Cryptography

Algorithms, Protocols, and Standards for Computer Security

Zoubir Mammeri

WILEY

Cryptography

Cryptography

Algorithms, Protocols, and Standards for Computer Security

Zoubir Mammeri

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada.

Library of Congress Cataloging-in-Publication Data:
Names: Mammeri, Zoubir, author. | John Wiley & Sons, publisher.
Title: Cryptography : algorithms, protocols, and standards for computer security / Zoubir Mammeri.
Description: Hoboken, New Jersey : JW-Wiley, [2024] | Includes bibliographical references and index.
Identifiers: LCCN 2023030470 | ISBN 9781394207480 (hardback) | ISBN 9781394207497 (pdf) | ISBN 9781394207503 (epub) | ISBN 9781394207510 (ebook)
Subjects: LCSH: Cryptography. | Computer security.
Classification: LCC QA268 .M34 2024 | DDC 005.8/24--dc23/eng/20230807
LC record available at https://lccn.loc.gov/2023030470

Cover Design: Wiley
Cover Image: © zf L/Getty Images

Set in 9.5/12.5pt STIXTwoText by Integra Software Services Pvt. Ltd, Pondicherry, India

Contents

Preface

For millennia, human beings have used multiple forms of codes to protect their oral communications, entries of castles, their messages, and other belongings. Indeed, cryptography existed early in human history and civilizations, before the event of computers. Cryptography has been developed and improved over the centuries, in particular for protecting military secrets and spying on enemies, then for protecting industrial and economical secrets, then for protecting recent applications made possible with the use of the internet, and ultimately for protecting the privacy of electronic devices' users. In a highly computerized world, cryptography is the pillar of security. Encrypting and signing are the most performed cryptographic operations in the digital world.

Cryptography provides services to secure websites, electronic transmissions, and data repositories. For more than three decades, public-key cryptography has been enabling people, who never met before, to securely communicate and trust each other. Cryptography is not only used over the internet, but also in phones, bank cards, televisions, cars, aircrafts, door locks, implants, and a variety of other devices. Without cryptography, hackers could get into victims' emails, listen to their phone conversations, tap into their cable companies and acquire free cable services, or break into their bank accounts.

Cryptography is the discipline at the intersection of computer science and mathematics. It provides algorithms for guaranteeing confidentiality, integrity, authentication, and non-repudiation for parties that share data or exchange messages to perform operations and transactions in cyberspace. For example, customers' bank accounts or citizens' votes must remain confidential and not altered by any unauthorized third party. E-merchants, as well as clients, must be protected from each other; a customer, who ordered an article, could not deny ordering; and a merchant, who has been paid, could not deny having been. A person, who digitally signed an agreement or a contract, cannot deny having signed. Such protections, and many others, are provided thanks to cryptography.

Cryptography standards are needed to enable interoperability in cyberspace. In general, standard protocols follow rigorous procedures of testing before their adoption. Therefore, it is highly recommended to use only standard security protocols to build information security systems. Security, in general, and cryptography, in particular, have evolved at a rapid pace in the past two decades. Security technology has gone through tremendous changes in terms of protocols and standards. The continuous evolution of information technology, on one hand, and the discovery of vulnerabilities in standards, on the other hand, motivate the development of new standards. In the last 15 years, cryptography standards made tremendous advances that are not included in existing books. Some standards have become obsolete and others have recently been recommended. This book aims at providing a comprehensive description of recent advances in cryptographic protocols. The focus is on the NIST (National Institute for Standards and Technology, US) and IETF (Internet Engineering Task Force) standards, which are commonly used in the internet and networking applications.

This book, also, aims at providing a comprehensive description of notions, algorithms, protocols, and standards in the cryptographic field. It addresses algorithms through examples and problems, highlights vulnerabilities of deprecated standards, and describes in detail algorithms and protocols recommended in recent standards. In addition, it focuses on the basic notions and methods of security analysis and cryptanalysis of symmetric ciphers. The book is designed to serve as a textbook for undergraduate and graduate students, as well as a reference for researchers and practitioners in cryptography.

Definitions Used in the Book

Definitions included in this book are inspired by NIST and IETF glossaries [1,2]. They are not formal definitions. Rather, they are provided to summarize the basic notions of cryptography and facilitate the learning of algorithms and protocols.

1) Paulsen C, Byers RD. Glossary of Key Information Security Terms. NIST; 2019.
2) Shirey R. Internet Security Glossary, RFC 4949. Internet Engineering Task Force; 2007.

Organization of the Book

Chapter 1: This chapter introduces aims at introducing the main issues and notions of security in computer-based systems. The main properties of security (namely confidentiality, integrity, authenticity, and non-repudiation) are introduced. A taxonomy of attacks on digital assets is provided. Multiple components and practices, required to address from different perspectives the security of computer-based systems, are introduced in this chapter. The main technical components of security include cryptography, which is the focus of the remainder of the book.

