Information Security

Overview

Sun, Yeali S. (孫雅麗)

Lee, Anthony J.T. (李瑞庭)

Lin, Yeong-Sung (林永松)

Tsay, Yih-Kuen (蔡益坤)

{sunny,jtlee,yslin,tsay}@im.ntu.edu.tw

Dept. of Information Management

National Taiwan University

Course Objectives

- *Design* and *underlying principles* of **automated tools** for **protecting information**, including programs and data, *stored on computers or communicated over networks*
- Focus on the *fundamentals* and *applications* of **cryptographic technology**
- Will also briefly discuss **software security**
- 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 techniques/practices in this course

What *Sun Tzu* Has Said

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

孫子兵法怎麼說

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

Course Outline

- **Introduction**: basic concepts, architecture, model, etc.
- **Secret-Key (Symmetric) Cryptography**: classical techniques, block ciphers, DES, finite fields, AES, stream ciphers, applications, etc.
- **Public-Key (Asymmetric) Cryptography**: number theory, RSA, key management, ECC, etc.
- **Authentication, Hash Algorithms, and Digital Signatures**
- **Network Security**: IPsec, virtual private networks (VPNs), IP traceback, firewalls, denial of service, etc.
- **System and Application Software Security**: malicious software (including viruses), Web application security, etc.