Computer Science 3IS3 Midterm Test 1
SOLUTIONS

Day Class — Dr. F. Franek

DURATION : 50 minutes
McMaster University Midterm Test (CAS) — October, 2008

Please CLEARLY print:

NAME:

Student ID: | | | | | | | |

question	mark	out of
1-10		20
11 (bonus)		4
12		3
total		23

This test paper includes 9 pages and 10 multiple-choice questions and 2 written questions. You are responsible for ensuring that your copy of the paper is complete. Bring any discrepancy to the attention of your invigilator.

Special Instructions :

1. The multiple-choice questions of this test must be answered on the McMaster standard OMR answer sheet (bubble form). The forms will be evaluated using McMaster optical scanner (OMR). The OMR instructions are on the next page.
2. The written questions must be answered in the space provided in this questionnaire.
3. Documents to be returned: this questionnaire, the OMR answer sheet, and all scrap paper if used. All of these documents must bear your name and student number. Only the face page of the questionnaire need to bear your name and student number, and all the loose pages of the questionnaire, if any.
4. No memory aids or textbooks of any kind are allowed during the test.
5. No calculators, pocket computers, or PDA's are to be utilized.
6. No unauthorized scrap paper, crib sheets etc. are allowed to be used. The invigilator(s) will supply you with needed scrap paper when you ask.
7. You are not allowed to be involved in any communication of any kind concerning the questions and answers of this test with anybody except the invigilator(s) or the instructor. Any attempt of such communication will be considered a case of academic dishonesty.

continued on next page

OMR EXAMINATION - STUDENT INSTRUCTIONS

NOTE: IT IS YOUR RESPONSIBILITY TO ENSURE THAT THE ANSWER SHEET IS PROPERLY COMPLETED: YOUR EXAMINATION RESULT DEPENDS UPON PROPER ATTENTION TO THESE INSTRUCTIONS.

The scanner, which reads the sheets, senses the shaded areas by their non-reflection of light. A heavy mark must be made, completely filling the circular bubble, with an HB pencil. Marks made with a pen or felt-tip marker will **NOT** be sensed. Erasures must be thorough or the scanner may still sense a mark. Do **NOT** use correction fluid on the sheets. Do **NOT** put any unnecessary marks or writing on the sheets.

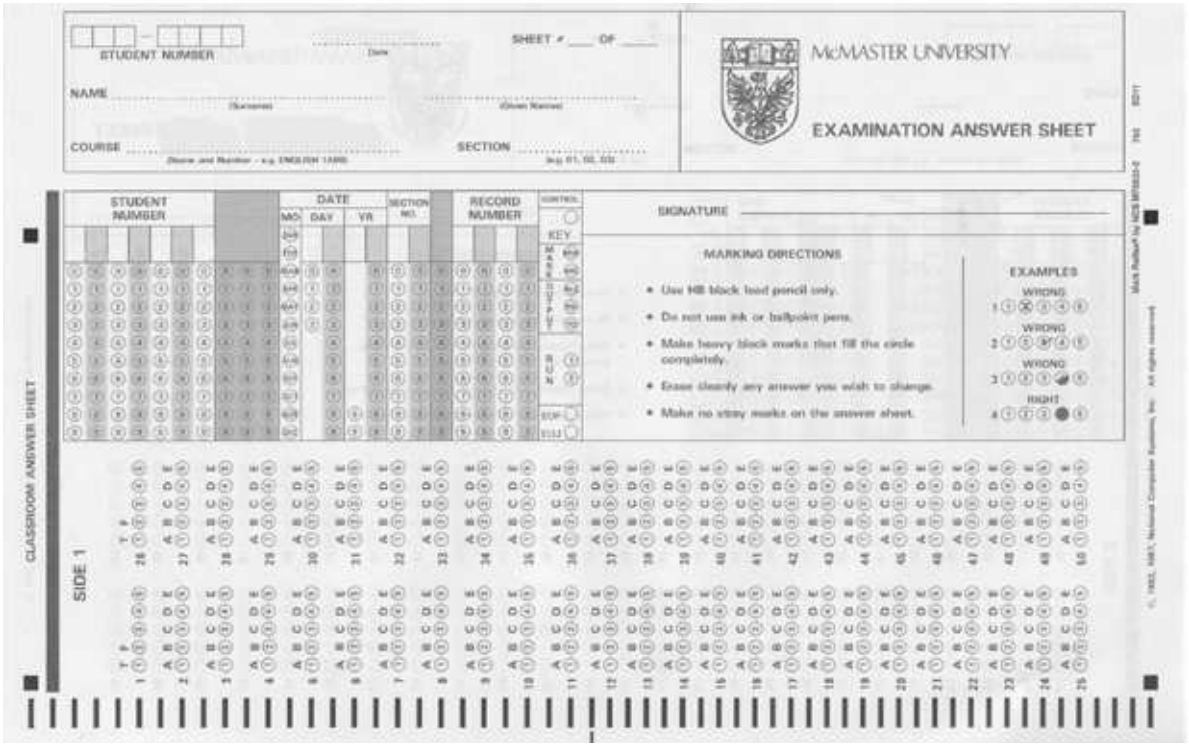
1. Print your name, student number, course name, section number and the date in the space provided at the top of Side 1 (red side) of the form. Then the sheet **MUST** be signed in the space marked SIGNATURE.