Chapter 2: Cryptography has developed and improved over time. Chapter 2 aims at providing a brief history of cryptography and presenting its main notions and techniques. Breaking cryptographic codes is a very ancient activity to disclose secrets. An overall categorization of attacks on modern cryptographic algorithms is discussed in this chapter. There exist two main categories of cryptographic systems: symmetric and asymmetric (also called public-key) cryptosystems. The design differences between both categories are briefly discussed. Message digest, digital signature, and digital certificate are of prime importance to establish trust between parties that share data and exchange messages. These notions are introduced in Chapter 2.

Chapter 3: This chapter aims at reviewing and presenting, with examples and exercises, the mathematical background useful to address cryptography algorithms. In particular, modular arithmetic and finite fields are of prime importance to understand the design of cryptographic algorithms. Fundamental theorems for cryptography are provided. In addition, to mathematical notions, computation algorithms (such as Extended Euclidean algorithm, square-and-multiply method to perform modular exponentiation, modular multiplication, Gauss's algorithm to solve congruence systems, Tonelli-Shanks's algorithm to find modular square roots, and Rabin's algorithm to test irreducibility of polynomials), which are often used in cryptographic algorithms, are introduced with examples and exercises. Readers who have a sufficient background in the reminded notions and algorithms can skip this chapter.

Chapter 4: Shift and substitution ciphers have been used in written text transmission; and dominated the art of secret writing for at least two millenniums. The most known historical ciphers in this category include Caesar's, Vigenere's, Affine, One Time Pad, and Enigma ciphers. All those ciphers are original inventions, with ideas and principles that inspired authors of modern cryptographic algorithms. Before presenting modern cryptographic algorithms, Chapter 4 aims at providing an overview of historical ciphers and their ingenious ideas. Methods used to break historical ciphers have widely been exploited to design modern ciphers.

Chapter 5: This chapter introduces three notions of cryptography: hash functions, message authentication codes, and digital signature. All of them are of paramount importance for providing integrity and authentication guarantees. Hash functions produce digital fingerprints, also called message tags, which are mainly used to verify the integrity of messages and files, to generate and verify digital signatures, and to generate random numbers. Approaches to design hash functions and standard hash functions (i.e. SHA-1, SHA-2, and SHA-3) and standard Message Authentication Codes (i.e. HMAC and KMAC) are described in detail. Common attacks against MAC algorithms and digital signatures are discussed.

Chapter 6: Stream ciphers are symmetric ciphers that encrypt and decrypt bits individually. They are used, in particular, to secure communications in wireless and cellular networks. Stream ciphers are well-suited to hardware implementation and they are generally faster than block ciphers. They also are well-suited to encrypt and decrypt continuous data at high rate and when devices have limited memory to store long messages. Often, stream ciphers are designed using LFSRs (Linear-Feedback Shift Registers) combined with nonlinear filtering functions. Chapter 6 aims at providing a discussion of the design principles of LFSRs and stream ciphers to produce keystream bits, used to encrypt plaintexts and decrypt ciphertexts. It also provides a detailed description of the most known and standard stream ciphers: A5/1, E0, SNOW 3G, ZUC, Chacha20, RC4, Trivium, and Enocoro.

Chapter 7: This chapter addresses block ciphers, which are the most used algorithms to secure data and messages. Data or messages are split into blocks of a fixed size (e.g. 128 bits) and plaintext blocks are encrypted individually to generate

ciphertext blocks of the same bit-length than that of a plaintext block. In addition to ciphering, block ciphers can be used to generate pseudorandom numbers or to build hash functions and MACs (Message Authentication Codes). A huge number of block ciphers are published in literature. However, a very small number of them are standards that are used in operational cryptosystems. This chapter introduces the basics of construction of block ciphers and presents in detail the standard block ciphers, currently in use, namely TDEA (Triple Data Encryption Algorithm) and AES (Advanced Encryption Standard). Known attacks against block ciphers are discussed.

Chapters 8 and 9: A block cipher, such as AES or TDEA, takes a fixed-size plaintext block and returns a ciphertext block of the same size. However, in many applications, a plaintext (e.g. a text file or an image) is composed of several (maybe in thousands or even more) blocks. When plaintext blocks are repeated in the same data or message and identically encrypted, an attacker may infer some information regarding the ciphertexts that he/she intercepted. In addition, in many applications, the recipient of a message may need to authenticate the message sender. Chapter 8 addresses standard operation modes of block ciphers to guarantee confidentiality. The NIST recommends 11 modes (ECB, CBC, CBC-S1, CBC-S2, CBC-S3, OCB, CTR, CFB, FF1, FF-3, and XTS-AES) for guaranteeing confidentiality. Chapter 9 focuses on modes of operation of block ciphers to provide either authentication or confidentiality and authentication. NIST recommends three modes (CMAC, GMAC, and Poly1305-AES), for authentication-only, and six modes (CCM, GMAC, AED-ChaCha20-Poly1305, KW, KWP, and TKW) for authentication and confidentiality. All the 20 operation modes recommended by NIST are addressed in detail in Chapters 8 and 9. Known attacks against operation modes are also discussed.

