Introduction to Security Architecture

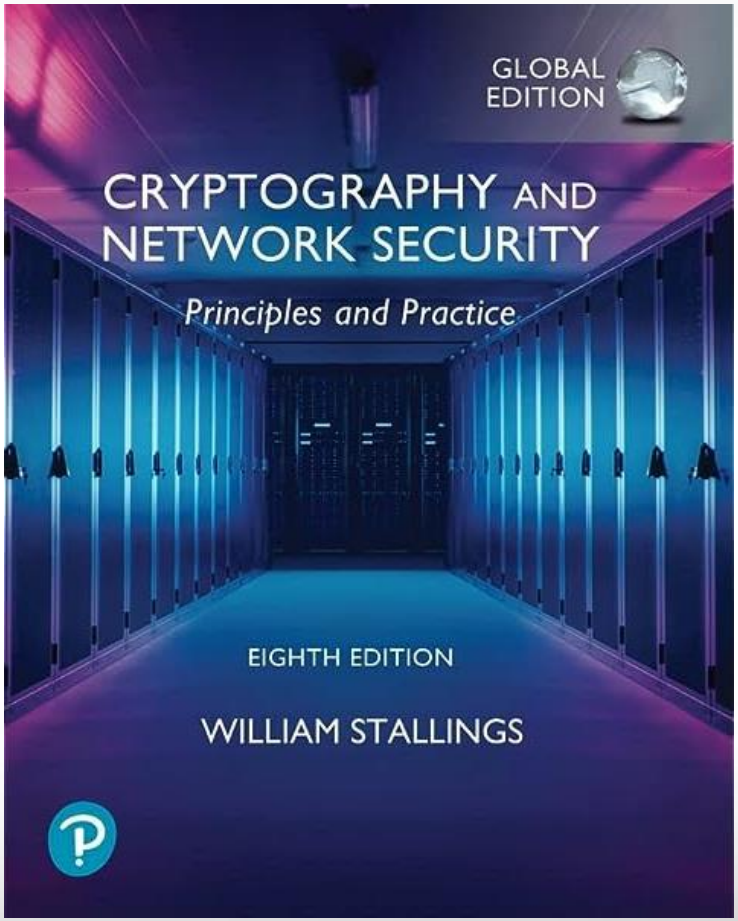
Jason Lin

Course Information

- Instructor
  - 林傑森 (Email: jasonlin@cs.nchu.edu.tw)
- TA
  - 謝立宇 (Email: cjh9027@gmail.com)
  - 黃紹綸 (Email: lauren444416@gmail.com)
- Office Hours
  - Instructor: Thursdays 3:00 pm – 4:00 pm @ 理學大樓 913
  - TA: by appointment @ 理學大樓 922B
- Learning Platform
  - NCHU iLearning 3.0
- Lectures
  - Wednesdays 2:10 pm – 5:00 pm @ 理學大樓 821

Class Materials

- Textbook
  - "Cryptography and Network Security: Principles and Practice", by William Stallings, 8th Edition, Pearson, 2022.
- Lecture Notes
  - Please check iLearning 3.0



Tentative Schedule (1/2)

Week	Date	Topics
1	2/21	Introduction to Security Architecture
2	2/28	National Holiday (No Class)
3	3/6	Overview of Cryptographic Techniques
4	3/13	Basic Number Theory
5	3/20	Basic Number Theory
6	3/27	Classical Encryption Techniques
7	4/3	Compensatory Holiday (No Class)
8	4/10	Finite Fields
9	4/17	Midterm Exam
10	4/24	Symmetric-Key Encryption
11	5/1	Symmetric-Key Encryption

Tentative Schedule (2/2)

Week	Date	Topics
12	5/8	Asymmetric-Key Encryption
13	5/15	Self-Directed Learning Week (No Class)
14	5/22	Asymmetric-Key Encryption
15	5/29	Data Integrity Algorithms
16	6/5	Data Integrity Algorithms
17	6/12	Self-Directed Learning Week (No Class)
18	6/19	Final Exam

