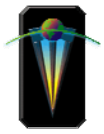
CSI 2911 School of Information Technology and Engineering,
Computer Science Program



Midterm EXAM
Mar. 2, 2011

NAME:……

STUDENT NO……

This is a closed book, closed laptop test. Time: 70 min.

Please answer the multiple choice questions 1-16 (marked MC in the exam) on the coding answer sheet provided. Answer questions 17-19 on this handout in the space supplied, and turn it in together with the coded sheet at the end of the test. Questions 1-16 are worth 0.5 points, question 17 and 18 are worth 1 point, question 19 is worth 5 points, the whole midterm is 15% of the course mark.

1. **(MC)** Moor's 3Rs of Computer Ethics are:

   - a) reason, relativity, reliability
   - b) reason, readability, relativity
   - → c) reason, relativity, responsibility
   - d) rationalism, relativity, responsibility

2. **(MC)** When I sign up for my bank's Electronic Banking, a menu asks me whether I want to receive a newsletter with announcements of new products. The "**yes**" answer is already checked, i.e. if I don't do anything I will receive the newsletter. Is this

   - a) opt-in
   - → b) opt-out
   - c) implied

3. **(MC)** An internet airline ticket purchase system service states that it will retain customers' credit card numbers indefinitely. Which PIPEDA principal is violated by this practice:

- a) Accountability
- b) Consent
- c) Safeguards
- d) Limiting use disclosure and retention

4. **(MC)** Which of the following IS NOT a rule of the CIPS Code of Ethics:

   - a) Demonstrate Competence and Quality of Service
   - b) Protect the Public Interest and Maintain Integrity
   - c) Uphold Responsibility of the IT Profession
   - d) Maintain Data Confidentiality at all times

5. **(MC)** Suppose you are a professional software developer in a company and your job is to test a new release of an elevator control software. The marketing arm of the company presses you to cut testing short so that the new release can beat the competition to the market. What will be your most appropriate action according to the 1990 Ontario Professional Engineer's Act:

   - a) to refuse, evoking the CIPS Code of Ethics
   - b) to comply but inform the media of this situation
   - c) to warn the employer of the consequences
   - d) None of the above

6. **(MC)** Relationship between security and privacy can be best described as:

   - a) there can be no security without privacy
   - b) there can be no privacy without security
   - c) security puts privacy at risk
   - d) privacy puts security at risk

7. **(MC)** According to Moor, computers are "**logically malleable**". This means that computer technology

   - a) depends on logic for its operation
   - b) applies to any process that has inputs, outputs, and connecting operation
   - c) implements logical operations in a physical medium
   - d) is able to modify information logically

8. **(MC)** Problems with the **Terac-25** radiation machine were due to

   - a) operator errors
   - b) software design errors
   - c) poor user interface design
   - d) all of the above

9. **(MC)** The Use Limitation principle (one of the OECD privacy guidelines) means that

- a) the group of people who have access to the collected information is limited
- b) the use of collected information is limited to the stated purpose
- c) there is a limitation on the time during which the collected information may be used

10. **(MC)** Which on of the following is a property of a P2P network

- a) In the network some nodes have special duties like service to others or control other network nodes
- b) Centralized control
- c) all of the above
- d) none of the above

11. **(MC)** Software freedom means

- a) The freedom to see the code and run the program
- b) The freedom to earn money from the software
- c) all of the above
- d) none of the above

12. **(MC)** In PIPEDA, the "identifiable information" means

- a) person's unique identifier, e.g. SIN or Student Number
- b) individual's name and address
- c) information in anonymized data that could be linked to individual
- d) a government assigned number e.g. Driver's License or OHIP number

13. **(MC)** What is the current situation regarding patenting algorithms in the US:

- a) they cannot be patented
- b) they can be patented
- c) the Supreme Court will decide the issue in 2011
- d) the Patent Office makes a decision for each case

14. **(MC)** The term **Copyleft** is

- a) the legal right of creative artists or publishers to control the use and reproduction of their original works
- b) offer the right to distribute copies and modified versions of a work and requiring that the same rights be preserved in modified versions of the work
- c) a set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work
- d) all of the above