Chapter 10: Modern cryptographic security relies on the computational difficulty to break ciphers rather than on the theoretical impossibility to break them. If adversaries have enough resources and time, they can break any cipher. The security analysis of block ciphers and their modes of operation is a wide field in cryptanalysis. It aims at finding bounds on the amount of data to encrypt with the same key without compromising the security of encrypted data. Chapter 10 introduces security analysis in which adversaries are given black boxes that simulate block ciphers or their modes of operation. Then, adversaries query black boxes, receive ciphertexts, plaintexts, or tags, and try to guess some information about the used keys or to forge signatures or message tags. Secure ciphers are those ciphers for which the advantage of adversaries is negligible if their resources and time remain below some limits. The analysis of different scenarios of attacks is an approach to assess the security of ciphers from a probabilistic point of view.

Chapter 11: Cryptanalysis is the science and techniques of analyzing and breaking cryptographic algorithms and protocols. It is a very exciting and challenging field. There exist hundreds of cryptanalysis attack variants. Chapter 11 aims at presenting the most known cryptanalysis attacks against symmetric ciphers, namely memory-time trade-off attacks, linear cryptanalysis, differential cryptanalysis algebraic cryptanalysis, cube attacks, divide-and-conquer attacks, and correlation attacks.

Chapter 12: The turning point in modern cryptography occurred in 1976–1977, when Diffie and Hellman on one side and Rivest, Shamir, and Adleman, on the other, proposed original schemes to secure systems without requiring a unique cipher key shared by both parties. The proposed schemes were and are still used to design public-key cryptosystems. The latter provide support to secure communications worldwide between people who do not a priori know each other. The first and still most widely used public-key cryptosystem is with no doubt RSA. Modern cryptography is founded on the idea that the key used to encrypt messages can be made public, while the key used to decrypt messages must be kept private. Chapter 12 aims to describe public-key algorithms and protocols, for providing confidentiality, integrity, and authentication guarantees. They include RSA, Diffie-Hellman key exchange, Menezes-Qu-Vanstone, and ElGamal cryptosystems. The security of public-key cryptosystems is based on either the integer factorization problem or the discrete logarithm problem over cyclic groups. Those problems are known to be computationally infeasible for large numbers; and they are discussed in this chapter. Known attacks against addressed algorithms are introduced.

Chapter 13: The second generation of public-key cryptosystems are based on elliptic curve theory. Elliptic curve (EC) cryptography algorithms entered wide use in 2004. After a slow start, EC-based algorithms are gaining popularity and the pace of adoption is accelerating. EC cryptosystems have been adopted by Amazon, Google, and many others to secure communications with their customers. EC cryptosystems amply outperform RSA-based cryptosystems. Until 2015, the NSA (National Security Agency, US) recommended 256-bit EC cryptography for protecting classified information up to the secret level and 384-bit for Top-secret level. Since 2015, the NSA has recommended 384-bit for all classified information. IETF standards have been proposed to support EC for Transport Layer Security. Chapter 13 aims at addressing different forms of EC-based algorithms, such as ECDSA, to provide confidentiality, integrity, and authenticity guarantees. Compared to RSA, EC-based algorithms make use of more difficult mathematical operations, which are addressed in this chapter.

Chapter 14: Keys are owned and used by entities that interact with each other to perform specific operations in different fields of activities. These keys are analogous to the combination of a safe. If adversaries know the combination of a safe, then the latter does not provide any security against attacks, even it is very complex. Keys are the most valuable items in computer security. Therefore, their protection is of paramount importance. Chapter 14 focuses on key management, which provides functions to secure cryptographic keys throughout their lifetime. It mainly includes key generation, storage, distribution, recovery, suspension, and withdrawal. This chapter aims at introducing the main mechanisms and protocols for key generation, key agreement, key transport, and key distribution over unsecure channels.

Chapter 15: Parties, which exchange encrypted messages over the internet, need to trust each other to secure their operations and transactions in e-commerce, e-banking, e-voting, etc. In addition, parties that exchange messages or access encrypted data inside a company or an institution, where messages/data are encrypted using symmetric keys, need to securely share their keys. Chapter 15 addresses both situations and presents different notions, including key distribution center, digital certificate, certification authority, and Public-key infrastructures (PKIs). PKIs are of paramount importance to establish trust between partners that do not a priori trust each other in the open digital world. Today, digital certificates are used by billions of end-entities, including web servers and their clients, to authenticate each other. The main protocol to secure communications over the internet is with no doubt TLS (Transport Layer Security); it is introduced in this chapter.

Chapter 16: Modern cryptography is fundamentally based on large random and prime numbers. In particular, keys should be generated using large random numbers; and RSA keys are generated using large prime numbers. Any weakness (in term of randomness) in a selected key may result in damage of data and messages protected by that weak key. Chapter 16 addresses algorithms and methods recommended to generate random and prime numbers. True random numbers are hard to produce by computer. In consequence, deterministic random number generators (DRNGs) are of common use in cryptography. However, it is of prime importance to use only DRNGs recommended by NIST and IETF. DRNGs cannot guarantee that generated integers are prime. Therefore, algorithms for testing primality are of common use in cryptography. When prime numbers are required, only provable and probable primes should be used. Probable primes are those integers shown to be prime by probabilistic tests. Both types of primes are discussed in this chapter.

