THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2006
Campus: City

COMPUTER SCIENCE
Software Security
(Time allowed: TWO hours)

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.**

Sample answers are written in boldface italic. *Instructor's comments are written in italic.*

A. Briefly explain how each of the biometric functionalities identified by Jain et al. might be used at an automatic teller machine (ATM) that is equipped with a video camera. The primary security goal is to prevent insiders from making unauthorised withdrawals from customer accounts, using a fraudulently obtained ATM card and PIN number.

1. Identification **(5 marks)**

Everybody have *[sic]* ***their unique biometric indentifican*** *[sic]* ***such as fingerprint. So it is possible to use the biometric to identify the customer when they are using*** *[an]* ***ATM.***

[2/5] A weak answer. The student has shown some ability to use the terminology of biometrics as defined in Jain's article. However this student has not demonstrated any knowledge of biometrics beyond the definitions of the terms. Although everyone has a unique biometric, we cannot jump to the conclusion that any single biometric measurement (such as a scan of a fingerprint) would accurately identify an individual in a large population. I think it is reasonable to assume that accuracy of identification would be important at an ATM, but I have no way of knowing whether the student has considered this as a design constraint. Even with these weaknesses I had considered awarding 3/5 marks, but the careless misspelling of the technical word "identification" tipped the scales toward a marginally non-passing mark.

The biometric functionalities that can be used are finger print, iris scan, voice recognition. If required some of the functionalities can be combined together. The biometric trait of the customer is obtained.

[0/5] A very weak answer. This student knows the names of some biometric technologies, but incorrectly guesses that these are what Jain calls "functionalities". I suspect that this student is unable to distinguish between Jain's identification and verification functionalities. This suspicion persists after reading their answers to questions 2, 3, and 4. Because the student has not convinced me that they understand the question, a mark of 0/5 seems most appropriate.

A fingerprint reader is used to match the users *[sic]* ***print with a print from a database in order to obtain an identity.***

[5/5] An excellent answer. In just a few words, this student has sketched a plausible design for an ATM that uses a biometric measurement to identify a customer. I'm disappointed (and a bit surprised) that they have chosen to ignore the video camera as a possible biometric input device,

but because they have specified the use of a fingerprint reader they do have a feasible design. If the fingerprint reader had not been specified, I would have awarded only 3/5 marks, for it would be a major error to assume that a typical video camera can be used to scan a fingerprint.

2. Verification **(5 marks)**

The person whos *[sic]* ***account is being used should have their identity verified using the*** *[sic]* ***facial recognition. The authorised user of the card should have the same identity as the person trying to withdraw money.***

[5/5] An excellent answer, convincing me that the student understands the functionality of verification and how it could be applied in the given situation. Note that I do not mark down for grammatical or spelling mistakes unless a technical term is misspelled, or the meaning is obscure.

Verification needs a large amount of database to be stored at one point but quite secured if the biometric prints of the persons are stored. This way is secured & can stop from being attacked easily. The authorised person trying to access his account can be authenticated by putting biometric prints on the display screen of ATM.

[0/5] A very weak answer. The student has not addressed all of the elements of this 5-mark question, even after using more than 50 words. (Note: I don't count words carefully, but in general it seems that significantly overlong answers are a symptom of muddled thinking; they rarely get full marks.) I am left with several questions after reading this response. I wonder why this student thinks that a typical user of an ATM will be able to verify their own fingerprint if it is displayed on the screen of the ATM. What purpose could be served by such a verification, anyway? How could this verification possibly address the stated security goal of preventing insiders from making unauthorised withdrawals? This answer does not show any understanding of either biometrics or security analysis. Of course anyone can write a muddled answer on an exam, and this is only a 5-point question. Quite possibly this student will obtain a good grade on the exam by answering other questions more carefully and correctly.

3. Screening **(5 marks)**

After a customer has been authenticated (by ATM card followed by PIN), screening should be possible without further confirmation of identity. Biometric features may be required if screening was done on the basis of that trait (I cannot imagine why, however).

