Introduction to Computer Security

Chenyi Zhang

zhang_chen_1@sina.com

Text book

- William Stallings, Lawrie Brown
  Computer Security — Principles and Practice
  Pearson 2012 for the second edition

Authorized Chinese edition (English version) available from the Publishing House of Electronics Industry ($\sim$ 73 RMB on `www.amazon.cn`)

Grading

- Homeworks (week 4, 7, 10)— 10% each
  will be due in 3 weeks after release
- Final project — 70%
- No close book exam
- Types of questions: (group) design & explanation, article reading, may be required to search the Internet (e.g. wikipedia can be a good source of information)

About this course (in a word cloud)

A Few Concepts in Computer Security

- Authentication
- Password
- Access control
- Cryptography and Cryptanalysis
- Bookkeepings
- ...

Attackers vs Defenders

Security is about protection of assets

- Prevention
- Detection
- Reaction

Topics in Computer Security

What is Computer Security

The NIST Computer Security Handbook [1995]:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Main topics in security (C.I.A)

Confidentiality

- Data confidentiality assures that confidential information is not disclosed to unauthorized individuals
- Privacy assures that individual control or influence what information may be collected and stored

Examples

- Student grade information maby be considered an asset with high confidentiality (only be available to students, their parents, and their employers)
- Course information: low confidentiality rating; often available publicly

Integrity

- Data integrity assures that information and programs are changed only in a specified and authorized manner
- System integrity assures that a system performs its operations in unimpaired manner

Examples

- A hospital patients allergy information (high integrity data): a doctor should be able to trust that the info is correct and current
- Entries Wikipedia are of relatively high integrity (semantically) which is only edited by experts
- Cookies in your browsers are of high confidentiality and high integrity

Availability

- Availability assures that systems works promptly and service is not denied to authorized users

Examples

- A public website for a university: a moderate availably requirement; not critical but causes embarrassment
- The authentication server for `i.jnu.edu.cn` needs to be of relatively high availability
- DNS service should be of high availability

What is the course about

- Security concepts and terminologies
- Theory, Analysis, Creativity, Problem solving
- Not a programming course

Technical Topics

- Basic cryptography
  - why they are "secure"
  - symmetric cryptography and asymmetric cryptography
  - basic cryptanalysis
  - block cipher and stream cipher
  - secure hash function
  - digital signature
  - RSA, ElGamal encryption
  - Computational complexities, (e.g., NP vs P)
  - Other interesting topics: eg. ECC, secret sharing, zero-knowledge protocols

Technical Topics

- Basic cryptography
  - why they are "secure"
  - symmetric cryptography and asymmetric cryptography
  - basic cryptanalysis
  - block cipher and stream cipher
  - secure hash function
  - digital signature
  - RSA, ElGamal encryption
  - Computational complexities, (e.g., NP vs P)
  - Other interesting topics: eg. ECC, secret sharing, zero-knowledge protocols
- Applied cryptography
  - PKI, Key Distribution,
  - Authentication, password, Secure Email,
  - SSL, IPSec, online payment protocols, Digi-cash
  - Blockchain, smart contract, Bitcoin & other coins?

Other Technical Topics that We May Discuss

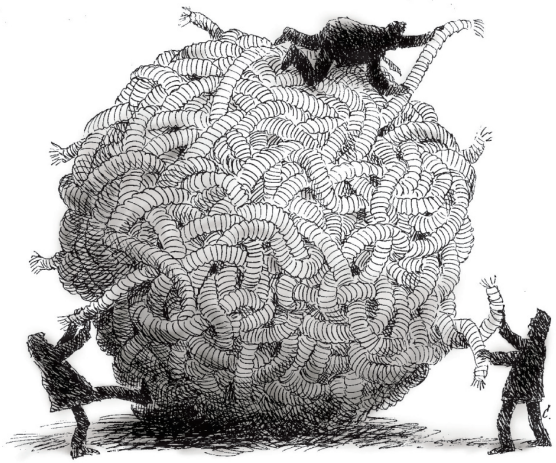
- Access Control & Information flow
- Intrusion Detection
- Web security
- Wireless Network Security
- Operating System security
- Software security
- Database security
- Physical security
- Human behaviour (attack based on social engineering)
- ...

The Challenges of Computer Security

- Computer security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
- The great advantage that the attacker has is that he or she need only find a single weakness while the designer must find and eliminate all weaknesses to achieve perfect security.
- It requires regular, even constant, monitoring, and this is difficult in todays short-term, overloaded environment
- Security is too often an afterthought rather than being an integral part of the design process
- As a designer, look through things with attackers eyes

Security by obscurity

- Making things complex don't always makes it secure
- By making things obscure, you're essentially relying on something that you have no assurance of
- Like a really complicated knot to stop you stealing something
- Sometimes adding more security mechanism only introduces more vulnerability to the system



Kerchkhoffs's principle

Courtesy of wikipedia, by Dutch cryptographer Auguste Kerckhoffs in the 19th century

Principle

A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.