15. **(MC)** In the PUNCHSCAN e-voting system discussed in class

- a) the voter can verify it their vote has been tallied correctly and CAN prove this to a third party
- b) the election officials can see how the voters vote and then they encode their vote
- c) the vote is encrypted and then all votes are decrypted for verification
- d) the voter can verify it their vote has been tallied correctly and CANNOT prove this to a third party

16. **(MC)** The <u>main</u> source of failure in the Stereotactic Surgery case discussed in class is attributed to

- a) software errors
- b) bad GUI design
- c) retrofitted nature of different components
- d) inability to apply different software updates

17. Give (a) the control definition of privacy and (b) the restricted access definition of privacy (Moor).
    a) we have control over information about ourselves

    b) we decide who has access to what information about ourselves and when

18. List Bynum's SEVEN levels (or types) of policies to guide one's professional conduct

international treaties and agreements,
laws,
regulations
standards of good practice,
professional codes of ethics,
corporate policies, community and
personal values

19. Case to Analyze: analyze the "Losing $100K - Fossbakk" case as presented and discussed in class (see below for a summary of this case). Specifically address the following IN THE SPACE PROVIDED. Point format answers are welcome.

a. . What are the ethical issues; what is your opinion about this case?

E.g. is it correct for a rich bank to take financial advantage of a mistake of an older person, who is obviously not well versed with technology?

b. Perform a **"roles and responsibilities analysis"**

Ms. Fossbakk – bank client, is responsible for entering her information correctly
The bank is responsible for the integrity of the transactions
For using the best and TESTED technology
The thief is responsible for taking the funds and spending them
Banking system's GUI designers are responsible for providing a robust interface

c. Perform a **“stakeholder analysis”**

Ms. Fossbakk stands to lose her life savings
The bank stands to lose reputation
The bank’s systems designers have their professional credibility at stake
The thief gets a prison sentence
The banking public stands to gain from a better system
The minister gains politically as protector of the “underdog”
….

d. Draw some key ethical conclusions

responsibility of the bank cannot be strictly limited to its legal obligations

e. Draw some **lessons** for the future

better user experience testing needed
better analysis of “what if” user errors needed
bank must be more sensitive to clients with limited computer experience
bank could provide training (eg on-line) for such users

….

The Fossbakk case: An ordinary bank customer, Grete Fossbakk, used Internet banking to transfer a large amount to her daughter. She keyed one digit too many into the account number field,
however, inadvertently sending the money to an unknown person. This individual managed to gamble away much of the sum before police confiscated
the remainder. Subsequently, the case received extensive media coverage in Norway. The Minister of Finance criticized the bank's user interface and requested new and improved Internet banking regulations. Suddenly, the risk to Internet banking had become apparent to both the government and ordinary citizens. Clearly, the user made a slip. She also had the chance to correct the typo before she hit the confirm button.
However, as we shall see, the system also had every opportunity to catch her mistake. Yet this did not happen. The system's developers had neglected to build in a simple check
that would detect if the correct input were missing.

Fossbakk's daughter's account number w as 71581555022, but she inserted an extra 5 and keyed in 715815555022. The user interface accepted only 11 digits in this field (the standard length of a Norwegian account number), thus truncating the number to 71581555502. The last digit is a checksum based on a modulo-11 formula. This will detect all single keying errors and errors where two consecutive digits are interchanged. Inserting an extra 5 changed both the ninth and tenth digits.
The average checksum control will catch only 93 percent of the cases in which such errors occur. For Fossbakk, the final eleven-digit number was a legal account number.
However, only a small fraction of all legal account numbers are in use. Further, the chance of mistyping the account number so that it benefits a dishonest person without income or assets is overwhelmingly low in a homogeneous country such as Norway. Our user was thus extremely unlucky. The person who received her $100,000 transaction and kept the proceeds has been sentenced to prison, but this does little to help Ms. Fossbakk get her money back.