[0/5] A very weak answer. It seems quite possible that the student actually does understand the functionalitiy of screening, and how it might be useful in the given situation, but this answer does not demonstrate any of this understanding. (Please note that I will be reading your answer to try to determine if you understand the words you are using. In this case we could have substituted any biometric functionality for the word "screening" in these sentences without affecting their validity.)

Capture the user's face and physical description using the video camera during the withdrawal transaction and assign that video recording to the occurred *[sic]* ***transaction, so it can be viewed later exactly who was making the withdrawal.***

[2/5] A weak answer. The student has sketched how an ATM system might maintain an audit record that could be used to support the identification and verification (authentication) functionalities. However they do not seem to recall Jain's discussion of screening. This is a fairly

CONTINUED

difficult question, because Jain does not emphasise screening in his article, and this functionality was not emphasised in any of the student presentations. I am more generous in awarding partial credit on difficult questions. If a question requires knowledge of a basic term in security, and an answer seems to betray a student's ignorance of this term, I would be likely to award zero marks.

Sometimes we have such question like "Is this person wanted on the screen". Airport security staff may encounter such question.

[3/5] A barely adequate answer to a difficult question. This student clearly recalls Jain's definition of screening, and can express this understanding cogently in their own words. However they have not been able to apply it to the security goal at hand.

If the person is not identified as a customer, is the person one of the employee? A match is then attempted to be made with the list of employee images on file in the computer database.

[5/5] A good answer to a difficult question.

4. Of the three possible uses you explained above, which seems the most appropriate mitigation for the insider threat of unauthorised withdrawals? Explain briefly. To receive full credit, you should use Chinchani's methodology to describe how a biometric system could mitigate the insider threat. **(10 marks)**

The insiders may get ATM card and pin but not the biometric features of customer. The insiders cannot fake the customer even [though they] may have [accessed] the atm card and pin # of the customer [using their privilege] as bank staff.

[2/10] This student seems to think it is impossible for an insider to attack the biometric database, or to spoof the biometric reader. Jain discusses these attacks, and many others, in his article. I'm left with the impression that this student has not read Jain's article carefully, and they made no attempt to use Chinchani's methodology.

I think the most appropriate mitigation for insider threat of unauthorised withdrawals is identification. Face recognition algorithms might not [be] 100% correct and retrieve the feature might 100% meet as the the pervious *[sic]* ***supplied. The computer system only can tell how much confidence for feature just captured. To solve this problem ATM might collect multi-biometric feature of ownder when insider try to use fraud card in the ATM, such as fingerprint or Iris.***

[2/10] I had difficulty assigning an accurate mark to this answer, as I had difficulty understanding its line of argument. The student has focussed their answer on a shortcoming of biometrics in this application, rather than explaining why they think it would be more useful if it were used in the identification functionality than in the other functionalities. They made no attempt to draw a Chinchani diagram.I am left with the impression that this student understands something about multibiometric systems, and that they have not considered how unacceptable it would be if some users were unable to enrol successfully enough (even with many biometric choices) to get an accurate identification each time they used an ATM. Furthermore, using multiple biometrics would greatly increase system cost and complexity, so it would be completely unacceptable to a bank unless it also greatly mitigated the threat of insider fraud. Thus this is a weak answer at best.

To mitigate insider threat, once we have a picture of the imitating person, and once we determine that the person is not the true owner of the account, we can reverse engineer to see if

the person captured on the camera matches with any other picture stored in the database, i.e. does the imitating person have an account? If so, we can make a note of it and deny the transaction request.

[1/10] This is a very muddled description of a system, and no attempt was made to draw a Chinchani diagram. The term "reverse engineer" is misused. The term "screening" is never used. It is not at all clear how "we" can "determine that the person is not the true owner of the account", or when "we" would make this determination. Apparently this determination is made online, however, because the suggested reaction is to deny the transaction request – so this is actually a second authentication process (the first one being when "we" determined that the person is not the true owner) rather than a screening process (against a list of all employees or a more restricted list of employees that are being checked for possible insider fraud activity).

B. Butler Lampson, in his article "Computer Security in the Real World", identifies four goals of security: Secrecy, Integrity, Availability, and Accountability. He identifies three basic mechanisms for implementing security: Authentication, Authorisation, and Auditing. His five defensive strategies are isolate, exclude, restrict, recover, and punish.

