Network Security: theory & practice

Liang CAI
Associate Professor
Computer Science & Technology
Zhejiang University

My Info

- NAME
  - Cai Liang 蔡亮
  - Associate Professor, Computer Science & Technology
  - Chairman of Software Engineering
  - Zhejiang University
- Office Location
  - No. 515 . Main Section, Cao Guangbiao Building, YuQuan Campus
- Tel: 89952420 Email: LeonCai@zju.edu.cn

TA Info

- NAME
  - Wan ZhiYuan 万志远
  - Post-Doc, Computer Science & Technology
  - Zhejiang University
- Office Location
  - No. 405, Cao Guangbiao West Building, YuQuan Campus
- Tel: 87952420，13858183310
- Email: WanZhiYuan@zju.edu.cn

Course Outline

- Reference textbook
  - 英文原版：Computer Network Security: Theory and Practice, Springer-Verlag New York, LLC
  - 影印版：Computer Network Security: Theory and Practice, 高等教育出版社
  - Expensive textbook, No textbook, also OK!
- FYI Oriented, not mathematics centric
- Evaluation/Grading
  - Quiz / Discussion (10)
  - Homework (10):
  - Group Project on Selected Experiments(30)
  - Final Exam (50)
- Slides: pan.baidu.com/s/1c113Rig pass: sj8y

Welcome to Network Security Boot Camp

Quick Survey:

protect or attack?

You Will Never Achieve a Perfectly Secure System!

What info-system is strongest ?

Well … Maybe If You Do This:

In This Class:

Privacy

Availability

Control

Dependability

Speed

Money

New features

Profitability

Cost-Benefit

What do you think?

- What do you think of when you think of "information security"?
  - Why information system is unsecure?
  - Where it can be attacked?

Where are Computer Systems vulnerable?

1. Hardware
2. Software

5. Operators

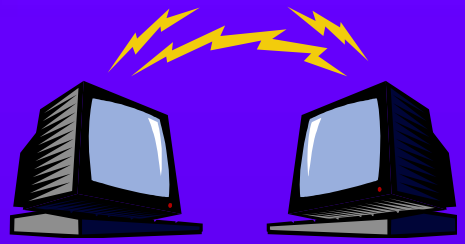
3. Data

4. Communications

What are the targets for a hacker?

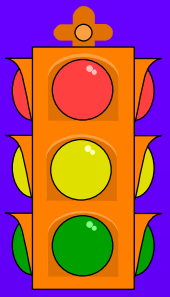
What kind of information systems are you likely to hack if you are an expert-hacker?

nowadays computer systems are everywhere!



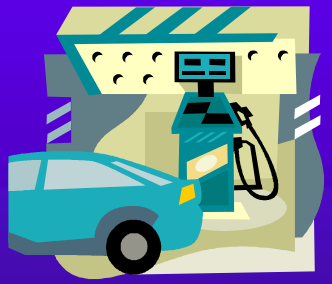
TV/Telecom

Banking & Finance



Transportation (movie?)

electrical power systems



Gas & Oil

water supply systems

government services and emergency services

Yes,
they are real!

Course Outline

- Network security overview
- Applied Cryptography Basics, Crypto placements in networks, public-key Infrastructure (PKI)
- TCP/IP Security, weakness of the protocols
- IPsec, SSL/TLS; secure email (PGP, S/MIME), Kerberos, secure remote logins
- Wireless network security: WEP, WPA, WPA2, Bluetooth security, wireless mesh network security

Course Outline

- Network perimeter security, Firewall configurations and DMZ
- Viruses, worms, Trojan horses;
- Web security, denial of service attacks
- Intrusion detection: network-based and host-based detections, signature and behavioral detections, honeypot systems

Security Resources – gov/com

www.cert.org（US CERT Team）

www.cert.org.cn（Chinese CERT Team）

www.infosec.org.cn（Chinese infosec forum）

www.wooyun.org

www.securityfocus.com（famous bug sites）

xforce.iss.net（exploits from ISS）

Security Resources – research

- **CRYPTO - International Cryptology Conference**
- **S&P - IEEE Symposium on Security and Privacy**
- **CCS - ACM Conference on Computer and Communications Security**
- **USENIX Security Symposium**
- **NDSS - Network and Distributed System Security Symposium**
- **CSFW - Computer Security Foundations Workshop**

Security Resources – hackers

www.phrack.com (famous phrack magazine)

www.antionline.com (classic hacker site)

packetstormsecurity.com (classic hacker site)

www.nmrc.org/pub/faq/hackfaq/ (Hacker's FAQ)

astalavista.box.sk (search engine for security websites)

This course gives you information that can be used for good or evil. It is your ethical responsibility to use this information carefully and considerately. If you do not plan to do so, you are free to drop this class.

