STI

MEI/MES

2020/2021

T1 - Computer and Network Security Concepts

Contents

- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

Contents

- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

The field of network and Internet security consists of:

measures to deter, prevent, detect, and correct security violations that involve the transmission of information

Cryptographic algorithms and protocols can be grouped into four main areas:

Symmetric encryption

- Used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords

Asymmetric encryption

- Used to conceal small blocks of data, such as encryption keys and hash function values, which are used in digital signatures

Data integrity algorithms

- Used to protect blocks of data, such as messages, from alteration

Authentication protocols

- Schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

Computer Security Objectives

Confidentiality

- 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

- 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

- Assures that systems work promptly and service is not denied to authorized users

Network and Computer Security Requirements

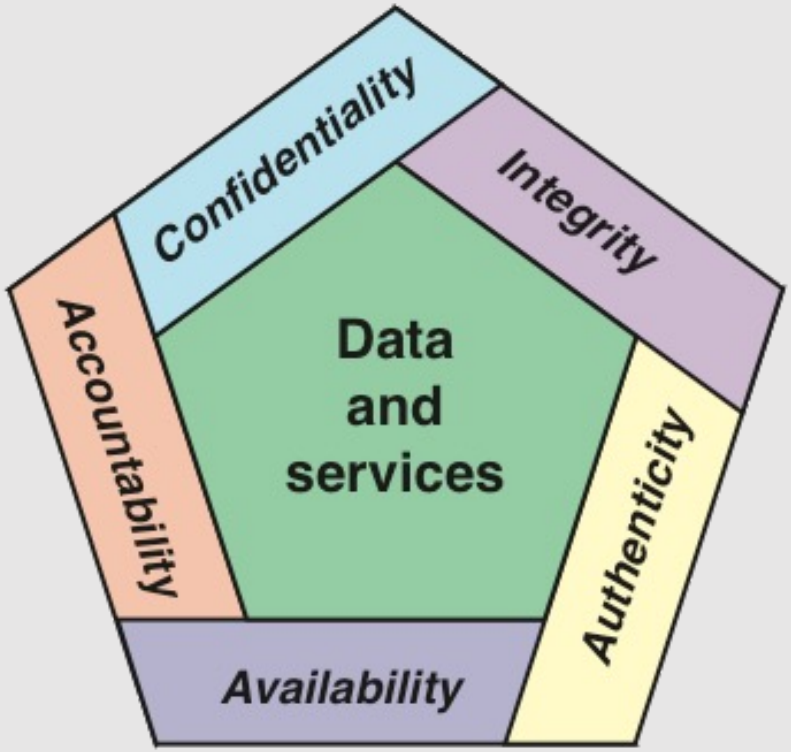


Figure 1.1 Essential Network and Computer Security Requirements

Table 1.1
Threats and Attacks (RFC 4949)

RFC 4949: "Internet Security Glossary, Version 2"

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

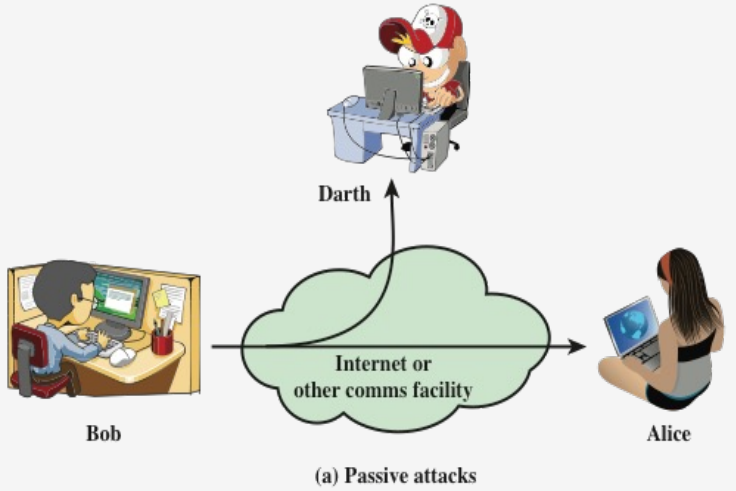
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Contents

