CS5231: Systems Security

Lecture 1: Overview

About This Module

- Principle and practice of systems security
  - Understanding security principles through practice
  - Learning skills of programming, system administration, and etc.
- Research frontier of systems security

Uniqueness of This Module

- Think in a different angle
  - How various systems can fail
  - How to prevent such failures
- Learn to think like a hacker, behave like a defender
  - Make no assumptions of hackers
- Heavily based on system programming
  - Have fun!

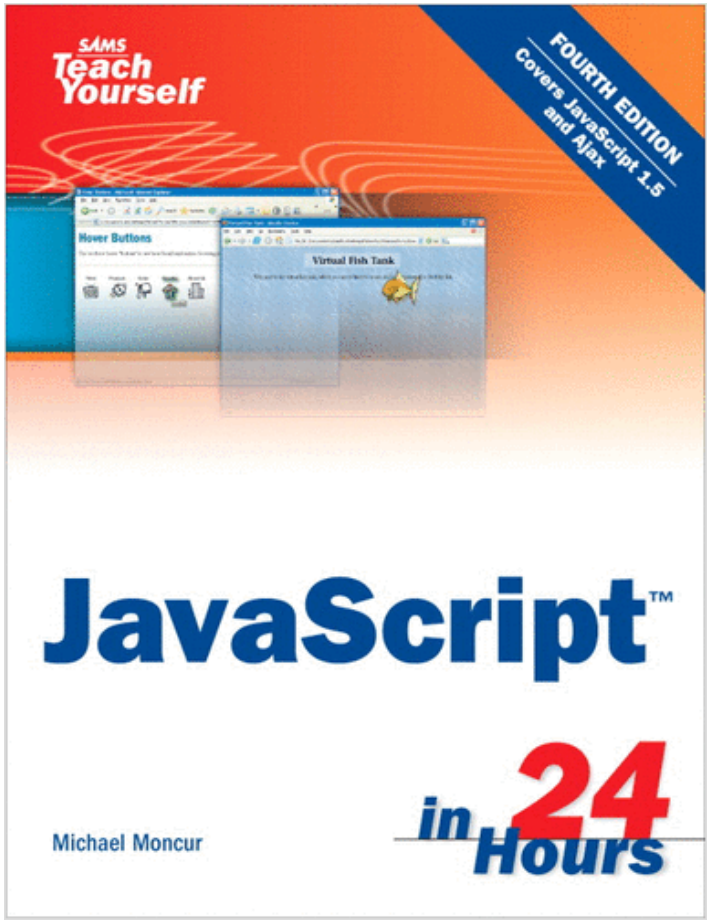
The Security Problem

What are the recent security incidents in news?

Why Does This Happen?

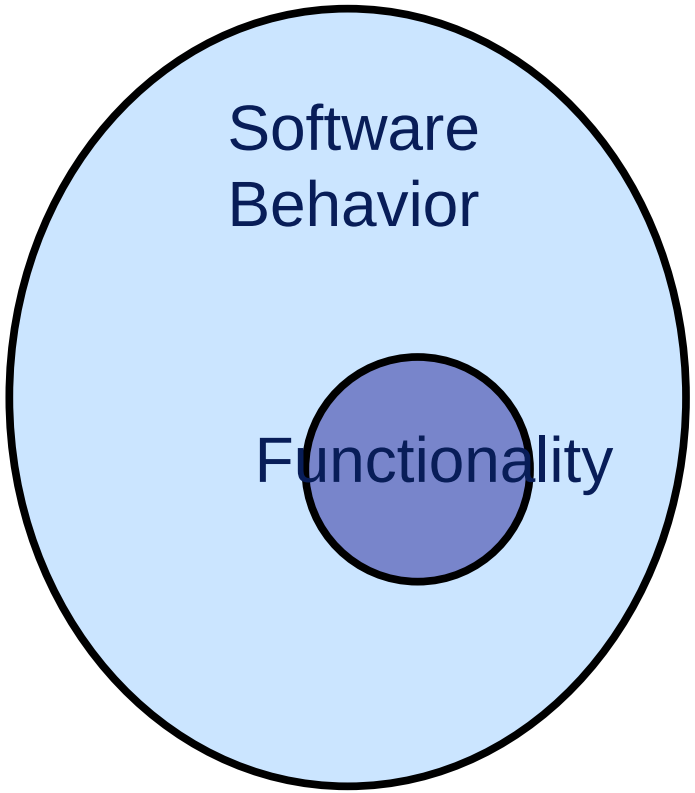
- Functionality: the primary concern during design and implementation.
  - Security is the secondary goal
  - Unawareness of security problems
- Unavoidable human mistakes
  - Awareness
  - Lazy programmer
- Complex modern computing systems

