CSC347 – Introduction to Information Security

Sergey Gorbunov

sgorbunov@cs.toronto.edu

http://www.cs.utoronto.ca/~sgorbunov/347f13/

Administrative

- ✓ Instructor: Sergey (sgorbunov@cs.toronto.edu)
- ✓ Office Hours: Wed 2-3pm
- ✓ Location: CC-3083
- ✓ Course Website:
  http://www.cs.utoronto.ca/~sgorbunov/347f13/
- ✓ Teaching Assistant: Andy Chow (chow@cs.toronto.edu)
- ✓ Prerequisites: CSC209H5, 236H5, 290H5
- ✓ Will be mainly follow Arnold Rosenbloom's course material

Grading

- 3 Assignments x 20% each:
  - ✓ Work individually or with a partner
  - ✓ Submit on time else: pay 30% with at most 48 hours late

- 1 Case Study x 10%:
  - ✓ Work with a partner
  - ✓ Submit a 2 page report on a selected topic of research
  - ✓ Give a 5 minutes presentation (short, simple, informative)

- 1 Final Exam x 30%:
  - ✓ 3 hours
  - ✓ Non-Programmable Calculators, 2 pages of double-sided Letter

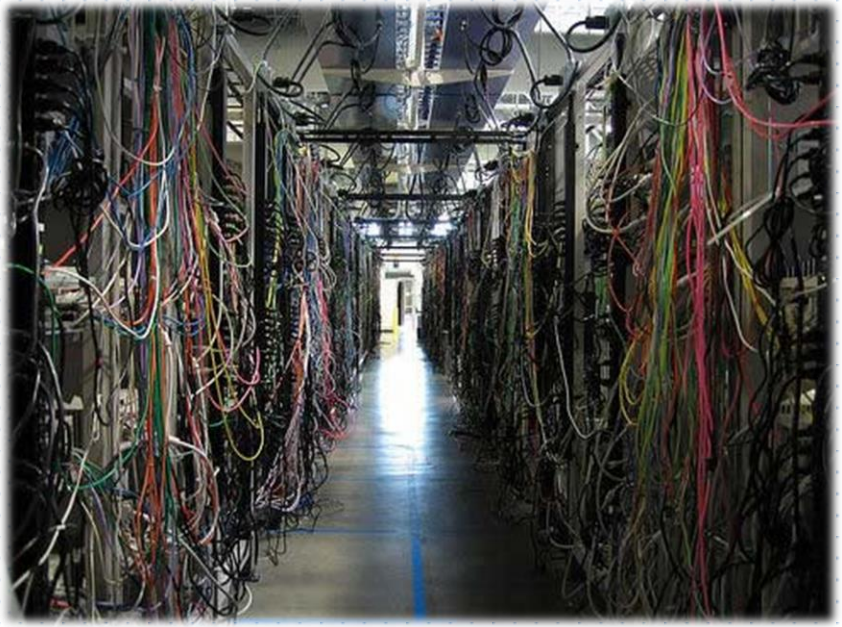
What is information security?

- "is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc...)" – from Wiki

- "The U.S. National Information Systems Security Glossary defines "Information System Security" as the protection of information systems against unauthorized access to or modification of information, whether in storage, processing or transit…"

What is information security?

- **Study of assumptions.**
  - Know user requirements and constraints
  - Come up with a solution
  - Understand assumptions you make



Security Properties

- **Confidentiality**: protect information from unauthorized users, attackers. Example: your student records, financial information

- **Integrity**: prevent malicious modifications/changes to the systems and data. Example: attacker might with to change the amount of money in your or his account. Integrity is hard to ensure.

