Lesson 4: Introduction to network security

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Dr. Justo Carracedo Gallardo
carracedo@diatel.upm.es

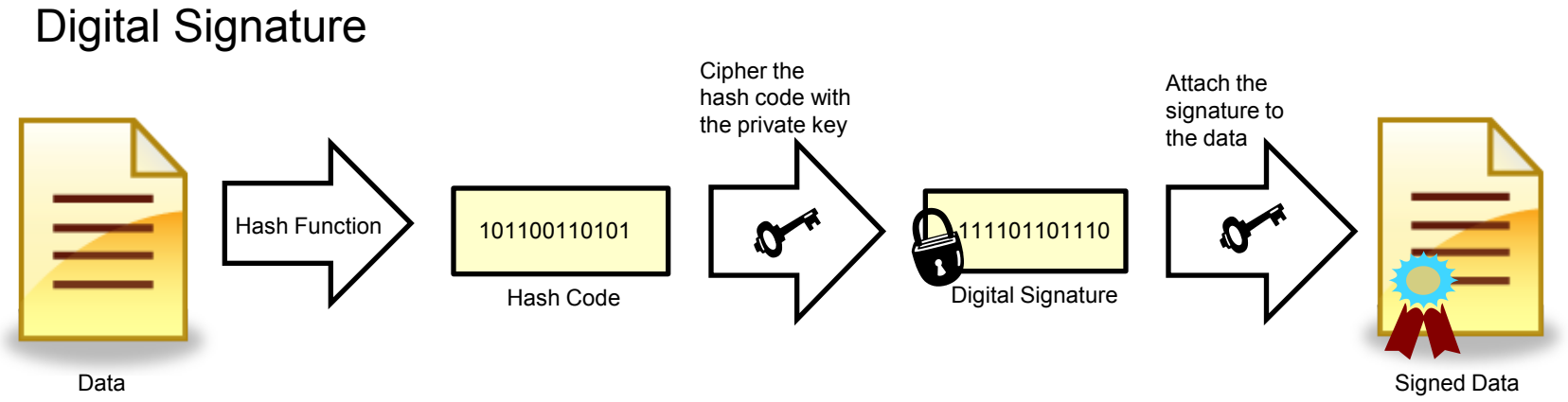
Technical University of Madrid
University Professor at the Telecommunication School (EUITT)

What is Network Security? (I)

- **A group of techniques** that try to *minimize* the vulnerability of the systems or the information contained within them.
- The aim is to make it more expensive to break security measures than the value of what is being protected.
- ***Total security*** **doesn't exist**: any protection measure is subject to being broken.

What is Network Security? (II)

- Today's **security technologies** offer computer networks a **much higher protection than the one available in the real world** for the exchange of paper documents.



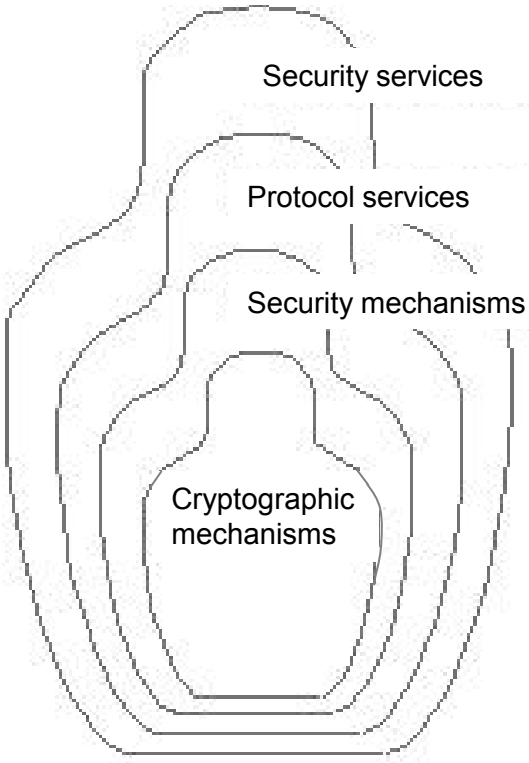
How to Protect Networks: Mechanisms, Protocols and Security Services (I)

- ***Security mechanisms*** are used to build the security protocols which allow security services to be provided.
- Security mechanisms are "**shields**" that thanks to security services protect the communication between users from the different attacks.