Impatient Programmers



- Maybe enough for learning basic functionality
- Never enough for to learn subtle implications of functionalities
- Result: programs can do more than you expect

Security: Mission impossible



- But in practice, we need to make the security problem under control.
- Need better understanding of whole system

Principle of Easiest Penetration

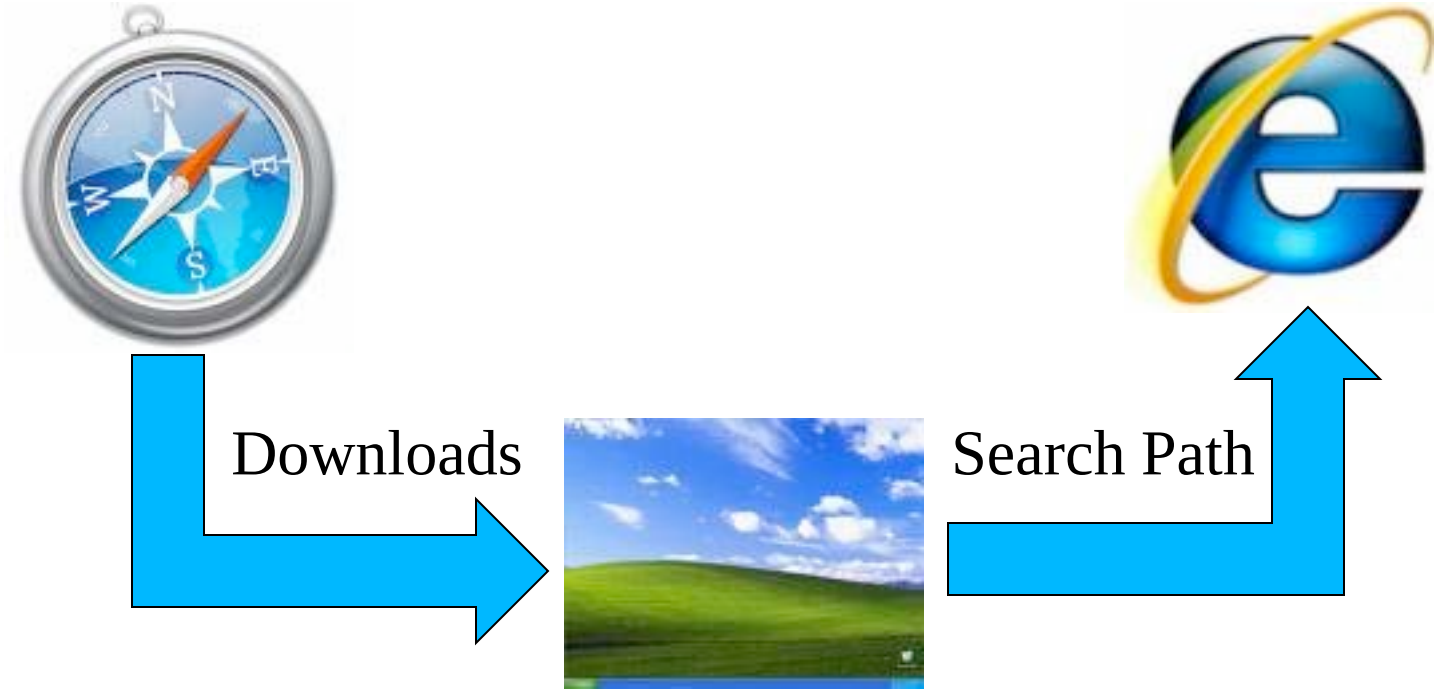
- Security is about every aspect of a computing system
  - Hardware, software, data, and people.
- Principle of easiest penetration:
  - Any system is most vulnerable at its *weakest point*.
  - Attackers don't follow any rules. Don't underestimate their creativity.

