Computer Security
Theory

Christian Rossi

Academic Year 2023-2024

Abstract

The course topics are:

- Introduction to information security.
- A short introduction to cryptography.
- Authentication.
- Authorization and access control.
- Software vulnerabilities.
- Secure networking architectures.
- Malicious software.

Contents

CHAPTER 1

Introduction

1.1 Basic security requirements

The fundamental security principles, known as the CIA paradigm for information security, outline three key requirements:

- *Confidentiality*: only authorized entities can access information.
- *Integrity*: information can only be modified by authorized entities in authorized ways.
- *Availability*: information must be accessible to all authorized parties within specified time limits.

It's worth noting that the availability requirement can sometimes conflict with the other two, as higher availability exposes the system for longer durations.

1.2 Definitions

Definition (*Vulnerability*)**.** A vulnerability is a flaw that can be exploited to violate one of the constraints of the CIA paradigm.

Definition (*Exploit*)**.** An exploit is a specific method of leveraging one or more vulnerabilities to achieve a particular objective that breaches the constraints.

Definition (*Asset*)**.** An asset is anything of value to an organization.

Definition (*Threat*)**.** A threat is a potential event that could lead to a violation of the CIA paradigm.

Definition (*Attack*)**.** An attack is a deliberate use of one or more exploits with the aim of compromising a system's CIA.

Definition (*Threat agent*)**.** A threat agent is any entity or factor capable of causing an attack.

Definition (*Hacker*)**.** A hacker is an individual with advanced knowledge of computers and networks, driven by a strong curiosity and desire to learn.

Definition (*Black hats*)**.** Malicious hackers are commonly referred to as black hats.

1.3 Ethical hacking

White hats, also known as security professionals or ethical hackers, are tasked with:

- *Identifying vulnerabilities.*
- *Developing exploits.*
- *Creating attack-detection methods.*
- *Designing countermeasures against attacks.*
- *Engineering security solutions.*

Since no system is invulnerable, it's crucial to assess its risk level. This involves evaluating the potential damage due to vulnerabilities and threats through the concept of risk:

Definition (*Risk*)**.** Risk is a statistical and economic evaluation of potential damage resulting from the presence of vulnerabilities and threats:

$$\text{Risk} = \text{Asset} \times \text{Vulnerabilities} \times \text{Threats}$$

Assets and vulnerabilities can be managed, but threats are independent variables.

To ensure system security, a balance must be struck between cost and reducing vulnerabilities and containing damage. The costs of securing a system can be categorized as direct and indirect. Direct costs include management, operational, and equipment expenses, while indirect costs, which often form the larger portion, stem from:

- *Reduced usability.*
- *Slower performance.*
- *Decreased privacy* (due to security controls).
- *Lower productivity* (as users may be slower).

It's important to note that simply spending more money on security may not always resolve the issue.

In real-world systems, setting boundaries is essential, meaning that a portion of the system must be assumed as secure. These secure parts consist of trusted elements determined by the system developer or maintainer. For example, the level of trust in a particular system can be determined at the software, compiler, or hardware level.

CHAPTER 2

Cryptography

2.1 Introduction

Definition (*Cryptography*)**.** Cryptography is the study of techniques to allow secure communication and data storage in presence of attackers.

The features provided by cryptography are:

- *Confidentiality*: data can be accessed only by chosen entities.
- *Integrity/freshness*: detect or prevent tampering or replays.
- *Authenticity*: data and their origin are certified.
- *Non-repudiation*: data creator cannot repudiate created data.
- *Advanced features*: proofs of knowledge or computation.

2.1.1 History

Cryptography is as old as written communication. It was born for commercial or military uses. The first cryptographic algorithms were computed by hand with pen and paper.

The original approach consisted in a battle of wits between cryptographers (ideate a method to obfuscate a test) and cryptanalyst (break the cipher).

A turning point came when Bellaso (1553) was the first to have the idea to separate encryption method from the key.

In 1883 Kerchoff found six principles to obtain a good cipher:

1. It must be practically, if not mathematically, unbreakable.
2. It should be possible to make it public, even to the enemy.
3. The key must be communicable without written notes and changeable whenever the correspondents want.
4. It must be applicable to telegraphic communication.

5. It must be portable, and should be operable by a single person.

6. Finally, given the operating environment, it should be easy to use, it shouldn't impose excessive mental load, nor require a large set of rules to be known.

In 1917 the first mechanical computation (given by the rotor machine by Hebern) changed the cryptography. This rotor machine were commercialized to people at the beginning of 1920. At the start of World War II the Germans upgraded this rotor machine with a new version called Enigma. Enigma's workflow where then decrypted by cryptanalyst at Bletchey park, that led Eisenhower to the win of the war.

After World War II, in 1949 Shannon proved that a mathematically secure ciphers exists.

Later, in 1955, Nash argued that computationally secure ciphers are also ok. Consider a cipher with a finite, λ bit long, key. The conjecture is that if parts of the key interact complexly in the determination of their effects on the ciphertext, the attacker effort to break the cipher would be $\mathcal{O}(2^\lambda)$. This means that the owner of the keys takes $\mathcal{O}(\lambda^2)$ to compute the cipher. This means that the computational gap is unsurmountable for large λ.