5. Describe an *advantage* of using Microsoft's IRM v1.0 in New Zealand's e-government initiative, which was identified by Garden in one of your required readings. To receive full credit you must use Lampson's terminology for goals, mechanisms, and defensive strategies. **[5 marks]**

The advantage of IRM1.0 is the file owner can make file only be seen by the specified reader and to reach the goal of secure and integrity. The machine *[mechanism?]* ***was used authentication the reader by supplied user name and password. Also have to authorisate*** *[sic]* ***by IRM server, the priviledge*** *[sic]* ***to the file, the defensive strategies was use the exclude, restrict. Because someone have no priviledge can't see the file. The right of editing and redistributing was restricted.***

[1/5] The statement of the advantage is very unclear. I can understand a goal of "integrity" but not a goal of "secure and integrity", so I will ignore the "secure" part of the goal. A file that can "only be seen by the specified [authorised] reader" would support a goal of confidentiality, but not a goal of integrity. It seems possible that this student doesn't understand the distinction between integrity and confidentiality, and it also seems possible that they have written "secure" where they meant to write "confidentiality". Either way it is a major error. Another error in this answer is its lack of distinction between Lampson's strategies of "restrict" and "exclude".

For example, IRM can protect email only be read and write by authorised people. This can provide the secrecy and integrity. The Autor *[sic]* ***can authorise who can read or modify the email, and others have to be authenticated before they can read and modify the email. It use restrict strategies to defens*** *[sic]* ***unauthorised access.***

[4/5] Despite its spelling and grammatical mistakes, the answer is quite understandable and reasonably accurate to the first half of the question. It makes a reasonable guess as to what Lampson means by "restrict" but in fact Lampson's restriction strategy refers to a system that restricts the damage that can be done by an adversary during an attack. Lampson's "exclude" strategy is the one being used in IRM (or any access control system), but this is not very common terminology so I will deduct only one mark for its misuse. I'm a little disappointed that the student has identified what I would consider to be two advantages, but they have done an adequate job of arguing that IRM can promote both a goal of confidentiality and a goal of integrity. Generally,

when a student provides two answers (or if they provide a compound answer as in this case), I try to mark the stronger of the two answers, then I deduct points for any errors in the weaker answer. This results in full marks if both answers are correct, and it tends to penalise students who write two answers to a single question in the hope that one of their answers will be correct enough to receive some marks.

With IRM, we can meet the goals *[sic]* ***of secrecy, as without Authorisation, you will be exclude from read the files.***

[5/5] This is a very well-directed answer. In just 20 words, the student has included all the required elements.

6. Describe a *risk* of using Microsoft's IRM v1. 0 in New Zealand's e-government initiative, which was identified by Garden in one of your required readings. To receive full credit you must use Lampson's terminology for goals, mechanisms, and defensive strategies. **[5 marks]**

The tracking (or logging) system of the information uses or access *[accesses?]* ***is the weakness of MS IRM v1.0, so it becomes as a risk for secrecy. Therefore, it should introduce a robust auditing system to them and hence it can recover from information loss and enable to punish the crackers.***

[1/5] I can't quite understand the first sentence, but it seems the student believes that IRM logs all accesses or uses. After reviewing Garden's article and the student presentation on it, I don't find any support for this line of argument. The only mention of logging I can find in Garden's article is a figure in an appendix (at page 75), showing a screenshot of an administration window. It seems that some server-side logging function can be turned on or off by an administrator. I conclude that, if a governmental agency (or any other user of IRM) thought that the confidentiality risk of maintaining an audit log was greater than its benefit (e.g. for understanding patterns of use, and for investigating possible misuses), then they could disable the logging feature. In any event, Garden did not identify the existence of an audit log as a risk in his article.

The second sentence of this answer is even more obscure. Apparently the student believes that the introduction of an "auditing system" would mitigate the confidentiality risk of an audit log. I don't understand this proposal, so I cannot give it good marks.

One risk is the potential of losing access to files because the owner has left without first revoking restrictions. This damages the <u>availability</u> of the resource.

[5/5] An excellent answer.

C. (Other questions…). **[65 marks]**