Example

- Windows Vista speech recognition
  - Users can use voice to input text
  - Control the Windows system
- What can go wrong?
  - Let's see a video

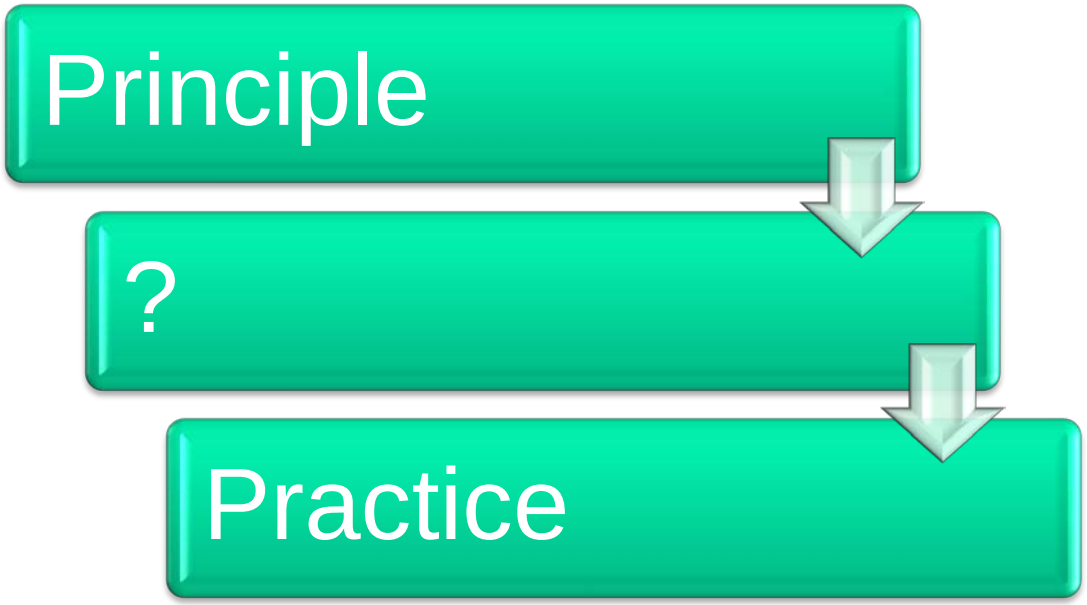
Another Example