Grading Policy

- Class Participation: 10%
  - In-class activities and roll call
- Homework: 35% (7% each)
  - 5 written/programming assignments
- Two Comprehensive Exams: 40% (20% each)
  - Temporarily decided to be held on 4/17/2024 and 6/19/2024
- Final Project: 15%
  - Self-directed learning on implementing a cryptosystem

Homework Policy

- The **grading rubric** will subject to change for each homework.
- Every turned in non-programming assignment must be submitted as a hard copy in class on the due date. It can be handwritten or typed but it MUST be **legible** and **readable**.
- For programming assignments, you must submit them on **iLearning** including the source code along with a brief report.
- Penalty for late homework within a week: **30%**. Late homework submitted after a week of the due date will **not be accepted**.
- I do not tolerate **plagiarism**. For those who get caught, their grades will be divided by the number of plagiarists (including the original author).

Motivations

- Computers are **everywhere**; they impact almost every aspect of modern life to one degree or another.
- The act of placing information in computerized systems is an act of trust. We trust that the information is **secure**.
- Cybersecurity market reaches $75 billion in 2015; expected to reach $10.5 trillion by 2025
  - https://www.forbes.com/sites/bethkindig/2023/09/29/the-next-market-ai-will-disrupt-is-cybersecurity/
- One million Cybersecurity Job Openings in 2016
  - http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016

Security is an Endless Path (1/2)

- The advancement of information technology leads to new security issues
- Security can be looked at as a tradeoff between (cost of) risks and benefits
  - Cost of implementing the security mechanism and the amount of damage it may prevent
- Tradeoff considerations are **security**, **user convenience**, **business goals**, and **expenses**

Security is an Endless Path (2/2)

- An important tradeoff involves user convenience
  - Between **difficulty of use** and **willingness of users**
  - If users will not use a system because of cumbersome security mechanisms, there is no benefit to having security
  - If users go out of their way to circumvent security, the system may be even more vulnerable

Policy and Education

- Cornerstone of a security effort is to
  - Implement proper policies
  - Educate users about those policies
- Information security policies should be
  - Flexible enough not to require frequent rewrites
  - Comprehensive enough to ensure coverage of situations
  - Available to all members of the organization
  - Readable and understandable