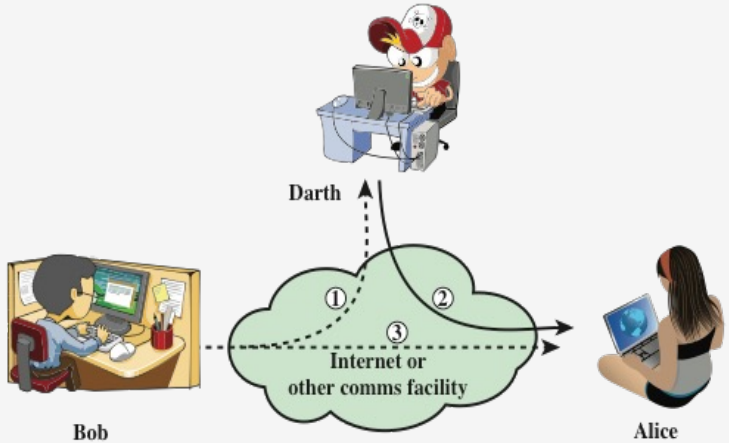
- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

Security Attacks

- A means of classifying security attacks, used both in X.800 and RFC 4949, is in terms of *passive attacks* and *active attacks*
- A *passive attack* attempts to learn or make use of information from the system but does not affect system resources
- An *active attack* attempts to alter system resources or affect their operation



(a) Passive attacks



(b) Active attacks

Figure 1.2 Security Attacks

Passive Attacks

- Are in the nature of eavesdropping on, or monitoring of, transmissions
- Goal of the opponent is to obtain information that is being transmitted
- Very difficult to detect, emphasis is on prevention rather than detection

Two types of passive attacks are:

- The release of message contents
- Traffic analysis

Active Attacks

- Involve some modification of the data stream or the creation of a false stream
- Difficult to prevent because of the wide variety of potential physical, software, and network vulnerabilities
- Goal is to detect attacks and to recover from any disruption or delays caused by them

Masquerade
- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

Replay
- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

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

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

Contents

- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

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 indentified, or authenticated, so that access rights can be tailored to the individual

Data Confidentiality

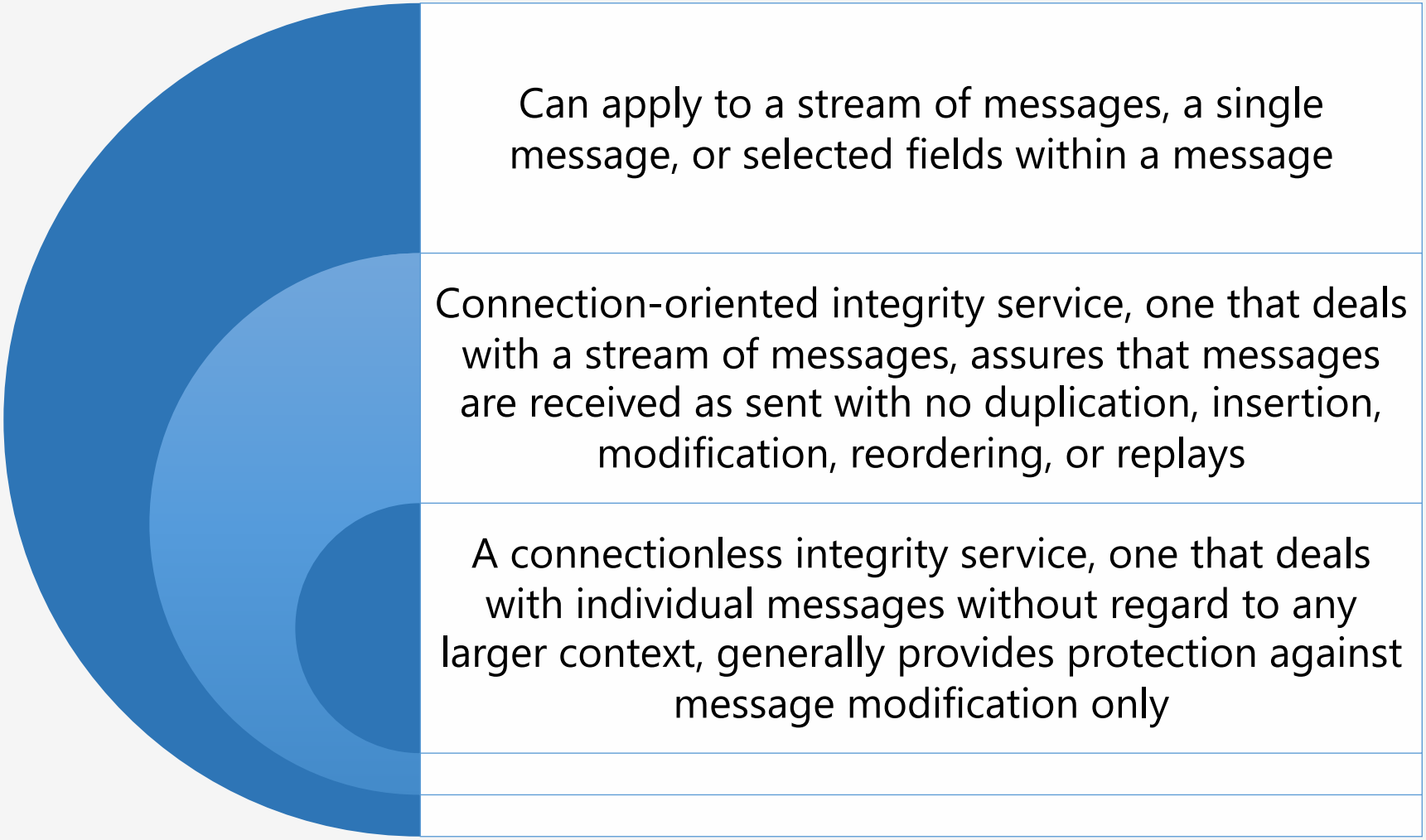
The protection of transmitted data from passive attacks

