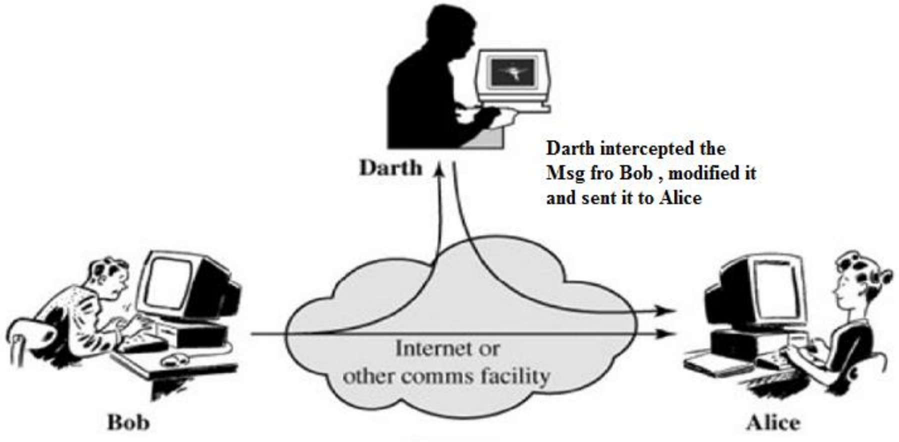

Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

❑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

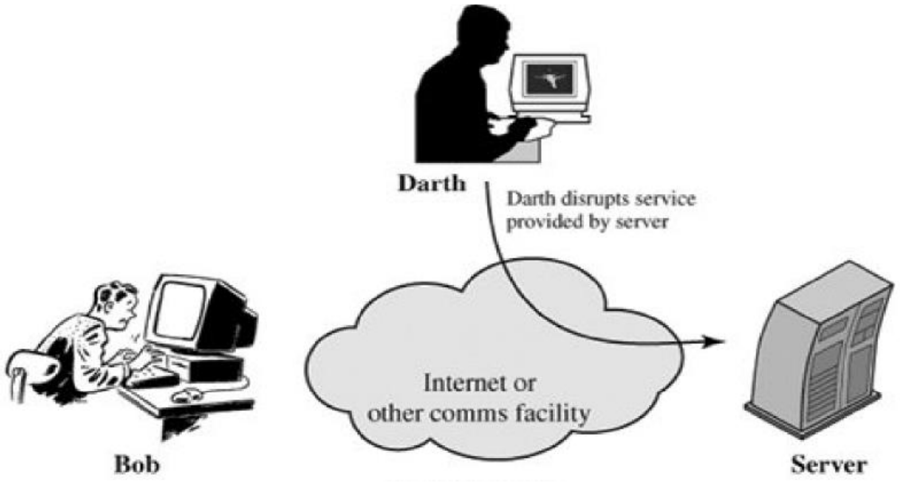