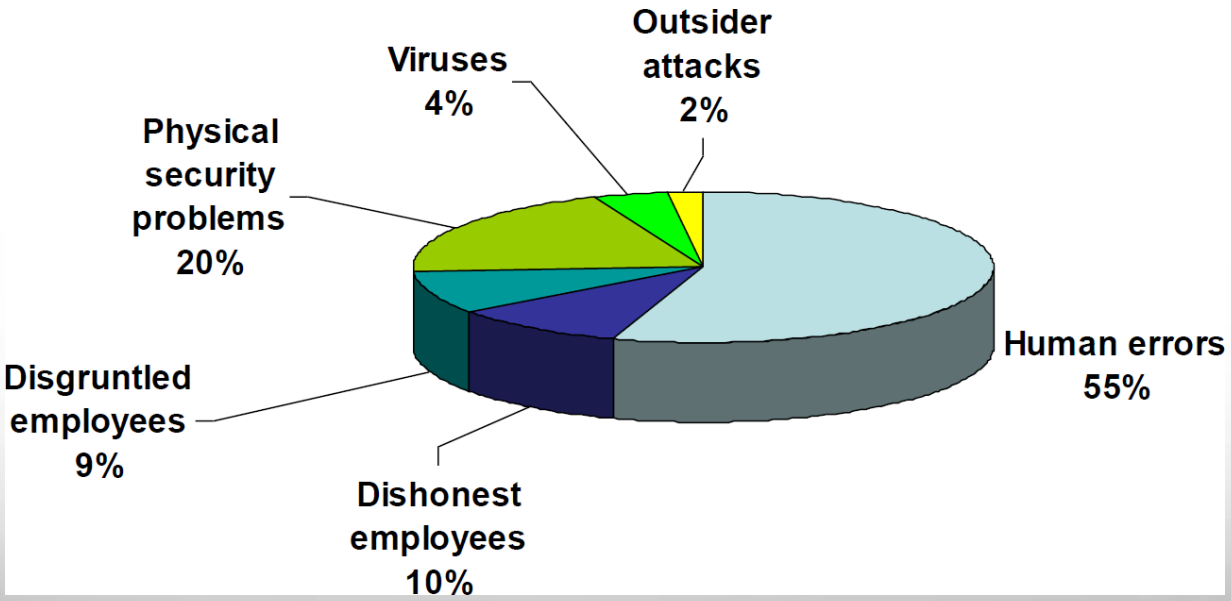
Threats and Attacks

- Threat (威脅)
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- Attack (攻擊)
  - An assault on system security that derives from an intelligent threat (especially in the sense of a method or technique).

Source: RFC 4949

Threats to Security (1/4)

- Threats to security fall into three main categories:
  - Hackers
  - Malware
  - Organizational Insiders



Threats to Security (2/4)

- Hacker (駭客)
  - Anyone who attempts to penetrate the security of an information system, regardless of intent.
  - There are a number of different reasons that people do this, and not all hackers are truly malicious.
    - Corporate spies searching for trade secrets
    - Investors seeking “inside information”
    - Teenagers seeking thrills
    - …

Threats to Security (3/4)

- Malware (惡意軟體)
  - A computer program that carries out malicious actions when run on a system.
  - Some types:
    - Virus (病毒): a piece of code that inserts itself into an application and executes when the application is run.
    - Worm (蠕蟲): a standalone malware that replicates itself in order to spread to other computers via network.
    - Trojan horse (木馬): a malicious code or software that looks legitimate but can take control of your computer.
    - Backdoors (後門程式): a covert method of bypassing normal authentication procedures over a network to allow future access.
    - Ransomware (勒索軟體): a malware that disables victim's access to data until ransom is paid.

Threats to Security (4/4)

- Organizational Insiders (組織內部人士)
  - Someone from within the organization that attempts to go beyond the rights and permissions that they legitimately hold
  - Security professionals and system administrators are particularly dangerous
  - Never give one person too much unconstrained power

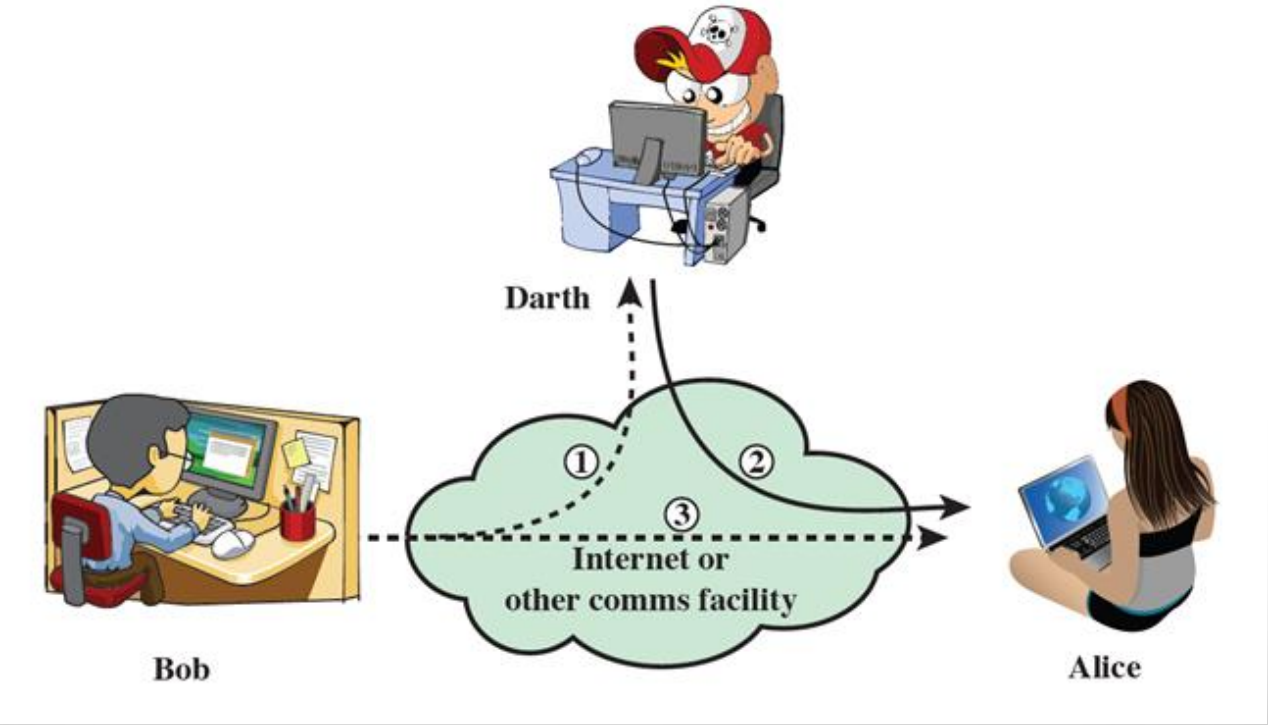
Types of Security Attacks (1/3)

