

Foundations of Computer Security

Andrea Pintér-Husztí

Contents

- 1 Basic computer security concepts
 - Computer Security Concepts
 - Network Security services

1. *Journal of Management Studies*, 1996, 33, 1, 1-14.

- A transmits a file containing payroll records to B .
 E , who is not authorized to read the file, is able to monitor the transmission capture a copy of the file.
- Network manager A transmits a message to a computer B to update an authorization file to include the identities of a number of new users. M intercepts the message, alters its contents to add or delete entries and then forwards the message to B .
- A sends a message to a stockbroker B with instructions for various transactions. The investments lose value and A denies sending the message.

Concept of Computer Security

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).

Security objectives - CIA triad

NIST Special Publication 800-33:

Confidentiality The requirement that private (*privacy*) or secret information not be disclosed to unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.

- Integrity**
- Data integrity: The property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit.
 - System integrity: The quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation.

Availability Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users.

Further security objectives

Accountability Accountability is the requirement that actions of an entity may be traced uniquely to that entity.

Accountability is often an organizational policy requirement and directly supports non-repudiation, deterrence, intrusion detection and prevention.

Assurance The basis for confidence that the security measures, both technical and operational, work as intended to protect the system and the information it processes. The other four security objectives (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation.

Security Objective Interdependencies

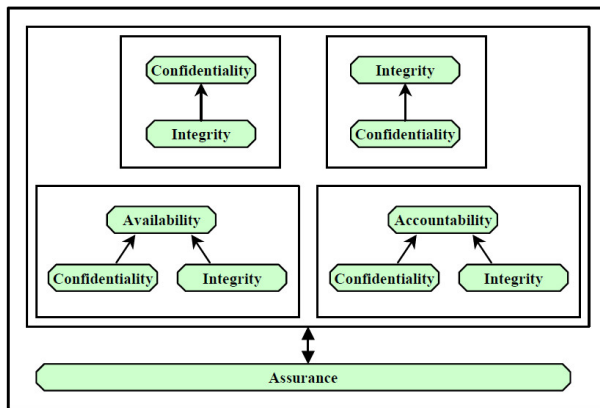


Figure 2-1 Security Objective Dependencies

ábra: NIST Special Publication 800-33

Security Objective Interdependencies

- Confidentiality is dependent on Integrity: If the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid.
- Integrity is dependent on Confidentiality: If the confidentiality of certain information is lost (e.g., the superuser password), then the integrity mechanisms are likely to be by-passed.
- Availability and Accountability are dependent on Confidentiality: If confidentiality is lost for certain information (e.g., superuser password), the mechanisms implementing Availability and Accountability are easily bypassable.
- Availability and Accountability are dependent on Integrity: If system integrity is lost, then confidence in the validity of the mechanisms implementing Availability and Accountability is also lost.

Authentication

Authentication Encompasses identity verification, message origin integrity, and message content integrity.

- Entity authentication: The process by which one entity (the verifier) is assured of the identity of a second entity (the claimant) that is participating in a protocol.
- Message Authentication Code (MAC): A short fixed-length value which protects both the *message origin* and *message content integrity*, but not non-repudiation.

Levels of impact

There are three levels of impact on organizations or individuals.

Low The loss could be expected to have a *limited* adverse effect on organizational assets, or individuals. For example the loss result in minor damage to assets, minor financial loss, minor harm to individuals, and the organization is able to perform its primary functions.

Moderate The loss could be expected to have a *serious* adverse effect on organizational operations, on organizational assets, or individuals. For example the loss result in significant damage to assets, significant financial loss, significant harm to individuals, and the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced.

High The loss could be expected to have a *catastrophic* adverse effect on organizational operations, on organizational assets, or individuals. For example the loss result in major damage to assets, major financial loss, catastrophic harm to individuals involving loss of life or life-threatening injuries, and the organization is not able to perform its primary functions.

Examples - Confidentiality

Low Subject requirements may be assigned a low confidentiality rating.

Moderate Student enrollment information may have a moderate confidentiality rating.

High Student grade information is an asset whose confidentiality is considered to be highly important by students. Grade information should only be available to students and employees that require the information to do their job.

Examples - Integrity

Low Many Web sites offer anonymous online polls to their users with very few safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.

Moderate A Web site offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries. If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue. The Web master may experience some data, financial, and time loss.

High A hospital patients' allergy information stored in a database. An employee (e.g. a nurse) who is authorized to view and update this information deliberately falsifies the data. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

Examples - Availability

Low An online telephone directory lookup application. Although the temporary loss of the application may be an annoyance, there are other ways to access the information.

Moderate The public Web site for a university provides information for current and prospective students and donors.

High Consider a system that provides authentication services for medical databases. An interruption of service results in the inability for doctors to access the patients' medical records.

The Architecture

OSI (Open Systems Interconnections) security architecture (X.800 standard recommendation):

Security Attack Any action that compromises the security of information.

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 data processing systems and information transfers. A security service makes use of one or more security mechanisms.