- Safari Carpet Bomb



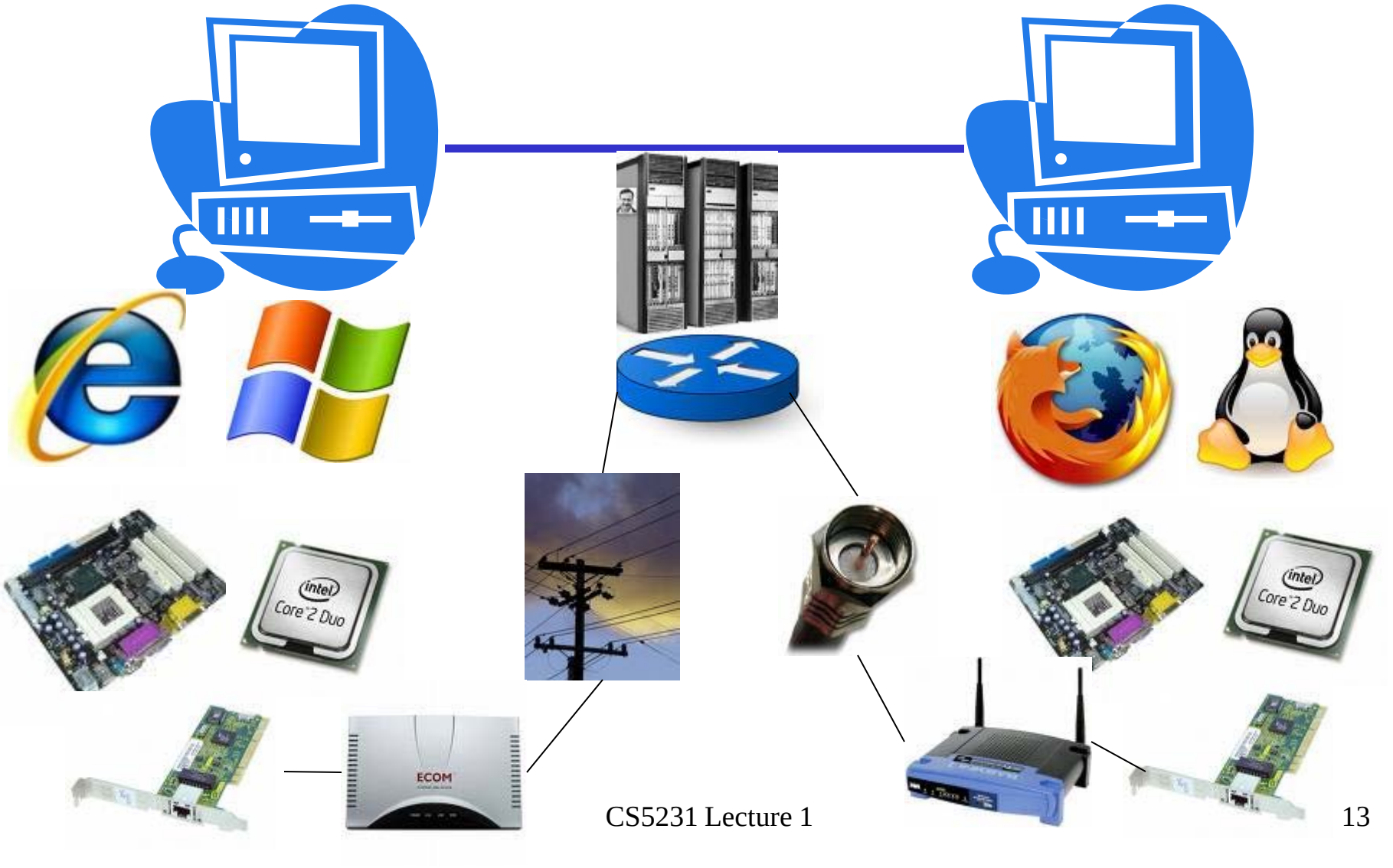
Methodology

Importance of Details



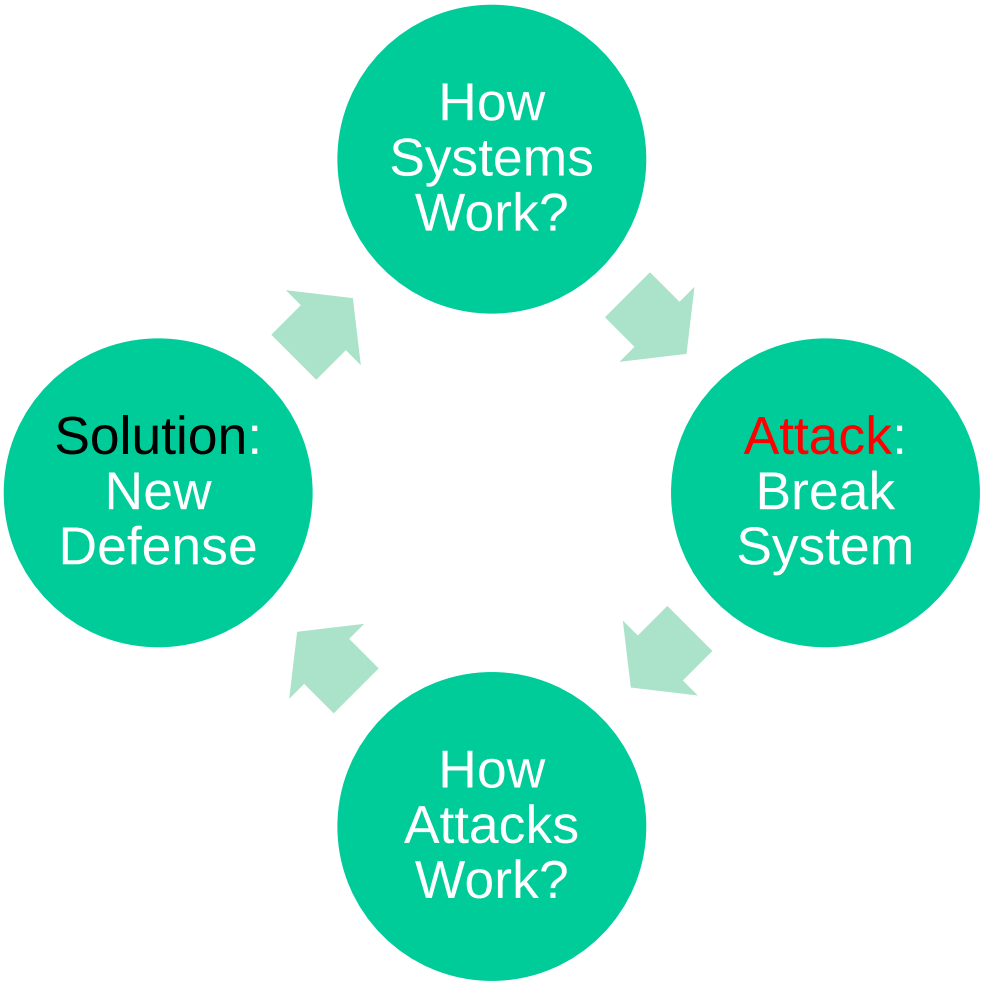
Most of security problems we see are practical problems.