- **Active attacks**–modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

- **Passive attacks**–eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows

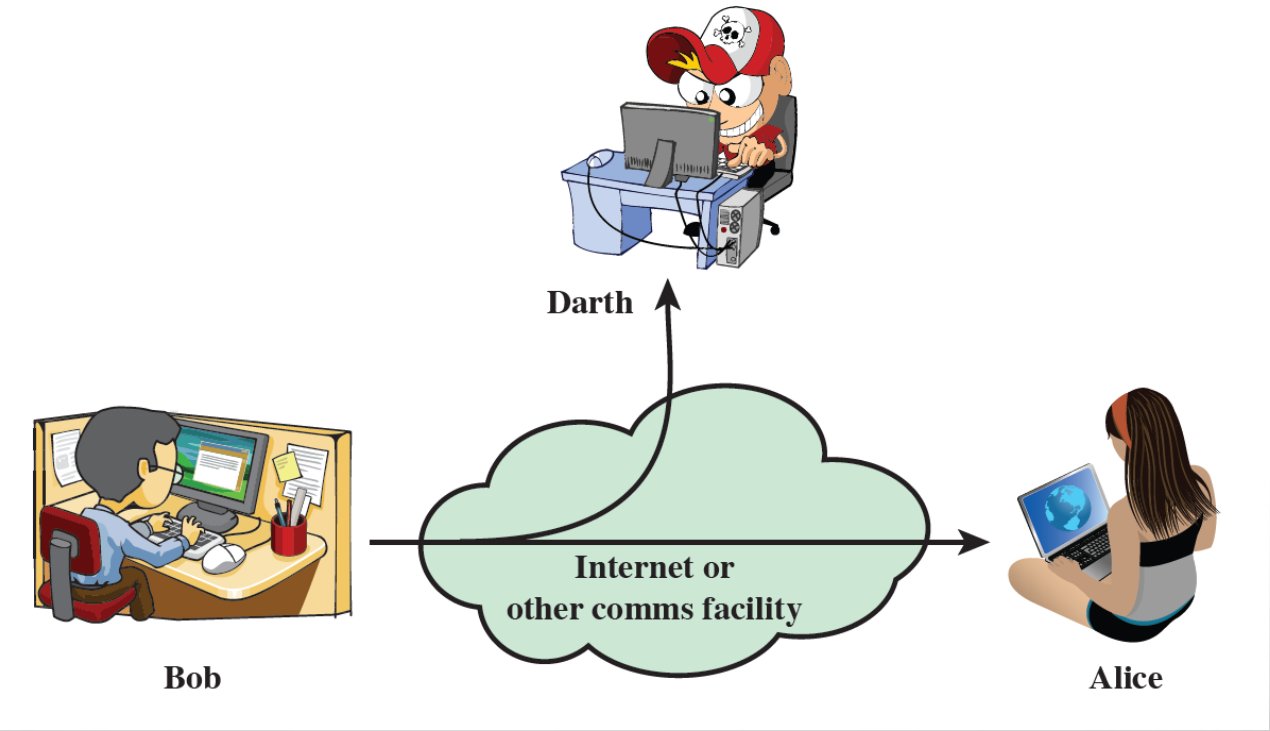
Types of Security Attacks (2/3)

