

Information Security

Course Introduction

Sun, Yeali (孫雅麗)
Lin, Yeong-Sung (林永松)
Tsay, Yih-Kuen (蔡益坤)

Department of Information Management
National Taiwan University

Course Objectives

- 🌐 Get familiar with **security issues** in multi-user information systems and computer networks
- 🌐 Understand the **fundamental techniques**, particularly cryptography, for security
- 🌐 Practise **application of security techniques** in practical areas such as electronic commerce, network intrusion protection, and security management

Main Focuses

- 🌐 *Design and underlying principles of **automated tools for protecting information**, including programs and data, stored on computers or communicated over networks*
- 🌐 *In particular, *fundamentals* and *applications* of **cryptographic technology** (including cryptographic algorithms and protocols)*
- 🌐 *Some other aspects of information security:*
 - ☀️ **Physical** and **administrative** means essential
 - ☀️ **Biometrics** also useful
 - ☀️ **Caution** by programmers and users a must

Will seldom address these other aspects in class.

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

— *The Art of War, Sun Tzu*

故用兵者，
無恃其不來，恃吾有以待之；
無恃其不攻，恃吾有所不可攻也。

— 孫子兵法 九變篇

Strength of a Chain

A chain is only as strong as its weakest link.

— *English Proverb*








The probable origin:

In every chain of reasoning, the evidence of the last conclusion can be no greater than that of the weakest link of the chain, whatever may be the strength of the rest.

— *Essays on the Intellectual Powers of Man, Thomas Reid, 1786*

An equivalent: 木桶理論

Course Subjects/Outline

-  **Overview**: basic concepts, architecture, model, etc.
-  **Secret-Key (Symmetric) Cryptography**: classical techniques, block ciphers, DES, finite fields, AES, pseudorandom number generation, stream ciphers, etc.
-  **Public-Key (Asymmetric) Cryptography**: number theory, RSA, ECC, etc.
-  **Digital Signatures**
-  **Hash Functions** and **Message Authentication**
-  **Key Management** and **User Authentication**
-  **Network Security**: IPsec, virtual private networks (VPNs), IP traceback, firewalls, denial of service, etc.