# 1.5 How do we define security?

## How do we define security?

In this section we'll look at basic security terminology, the OSI model and network layers, as well as introduce some network attacks.

As a security expert responsible for security design, it is necessary to understand three things:

- Who or what is being protected?
- Who or what is attacking?
- What are the attacker's powers?

The answers to these questions make up what is called the **threat model**. Before starting to talk about securing a network, it is necessary to reason on what the potential threats are for that specific network.

As part of any analysis, we have principals. These **principals** are actors and participants that have a role in our analysis. Some agents are honest and some are not. As in many examples, let's consider Alice and Bob.

Alice and Bob use the Internet to exchange information. Alice and Bob are the honest agents. However, the Internet is vast and the communication between Alice and Bob is of some kind of interest for Charlie, who is a dishonest agent. Charlie is exploiting some Internet vulnerabilities to get access to the information exchanged by Alice and Bob.

Once we have identified the principals that can affect the security, we need to understand what security means.

Security can be defined as a combination of policy and mechanism.

A security policy is just a statement about what is allowed and not allowed to do in a system or on the 'object' being protected. This is defined by defining **security properties** that must hold. The most common security properties are Confidentiality, Integrity and Availability, which constitute what is commonly known as the CIA triad.

### Confidentiality

Assures that private or confidential information is not disclosed to unauthorised individuals.

### Integrity

Assures that information and programs are changed only in a specified and authorised manner.

### Availability

Assures that systems work promptly and service is not denied to authorised users.

Once we have the security properties we need **security mechanisms** which describe how to implement the security properties. We can think of the mechanisms as tools, methodologies or procedures for security enforcement.

For example, let's say to protect the integrity of the network we have introduced the security mechanisms 'Only "root" can execute this script'. We can then enforce this property by asking users to input the admin password in addition to checking if the user ID has root privileges.

A different example of a property is that voters can only vote once in any given election. This is then implemented in many countries by staining the voters' fingers with indelible ink to detect if they return back. In other countries the name of the voter is deleted from a database.

We can refer to security mechanisms based on their type. The following three are the most important.

### Deter

Deterring or discouraging unauthorised people from attempting to gain access to your facility, and, in our case, to our network, by implementing measures that unauthorised people perceive as too difficult or needing special tools and training to defeat (eg firewalls, cryptography, etc).

### Detect

Detecting unauthorised access as early as possible and implement measures to work out whether an unauthorised action is occurring or has occurred (eg Intrusion Detection Systems).

### Deny

Prevent unauthorised access by implementing measures to block unauthorised access (eg firewalls).

The above three are most important but there are other strategies such as delaying unauthorised users once they compromise the network, recovering after an attack by taking remedial steps, and insuring by passing the consequences of risk to someone else.

There are many mechanisms you may choose to employ. Here are some examples.

- **Identification of principals**: requiring usernames to identify users.
- **Authentication**: password checks to ensure a user is who they claim to be.
- **Authorisation**: checking if the principal is allowed to do the requested action.
- **Physical protection**: locks, swipe cards and enclosures.
- **Encryption and decryption algorithms**.
- **Economics**: a common assumption from economics is that adversaries are rational and self-interested, hence if emails are associated with a cost we will have less spam as the spammer will not want to lose money.
- **Deception**: getting an adversary to reveal themselves by using honeypots on extremely vulnerable servers which are deployed as 'weak entities', to see who will attack, and how they will attack it. Lessons learned from honeypot can be used to protect production servers.
- **Randomness, unpredictability**: not using common words for passwords.

Are there any other mechanisms you know of? Share them in the weekly forum.