Chapter 9
Information Security

9.1 What is Information Security

The Internet of Things (IoT) has revolutionized connectivity, enabling various devices and systems to connect to the Internet. However, this connectivity also introduces security risks that demand attention. Furthermore, when handling databases or big data containing sensitive or personal information, information security is also a critical concern.

Information security, as defined in JIS Q27000:2014, is the practice of maintaining the confidentiality, integrity, and availability of information. This encompasses preserving characteristics such as authenticity, accountability, non-repudiation, and reliability [1]. For detailed definitions of these terms, please refer to Table 9.1.

Among them, confidentiality, integrity, and availability are called three major elements of information security, as shown in Fig. 9.1. They serve distinct purposes: confidentiality aims to prevent information leakage, integrity safeguards against tampering and data loss, and availability ensures access to necessary data when required. Enhancing confidentiality and integrity can effectively reduce the risk of information leakage and data falsification. However, taking extreme measures to achieve this can result in significantly decreased availability. Conversely, when availability is a top priority, maintaining high levels of confidentiality and integrity might be challenging. These three elements are often in tension with one another, making it crucial to strike a well-balanced approach in considering them.

W. Weng, *A Beginner's Guide to Informatics and Artificial Intelligence*,
https://doi.org/10.1007/978-981-97-1477-3_9

Table 9.1 Characteristics of information security

Confidentiality	The characteristic of being inaccessible or unusable by unauthorized individuals, entities, and processes
Integrity	The characteristic of safeguarding the authenticity and completeness of information assets
Availability	The characteristic of being accessible and usable by authorized entities upon request
Authenticity	The characteristic of ensuring that an entity or resource matches its claimed identity
Accountability	The characteristic of ensuring that the actions of an entity can be uniquely tracked, either from the action itself or from the entity
Non-repudiation	The characteristic of verifying the undeniable occurrence of an activity or event
Reliability	The characteristic of aligning with intended actions and results

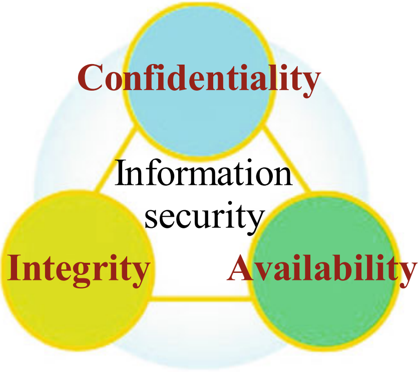

Fig. 9.1 Three major elements of information security

9.2 Risks, Threats, and Vulnerabilities

The primary objective of information security is to safeguard valuable information assets [2]. Information assets include personal information, such as credit card numbers, user IDs, and passwords for individuals, as well as customer information, confidential data, and accounting records for organizations and companies. It is crucial for both individuals and organizations to shield their information assets from potential risks, such as falsification, theft, destruction, and loss. Detailed examples of such risks include theft or loss through removable storage media, network breaches, social engineering attacks, unauthorized access, or the loss of personal computers and smartphones, as illustrated in Fig. 9.2.

A risk arises from threats to the vulnerability of information assets and has the potential to cause damage [2]. The level of risk is determined by the value of information assets, the level of threat, and the degree of vulnerability (Eq. 9.1). Minimizing

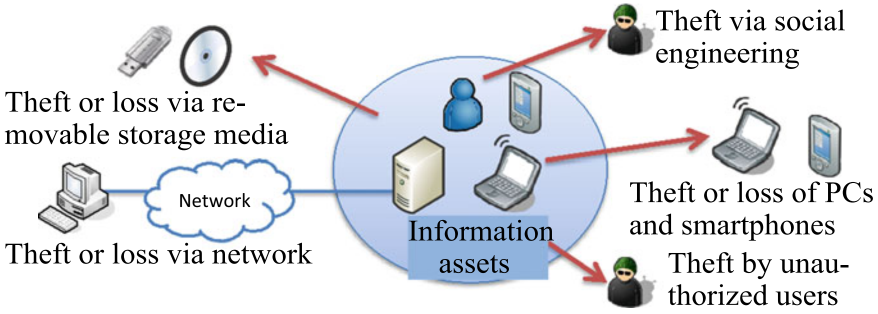
Theft via social engineering
Theft or loss via removable storage media
Network
Theft or loss via network
Information assets
Theft or loss of PCs and smartphones
Theft by unauthorized users