Active Attacks

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



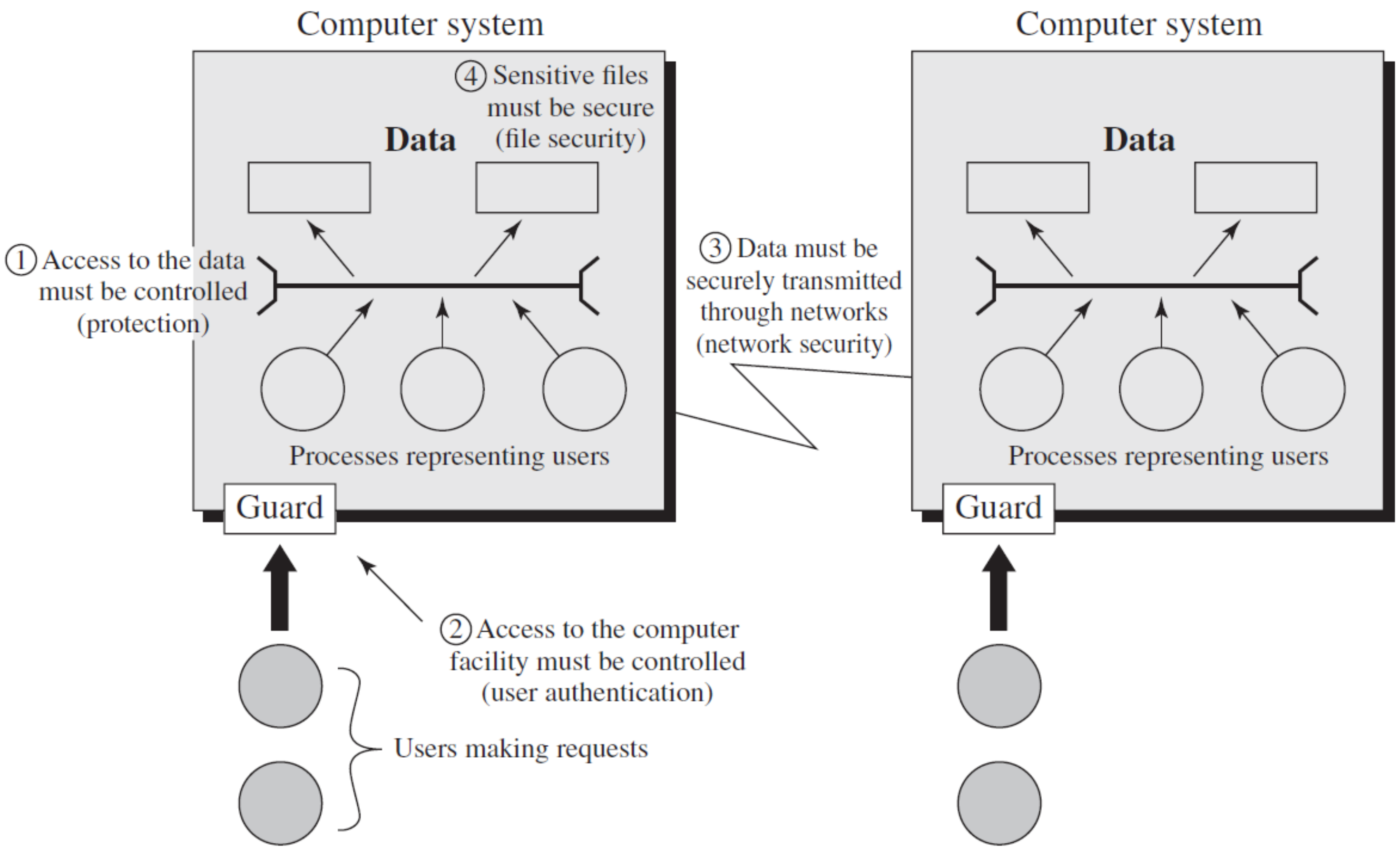
Darth intercepted the Msg fro Bob , modified it and sent it to Alice