Appendix: A series of 200 multiple choice questions (with answers), relating to computer security in general and to cryptography in particular, are proposed for knowledge testing. These MCQs were collected from various sources, including questions for job applicants, course certification, and exams in IT security field.

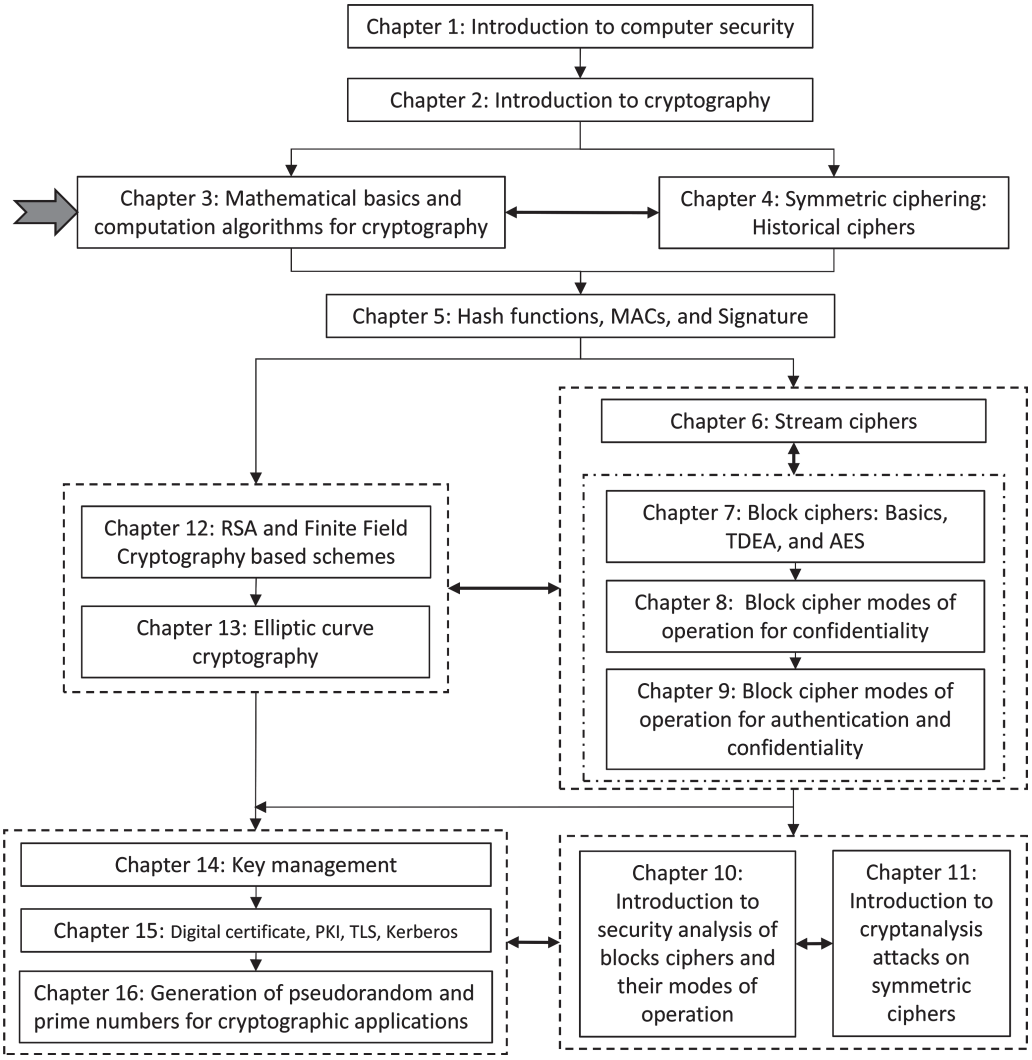
Using the Book as a Course

Some chapters are independent of each other, while some chapters are grouped into blocks, because they share notions, objectives, or mathematical background. Chapter blocks are marked with dotted lines. Therefore, the book may be used in different ways, depending on the audience. In particular, chapters focusing on symmetric-key algorithms are independent of those addressing public-key algorithms. Various learning paths are suggested in the figure below, where single arrows show the recommended sequential reading order of chapters, while double arrows indicate that the reader can focus on chapter blocks in any order.

Chapters 1 and 2 are introductive. Therefore, it is recommended to read them. Chapter 3 recalls mathematical background. It could be skipped and, at any time, the reader can return to this chapter to learn about mathematical notions used in the other chapters. For readers not familiar with modular arithmetic and algebra notions, it is recommended to take time to address the exercises given in Chapter 3.

Chapter 4 is a review of historical ciphers. It is recommended in order to learn some roots of modern cryptography. Chapter 5 presents notions relevant to both symmetric and asymmetric cryptosystems.

The two big chapter blocks (i.e. symmetric and asymmetric algorithms, protocols, and standards), may be addressed in any order. However, we recommend finishing a block before starting the other one. Chapters 10 and 11 focus on advanced notions in cryptanalysis of symmetric ciphers. Therefore, they are recommended for graduate students.