- **Availability**: attackers are not able to prevent honest users from using the system or accessing the data
- Example: perform Denial of Service (DOS) attacker on the webserver

Our Course

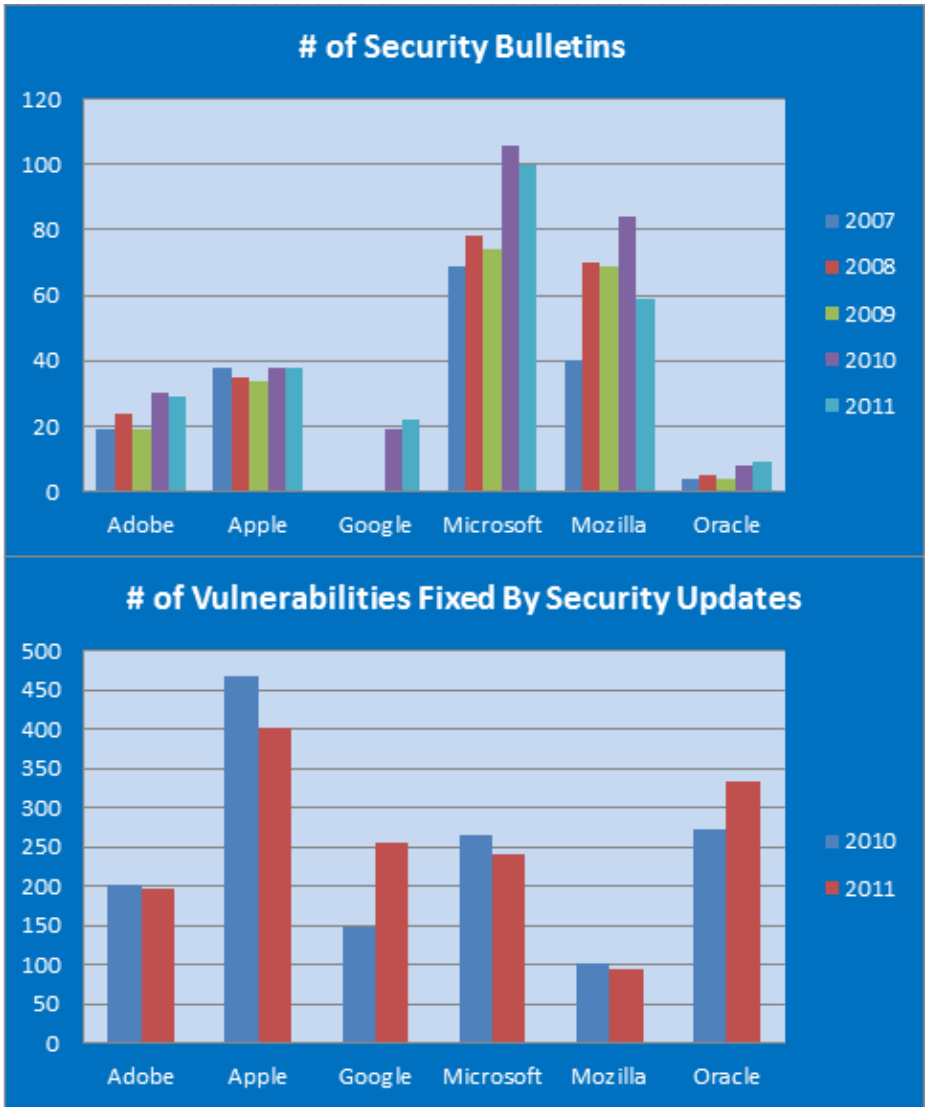
- **Software Security** (3 weeks): how to identify software vulnerabilities (buffer overflows, SQL injections, Cross-Site Scripting attacks)
- **Cryptography** (3 weeks): using mathematics to guarantee something about the security of the data (secret and public key cryptography, hash functions and digital signatures, public key infrastructure)
- **Systems Security** (3 weeks): understand what goes into building a secure system (access control mechanisms, malware, viruses, information flow control)
- **Network Security** (3 weeks): identify, prevent and protect computer networks (basic network protocols, denial of service, flooding, injections, firewalls, network intrusion systems)

Why info sec?