View of Network



Is This a Security Device?

Methodology



Learning to Attack

- If you know the enemy and know yourself, you need not fear the result of a hundred battles.

知己知彼，百战不殆。

Sun Tzu, Art of War

- To prevent attack, we need to learn how attack happens

Ethical Issue

Ethical Use of Security Information

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - Do *not* try these at home
- Purpose of this class
  - Learn to prevent malicious attacks
  - Use knowledge for good purposes

Don’t Cross the Line

Overall Goal

Your Objective in This Module

- Grades in transcript vs. Expertise in CV
  - How do you distinguish yourself with other?
  - How will others evaluate your CV?
- Managing rapid changes in security
  - Tools vs. spirits

Technical Skills

- UNIX/Linux administration
- Open source compiler and project management
  - gcc, make, autoconf, gdb, nasm
- Programming languages
  - C/C++, assembly language
- System and kernel programming
- Source code version control

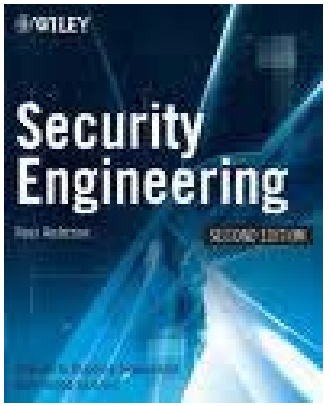
Administrative Issue

Administrative Issues

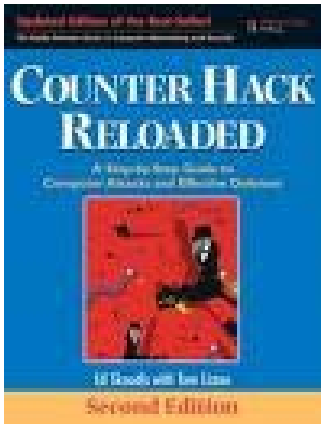
- In class tests: 30%
- Three individual projects: 30%
- Final group project: 40%
- Module resources on IVLE
- Supplementary resources at

  http://www.comp.nus.edu.sg/~liangzk/cs5231/
- TA mailing list: cs5231ta@googlegroups.com

Text Book



- Main book: (Not required)
  - Security Engineering (available online)
- Supplementary book:
  - Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses, by Ed Skoudis



Projects

Individual Homework Projects

- Programming assignments
  - Memory attacks
    - Assembly, C, gdb
  - Web attacks
    - PHP, HTML, JavaScript
  - Linux kernel hacking
    - C

Group-based Final Project

- Project Goal:
  - Apply our methodology: Modifying a system to extract its operation details, understanding attacks, and design solutions.
- Each group is expected to have three to four students
  - Joining forces for more interesting results
  - Limited slots in final presentation
  - Please announce your group information to the TA mailing list

Project Proposal

- Due date: February 13th, 2012
- What to submit:
  - Problem description
  - Your solution and its novelty
  - The platform and tools used in project
  - Project schedule
- You need to make sure your group is capable to handle the technical challenge independently

Progress Report

- Due date: March 12th, 2012
- How is your progress compared to your proposal?
- If you have difficult or question, raise them early