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



Darth disrupts service provided by server

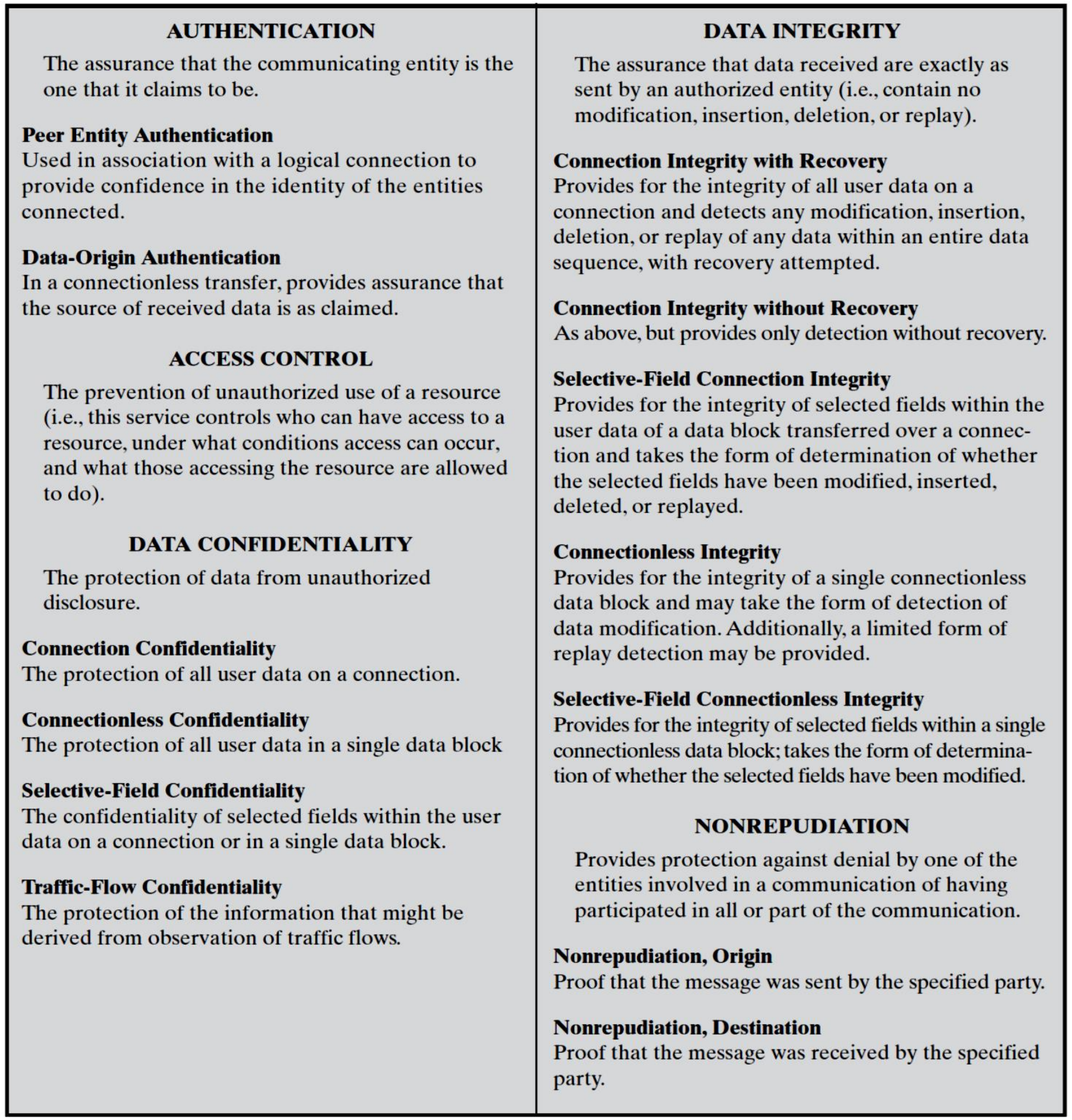
Scope of Computer Security


Computer system
Data
④ Sensitive files must be secure (file security)
① Access to the data must be controlled (protection)
Processes representing users
Guard
③ Data must be securely transmitted through networks (network security)
Computer system
Data
Processes representing users
Guard
② Access to the computer facility must be controlled (user authentication)
Users making requests

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 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.