2. Mark your student number in the space provided on the sheet on Side 1 and fill in the corresponding bubbles underneath.

3. Mark only **ONE** choice from the alternatives (1,2,3,4,5, or A,B,C,D,E) provided for each question. If there is a True/False question, enter response 1 (or A) as True, and 2 (or B) as False. The question number is to the left of the bubbles. Make sure that the number of the question on the scan sheet is the same as the question number on the examination paper.

4. Pay particular attention to the Marking Directions on the form.

5. Begin answering questions using the first set of bubbles, marked "1".



A picture of the answer sheet

continued on next page

Questions 1 – 10 are multiple-choice questions and are to be marked on the McMaster standard OMR answer sheet (see the instruction above). For each question, always select only one answer, even if you think that there are more correct answers than one. Strive for the most appropriate answer. There always is at least one correct and most-appropriate answer for each question. In the case that there are more correct and most-appropriate answers, selecting one of them will earn you the full credit. For some questions, partial credit may be awarded for an almost correct answer. The negative marking is not used, i.e. incorrect or missing or multiple answers earn 0 mark.

Question 1 [2 marks] We are discussing ACS (access control system) with ACM (access control matrix) a. We are assuming that our access control system has the six primitive operations (create subject, create object, enter r into $a[s, o]$, delete r from $a[s, o]$, destroy subject, delete object).
Consider a set of rights $\{read, write, execute, modify, own\}$. We want to create a multi-operational command $delete\_all\_rights(p, q, s)$ that causes the subject p to delete all rights the subject q has over an object s.
Which of the three commands below is correct?

C1: **command** $delete\_all\_rights(p, q, s)$
  for all r **in** $a[q, s]$
    delete r **from** $a[q, s]$
  end

C2: **command** $delete\_all\_rights(p, q, s)$
  if $read$ **in** $a[q, s]$ **then delete** $read$ **from** $a[q, s]$
  if $write$ **in** $a[q, s]$ **then delete** $write$ **from** $a[q, s]$
  if $execute$ **in** $a[q, s]$ **then delete** $execute$ **from** $a[q, s]$
  if $modify$ **in** $a[q, s]$ **then delete** $modify$ **from** $a[q, s]$
  if own **in** $a[q, s]$ **then delete** own **from** $a[q, s]$
  end

C3: **command** $delete\_all\_rights(p, q, s)$
  if $modify$ **in** $a[p, q]$ **then**
    if $read$ **in** $a[q, s]$ **then delete** $read$ **from** $a[q, s]$
    if $write$ **in** $a[q, s]$ **then delete** $write$ **from** $a[q, s]$
    if $execute$ **in** $a[q, s]$ **then delete** $execute$ **from** $a[q, s]$
    if $modify$ **in** $a[q, s]$ **then delete** $modify$ **from** $a[q, s]$
    if own **in** $a[q, s]$ **then delete** own **from** $a[q, s]$
  end

A. Only C1 is correct.
$\Longrightarrow$B. Only C2 is correct.
C. Only C3 is correct.
D. The are all correct.
E. None is correct.

continued on next page

Explanation:
There is not basic operation **for all**, so C1 is wrong. C2 is correct. C3 is not correct, as the specification of the command $delete\_all\_rights(p, q, s)$ does not stipulate any relation of p to q, hence C3 is wrong. Thus B is the correct answer.

Question 2 [2 marks] Consider an abstract simple ACS. What is a proper definition of a "leaked right"?

A. A generic right r is leaked if it is added to the contents of an ACM cell.

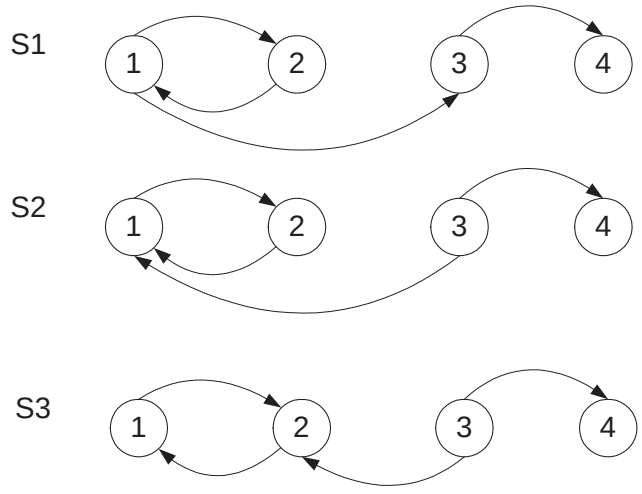
$\Longrightarrow$B. A generic right r is leaked if it is added to the contents of an ACM cell that does not already contain it.