How to Protect Networks: Mechanisms, Protocols and Security Services (II)

Mechanisms => **Protocol** => **Service**

Security mechanisms are based mainly on cryptographic techniques. Therefore, most of them are *cryptographic mechanisms.*

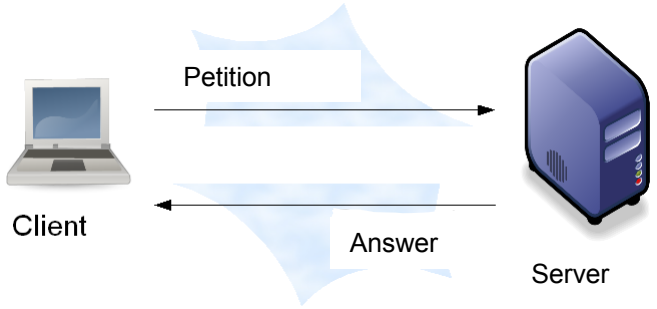


The base on which security services are created is ***cryptography***.

What's important to the end user are the **services!**

How to Protect Networks: Mechanisms, Protocols and Security Services (III)

- A **security protocol** is:
  - a group of rules and formats that determine the exchange of pieces of information
  - two or more entities intervene in the process
  - it is designed so that certain ***Security Services*** are provided to the users



How to Protect Networks: Mechanisms, Protocols and Security Services (IV)

- **Security services** protect the communication between users from different types of attacks:
  - **Attacks to the identity of entities**
    - Identity interception
    - Identity theft (*masquerade)*
  - **Attacks to services**
    - Denial of service (DoS)
  - **Attacks to information**
    - Data revelation
    - Data forwarding
    - Data manipulation
    - Repudiation of sent or received data

Important Security Services (I)

- Entity authentication
- Data confidentiality
- Data integrity
- Access control
- Non-repudiation
- Availability
- Anonymity

Important Security Services (II)

- **Authentication**

  This service guarantees that the communicating entity is who it claims to be.

- **Data confidentiality**

  Provides data protection to avoid them being revealed accidently or on purpose to an unauthorised person.

- **Data integrity**

  This service guarantees the receiver that the data they receive is exactly the same as the data that was sent. It detects when something has been added, deleted or changed.

Important Security Services (III)

- **Access Control**

  To avoid an unauthorised use of the network's resources. Who can do what?

- **Availability**

  The property of a system or resource to be accessible and useable by the authorised entities.

- **Anonymity**

  Hides a person's identity when performing an online operation:

  - Suggestions or claims
  - Polls
  - Electronic vote
  - Electronic money

Important Security Services (IV)

- **Non-repudiation**
  - **With proof of origin**

    The receiver of the message obtains demonstrable proof of the origin of the received data.
  - **With proof of sending**

    The receiver or the sender of the message obtains demonstrable proof of the date and time that it is sent.
  - **With proof of delivery**

    The sender of the message obtains proof, demonstrable to third parties, of the delivery of the data to the correct receiver.

Attackers... Hacker/Cracker

- **Knowing your enemy**

  There are several ways to classify attackers: by their knowledge, by their intentions, by the damage they cause, etc.

- **Definition of hacker and cracker** (*jargon dictionary*)

  Hacker: a person specialised in a topic who enjoys exploring it for the sake of learning and overcoming barriers. Applied to IT, the term refers to a person whose ability to understand computer systems, their design and programming, allows them to master the systems for a particular use.

  Cracker: applied to IT, a person who breaks into a computer system changing or damaging some type of information or element. Their motivation is usually a financial gain.

Security Policies

- The best way to protect a computer network is to **define clear action policies** (*security policies*) **and to raise computer security awareness.**

  Humans are usually the weakest link, so it is important to learn how to avoid failures derived from **social engineering**: an attacker's ability to manipulate people into performing actions for their gain and, therefore, infringing upon the defined protection measures.

intypedia

INFORMATION SECURITY ENCYCLOPEDIA

Contact: info@intypedia.com