

Principle of Information Security

— Course Introduction

胡天磊, Dr. HU Tianlei

Associate Professor

College of Computer Science, Zhejiang Univ.

htl@zju.edu.cn

Course Outline

- Objectives & Contents
- Topics & Materials
- Evaluation & Grading

Objectives

Introduce theories and concepts of Computer Security

- Introduce concepts of information security in general
- Concentrate on concepts and essences instead of details

Why learn this course?

- Make “yourself” more secure.
- Show you the next steps to becoming an information security expert.

Course Outline

Part 1: Concepts and Bases of Information Security

week 1

- Course Introduction
- History, Concepts, and Bases of Information Security

Part 2: Cryptography

week 2-3

- History, Concepts, and Bases of Cryptography (HW1. Password cracking)
- Symmetric/Secret Key Cryptography
- Asymmetric/Public Key Cryptography (HW2. Large number arithmetic)

Part 3: Security Services

week 4-6

- Digital Signature, One-way Hash, and MAC (HW3. Using PGP)
- Authentication & Authorization

Part 4: Internet and Security

week 7-8

- Internet Infrastructure and TCP/IP
- IP Security (HW4. Using Wireshark)
- Malicious Code: Trojan, Virus, Worm, Botnet, Spam, and ...

Course Materials

References:

- 《Cryptography and Network Security: Principles and Practice, Fifth Edition》
- 《密码编码学与网络安全:原理与实践(第5版)》
- Author: William Stallings , Publisher: 电子工业出版社, Date: Jan 1st, 2011
- <http://product.china-pub.com/54027>
- 《Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition 》
- 《应用密码学——协议、算法与C源程序》
- Author: Bruce Schneier, Publisher: 机械工业出版社, Date: Jan , 2000
- <http://product.china-pub.com/94>
- 《Computer Security: Art and Science 》
- 《计算机安全学：安全的艺术与科学》
- Author: Matt Bishop, Publisher: 电子工业出版社, Date: May, 2005,
- <http://product.china-pub.com/24817>

Textbooks are not required for this course.

Logistics & Contacts

- 学在浙大: <https://courses.zju.edu.cn/course/56852>
- 教师: 胡天磊 / HU Tianlei
 - htl@zju.edu.cn
 - 13958091761
- 助教:
 - 肖瑞轩 / XIAO Ruixuan
 - xiaoruixuan@zju.edu.cn
 - 15123324332
 - 刘雨辰 / LIU Yuchen
 - liuyuchen0921@zju.edu.cn
 - 18066331397

Evaluation and Grading

- In Course 5+ points
- Homework 45 points
 - Will be released soon on 学在浙大 / Learning in ZJU
- Final Exam 50 points
 - Date TBD

Ok, Let's Begin!

You Will Never Achieve a
Perfectly Secure System!

You Will Never Achieve a
Perfectly Secure System!!

You Will Never Achieve a
Perfectly Secure System!!!

Well ... Maybe If You Do This:



In This Class:



Privacy

Availability

Dependability



Speed

Money

New features

Profitability

Cost-Benefit

Top Common Security Myths

(from *Secure Computing Magazine*)

- My home PC/Laptop is safe from attack by hackers.
- Our company won't get hacked - hackers don't attack companies like ours.
- Servers on internal networks are safe from attack.
- If I have a firewall, my network can't be hacked.
- People on my private network can be trusted; most security breaches are from outside the company.
- Hackers are just geeks out to show they can break into networks.

Security Myths: Case Study #1

- Hackers are just geeks out to show they can break into networks?
- What are hackers looking for?

Thrill?


Challenge?

Excited?

What others say ...

"A highly computerized society like the United States is extremely vulnerable to electronic attacks from all sides. This is because the U.S. economy, from banks to telephone systems...relies entirely on computer networks."—Foreign Government Newspaper

Information Age Threat Spectrum



| | | |
|---------------------------|------------------------------|---|
| National Security Threats | Info Warrior | Reduce U.S. Decision Space, Strategic Advantage, Chaos, Target Damage |
| | National Intelligence | Information for Political, Military, Economic Advantage |
| Shared Threats | Terrorist | Visibility, Publicity, Chaos, Political Change |
| | Industrial Espionage | Competitive Advantage Intimidation |
| | Organized Crime | Revenge, Retribution, Financial Gain, Institutional Change |
| Local Threats | Institutional Hacker | Monetary Gain Thrill, Challenge, Prestige |
| | Recreational Hacker | Thrill, Challenge |

Cyber Terrorism

The nations in the world nowadays are increasingly dependent on information technology (hardware and software)

This hardware and software have proven relatively easy to exploit, putting the nation at risk from “cyberterrorist” acts.