Fig. 9.2 Security risks for information assets

risk is crucial in information security.

$$\boxed{\begin{array}{c}\text{Information security risk} = \text{value of information asset} \\ \times \text{ level of threat } \times \text{degree of vulnerability}\end{array}} \tag{9.1}$$

Potential sources of threats and vulnerabilities include human, physical, and technical factors.

(1) **Threats and Vulnerabilities from Human Factors** (Table 9.2)

Potential threats from human factors include those resulting from human errors and social engineering. Social engineering includes various techniques, such as shoulder hacking, i.e. observing someone entering a password by looking over their shoulder, and password spoofing, i.e. identity fraud over the phone to trick individuals into revealing their passwords.

Table 9.2 Threats and vulnerabilities from human factors

Threats	Vulnerabilities
Human error • Maloperation due to assumptions • Unintended operating mistakes	• Illness, fatigue, excessive workload • Misunderstanding or inadequate understanding of operations • Misleading information in operating manuals
Sabotage • Laziness or inattention to security rules	• Inadequate operator management • Inadequate education about obeying rules • Inadequate punishment for breaking rules
Internal crime • Intentional theft of information by personnel within the organization	• Inadequate operator management • Inadequate access management • Inadequate punishment for breaking rules
Social engineering • Theft of passwords • Theft of information by impersonating an administrator	• Inadequate knowledge about social engineering techniques

(2) **Threats and Vulnerabilities from Physical Factors** (Table 9.3)

Environmental physical threats include various sources, such as natural disasters, equipment failures, and physical destruction. Vulnerabilities often stem from inadequate equipment and facility management. Effective countermeasures, such as equipment redundancy, can reduce these physical threats.

(3) **Threats and Vulnerabilities from Technical Factors** (Table 9.4)

Threats resulting from technical factors often involve intentional actions. Technical threats include a range of issues, such as unauthorized access, eavesdropping, Denial-of-Service (DoS) attacks, and computer viruses. These actions fall under the category of cybercrimes. A common technical vulnerability is a "security hole", which refers to a bug or defect in the operating system or software that may lead to technical threats. Therefore, when a security hole is identified, it is essential to fix it promptly to maintain security.

Table 9.3 Threats and vulnerabilities from physical factors

Threats	Vulnerabilities
Natural disasters • Fire, earthquake • Thunderstorm (including blackout caused by lightning)	• Lack of fireproofing and earthquake-proofing measures • Inadequate lightning strike surge protection
Equipment failure • Equipment failure or loss not caused by natural disasters	• Inadequate equipment failure measures (redundancy and updates) • Incorrect equipment setting • Inadequate equipment rental management
Intruders • Physical damage by intruders • Theft of equipment by intruders	• Inadequate lock management for equipment areas • Inadequate entrance/exit management for equipment areas

Table 9.4 Threats and vulnerabilities from technical factors

Threats	Vulnerabilities
Unauthorized access • Impersonation, cracking	• Security holes in information devices and software
Eavesdropping • Phishing scams, spyware	• Inadequate anti-virus measures • Inadequate education about attack techniques • Security holes in information devices and software
DoS attacks • Denial-of-Service (DoS) attacks, distributed DoS (DDoS) attacks	• Inadequate measures against DoS attacks • Security holes in information devices and software
Computer viruses • Malware • Worms, Trojans, bots	• Inadequate anti-virus measures • Inadequate education about attack techniques • Security holes in information devices and software

• Questions

1. How can you prevent the leakage of recipients’ personal information (email addresses) when sending an email to multiple recipients who do not know each other?