- An **active attack** attempts to alter system resources or affect their operation

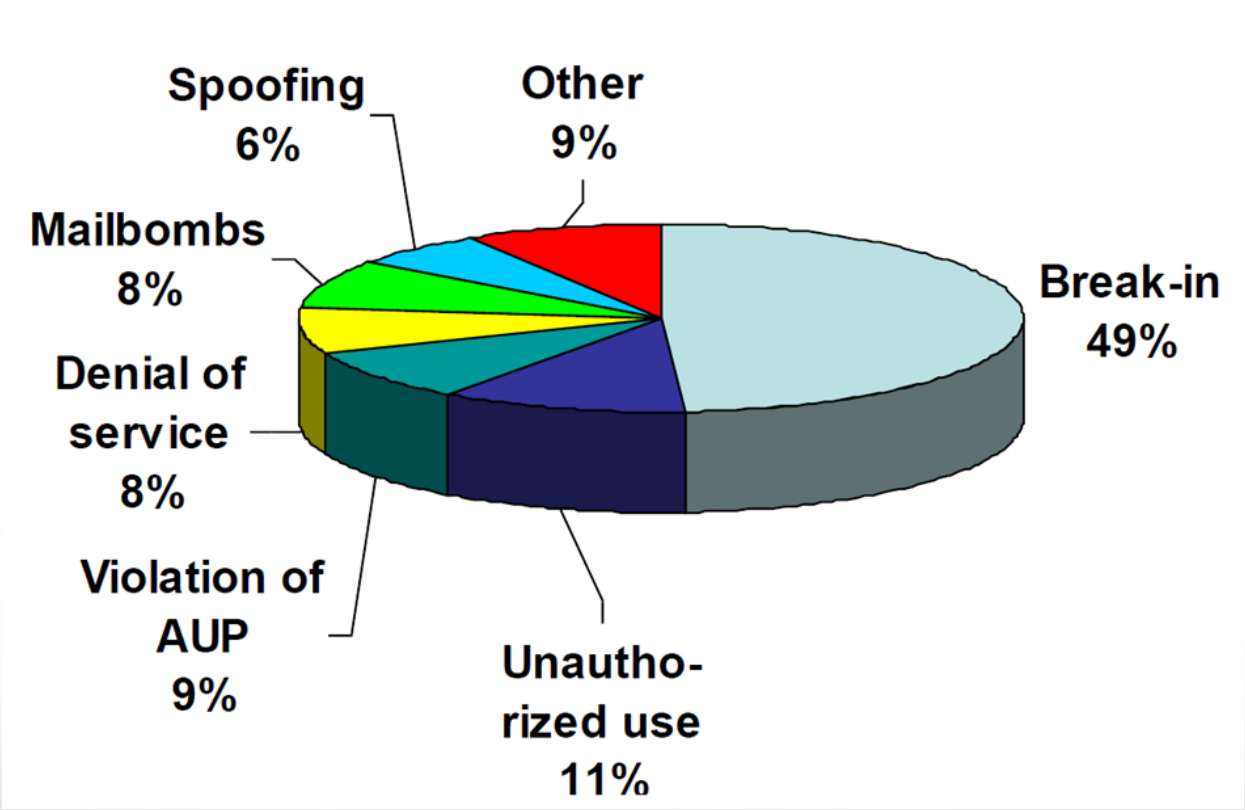


Types of Security Attacks (3/3)

- A **passive attack** attempts to learn or make use of information from the system but does not affect system resources



Breakdown by Type of Attack



Source: ARNES SI-CERT

資訊安全之定義與範圍

- 安全：一種放心，沒有危險的感覺
- 資訊安全：
  - 於網路儲存、傳送與存取資料時，保護其內容避免遭受到竊取、破壞、偽造等攻擊或出現未經授權的存取動作。
- 資訊安全包含的範圍：
  - 機密文件的存取權限
  - 機密文件攜入、帶出公司的審核程序
  - 員工的資訊安全知識訓練
  - 機器放置地點有否考量天然災害
  - 檔案是否定期備份
  - …