For feedback, contact the author at
zoubir.mammeri@irit.fr or zoubir.mammeri11@gmail.com

1

Introduction to Computer Security

Information and computer technologies (ICT), or simply IT technologies, are everywhere, in all fields of activities (business, commerce, transportation systems, health, leisure, education, administration, national security, army, etc.). Nowadays, human beings are more than ever dependent on IT technologies. Therefore, IT security became a paramount concern for any owner or user of electronic devices.

Since the early stage of computers, cyberattacks have never stopped. Worse, statistics provided annually by cybercrime observers and experts often show increases in attacks worldwide. In particular, ransom attacks have become the most lucrative criminal activities in the cyberspace. Partial or total shutdown of systems, as long as ransoms are not paid, results in losses in billions of dollars for companies, hospitals, e-merchants, banks, and individuals.

This chapter aims at providing an introduction to the main issues and notions of security in computer-based systems and tries to answer the following questions:

- What are the security issues and requirements?
- Why and how do security attacks occur?
- How to face security attacks? That is, what are the countermeasures to security attacks?

Security techniques encompass at least two distinct domains:

- Technical domain, including hardware and software design to address security;
- Organizational domain, including education, staff training, and laws to make involved people aware of IT security.

This book addresses security from a technical point of view only; in particular, it addresses cryptography. However, it should be clear that technology alone is not enough to address security. Imagine that you use a sophisticated alarm system in your home, but the code to access the system is "1234"; or if a teenager in your family does not protect the house alarm code when he/she is at school or at sport club; or even worse, he/she forgets switching on the alarm system when he/she leaves your home. Therefore, organizational issues (including education to security) are of prime importance.

Several books (including [1–9] and journal papers [10, 11]) addressed in detail IT security. This chapter aims only to present the notions of IT security, in particular the security services that can be supported by cryptographic algorithms.

1.1 Introduction

1.1.1 Why Do Attacks Occur?

Since the dawn of time, evil behavior of human beings have emerged: stealing or destroying belongings of others, injuring or even killing others, having interest in details or even disclosing the private life of others, etc.

Different human's defaults result in misbehaving; they include:

- Ego (i.e. Be the best and the center of the world).
- Greediness (i.e. Own all or the maximum of things/goods).
- Curiosity (i.e. Know private details about the others).
- Revenge (i.e. Having been mistreated, seek revenge without going through justice).

Cryptography: Algorithms, Protocols, and Standards for Computer Security, First Edition. Zoubir Mammeri.

- Competition (i.e. Be the first in sport, business, science, ...).
- Beliefs (religion) (i.e. Having some religious beliefs, do not agree with those of others or worse hate and fight them).
- Opinions (politics, ideology) (i.e. same reasons as those for religious beliefs).

Therefore, there is no unique profile (or reason) for potential attackers and criminals to act. Attacks on computer-based systems are one of the evil facets of humanity. We would say, times change, but the original flaws remain. Attacks can be prevented, detected, and handled to mitigate their effects. We cannot ignore them or naïvely hope that they will definitely cease. From ICT point of view, attacks may be classified as:

- Theft of private or confidential data.
- Data disclosure regarding privacy of individuals (their home, their beliefs, ...) or disclosing industrial and business secrets of companies, strategies of governments, and national defense secrets.
- Threats and ransoms (via email) to extort secrets (in case of spying) or money.
- Sabotage of ICT resources, which may be data alteration to force the use of erroneous/false/fabricated data, data deletion to prevent data owners to access their data, or computer shutdown or slowing down to make it unusable by its users.
- Sabotage of physical equipment (such as cars, trains, satellites, antennas, factories, smart grids, smart homes, nuclear plants, hospitals, patients...), for example, exploiting vulnerabilities of wireless communications and/or viruses.

When we disregard security issues, all of us are convinced that computers and the internet would be a revolution never seen before. Using Internet, communications between people and between devices became easy and worldwide. Communication borders between people have been deeply transformed and abolished to some extent. Internet has transformed earth into a village, from the communication point of view. Using Internet has so many benefits in almost all domains: industry, economy, society, health, learning, leisure, politics, democracy, etc.

Unfortunately, when security is of concern, the internet is probably the worst technology that harms computer-based assets. Internet became a haven for hackers, cyberterrorists, government-sponsored espionage agencies, etc., allowing attackers to operate from anywhere on earth, in particular from hostile countries or countries without deterrent and applicable laws.

1.1.2 Are Security Attacks Avoidable?

A drastic solution was suggested by Gene Spafford: "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards," quoted in [12]. Unfortunately, Spafford's solution prevents any use of computers or systems. In practice, using a computer (or any other electronic device) is risky for any user.

The objectives of security techniques are to minimize the risks at reasonable cost. For example, protection of one's family pictures and the protection of national security and defense systems do not involve similar risks or similar costs. One thing should be clearly understood: there is no 100% secure and reliable system, which is human-made and (directly or indirectly) accessible to attackers. In practice, many risks are taken into consideration only when attacks are reported. In preference, the attacks should first affect others, and we are happy to learn from their misfortunes (credit card stealing, lock of cars, shutdown of hospital services, etc.).

