

Security Information & Security Overview

Lecture 1

HCIA-Security

Prepared by
Dr. Abdelrhman Ahmed

Forward

- **Information security is the process of ensuring safe data communication and preventing issues such as information leakage, modification, and disruption.**
- **This document describes the basic concepts and protection measures of information security, as well as information security risks and associated assessment and avoidance methods.**

Objective

- Upon completion of this course, you will be able to:
 - Describe the definition and characteristics of information security.
 - Explain the characteristics and differences of security models.
 - Differentiate between security risks.

Information

information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business.

— ISO/IEC Guidelines for the Management of IT Security (GMITS)

Information can be communicated in several different ways: messages, signals, data, intelligence, or knowledge. It may exist in multiple forms, for example, data/programs stored and processed in information facilities, printed or written papers/emails/design drawings/business solutions, or messages in slides or sessions.



Information Security

- Information security refers to the preservation of the confidentiality, integrity, and availability of data through security technologies.
- These technologies include computer software and hardware, network, and key technologies. Organizational management measures throughout the information lifecycle (generation, transmission, exchange, processing, and storage) are also essential.
- The following will be affected if information assets are damaged:



National
security



System operating and
continuous development



Personal privacy
and property

Information Security Continuous

The aim of information security is to protect data against threats through technical means and effective management.

Information security is to protect hardware, software, and system data on information networks from occasional or malicious damage, tampering, and leakage.

It ensures continuous and reliable system operating as well as uninterrupted information services.

Information Security Development

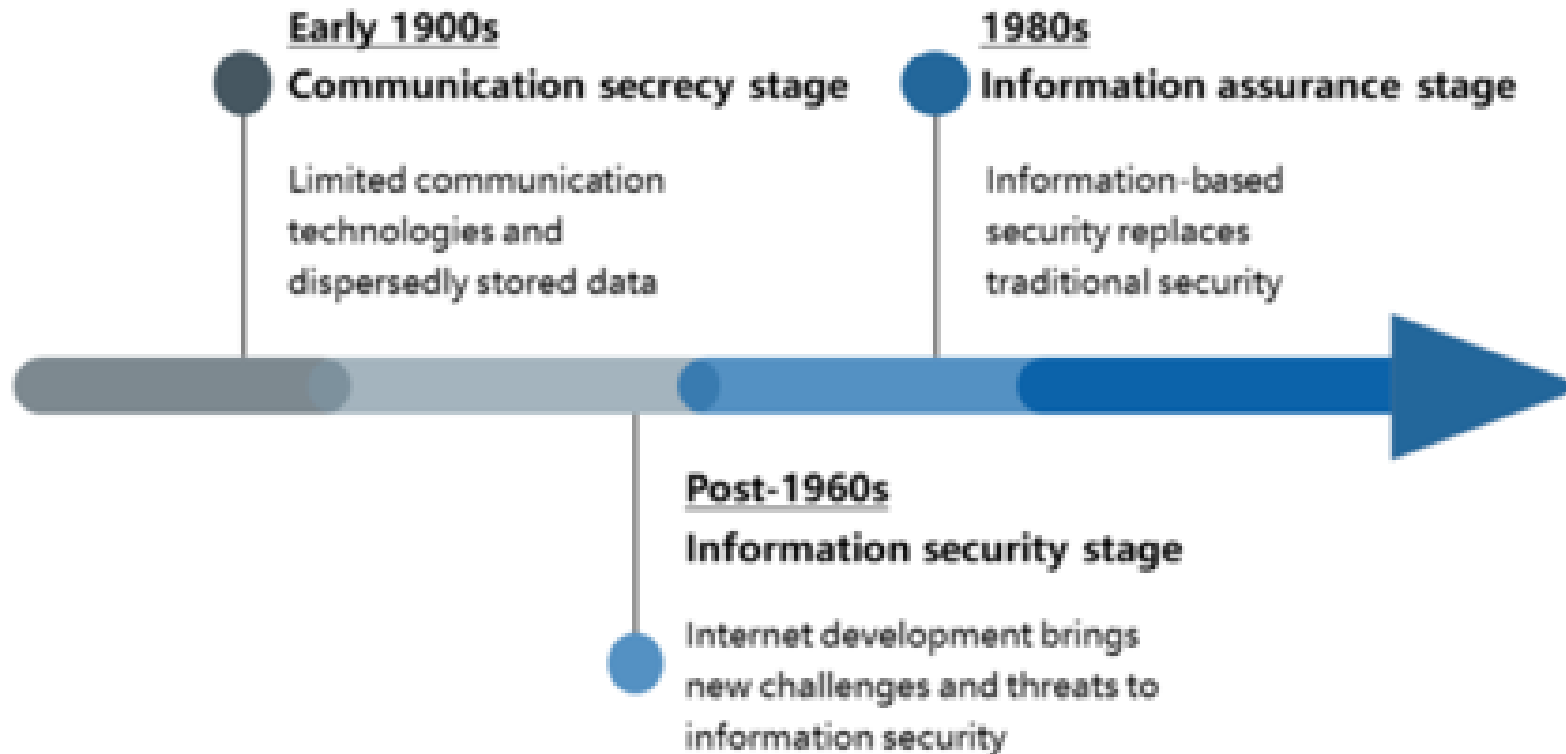


Photo or Information Leakage?