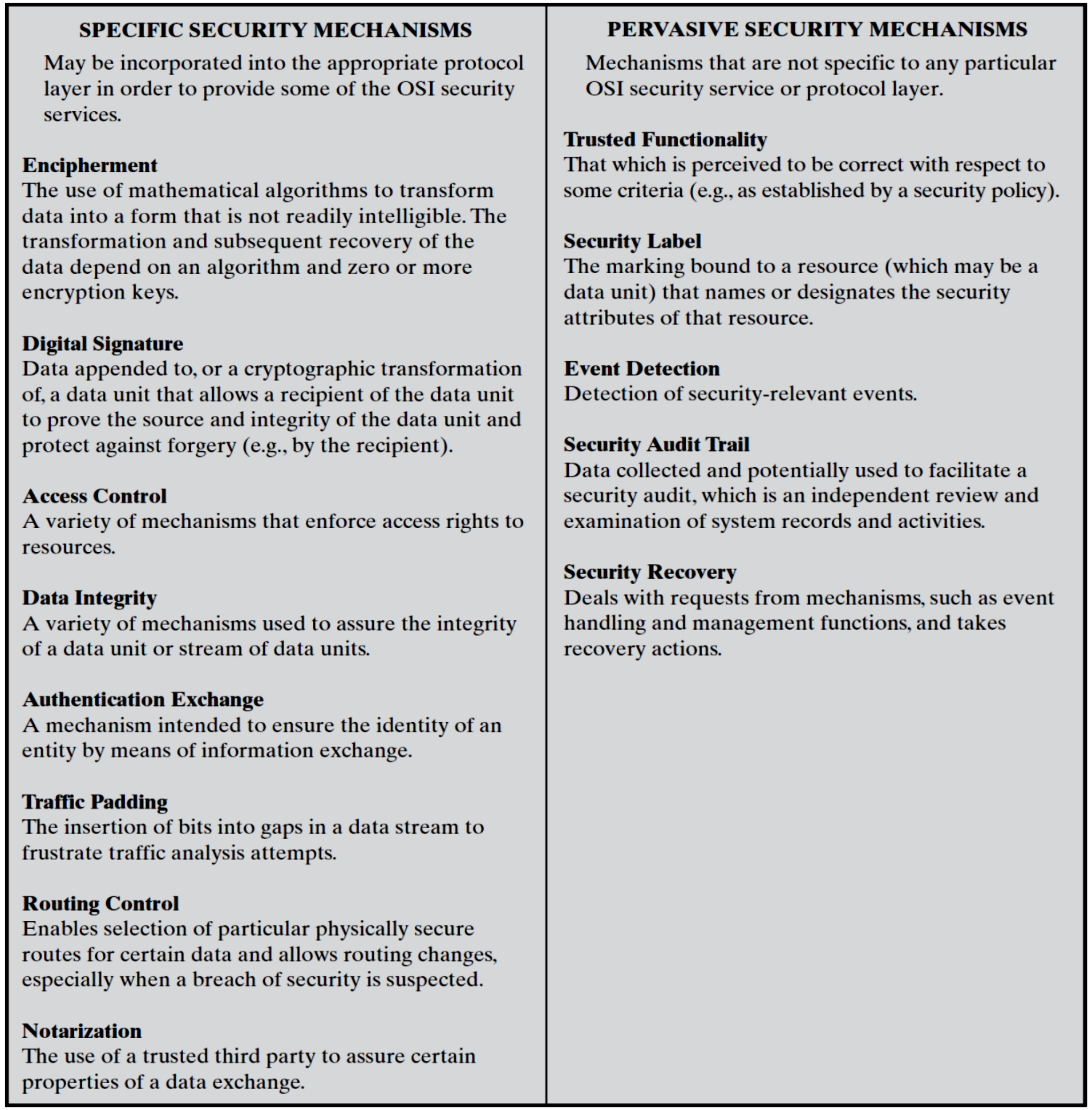
NONREPUDIATION

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.

