UNIVERSITÀ DEGLI STUDI
DI GENOVA

University of Studies of Genoa

Computer Security

Lorenzo Vaccarecci

2024-2025

Contents

Chapter 1

Introduction

Computer security deals with the preventon and detection of unauthorized actions by users of a computer system.

- **Authorization** is central to definition
- Sensible only relative to a security policy, stating who (or what) may perform which actions

1.1 Information Security

Is even more general. It deals with information independent of computer security.

1.1.1 Key Concepts

- Security concerns the protection of assets from threats
- Owners value their assets and want to protect them
- Threat agents also value assets, and seek to abuse them
- Owners analyse threats to determine which ones apply; these are the risks that can be costed. This helps the selection of countermeasures, which reduce the vulnerabilities (may remain leaving some residual risk, owners seek to minimise that risk)

$$\text{Risk}_E = \text{Pr}_E \cdot \text{I}_E$$

where Pr_E is the probability of an event E and I_E is the impact of the event E.

1.2 Protection countermeasures

- **Prevention**: try to prevent security breaches by system design and employing appropriate security technologies as defences
- **Detection**: in the event of a security breach, we try to ensure that it will be detected. Logging and MACs (file hashes to detect alteration) are primary methods of detection, although intrusion detection systems which activelyy watch for intruders are more common
- **Response**: in the event of a security breach, we must respond or recover the assets. Responses range from restoring backups through to informing appopriate concerned parties or law-enforcement agencies

1.3 Security Properties

1.3.1 Confidentiality

Information is not learned by unauthorized principals

Confidentiality is sometimes characterised as the unauthorized reading of data, when considering **access control** measures. But in general we are concerned with unauthorized learning of information, which is more subtle to contend with. Confidentiality presumes a security policy saying who or what can access our data. The security policy is used for access control.

- **Privacy**: confidentiality for individuals
- **Secrecy**: confidentiality for organizations
- **Anonymity**: keeping one's identity private

1.3.2 Integrity

Data has not been maliciously altered

Intergrity has more general meanings elsewhere, but in computer security we are concerned with preventing the possibly malicious alteration of data, by someone who is not authorized to do so. Integrity in this sense can be characterised as the unauthorized writing of data. Again, this presumes a security policy saying who or what is allowed to alter the data.

1.3.3 Authenticity

Data or services available only to authorized identities

Authentication is th processo of verification of identity of a person or system. Some form of authentication is a pre-requisite if we wish to allow access to services or data to some people but deny access to others, using an access control system. Methods for authentication are often characterised as:

- something you have
- something you know
- something you are

Also, where you are may be implicity or explicity checked. Several methods can be combined for extra security.

1.3.4 Availability

Data or services can be accessed in a reliable and timely way

Threats to availability cover many kinds of external environmental events as well as accidental or malicious attackks in software. In computer security we're concerned with protecting against the second kind of threat, rather than providing more general forms of fault-tolerance or dependability assurance. Ensuring availability means preventing **denial od service** (DoS) attacks, insofar as this is possible. It's possible to fix attacks on faulty protocols, but attacks exhausting available resources are harder, since it can be tricky to distinguish between an attack and a legitimate use of service.

1.3.5 Accountability

Actions are recorded and can be traced to the party responsible

If prevention methods and access controls fail, we may fall back to detection: keeping a secure audit trail is important so that actions affecting security can be traced back to the responsible party. A stronger form of accountability is non-repudation, when a party cannot later deny some action. Creating an audit trail with machine logs is a tricky problem: if a system is compromised, the logs may also be tampered with. Ways around that problem are to send log messages to an append-only file, a separate server, or even a physically isolated printer.

1.4 Implementing a security solution

- A **security analysis** surveys the threats which pose risks to assets, and then proposes policy and solutions at an appropriate cost.
- A **threat model** documents the possible threats to a system, imagining all the vulnerabilities which might be exploited
- A **riks assessment** studies the likelihood of each threat in the system environment and assigns a cost value, to find the risks
- A **security policy** addresses the threats, and describes a coherent set of countermeasures

The costs of countermeasures is compared against the risks, and juggles to make a sensible trade-off. This allows a security solution to be designed, deploying appropriate technologies at an appropriate cost. Partly this is a budgeting exercise; but it's also important to spend effort in the right place.