After the Chinese government invited bids for oil production equipment, Japanese intelligence experts used this simple photo to uncover the following secrets of the Daqing Oilfield:

- ☐ **Located between 46°N and 48°N, as indicated by the clothing of Wang Jinxi**
- ☐ **Diameter of the oil well, inferred from the handle rack**



Communication Security

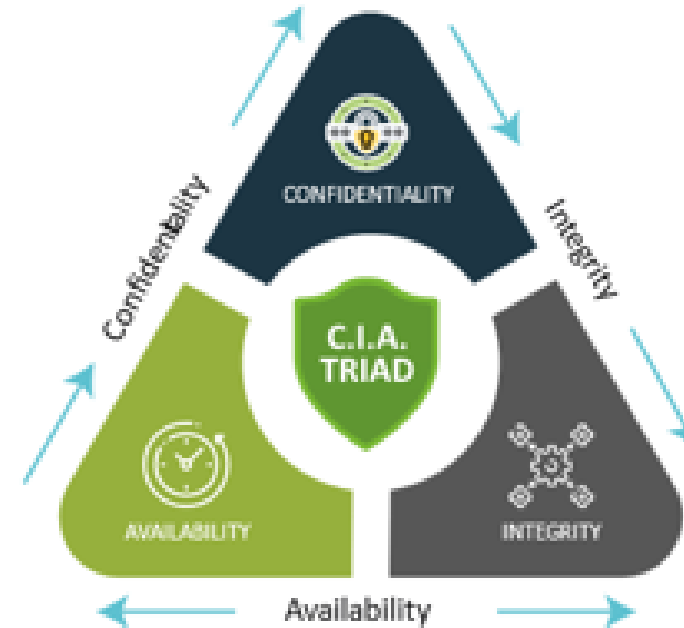
In the early 1900s, communication technologies were underdeveloped, and data was stored in different locations.

- **Information system security was limited to physical security of information and cipher based security of communication (mainly stream cipher).**
- **As long as information was in a relatively secure place and unauthorized users were prohibited from accessing the information, data security could be generally guaranteed.**
- **In the case mentioned previously, it was ignored that the photo might reveal sensitive information about the oilfield. By limiting the dissemination or recipients of the photo, information leakage could have been prevented.**

Information Security Period

The application of computer and network technologies entered a practical and large-scale use stage, and data transmission could be completed through computer networks.

The main objective of information security was to ensure information integrity, availability, and confidentiality.



Information Security Stage

- Since the 1990s, Internet technologies have developed rapidly, and information leaks have increased.
- As a result, in addition to confidentiality, integrity and availability, information security began to focus on more principles and objectives, such as controllability and non repudiation.