Hint: think about where to enter recipients’ email addresses, such as in the new message window of Outlook (Fig. 9.3).

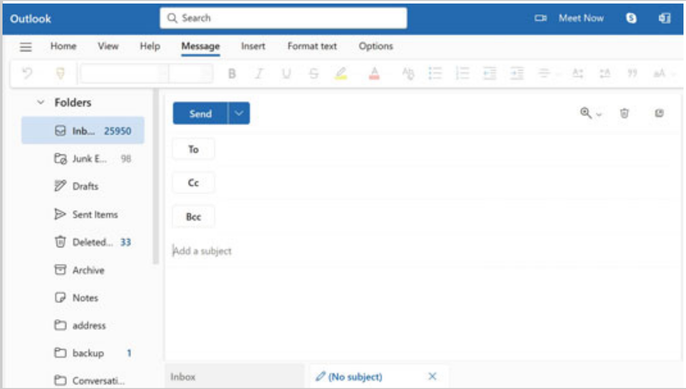

Fig. 9.3 New message window in Outlook

Please note that not all questions in this chapter can be answered based on the content of this book. For questions without answers in the book, feel free to respond based on your experience or personal understanding.

2. Choose the incorrect items for managing a USB disk containing personal information (multiple choices allowed).
   A. Leaving it in a bag in your car before locking the car and going to eat at a restaurant.
   B. Leaving it on the desk in your university lab before locking the lab door and going home.
   C. Taking it with you when going home.

9.3 Security Measures for Users

9.3.1 Management of User IDs and Passwords

A combination of a user ID (account) and password is commonly used for user authentication in determining access to an information system. A user ID is a system-registered identifier designed to uniquely identify a user, whereas a password is a string of characters known only to the user. Effective password management practices include: (1) Not sharing your password with others. (2) Using unique passwords for different systems. (3) Avoiding writing down the combination of user ID and password on paper. (4) Not using easily guessable passwords, such as birthdays or dictionary words.

• Questions

3. Do you think setting a login password ensures computer security? Why?

9.3.2 Anti-virus Measures

Malware and computer viruses, in a broad sense, refer to programs designed to intentionally harm software or data. In a narrower sense, they are defined as programs that are:

- Self-replicate: capable of infecting other programs or systems by copying themselves.
- Latent: can remain hidden, with symptoms appearing only under specific conditions, like at a specified time, after a set amount of time, or after a certain number of executions.
- Pathogenic: can destroy files, such as programs and data, and operate in ways unintended by the user.

While viruses can exploit system vulnerabilities, they are frequently introduced into a system through files downloaded from the Internet or email attachments. A vital measure for protection is to use anti-virus software to scan external files for viruses. Nevertheless, installing anti-virus software alone is insufficient. Regularly update your anti-virus software with the latest virus definition files. Additionally, it is recommended to keep the operating system, software, and applications up to date while addressing any security vulnerabilities within them.

Table 9.5 Access rights and settings

Access rights	Read	Rights to read files and folders
	Write	Rights to create and overwrite files and folders
	Modify	Rights to read, write, and delete files and folders
	Full control	Rights to fully access files and folders, and modify access rights settings
Settings	Enable	Enable access
	Disable	Disable access (takes priority over the enable option)
	Empty	Inherit the settings of the parent folder

9.4 Security Measures for Administrators

9.4.1 Create Information Security Policy

One important security measure is the creation of information security policy, establishing fundamental principles for ensuring information security. Information security policy is particularly effective in addressing threats from humans. This policy helps define the rules for handling information assets and establishes a system for compliance with these rules.

9.4.2 Access Management

System administrators should implement security measures to control and restrict access to information assets. These measures may include a combination of physical and electronic security measures. Physical security measures can regulate access to facilities where information assets are stored through the use of physical keys, integrated circuit (IC) cards, and biometric authentication. Electronic security measures can manage access to data, including files and folders, by defining access rights for individual users or groups. Access rights can be customized for each specific file and folder. Table 9.5 presents an overview of the available access rights and settings.

