THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2004
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: TWO hours)

COMPSCI 725 students were allowed 20 minutes to complete this sample exam. The questions are in **boldface type**, *sample student answers are in* roman type, *and the instructor's assessment and comments are in italic type.*

NOTE: Attempt **ALL** questions in the 12-page script book provided, using approximately **25** words to answer each 5-mark question, **50** words to answer each 10-mark question, and approximately **75** words to answer each 15-mark question. Total possible: **100 marks.**

There are three security goals in the common "CIA" taxonomy: Confidentiality, Integrity, Availability. Some authors, including Butler Lampson in his article "Computer Security in the Real World", include a fourth goal of "Accountability".

1. **Give a brief definition of Accountability. [5 marks]**

According to Butler Lampson, in his article "Computer Security in the Real World", he defined accountability as knowing the required information from the given or specific resources.

1/5: Too vague. I'm not convinced this student read the Lampson article.

Accountability is the notion of a system having to provide precise information of its previous states at a later point in time.

2/5: This is a good definition of auditing. There's no mention of user accountability, and I can't be sure of what is meant by "precise information".

Anybody who gets into the system should be recorded, and he is responsible for what he did.

5/5: Excellent. Note that I am not considering a student's grammar or elegance of expression when I assign marks to their answer. Indeed I would greatly prefer to see a definition "in your own words" because I am not interested to know whether you have memorized definitions. In any event, this is not a very representative question for my final exams. There will be few, if any, questions on the actual final exam which could be answered adequately by a direct quotation from the required readings. So please do not think you must memorize the wording of definitions. Your understanding of these definitions is what is important!

2. **Name any system or application area that was described in any required reading for COMPSCI 725 this term, and briefly describe an accountability goal that is appropriate for this system. [5 marks]**

Take the PKI system as an example. One of its accountability goals is to recognize the person who response to a single key.

0/5: I don't understand what is meant by "response to a single key". This student should use standard security terminology when responding to exam questions. They should also include more information in their discussion, so that I can be reasonably sure they are making a relevant point. PKI is not a recognition technology. It is an authentication technology, so the word "recognize" seems irrelevant here.

In IDS (Intrusion Detection System, Auditting is an essential part for tracking what has gone wrong and what is going wrong. In "Computer Security in the Real World", Accoutability [sic] spots where the comfidentiality [sic], Integity [sic], Availability have been compromised.

1/5: This student has misspelled several basic terms in security. Their first sentence discusses auditing (the keeping of records), not accountability (holding someone responsible for their actions). In their second sentence, they have not supplied any specific information about their IDS example, leaving me quite uncertain that they actually have an accountability goal in mind. However, their answer to Q1 convinced me that they have some understanding of the relationship between auditing and accountability. In response to that question they wrote "Accountability is to hold someone responsible for something he has done to the system so that he cannot falsely deny his action. Accountability can be implemented by auditting." I would give 5/5 to their Q1 answer, even though it included some irrelevant (and not quite accurate) detail. To hold someone accountable, we need more than just an audit record! We also must be able to connect a user with their audit record. At page 40, Lampson describes the "gold standard" for security implementations: we need some method to ***au****thenticate the principals, some means of* ***au****thorizing access, and (as pointed out by this student) we need to keep* ***au****dit records. Their total 6/10 mark for these two questions seems appropriate to me, although I might easily have given 7/10 if I were convinced they knew what an IDS was – for example by discussing a more specific accountability goal, or by discussing their goal using some specifics from their IDS example. One way to determine whether they have not included enough specifics is to substitute the name of any other security system for the "IDS" in their answer. Note that "voting system" or any other system would make just as much sense in the context of their answer, so they really haven't given me any IDS-specific information.*

In the software companies, sometimes they want to keep track of the distribution of their softwares. Together with the idea of protecting the users from illegally copying their software, the watermarking is used.

One kind of watermarking is to have a different watermark for each copy of the software, so that a company can know that who is responsible for any illegal operation that might occur on the particular copy.

4/5: This answer would be fine if it had named a system. Also, there is too much detail about one detail (watermarking) of an implementation. The 25-word answer should name a system and discuss an accountability goal. The implementation is largely irrelevant. However because the detail is not incorrect, and is not completely irrelevant, I am not deducting a second mark for this defect.

3. **For the same system or application you used as an example in question 2, briefly describe an appropriate confidentiality goal. [5 marks]**

In PKI, when message send between users they have encrypt the message. So that when someone in between intercept the message he/she still can't figure out what is the meaning of that "encrypted message".

4/5: This student has confused an application of PKI (secure messaging) with PKI itself. However in all other respects this answer is fine.

WindowXP. The confidentiality goal is that the system or private files must be kept confidential so that any third parties would not be able to get access to these files.

4/5: This goal has a subtle error, in my opinion. I don't think Windows XP security relies on third parties being unable to read system files. Write-access (integrity) for system files is, I think, much more important for system security than any form of confidentiality except controlling execution rights. The control of execution rights to a file is not about keeping third parties (as security principals) from reading the file, instead it is a matter of keeping the file inaccessible ("confidential") from the CPU's execution pipeline except when the CPU process (as a security principal) is properly authenticated to execute that file. This grade of 4/5 is somewhat harsh but I'd expect this student to do quite well on the rest of the examination, as this is a rather subtle error.

[In DRM] however, the user loose [sic] their confidentiality if the content owner record their action. Because the users are reluctant to let others know what they are interested in.

5/5: Very nice! The student has described a goal, and argued for its appropriateness. I don't care about the misspelling of the non-technical word "lose" in an examination. (Note: MSc theses at our institution are expected to be more or less free of such errors, however other people can – and should – be asked to proofread your thesis. You can't ask someone to proofread your examination script! ;-)

4. Sometimes accountability comes into conflict with confidentiality. Analyse your two goals fromr questions 2 and 3, in the context of your chosen system or application, for any conflict that would make it impossible for any implementation to completely achieve both goals (at least in some situations). [5 marks]

Since accountability deals with making information available while confidentiality deals with keeping it private, they might sometimes be conflicting. Using my University example from above [of controlling access to my portion of a filesystem] the two goals are not mutually exclusive.

1/5: No specific situation has been analyzed for a conflicting requirement, and no other argument has been supplied for it being impossible to meet both goals. The student has only argued that the goals "might sometimes be conflicting".

In this example [Windows product activation], accountability is in conflict with confidentiality. User has to remain as much as possible anonymous, while at the same time he has to be taken accountable for his actions (in this case, product activation). It is impossible to have user completely anonymous and yet accountable for his actions.

5/5: Excellent. This student has shown a clear conflict between confidentiality and accountability, in a specific setting. Their answer is somewhat overlong, but it is somewhat repetitious so it's not as though the student is "packing it full" of extraneous information. A minor revision by a competent technical editor could cut it down to the 25-word suggested length.