Information Security Stage

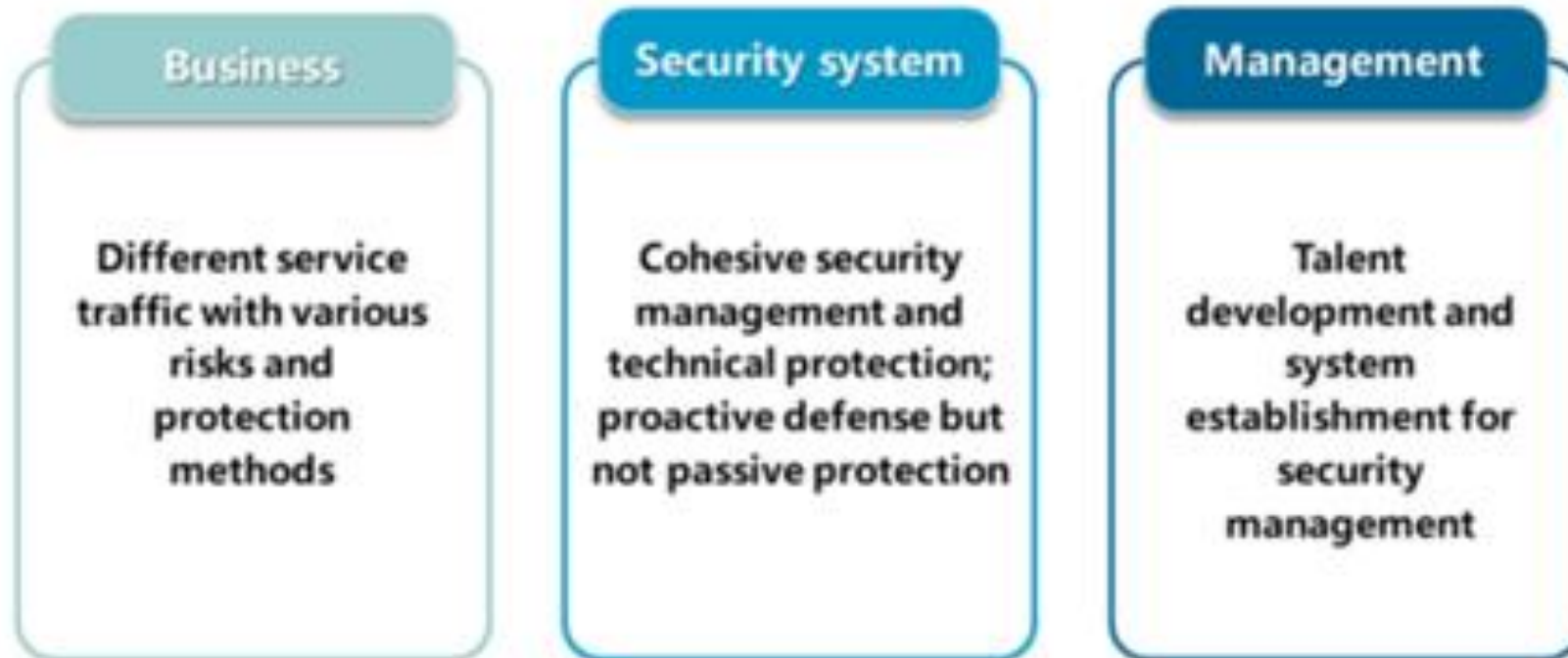
- **Confidentiality**
 - Ensures that information can be obtained only by authorized users.
- **Integrity**
 - Ensures the accuracy and integrity of information and its processing method.
- **Availability**
 - Ensures that authorized users can obtain desired information and use related assets.
- **Controllability**
 - Implements security monitoring to protect information and its system against attacks.
- **Non-repudiation**
 - Prevents the information sender or receiver from denying the information.

Information Security Stage

- ❖ Information security involves information confidentiality, integrity, availability, controllability, and non-repudiation.
- ❖ In general, information security is to ensure the effectiveness of electronic information. Confidentiality means resisting passive attacks by adversaries and preventing information leakage to unauthorized users.
- ❖ Integrity means resisting active attacks by adversaries and preventing unauthorized tampering.
- ❖ Availability is to ensure that information and information systems are used by authorized users.
- ❖ Controllability is to implement security monitoring on information and information systems.

Information Assurance Stage

❖ Business-oriented information security assurance



Case - WannaCry

- In 2017, the WannaCry ransomware crypto worm, propagated through Eternal Blue, infected over 100,000 computers, causing a loss of US\$8 billion.
- Exploiting the vulnerability of port 445 on Windows operating systems, the WannaCry ransomware crypto worm featured self-replication and included a "transport" mechanism to automatically spread itself. Among infected Windows operating systems in China, those on campus networks suffered most, and many laboratory data and final year projects were locked and encrypted. The application systems and database files of some large enterprises were encrypted and failed to run properly.



What are the Causes of Such Attacks?



Direct Cause

- Virus
- Vulnerability
- Trojan horse
- Backdoor program
- DDoS attack
- ...

VS



Indirect Cause

- Information system complexity
- Human and environment factors

What are the Causes of Such Attacks? Cont.

Information system complexity: The information system may be attacked during the design or operation process due to its vulnerabilities and defects.

Major issues are as follows:

- **Complex process:** In information system design, security is placed inferior to factors such as usability and enforceability. Due to human error and imperfect design methodology, the information system always has vulnerabilities.

What are the Causes of Such Attacks? Cont.

Complex structure: The information system may need to support multiple types of terminals (such as employee terminals, remote users, mobile terminals, routing devices, and servers) and data services (such as service data, management data, and voice data) on the network. All terminal and data types must be considered for cyber security management.

Complex application: Network redundancy and stability are preferentially considered during network topology design, and redundant links and backup devices may be added. The complexity of network application can lead to failure in rapid fault locating and rectification.

Human and environment factors: environmental threats and man-made damages.

Significance of Building Information Security

Increasing importance

- The information network has become the foundation of economic prosperity, social stability, and national development.
- Informatization profoundly influences the global economic integration, national strategy adjustment, and security priorities.
- Information security has transformed from a technical issue into a matter of national security worldwide.



Applicable to many technical fields

For example:

- Command, Control, Communications, Computers and Intelligence (C4I) system
- E-commerce system
- Biomedical system
- Intelligent Transport System (ITS)



Thank You