9.4.3 Firewall

Another security measure is the use of a firewall. A firewall is a communication device employed to safeguard client PCs in an internal network against potential threats from the Internet. The firewall functions by scrutinizing packets that traverse the connection point between the internal network and the Internet. It determines whether to permit or block the transmission of incoming packets based on their IP addresses and the applications using them. Its fundamental operation allows requests from clients in the internal network whereas rejecting requests from the Internet, with exceptions made as needed (as shown in Fig. 9.4).

For communication initiated by a client on the internal network, a mechanism called stateful packet inspection (SPI) is used to maintain the communication status and allow replies from the Internet to pass through temporarily (Fig. 9.5).

When a server is accessible to the public Internet, it is a common security practice to isolate its network environment from the rest of the organization's devices due to external threats. This isolated area between the Internet and the internal network is known as a Demilitarized Zone (DMZ). The relation between a firewall and a DMZ is illustrated in Fig. 9.6. Using a firewall to regulate communication between the Internet and the DMZ enhances security, reducing threats from the Internet and enabling secure use of Internet services from the internal network.

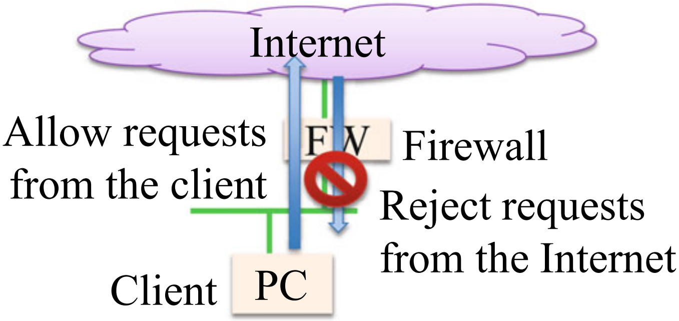
Internet
Allow requests from the client
FW
Firewall
Reject requests from the Internet
Client
PC

Fig. 9.4 Function of firewall

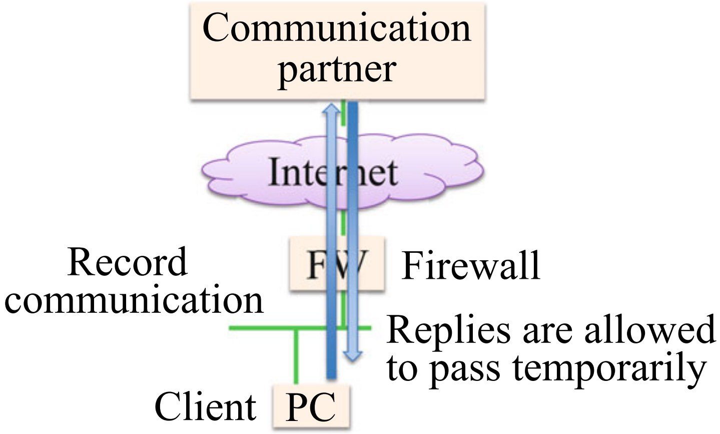

Fig. 9.5 Function of SPI

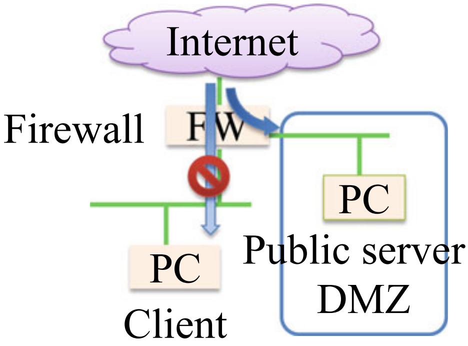

Fig. 9.6 Function of DMZ

9.5 Security Technologies

Encryption and authentication are security technologies that help maintain confidentiality and integrity. In the following, we will provide detailed explanations of these two technologies.