1.1.3 What Should Be Protected in Cyberspace?

Definition 1.1 Cyberspace*: it is the space composed of electromechanical devices, computers, communication links, and applications servers where humans interact using the provided facilities.*

Cyber comes from *Cybernetics*, which is a large discipline including control systems, electrical theory, mechanical engineering, logic modeling, and others. The main component of cybernetics is the computer. Starting from the 1960s most of engineering studies in cybernetics have been specialized and became computer science, electronics, automation, telecommunications, and so on.

From security point of view, protections focus on:

- *Physical entities*: including plants, labs, stores, parking areas, loading areas, warehouses, offices, machines, robots, vehicles, products, materials, etc. At this level, the protection is physical (e.g. protect doors, PCs, cables, etc.).

- *People*: protect life, health, the privacy of staff members, customers, and guests.
- *Data*: protect files, databases, messages, programs, servers...

This book focuses on data protection only. However, before focusing on data protection, below is a brief introduction to barriers used for physical protection to enforce data protection.

i) Physical barriers

They are used to deter the potential attackers; they include:

- Guards: deploy security agents in and around vulnerable areas.
- Fences: build high and impassable fences and walls.
- Restricted access technologies (alarms, locks): deploy alarm systems to detect intrusions and highly-resistant locks to prevent unauthorized access.

ii) Physical access restrictions

They are used to deter attacks; they include:

Isolation of computers or networks to make them inaccessible.
Encryption of removable media and storage in restricted-access areas.
Use remote storage systems (e.g. cloud servers) to store data in secure locations or to store copies of data to download in the event of damage of the original copies.

iii) Personnel security practices

They participate in improving data protection; they include:

- Limited access zones: according to the criticality of zones, different access rights must be granted to staff, personnel, customers, and visitors.
- Biometrics and badges: use biometrics and badges to enforce identification and authentication.
- Faraday cages: in some (critical) situations, Faraday's cages are used to enforce data protection. There is no communication interception, when communicating devices are inside a Faraday's cage.
- Training: security training includes awareness regarding the good practices, awareness regarding the abnormal behavior reporting, and enforcement of the spirit of loyalty and patriotism.

Notes

– Physical access barring is the first defense line and it is deterrent against attackers. Without physical protection measures, it is very unlikely that data protection would be assured.
– Physical protection comes with high costs; and it is mainly deployed by institutions and companies. The costs depend on the required protection level.

1.1.4 Security vs Safety

There are two different properties (or functional requirements) regarding ICT systems: safety and security. Unfortunately, those two terms are sometimes mixed up and used interchangeably.

- *Safety*: it aims at addressing the issues to protect systems against risks and threats that come with *technology*, including hardware failures, software errors, communication interferences, etc.
- *Security*: it aims at addressing the issues to protect systems against *human attacks* on computers, servers, and data.

To better understand the difference between safety and security, let's take the case of home security. We use robust materials to build safe houses regarding flood, fire, heat, rain, snow, and wind; it is the safety concern. We use robust locks, cameras, and alarms to make houses secure regarding thieves; it is the security concern.

1.1.5 Cybersecurity vs IT Security

Often, the three terms *cybersecurity, IT security*, or simply *security* are used interchangeably in the information technology and science fields. However, there exists some difference between those terms, as stated by the NIST [1] [13].

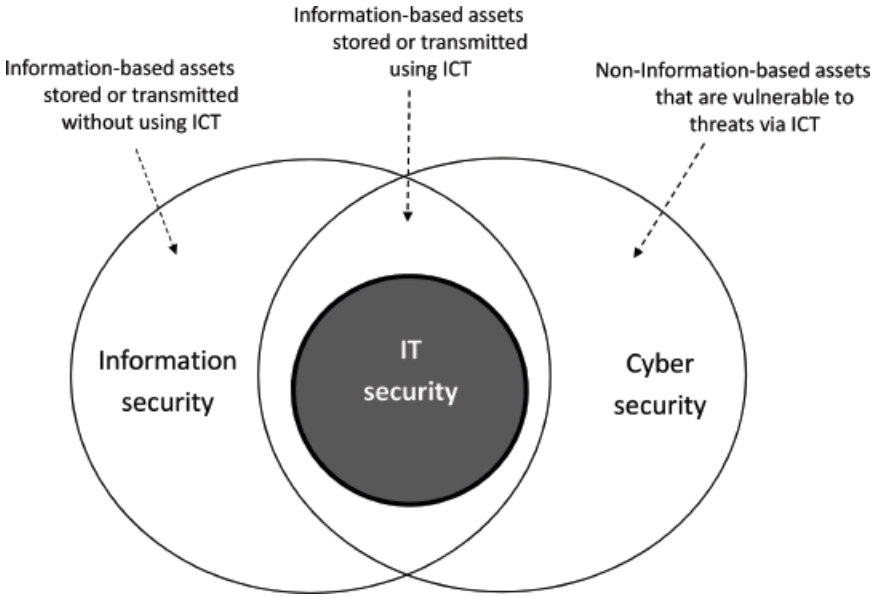


Figure 1.1 IT security vs cybersecurity.