Remember Google's motto: "Don't' be evil"

What are systems vulnerable **to**?

We may already know (from movie?)

- Wiretapping and Eavesdropping
- Trojan Horses
- Viruses, Worms

New idea ?

- Masquerading (IP spoofing)
- Timing Attacks (replay a encrypted password challenge)
- Distributed Denial of Service (Hacker's war)
- Information Leaks (Overt and Covert Channel)
- Cryptographic Attacks (WIFI WEP/WPA crack, BackTrack/XiaoPan OS/Beini, www.anywlan.com)

What are systems vulnerable **to**?

We may already know

- Password Cracking
- Malicious Active-X
- Malicious Email Attachments
- Screen Capture

New Idea?

Inference and Aggregation

Key, Sequence Prediction (pseudo random number)

Social Engineering (Phishing)

Router and DNS attacks (advanced version of phishing?)

Yes,

they are real!

Information Security – the Eternal Topic

It comes down to access. If there is any kind of access, the system might be vulnerable to misuse of that access.

Of course, if there is **no** access, the computer is useless

"The greatest threat you face is not the viruses or the hackers or the whatever, but rather complacency."

Michael Tucker, Editor, *SC Magazine*

Top Common Security Myths

(from *Secure Computing Magazine*)

- Our company won't get hacked - hackers don't attack companies like ours.
- My home PC is safe from attack by hackers.
- 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 who are out to show that they can break into networks.

Security Myths: Case Study #1

- Hackers are just geeks who are out to show that 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

INSIDERS

CyberTerrorism

- The US and other nations are increasingly dependent on information technology (hardware and software)
- This hardware and software has proven to be relatively easy to exploit, putting the nation at risk from “cyberterrorist” acts

CyberTerrorism

- 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 web pages of Mexican financial institutions.

Freeh, Testimony before Senate

Another reason to care: Money.

Industrial Espionage

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."

The Back Alleys of E-Commerce

- “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”

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

reported in The Register and online testimony transcript.

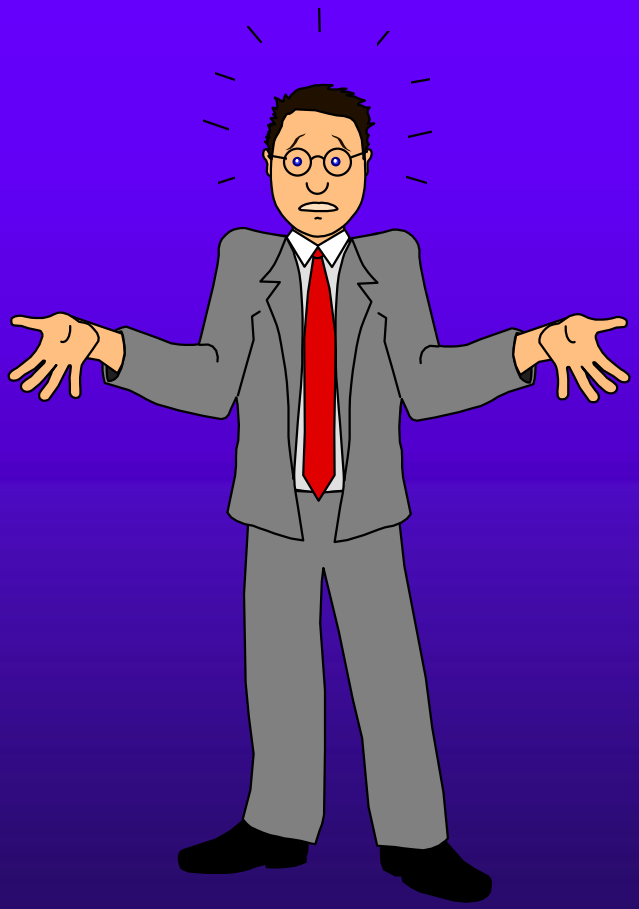
Industrial and Foreign Espionage

- Increased 260% in the US within 10 years
- 30% of the losses had foreign involvement.
- 58% perpetrated by current or former employees.
- There are at least 13 countries with nationally sponsored information warfare capabilities.

Industrial and Foreign Espionage (continued)

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

Chris Klaus, ISS

What is an Insider?

- People with legitimate access to or association with some aspect of the environment or the system.
- Insiders have increased opportunity 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 hot word "Flat World"
- The increasingly distributed nature of corporate resources, creates and 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 a corporate 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 huge 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 info tech 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 Global Security, testimony before the Senate Appropriations Subcommittee

reported in The Register and online testimony transcript