9.5.1 Encryption

Encryption is a technology that makes digital data unreadable to unauthorized parties. It involves the transformation of plain text into ciphertext, a form of text rendered unreadable through the use of specific keys or rules. The reverse process, turning ciphertext back into plain text, is known as decryption. Encryption serves two primary purposes: it safeguards data and communication paths to prevent eavesdropping, ensuring confidentiality, and it guarantees the integrity of transmitted data by preventing tampering during transit.

There are two main types of encryption systems: symmetric key cryptosystem and public key cryptosystem [2].

The symmetric key cryptosystem, in use for a long time, employs the same key for both encryption and decryption. While it requires the sender and receiver to share the key beforehand, it offers the advantage of being simple and both encryption and decryption processes are fast (Fig. 9.7). Data Encryption Standard (DES), Triple DES (3DES), and Advanced Encryption Standard (AES) are three standards for encryption. DES has a key length of only 56 bits, and hence is no longer recommended due to low encryption strength. AES is currently the mainstream standard.

In the public key cryptosystem, the keys used for encryption and decryption are separate, as depicted in Fig. 9.8. This system requires two types of keys: a public key and a private key, which are used in pairs. The public key is accessible to anyone, whereas the private key is available to only the key owner. The system operates either using the public key for encryption and its paired private key for decryption or using the private key for encryption and its paired public key for decryption. If data

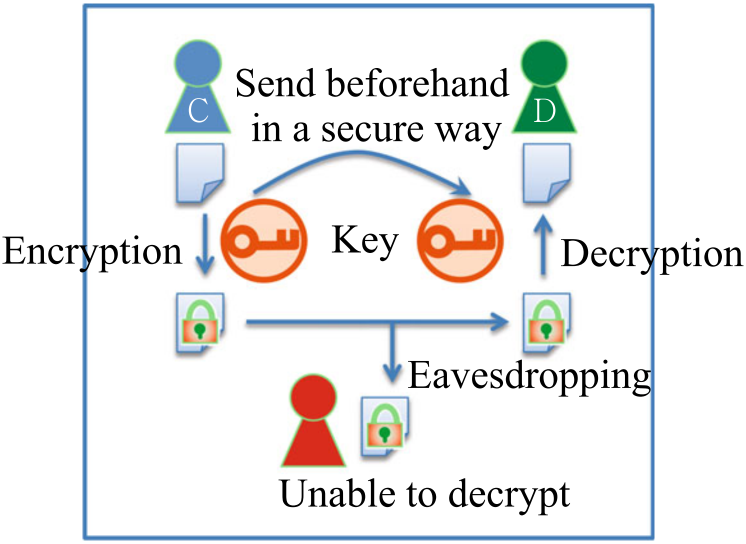

Fig. 9.7 Symmetric key cryptosystem

is encrypted with the public key, it can only be decrypted using the corresponding private key, and vice versa.

When the public key is used for encryption and the private key is used for decryption, there is no need to transmit the decryption key through the communication