Final Report and Presentation

- Final report due before reading week
  - Following the typical format of technical report or research papers used in our class
- Final presentation: last two weeks in class
  - 10 to 15 minutes for each group

Plagiarism Prevention

- Plagiarism is a serious offense in academia
- Information for plagiarism definition and prevention
  - `http://www.cit.nus.edu.sg/plagiarism-prevention/`
- We use the *Turn It In* tool to check all submissions
  - Submissions are compared with document on the Internet and against one another

Overview of Computer Security

Overview of Topics

- Software security
- Operating system security
- Web security

Example of Topics

- Malicious Code
  - Virus, rootkit, spyware
- Internet Attacks
  - Worm, buffer overflow, botnet
- Web Security
  - Cross-site scripting

Attacks: Basic Concepts

- Valuable components of computer system
  - Hardware, software, data
- *Vulnerability*: weakness in a system
- *Threat*: potential harmful situations
- *Attack*: threat + vulnerability
- *Control*: something reduce or removes vulnerability

Security Goals: CIA Triad

- Confidentiality
  - Protection from unauthorized disclosure
- Integrity
  - Protection from inappropriate modification
- Availability

Confidentiality

- *Confidentiality* ensures that computer-related assets are accessed only by authorized parties.
  - Example, access others emails
- Sometimes called **secrecy** or **privacy**

Integrity

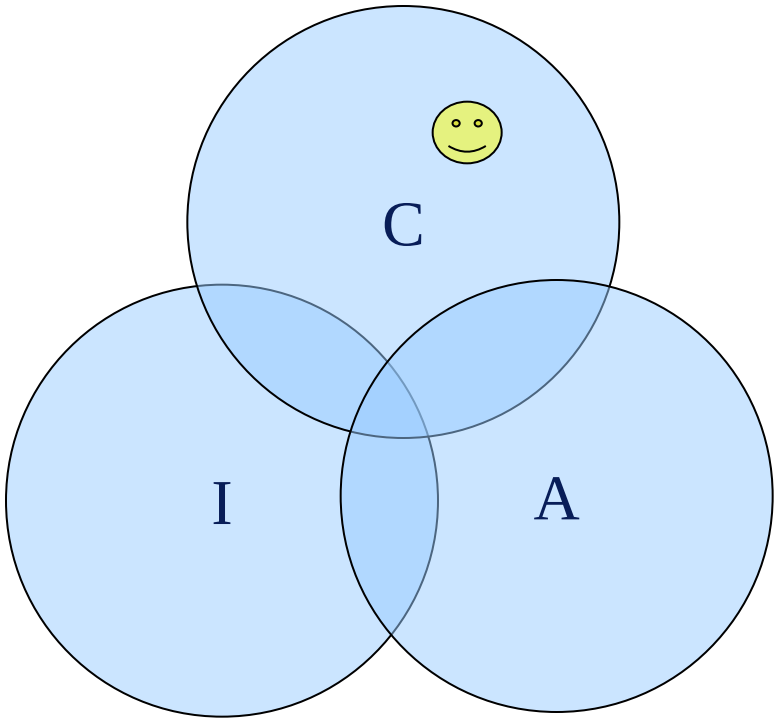
- *Integrity* means that assets can be modified only by authorized parties or only in authorized ways.
  - Example, change bank account balance by attack
- Modification: writing, changing, changing status, deleting, creating.

Availability

- *Availability* means that assets are accessible to authorized parties at appropriate times.
- Its opposite is better known:
  Denial of Service (DoS)

Balance of three goals

- The goals are often conflict
  - Zero availability means perfect secrecy.
- They can overlap or mutually exclusive.



History of Computer Security

Code Breaking in World War II

- Significant mathematical and technical advancement in coding
- Laying foundations of modern computer

Computer Viruses

- **1982, Elk Cloner**
  - First virus in the wild. Targeting Apple II
- **1986, (c)Brain**
  - First virus for IBM PC. A boot sector virus
- **1995, Concept virus**
  - First Macro virus
- **1998, CIH**
  - One of the most harmful widely circulated viruses
  - Overwrites both hard disks **and Flash BIOS**

Computer Worms

- 1978 Worm at Xerox PARC
- 1988 Morris Worm
- 1999 Melissa Worm (Email worm)
- 2001 CodeRed
- 2003 SQL Slammer (fastest in propagation)
- 2003 Blaster
- 2004 Sasser