- Money can be made legally from finding and exploiting vulnerabilities:
  Examples: white-hat hackers, penetration testers, security engineering.
  (Google will pay up to $20000 for remote code execution attacks, Mozilla $3000, Microsoft up to $100000)

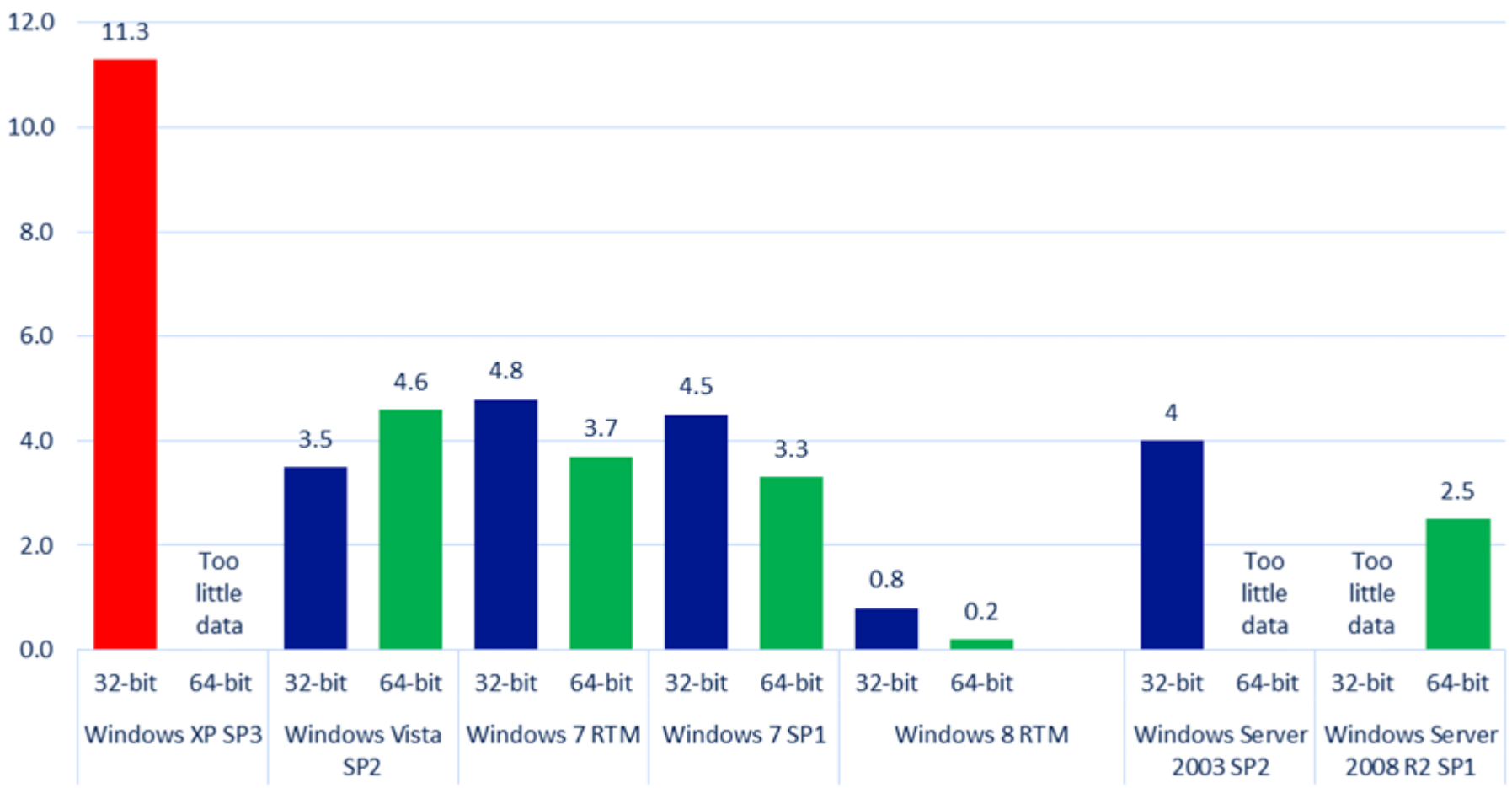
Why info sec?

- Security patching trends for major software vendors



Why info sec?

- Infection rates as of 2012 for Microsoft OSs




KEEP
CALM
AND
ENJOY
IT