- *Information security* is defined as: the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- *Cybersecurity* is defined as: the ability to protect or defend the use of cyberspace from cyberattacks. Cybersecurity is about securing devices (computers, mobile devices, applications, and data) that are accessible through ICT.

In practice, cybersecurity term is often used by people not directly involved or specialized in computer science (e.g. police officers, judges, presidents, and mayors) to talk about attacks made via Internet. Whereas IT security or simply security terms are used by those people directly involved in computers and software. In this book, *security* is used to designate *IT security*. Figure 1.1 provides an overall comparison of *IT security* to *Cybersecurity*, where:

- *Information* (of a company, country, or an individual) includes digital and non-digital (i.e. papers, frames, books, films, etc.). Non-digital information is not under the control of computers, while digital information is. Information security is concerned by the security of information whatever is the support and ways of access.
- *Cyberspace* is composed of computers and by other equipment (e.g. trains, cars, grid installations, robots, and water provisioning equipment). All those categories of equipment are vulnerable to attacks through ICT. Their protection requires specific methods and techniques; some of them are out of the computer field (e.g. smart grids and industrial equipment). Cybersecurity is concerned with the security of any assets vulnerable because they are connected to ICT systems.
- Intersection of information and cyberspace security is the IT security focusing on digital data, which are vulnerable to threats via ICT.

1.2 Security Terms and Definitions

1.2.1 Assets and Attackers

Three fundamental notions are at the core of security: asset, adversary, and attack vector.

***Definition 1.2 Asset**: it refers to any resource to protect. Assets to secure include hardware (laptops, work stations, disks, USB keys, routers, switches, cables, antennas), software (operating systems, libraries, applications, severs), and data (files, databases, messages).*

Definition 1.3 Adversary*: it is any entity that attacks or that is a potential threat to a system. It is also called attacker or threat agent.*

Definition 1.4 Attack vector*: it refers to any path or means by which an attacker can gain access to an asset. The adversary uses attack vectors (such as email, web servers, physical access, etc.) to gain access to protected assets.*

1.2.2 Vulnerabilities, Threats, and Risks

Definition 1.5 Vulnerability*: it refers to a known weakness of an asset that can be exploited by attackers.*

Example 1.1

– No password change for years, open account with no user in a company, and secret data stored in a place easy to access are examples of vulnerabilities.
– No update of phone software with recent security recommendations and a web camera with code 1234 are other examples of vulnerabilities.

Any entities, including the following, using computer-based systems are vulnerable:

- Companies, banks, and financial institutions
- Internet service providers and Telecom operators
- Hospitals, museums, and universities
- Government and defense agencies
- Smart cities and smart grids
- Industrial installations and factories
- Nuclear plants

Definition 1.6 Attack surface*: it is defined as the set of all vulnerability points of an asset, a system, or a network.*

The larger the attack surface is, the more difficult the protection is.

Definition 1.7 Threat*: it refers to any incident that has the potential to harm a system. A threat is something that may or may not happen; but if happens, it has the potential to cause serious damage.*

Threats depend on targets, for example:

- Threats on hardware: theft and sabotage.
- Threats on software: deletion, server access blocking, theft, alteration of functions or configurations, content change of web pages, and web server hacking.
- Threats on data: theft of private data, theft of intellectual properties, file deletion, file access blocking, and data alteration.

Definition 1.8 Risk*: It is defined as the potential for loss or damage, if a threat exploits a vulnerability.*

Example 1.2 Financial lofsses, loss of privacy, reputational damage, legal implications, and even loss of life are examples of security risks.

Figure 1.2 summarizes the relationships between the main terms of security:

– The legitimate owner of assets needs protection of his/her assets.
– The adversary threatens to use, alter, or destroy the assets.
– The assets have vulnerabilities, which may be exploited by the adversary.
– Vulnerabilities are loopholes for the adversary to design and mount attacks.
– The owner deploys countermeasures to minimize the risks relevant to the threats.

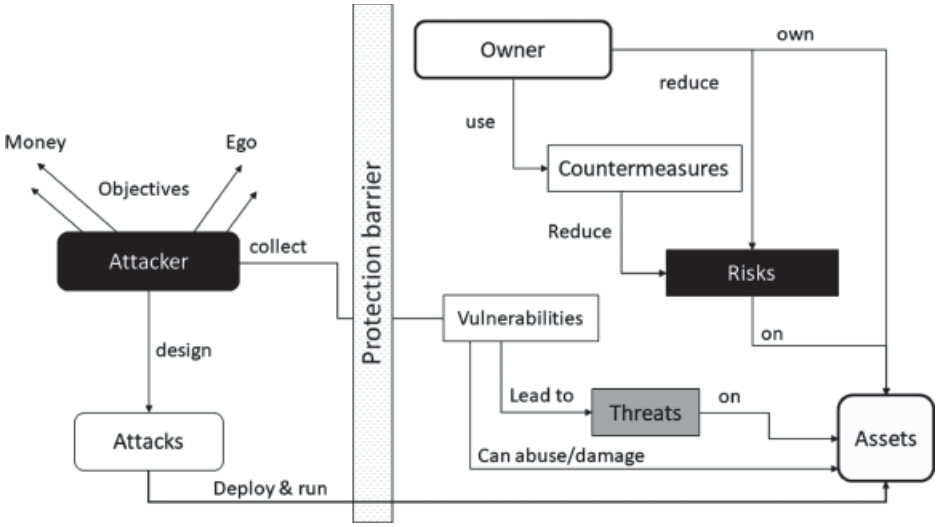


Figure 1.2 Relationships between basic security terms.