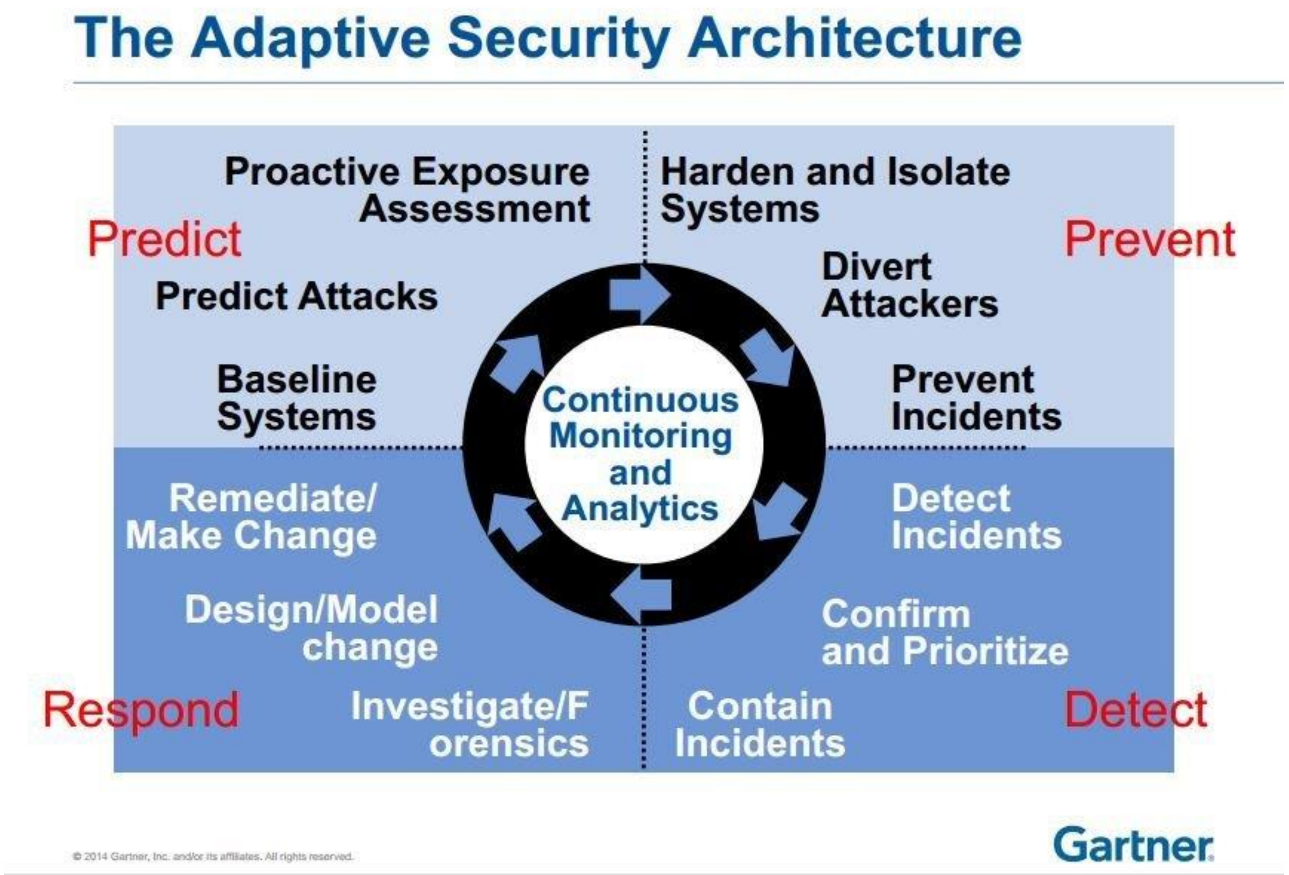
Security Mechanisms Mapped to Services

Service\Mechanism	Encipherment	Digital Signature	Access Control	Data Integrity	Authentication Exchange	Traffic Padding	Routing Control	Notarization
Peer entity authentication								
Data origin authentication								
Access control								
Confidentiality								
Traffic flow confidentiality								
Data integrity								
Nonrepudiation								
Availability								

Security Mechanisms Mapped to Services

Service\Mechanism	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	Y			

The Security Cycle



The Adaptive Security Architecture

Next Time

Classical Cryptography