Louis Freeh(the former FBI director), Testimony before Senate:

- The Tamil Guerrilla group, the Internet Black Tigers, conducted a successful "denial of service" attack on servers of Sri Lankan government embassies
- Italian sympathizers of the Mexican Zapatista rebels attacked the web pages of Mexican financial institutions.

The Stuxnet - Code Name "Olympic Games"

Stuxnet is a computer worm that was discovered in June 2010. It was designed to attack PC and industrial programmable logic controllers (PLCs).

Stuxnet reportedly ruined Iran's ability to build nuclear weapons. It is estimated that Stuxnet slowed down Iran's nuclear centrifuges. It is estimated that Stuxnet saved the United States and Israel from developing the ability to build nuclear weapons for 10 years.

In July 2013, Edward Snowden and the United States and Israel cooperatively developed a plan to destroy the Stuxnet worm.

References:

- <http://www.nytimes.com/2010/06/28/us/politics/28cyber.html>
- http://en.wikipedia.org/wiki/Stuxnet#cite_ref-sanger2012June_28-0
- <http://www.freebuf.com/articles/system/19059.html>
- <http://www.freebuf.com/news/19199.html>
- <http://www.freebuf.com/news/19439.html>

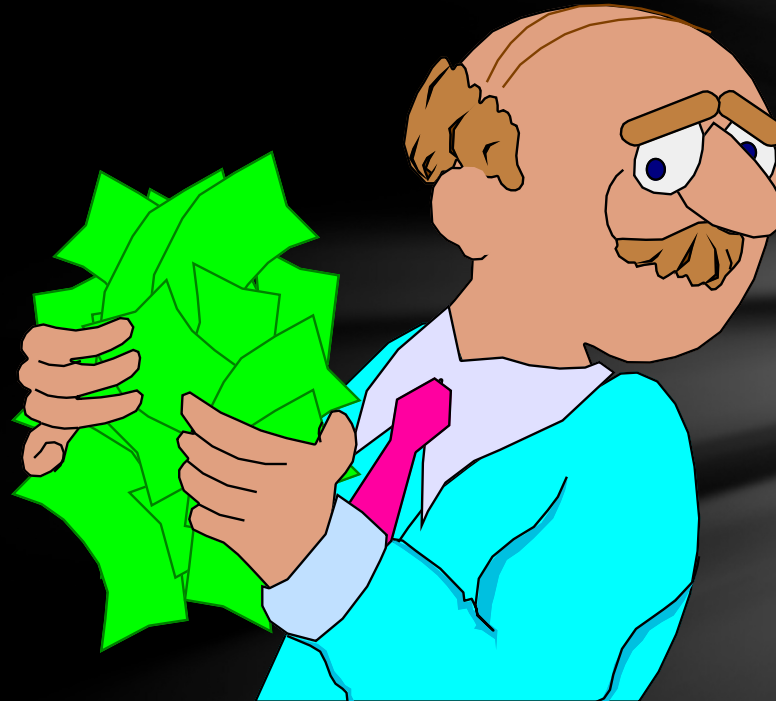
| Country | Infected computers |
|---------------|--------------------|
| Iran | 58.85% |
| Indonesia | 18.22% |
| India | 8.31% |
| Azerbaijan | 2.57% |
| United States | 1.56% |
| Pakistan | 1.28% |
| Others | 9.2% |

Data Sovereignty

Data sovereignty is the idea that data are subject to the laws and governance structures within the nation it is collected.

- A concept introduced by the Snowden revelation
 - **NSA's PRISM program**: designed to "receive" emails, video clips, photos, voice and video calls, social networking details, logins, and other data held by a range of US internet firms" such as American tech companies like Facebook, Apple, Google and Twitter among others.
 - **US Patriot Act**: US officials were granted access to any information physically within the United States (such as server farms), regardless of the information's origin.
- Recent Sino-US conflict accelerates its development:
 - Huawei & Tiktok vs Google & Facebook
 - Apple: partner with 云上贵州 to provide iCloud service to users in China;
 - Tiktok: try to partner with Oracle / Microsoft to address concerns by US authorities.
- **Why are these major countries worldwide paying more attention to data sovereignty nowadays?**

Another reason to care: Money.