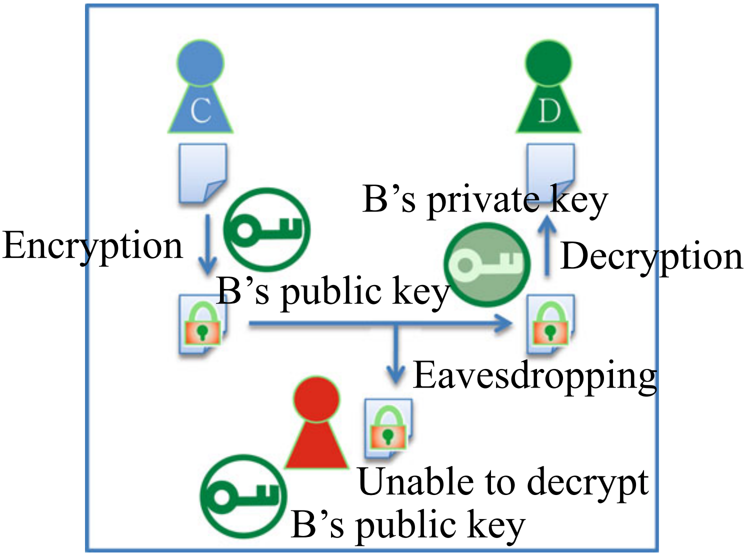

Fig. 9.8 Public key cryptosystem

channel. Therefore, the challenge of sharing keys before communication is eliminated. If the private key is used for encryption and the public key is used for decryption, it allows for data creator authentication. However, it is important to note that the public key cryptosystem is more complex than the symmetric key cryptosystem, and the encryption and decryption processes tend to be slower. The encryption method typically employs the Rivest, Shamir, Adleman (RSA) algorithm, known for its difficulty in factoring the product of two prime numbers.

9.5.2 Digital Signature and Digital Authentication

While encryption effectively safeguards against threats like eavesdropping and data falsification, it faces challenges when it comes to preventing user spoofing. To address this problem, a mechanism known as digital signature is employed. A digital signature uses the public key cryptosystem to encrypt a message using the user's private key. The user's identity will be confirmed if the encrypted message can be decrypted using the corresponding public key.

To verify a user's identity using a digital signature, it is crucial to confirm the rightness of their public key. This verification process is facilitated by the Public Key Infrastructure (PKI), a global authentication system. PKI employs digital certificates to validate the public key's authenticity and the user's trustworthiness. Digital certificates are issued and managed by certificate authorities. Users are required to preregister their public keys with a trusted certificate authority, which then issues a digital certificate. This combination of a digital signature and a digital certificate, like a real-world seal and a seal certificate, enables digital authentication and is often referred to as e-authentication.

9.5.3 Secure Encrypted Communication

Secure Socket Layer (SSL) was initially a protocol for encrypted communication using public key authentication. Subsequently, it was standardized under the name Transport Layer Security (TLS), though SSL remains a more common term.

SSL-based encrypted communication combines the advantages of both symmetric key cryptography and public key cryptography. It achieves this by encrypting communication data using a symmetric key, which, in turn, is encrypted with a public key. Using a symmetric key for data encryption reduces the processing load for both encryption and decryption, enhancing efficiency. Encrypting the symmetric key using a public key increases security. The public key of the communication partner, such as a web server, can be obtained from a digital certificate through public key authentication.

SSL operates at the transport/application layer in the TCP/IP model and can be used in many applications. One of its primary and widespread uses is in the form

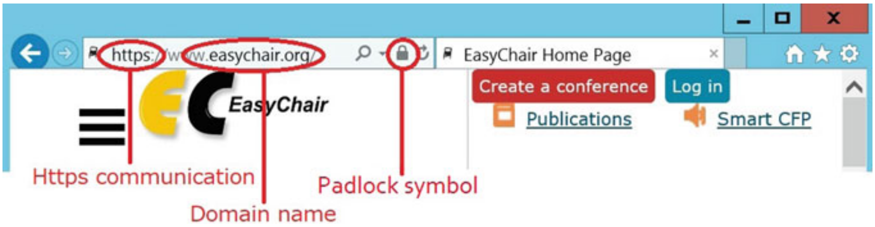

Fig. 9.9 Website using HTTPS

of HTTP Secure (HTTPS), which ensures encrypted communication on the World Wide Web (WWW).

A URL using HTTPS begins with “https://”. When the digital signature of the target server is successfully verified, a padlock symbol appears in the URL bar, and the background color may turn green. These indicators signal to the user that the website is secure. For example, Fig. 9.9 shows the URL of a website using HTTPS.

Exercises

1. According to the content of this book, is it possible to use artificial intelligence (AI) to detect a virus? if so, please briefly explain the mechanism.

*2. Describe the conflicting nature of the three major elements of information security.

*3. Describe the difference between the symmetric key cryptosystem and public key cryptosystem.

References

1. Information technology—security technology—information security management systems—terminology (JIS Q27000: 2014), Japanese Industrial Standards
2. Whitman ME, Mattord HJ (2012) Principles of information security, 4th ed. Cengage Learning, Boston, MA. http://almuhammadi.com/sultan/sec_books/Whitman.pdf