Security attacks during data transmission

Two main categories:

Passive attacks Eavesdropping on, or monitoring of, transmissions.

The goal of the opponent is to obtain information that is being transmitted. Very difficult to detect, because they do not involve any alteration of the data.

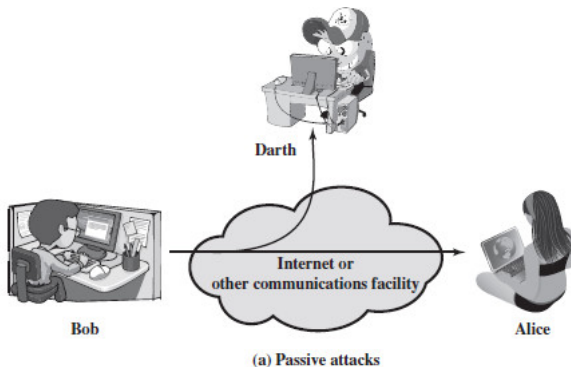
- Release of message contents
- Traffic analysis

Active attacks Modification of the data stream or the creation of a false stream. Difficult to prevent them absolutely, the goal is to detect them and to recover from any disruption or delays caused by them.

- Masquerade
- Replay
- Modification of data
- Denial of service (DOS)

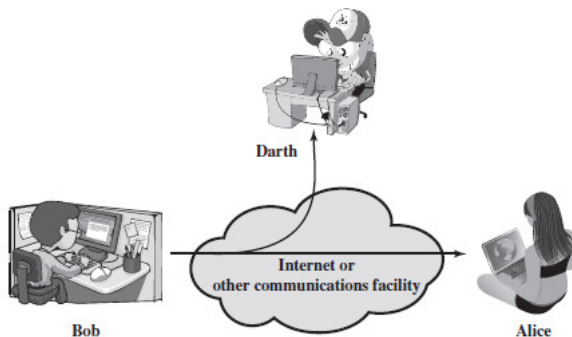
Release of message contents

We would like to prevent an opponent from learning the contents of a telephone conversation, an electronic mail message, or a transferred file.



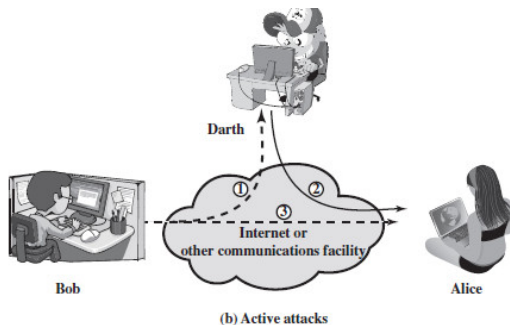
Traffic analysis

Suppose that opponents, even if they captured the message, could not extract the information from the message. An opponent might still be able to observe the pattern of these messages, could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing.



Masquerade

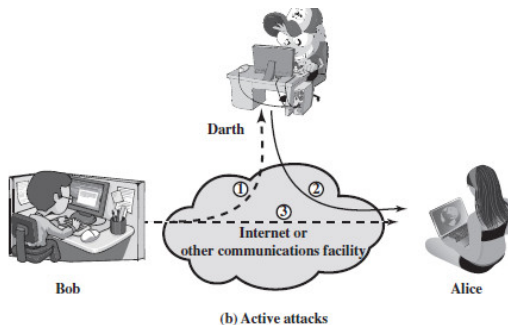
One entity pretends to be a different entity. (path 2) Usually includes one of the other forms of active attacks (e.g. replay).



...

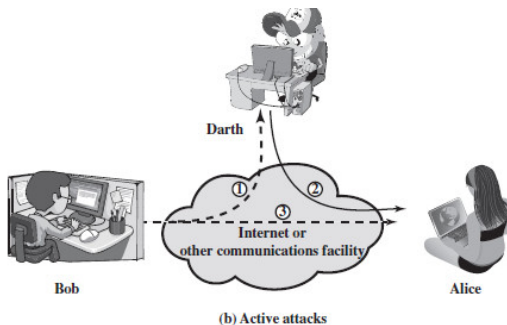
Replay

Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (paths 1, 2, and 3).



Modification of messages

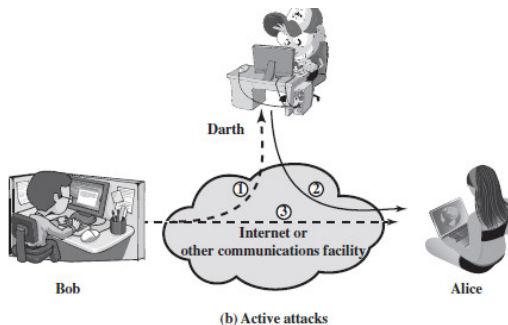
Some part of a message is altered, or the messages are delayed or reordered. (paths 1 and 2)



Navigation icons: back, forward, search, etc.

Denial of service

Prevents the normal use or management of communications facilities (path 3).



Navigation icons: back, forward, search, etc.

Relationship

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