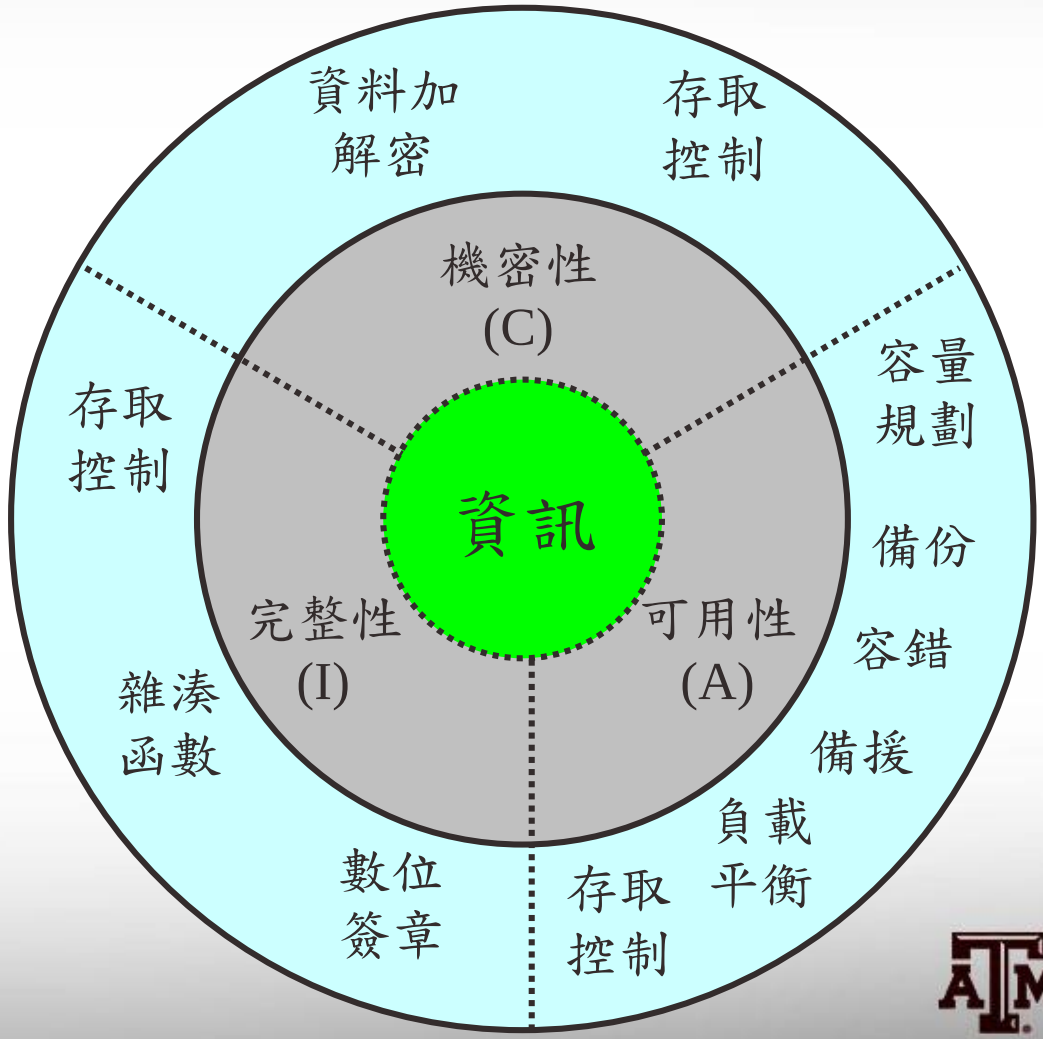
資訊安全的三大要素

- C-I-A triad
  - **C**onfidentiality (機密性)：防止非授權人員存取資訊，確保資訊傳遞與儲存的隱密性
  - **I**ntegrity (完整性)：防止資訊經非授權人員竄改，確保其在傳輸或儲存的生命週期中，保有正確性與一致性。
  - **A**vailability (可用性)：防止系統故障或者人為惡意阻斷服務，確保使用者操作資訊系統時，資料與服務的可獲得性