Industrial Espionage

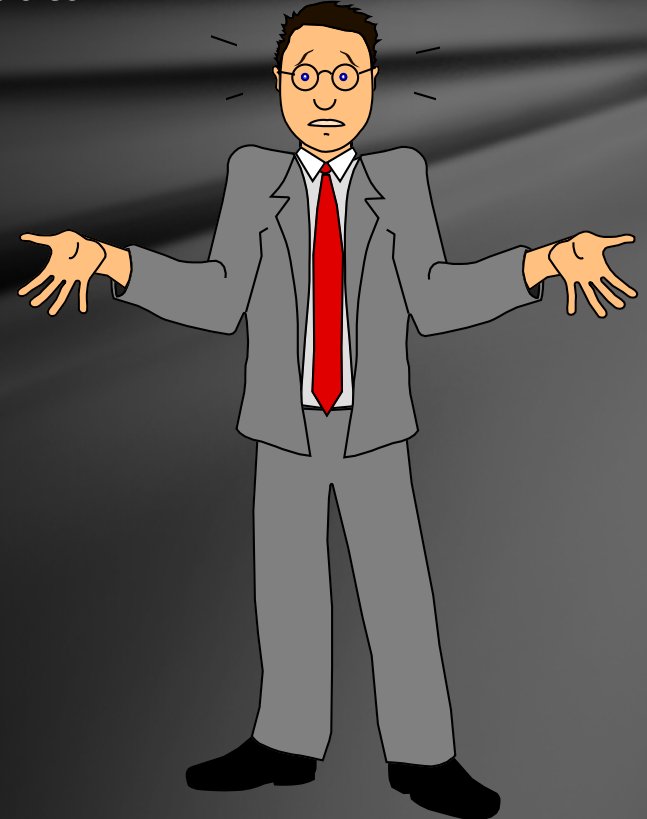
The Commercial Importance

- **According to the US Department of Commerce agency NTIA (National Telecommunications and Information Administration)**
 - *"By the 21st Century, telecommunications and information-related industries will account for approximately 20 percent of the U.S. economy."*
- **Mike Rasch, VP of Global Security, testimony before the Senate Appropriations Subcommittee**
 - *"The lure of big, fast-money scores in virtual commerce is making it common for skilled hackers to attack competitors in search of free intellectual property."*

Industrial and Foreign Espionage

- Most damaging stolen information: pricing data, manufacturing processes, and product development specifications.
- Other stolen information: customer lists, research, sales data, personnel data, compensation data, cost data, proposals, strategic plans, negotiating positions, and contract data.

It isn't
"just us Techies"
Anymore!!!



Security Myths: Case Study #2

- Most security breaches are from outside the company ?

Technology Helps Insiders!

- Over 80% of the attacks are [from insiders (internal)]
- As employees become more savvy they can go out on the Internet and find out how to break into sites pretty easily ... organizations need to protect against that.
- Many of these back doors are taking on espionage qualities.
- Many laptops now have a video camera for video conferencing built into the laptop or desktop. Back doors allow them to watch, listen -- and pump that information remotely over the network to a remote site (very dangerous to every people !)

By Chris Klaus, ISS

- <https://cloud.tencent.com/developer/news/316911>

What is an Insider?

- People with legitimate access to or association with some aspect of the environment or the system.
- Insiders have increased opportunities and knowledge in comparison with outside intruders.
- Insiders usually have a clearly defined motive (revenge, financial gain, information, etc.).

The Insider Problems are getting worse!

A buzzword, “Flat World.”

The increasingly distributed nature of corporate resources creates an expanded view of insiders.

- Developers
- Testers
- Everyone who works in the development lab
- Staff working in the company
- Sales force
- Consultants
- Delivery/Transport
- Customer
- Customer's insiders

“There is no longer a clear distinction between insiders and outsiders, between a corporate ally and an enemy. And preventing access is the exact opposite of what companies are trying to do.”

Beyond Computing, S. Dickey

Hidden Facts: Case Study #3

The vast difference between the fact and the reported news?

15-year-old kids is super hacker?

“All this talk of fifteen-year-old kids vandalizing the Web is a smoke screen behind which dangerous, professional crackers are pleased to take cover”

Mike Rasch, VP Global Security,
testimony before the Senate Appropriations Subcommittee

“To Report or Not To Report”

- An infotech company will typically lose between ten and one hundred times more money from shaken consumer confidence than the hack attack itself represents if they decide to prosecute the case.
- Estimate: fewer than one in ten serious intrusions are ever reported to the authorities.

Mike Rasch, VP of Global Security,
testimony before the Senate Appropriations Subcommittee

You need to know from the beginning ...

- You will never achieve a perfectly secure system.
- Hackers are not chasing for thrill, challenge, or excitement.
They hack your PC / Server / Mobile for “benefits.”
- Insiders are more dangerous than outsiders.
- Reported hacking events are much lesser than they happened.