Recent Threats

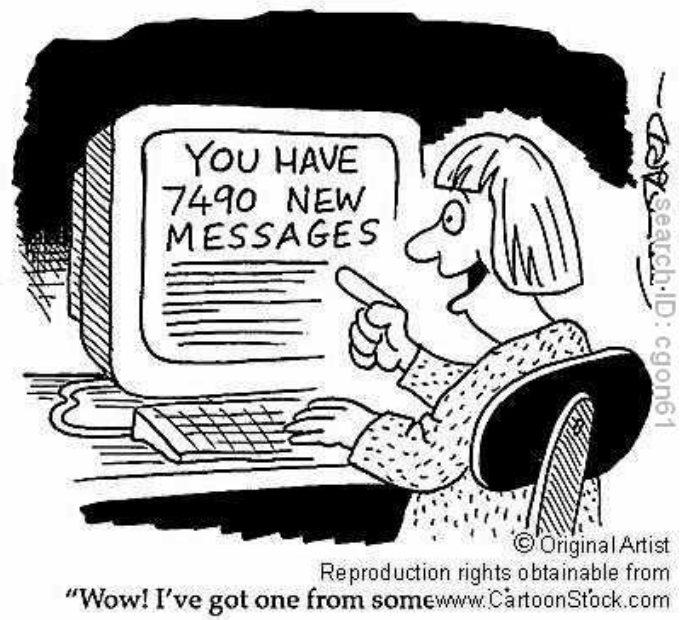
- Rootkit
  - Stealthy backdoor programs
- Spyware
  - Information theft, usually don’t propagate
- Botnet
  - A collection of compromised computers
- Mobile malware

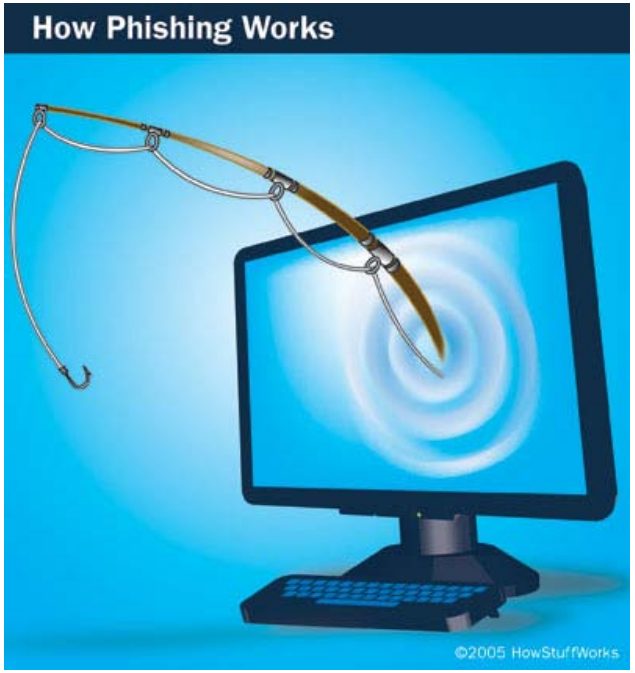
Threats on the Web

- Malicious code install through browsers
- Cross-site Scripting
  - Malicious JavaScript injected into browser sessions
- SQL Injection
  - Malicious SQL statements

Low-tech Threats

- Spam
  - Recapcha
- Phishing





Computer Criminals

- Amateurs
  - Normal users who discover system vulnerabilities during their job
- Crackers or malicious hackers
  - Students or computer professionals
  - For fun or to demonstrate their knowledge

Computer Criminals

- Career Criminals
  - Skilled computer professionals
  - Security forms a black market business over recent years
- Terrorist

Business Model of Career Computer Criminals

- Encrypt user data and “sell” passwords
- Lease bots
  - Blackmail big company
- Steal money from bank accounts or credit card accounts

Summary

- Learning principles through practice
  - Seeing is believing
- Practical skills
  - Experience with Linux and open source tools
  - Solutions for your new concerns

- Learn and solve cutting-edge research problems

Practice

- Setup a Linux Virtual Machine
  - 32-bit Ubuntu Linux 10.04
- Virtual Machine
  - VMWare Workstation
  - VirtualBox