對於機關(構)來說，還要做到法規的遵循 (Law compliance)

保護資訊不同的技術與方法

- 不同的安全需求會使用不同的方法與技術
- 密碼學為保護資訊安全之最重要且最常用的技術與基礎



資訊安全之建議

- 國際密碼學大師 Shamir 對商業安全有十項建議：
  1. 不要追求完美無缺的安全性
  2. 不要誤以為問題解決了，但根本的問題仍然存在
  3. 不要使用由下而上的策略解決問題
  4. 不要過分的使用密碼技術，反而造成使用者的不方便
  5. 不要使用太複雜的方法
  6. 不要使用太昂貴的設備
  7. 不要使用單一防線策略
  8. 不要忽略了可能發生的「神秘攻擊法」
  9. 不要太過於仰賴系統操作
  10. 不要太過於仰賴人員忠實

密碼學的主要目標

- Confidentiality (機密性)
  - The information cannot be understood by anyone for whom it was unintended.
- Authentication (確認性)
  - The sender and receiver can confirm each other's identity and the origin/destination of the information.
- Integrity (完整性)
  - The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.
- Non-repudiation (不可否認性)
  - The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

密碼協定與演算法

- Four main areas:
  - Secret-key encryptions: used to conceal the contents of blocks or streams of data of any size, including messages, files, encryption keys, and passwords
  - Public-key encryptions: used to conceal small blocks of data, such as encryption keys and hash values, which are used in digital signatures
  - Data integrity algorithms: used to protect blocks of data, such as messages, from alteration
  - Authentication protocols: schemes based on the use of cryptographic algorithms designed to authenticate the identity of entities

其餘資訊安全的目標 (1/2)

- Risk Management (風險管理)
  - The process of managing risks associated with the use of information technology
- Availability (可使用性)
  - The assertion that a computer system is available or accessible by an authorized user whenever it is needed.
- Access Control (存取控制)
  - A security technique that regulates who or what can view or use resources in a computing environment.

其餘資訊安全的目標 (2/2)

- Business Continuity Plan
  - A document that outlines how a business will continue operating during an unplanned disruption in service.
- Disaster Recovery Plan
  - A formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents
- Security Classification of Information
- Laws and Regulations

ACM A.M. Turing Award (1/3)

- It is an annual prize given by the Association for Computing Machinery (ACM) for contributions "of lasting and major technical importance to the computer field". It is generally recognized as the highest distinction in computer science, or the "Nobel Prize of Computing".
- The first recipient, in 1966, was Alan Perlis, of Carnegie Mellon University. The first female recipient was Frances E. Allen of IBM in 2006.
- Since 2014, the award has been accompanied by a prize of US$1 million, with financial support provided by Google.

Source: https://en.wikipedia.org/wiki/Turing_Award

ACM A.M. Turing Award (2/3)

- Some important milestones of cryptography made by the Turing award laureates

Year	Recipient	Major Works
1995	Manuel Blum	Computational Complexity Theory and its Application to Cryptography
⋮		
2000	Andrew Yao	Millionaires' Problem Pseudorandom Number Generator

ACM A.M. Turing Award (3/3)

Year	Recipient	Major Works
2002	Ron Rivest	RSA Public-key Cryptosystem
	Adi Shamir	
	Leonard Adleman	
⋮		
2012	Silvio Micali	Zero-knowledge Proof
	Shafi Goldwasser	
⋮		
2015	Whitfield Diffie	Asymmetric Public-key Cryptography Digital Signatures Key Exchange
	Martin Hellman	

密碼學的發展

古典
密碼學

近代
密碼學

現代
密碼學

後量子
密碼學

(58 BC–)

(1939–)

(1976–)

(2003–)

Julius Caesar

Alan Turing

RSA (Rivest–Shamir–Adleman)

Q&A

TEXAS A&M UNIVERSITY