- 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



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

Availability Service

- 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

Contents

- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

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

Contents

- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

Model for Network Security

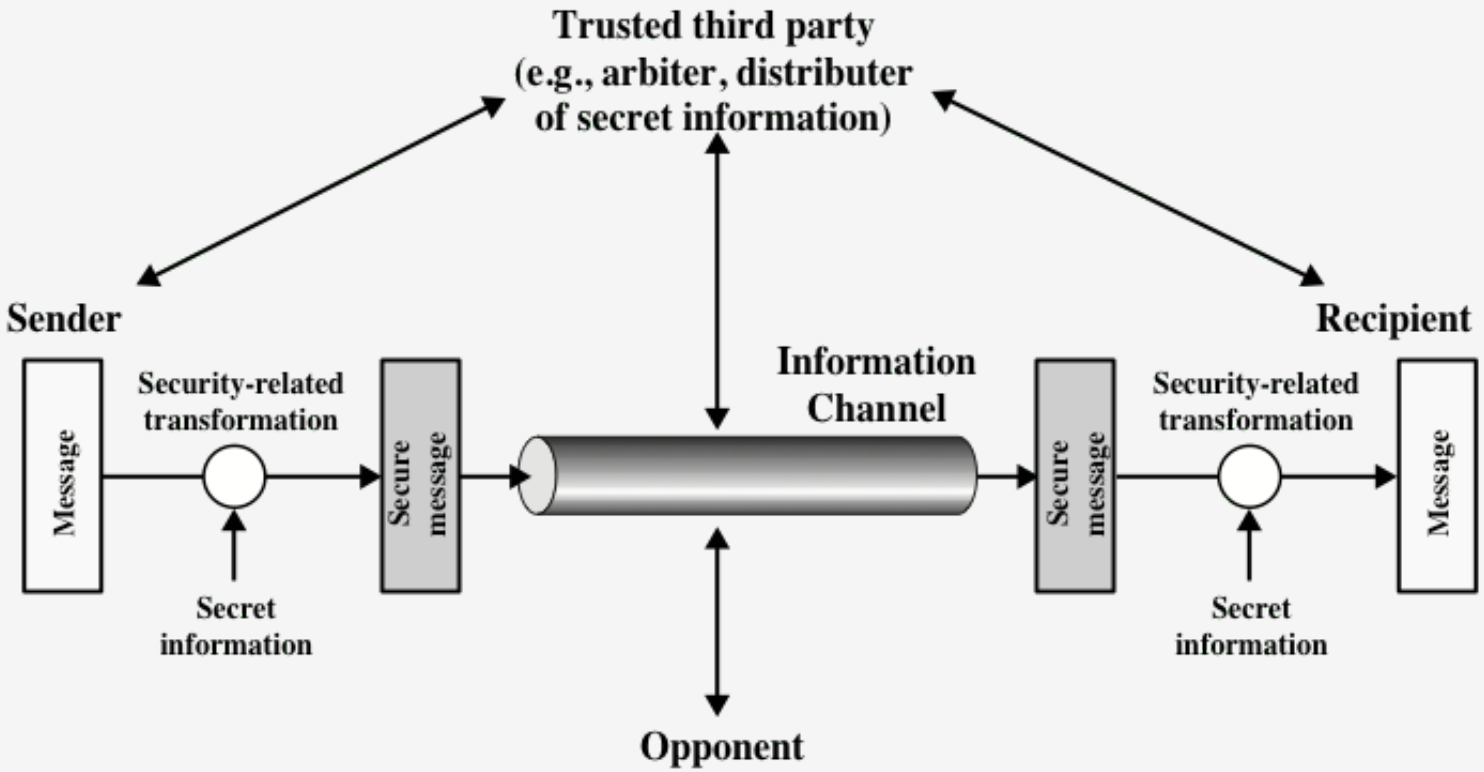


Figure 1.5 Model for Network Security

Network Access Security Model

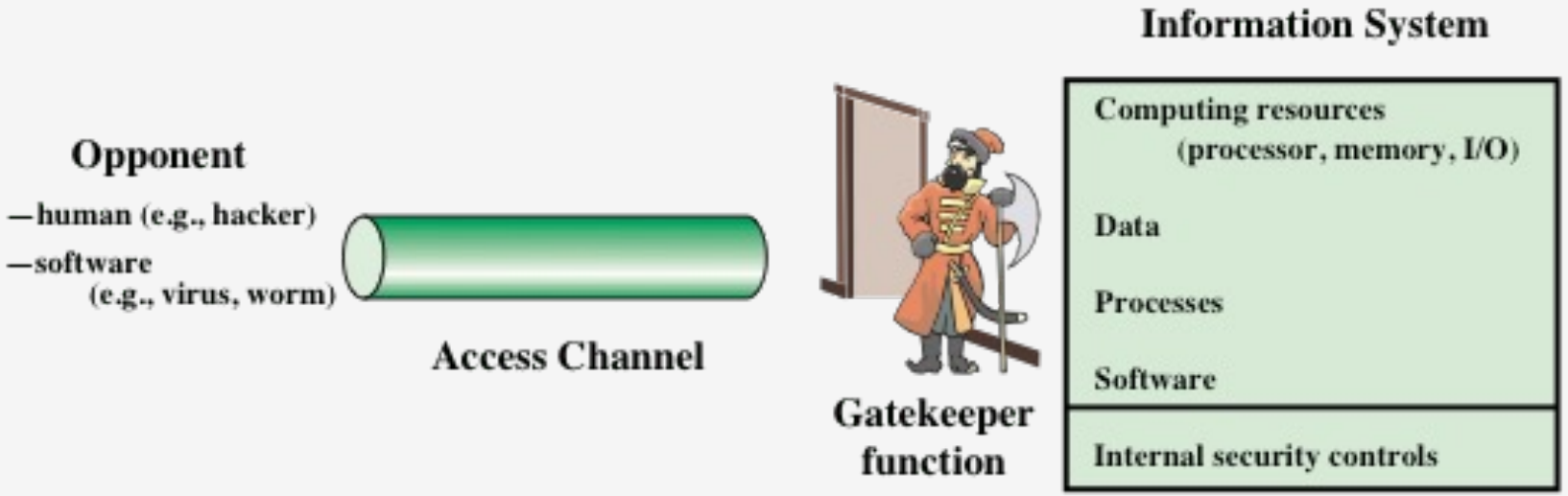


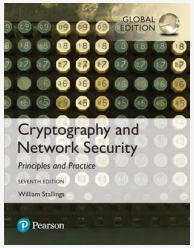
Figure 1.6 Network Access Security Model

Contents

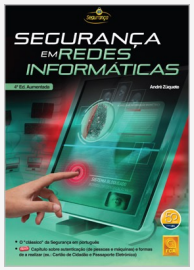
- Computer security concepts
  - ✓ Definition
  - ✓ Examples
  - ✓ Challenges
- Security attacks
  - ✓ Passive attacks
  - ✓ Active attacks
- Security services
  - ✓ Authentication
  - ✓ Access control
  - ✓ Data confidentiality
  - ✓ Data integrity
  - ✓ Nonrepudiation
  - ✓ Availability service
- Attack surfaces
- Security models
  - Network security model
  - Network access security model

Bibliography

Cryptography and network security, Stallings, Pearson, 2017, Chapter 1: Computer and Network Security Concepts



Segurança em Redes Informáticas, Capítulo 1: Introdução



Segurança Prática em Sistemas e Redes com Linux, Capítulo 1: Conceitos fundamentais