C. A generic right is leaked if it is added to the contents of an ACM cell by a mono-operational command.

D. A generic right is leaked if it is added to the contents of an ACM cell by a multi-operational command.

E. None of the above.

Question 3 [2 marks] Consider the following three state diagrams of systems. In all three cases, states 1 and 2 are secure, while states 3 and 4 are not. Which of the three systems is secure? The initial state is 1.



A. Only S1 is secure.

B. Only S2 is secure.

C. Only S3 is secure.

D. All three are secure.

$\Longrightarrow$E. None of the above.

continued on next page

Explanation:

The sentence "The initial state is 1" was added during the test as a correction. Answer E was changed from "None is secure" to "None of the above" during the test as a correction.

S2 and S3 are both secure while S1 is not, hence E is the correct answer.

Question 4 [2 marks] What does the term "confidentiality policy" mean?

A. It means a policy concerned with the protection of the information flow, i.e. the protection against an illicit transmission of information.
B. It means a policy concerned with the protection against the leakage of rights.
$\Longrightarrow$C. It means a policy concerned with both, the protection of the information flow and against the leakage of rights.
D. All of the above.
E. None of the above.

Explanation:
There is a partial mark for A and B. The correct answer is C.

Question 5 [2 marks] What does the BASIC SECURITY THEOREM state? We are considering the Bell-LaPadula model for this question.

A. A system with an initial secure state a σ_0 and safe system of transactions, will not enter an unsecure state.
B. A system with an initial secure state a σ_0 and system of transactions T such that every transaction preserves the simple security condition, will not enter an unsecure state.
C. A system with an initial secure state a σ_0 and system of transactions T such that every transaction preserves the *-property, will not enter an unsecure state.
$\Longrightarrow$D. A system with an initial secure state a σ_0 and system of transactions T such that every transaction preserves the simple security condition and the *-property, will not enter an unsecure state.
E. None of the above.

Explanation:
There are partial marks for B and C as D is the correct answer.

Question 6 [2 marks] Consider the Bell-LaPadula model.
There are 5 clearance levels, C1 is the lowest and C5 is the highest. There are 4 categories, P1, P2, P3, and P4.
Alice is cleared into (C3,{P1,P2}) level, while Bob is cleared into (C4,{P2,P3}) level.

A. Bob's security level dominates Alice's.
$\Longrightarrow$B. Bob's security level does not dominate Alice's.

continued on next page

C. We cannot decide between A and B, because Bob's and Alice's levels are not comparable.
D. Bob's security level dominates Alice's for category P2.
E. Alice's security level dominates Bob's for category P1.

Question 7 [2 marks] Security labels in the Bell-LaPadula model primarily inhibit information flow, while integrity labels in Biba's model primarily inhibit the modification of information. Imagine that we implement both systems and make the integrity levels and integrity categories and security levels and the security categories the same. Under what conditions could a subject read an object?

A. No subject could read any object.
B. Any subject could read any object.
$\Longrightarrow$C. A subject can read only objects on the same level and with the same categories.
D. A subject can read only objects on the same level, regardless of categories.
E. None of the above.

Explanation:
Bell-LaPadula requires for reading that $l(s) \geq l(o)$. Biba requires for reading that $i(s) \leq i(o)$. Since in our model $l(s) = i(s)$ and $l(o) = i(o)$ it follows that $i(s) = l(s) = i(o) = l(o)$. Thus C is the correct answer.

Question 8 [2 marks] What is the mutual relationship of Biba's and Clark-Wilson models.

A. Biba's model can be emulated in Clark-Wilson, and vice versa.
$\Longrightarrow$B. Biba's model can be emulated in Clark-Wilson, but not the other way around.
C. Clark-Wilson model can be emulated in Biba's model, but not the other way around.
D. Neither model can be emulated in the other one.

Explanation:
The Biba's model has no certification rules, so it cannot emulate Clark-Wilson. However, Clark-Wilson can emulate Biba's. Hence B is correct.

Question 9 [2 marks] Consider the rule ER4 of the Clark-Wilson model: *Only the certifier of a TP may change the list of entities associated with that TP. No certifier of a TP, or of an entity associated with that TP, may ever have execute permission with respect to that entity.*

A. This rule is about transaction integrity.
$\Longrightarrow$B. This rule is about separation of duty.
C. This is one of the certification rules.
D. All of the above.
E. None of the above.

