COMPSCI 1JC3

Introduction to Computational Thinking

Fall 2017

09 Information Security

William M. Farmer

Department of Computing and Software
McMaster University

November 7, 2017

McMaster University

Opinion on Assignment 3 (iClicker)

What did you think of the difficulty of Assignment 3?

A. Much too easy.
B. A bit too easy.
C. Just right.
D. A bit too hard.
E. Much too hard.

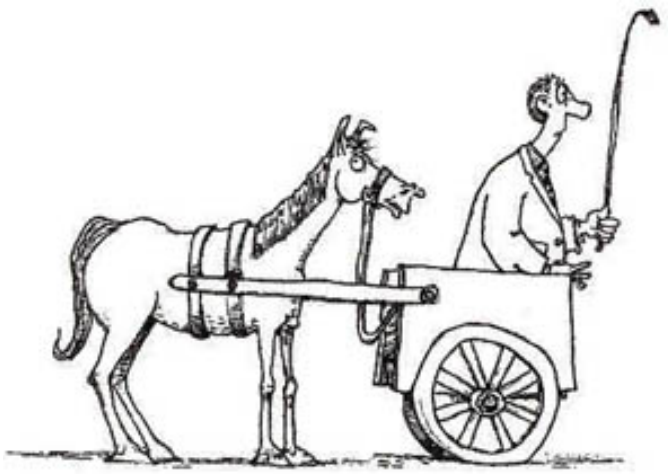
Admin

- Midterm Test 2 will be held on Friday, November 17.
- Assignment 4 is due on Friday, November 17.
- Office hours: To see me please send me a note with times.
- Are there any questions?

Advice

- Learn from your mistakes!
  - Failure offers much greater opportunity for growth and development than success — provided you do not lose confidence in yourself.
  - Review the midterm solutions and explanations.
- Put education first, marks second!
  - Your education is far more important than your marks.
  - Good marks naturally follow a serious pursuit of education.
  - After your first or second real-world job, marks will no longer have any importance in your career, but your level of education will remain crucial throughout your entire career.

Don't Put the Cart before the Horse!



Education delivers marks, but marks do not deliver education.

Review

1. Example of retrieving Beowulf from a web server.
2. Discussion on why the Web has been so successful.

The Information Age

- Information drives commerce and culture.
- Made possible by modern computing and communication technology.
- Key infrastructure: Internet.

The New Information World [1/3]

- World Wide Web.
  - The Web has become a universal library.
  - Essentially all new public information is put on the Web.
  - There are several projects to put vast amounts of old information on the Web.
- Commerce.
  - Information is now a major commodity.
  - Information systems are a major tool of commerce.
- Digital Property.
  - Much property is now digital.
  - Examples include books, articles, news, music, video, and software.
  - Digital property can be reproduced almost instantaneously at extremely low cost.

The New Information World [2/3]

- Information Ownership
  - Who should own intellectual and digital property?
  - Who should own the metadata about intellectual and digital property?
- Privacy.
  - Privacy is threatened by the new technology.
  - Example: Identity theft.
  - Encryption may enable some privacy to be preserved.
- Risks.
  - Much of the economy depends on computer networks and software.
  - Many systems of our economy are tied together.

The New Information World [3/3]

- Cybercrime.
  - Crime via the computer and communication networks is a new development of major concern.
  - Example: Original design of the Internet infrastructure is inadequate.
  - Crime can be perpetrated electronically from a distance.
  - National borders are no longer a major obstacle to crime.
- Information Warfare.
  - Warfare may now include attacks on information systems (possibly instead of on military resources).
  - Small countries and groups can attack large countries.

Information Security

- Concerned with the protection of:
  - Electronically stored and manipulated information.
  - The systems used to store and manipulate information.
- Growing, dynamic field.
  - Has major importance in the information age.
  - Network security is an important subfield.
- Closely related to the problem of software reliability.
  - Information systems and security mechanisms are heavily based on software.
  - Software is difficult to develop and maintain and very often unreliable.

Why is Information Security Unique?

- Concerned with misuse instead of proper use.
- Hard to engineer.
  - Involves most components of an information system.
  - Information security requirements clash with many other system requirements.
  - Cuts across component boundaries and levels of abstraction.
  - Hard to separate from other concerns.
- A system is only as secure as its weakest component!

Computer Hacking (iClicker)

Has anyone ever hacked into your computer?

A. No.
B. Yes, information on my computer was stolen.
C. Yes, information on my computer was modified.
D. Yes, I could not login to my computer.

What Needs to be Protected?

1. Data.
   - Confidentiality.
   - Integrity.
   - Availability.
2. Information systems.
   - System confidentiality.
   - System integrity.
   - Availability of services.
   - System resources (disk storage, CPU cycles, etc.).
   - Monitoring mechanisms.
   - Security mechanisms.
3. Your personal and organization's reputation.

Confidentiality

- Confidentiality (also called privacy) is the state in which information or resources are concealed.
- Confidentiality also applies to metadata about information and resources.
  - Examples include existence, location, protection, etc.
- Confidentiality is achieved by following the need to know principle, a special case of the principle of least privilege.
- Military interest in keeping information secret was the main driving force behind the development of mechanisms to achieve confidentiality in the years between World War II and the advent of the Internet.

Integrity

- Integrity is the state in which data or resources have not been accidently or maliciously modified or destroyed.
- Integrity also applies to metadata about information and resources.
  - Examples include origin, provenance, access history, etc.
- An integrity violation reduces the trustworthiness of the data or resources.
- There are two approaches to maintain integrity:
  - Prevention of unauthorized attempts to modify the data or resources.
  - Detection of integrity violations or unauthorized modifications.
- The banking industry has been a major player in the development of mechanisms to achieve integrity.

Availability

- Availability is the state in which information or resources can be used as needed.
- Availability is an important aspect of reliability.
- Denial of service attacks are attempts to block availability.
  - They are difficult to detect because they can look like legitimate, but possibly atypical, attempts to access information and resources.

Threats and Attacks

- A threat is a potential violation of confidentiality, integrity, or availability.
- An attack is an attempt to violate confidentiality, integrity, or availability.

Kinds of Threats

- System failure.
- System modification.
- Resource theft.
- Vandalism.
- System probing.
- Unauthorized access.
- Repudiation of origin.
- Denial of receipt.
- Delay.
- Denial of service.

Where do the Threats Come From?

- Faulty hardware.
- Faulty software.
- Configuration mistakes.
- Operational mistakes.
- Insiders.
- Hackers.
- Criminals, vandals, and terrorists.
- Malicious code (such as viruses).
- Natural disasters.

Kinds of Attacks

- Unauthorized system access.
  - To steal information.
  - To modify information.
- Denial of service attacks.
- Network probing.
- Network manipulation.
- Resourced theft.