1.3 Security Services

The three basic security services are referred to as the *CIA triad*. *CIA* stands for Confidentiality-Integrity-Availability. Sometimes, CIA are called basic properties of *security*. In addition to CIA, authentication, authorization, and non-repudiation are services often required in the cyberspace. Depending on the asset owner's needs, a single, two, or several services may be required. Figure 1.3 summarizes the main security services used to protect assets.

1.3.1 Confidentiality and Privacy

Confidentiality aims at guaranteeing that private or confidential information is not made available or disclosed to unauthorized entities. *Secrecy* is a term usually used synonymously with confidentiality.

Privacy is a specific case of confidentiality. Privacy protection aims at preventing disclosure of private-life data (see Section 1.7).

Example 1.3 The following are examples of information that require confidentiality protection:

– industrial secrets of companies
– business agreements
– defense secrets
– health data, bank accounts, and private meetings of individuals

1.3.2 Integrity

Asset integrity is a property whereby asset content and/or behavior have not been modified in an unauthorized manner after being created, updated, maintained, stored, or transmitted. According to the category of asset, three types of integrity are distinguished: data, system/software, and hardware integrity.

Data integrity: it is a property whereby data has not been modified in an unauthorized manner after being created, stored, or transmitted. Data modification includes the insertion, deletion, and substitution of data.

System/software integrity: it is a property whereby a system (e.g. a web server) or a software (e.g. a library) has not been modified in an unauthorized manner after being created, stored, or transmitted. Software modification includes deletion and alteration of some functions or some configuration parameters. System/software integrity aims at guaranteeing that a system or the software performs its intended functions in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulations of system or software.

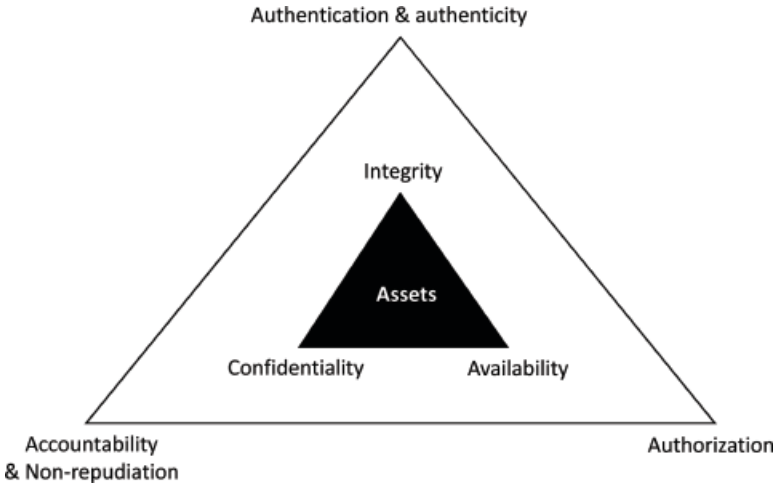


Figure 1.3 Overview of security services.

Hardware integrity: it is a property whereby a hardware component (e.g. a camera, a sensor, or a card reader) has not been modified in an unauthorized manner after being created and acquired or after maintenance operation.

Example 1.4 Examples of assets that require integrity guarantees:

- Your ID: if your ID is modified, you become somebody else.
- Web servers: if web server pages are modified, visitors would see inappropriate content or worse they would be asked to enter confidential data.
- Braking system of a car: if car brakes are sabotaged, then passengers and driver could be injured.

1.3.3 Availability

Asset availability is a property whereby asset content or services are available to be used by its legitimate users. An asset may become temporarily or definitely inaccessible, thus unavailable because of attacks. In a similar way to integrity, according to asset category, three types of availability are distinguished: data, system/software, and hardware availability.

Data availability: it is a property whereby data (i.e. files and databases) is accessible whenever requested by legitimate users. Both data deletion and data server blocking impact data availability.

System/software availability: it is a property whereby the function/service of a system (e.g. a web server) or a software is not slowed down or stopped by an attack. Therefore, it is not denied to authorized users. For example, a web server should process legitimate requests and not be blocked (totally or partially) by fraudulent requests.

Hardware availability: it is a property whereby a hardware component is available for use.

Notes

- Attacks targeting asset availability are frequent in today's Internet. In general, after stopping partially or entirely a system, attackers demand a ransom.
- Attacks against asset availability are the most difficult to address.

1.3.4 Authentication and Authenticity

Two types of authentication services are of interest in the IT security field: identity authentication and source authentication.

Identity authentication service is used to provide assurance of the identity of an entity interacting with a system. The question addressed by identity authentication is the following: Is the entity presenting an ID really the entity it claims to be?