Question 10 [2 marks] A software keylogger is a program

continued on next page

A. that logs keys used for Internet encryption (PGP).
B. that logs keys used for Internet encryption (PGP) and transmits them once a while to an outside site.
C. that logs keystrokes, mouse events, and clipboard contents.
$\Longrightarrow$D. that logs keystrokes, mouse events, and clipboard contents, and transmits them once a while to an outside site.
E. None of the above.

Explanation:
C is partially true, so a partial credit, D is correct.

continued on next page

Questions 11 and 12 are questions that require a written answer. The answers are to be provided in this questionnaire in the given space.

Question 11 [4 marks] Is it decidable whether a given access control system (also called a protection system in the textbook) is safe for a given generic right r? ("safe" means that the right r does not ever leak)?
Give an answer and a sketch of a proof for your answer.

During the test this question was changed to a bonus.

A sample solution: In general, it is not decidable.

Sketch of the proof:
We are assuming that it is decidable and argue by contradiction.

Take a TM (Turing machine) $\mathcal{T} =< \delta, K, M >$, K is the set of the states, M is the alphabet, $\delta : K \times M \to K \times M \times \{L, R\}$ is the transition function, and $q_{fin} \in M$ be a final state.

We must translate $\mathcal{T}$ to an ACS (access control system) $\mathcal{A}$:
The subjects of $\mathcal{A}$ will be the cells of the tape of $\mathcal{T}$: if $\{s_i; 1 \leq i \leq k\}$ are all the cells visisted by the head of $\mathcal{T}$ up to this moment, then s_i has right *own* w.r.t. s_{i+1} for $1 \leq i < k$ (i.e. the right *own* is used to keep linear ordering of the subjects and so "emulate" the tape), the righmost cell visited (s_k at this moment) has right *end* w.r.t. itself.
Moreover the states (elements of K) and the alphabet symbols (elements of M) are generic rights.

- if the head is in cell $s_i (1 < i \leq k)$ and $\delta(p, A) = (q, B, L)$, then
  command $c_{p,A}(s_i, s_{i-1})$
  if *own* **in** $a[s_{i-1}, s_i]$ **and**
  p **in** $a[s_i, s_i]$ **and**
  A **in** $a[s_i, s_i]$
  then
  delete p **from** $a[s_i, s_i]$
  delete A **from** $a[s_i, s_i]$
  enter B into $a[s_i, s_i]$
  enter q into $a[s_{i-1}, s_{i-1}]$
  end
- if the head is in cell $s_i (1 \leq i < k)$ and $\delta(p, A) = (q, B, R)$, then
  command $c_{p,A}(s_i, s_{i+1})$
  if *own* **in** $a[s_i, s_{i+1}]$ **and**
  p **in** $a[s_i, s_i]$ **and**
  A **in** $a[s_i, s_i]$
  then
  delete p **from** $a[s_i, s_i]$
  delete A **from** $a[s_i, s_i]$
  enter B into $a[s_i, s_i]$

continued on next page

enter q into $a[s_{i+1}, s_{i+1}]$
end

- if the head is in cell s_k and $\delta(p, A) = (q, B, R)$, then
  command $c_{p,A}(s_k, s_{k+1})$
  if *end* **in** $a[s_k, s_k]$ **and**
  p **in** $a[s_k, s_k]$ **and**
  A **in** $a[s_k, s_k]$
  then
  delete *end* **from** $a[s_k, s_k]$
  create subject s_{k+1}
  enter *own* **into** $a[s_k, s_{k+1}]$
  enter *end* **into** $a[s_{k+1}, s_{k+1}]$
  delete p **from** $a[s_k, s_k]$
  delete A **from** $a[s_k, s_k]$
  enter B into $a[s_k, s_k]$
  enter q into $a[s_{k+1}, s_{k+1}]$
  end

The right q_{fin} leaks if $\mathcal{T}$ enters the state q_{fin}. We started with an assupmation that the leaking of a generic right for an ACS is decidable, so it must be decidable if q_{fin} leakes in $\mathcal{A}$, hence it must be decidable if $\mathcal{T}$ halts (reaches state q_{fin}). Thus we have proven that the halting problem for any TM is decidable, a contradiction.

Question 12 [3 marks] Consider the UNIX file system. Classify its access control as either MAC (mandatory access control), DAC (discretionary access control), or OAC (originator controlled access), or combination of thereof. Justify your answer.

A sample solution:
It is a combination of DAC and OAC:
DAC: since the creator of a file (or the superuser) determines the access based on the identity of the subjects - (owner, a member of the group, or other).
OAC: since the creator of a file determines the access for all other subjects (except the superuser).

THE END.