THE UNIVERSITY OF AUCKLAND

SECOND SEMESTER, 2005
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.**

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.*

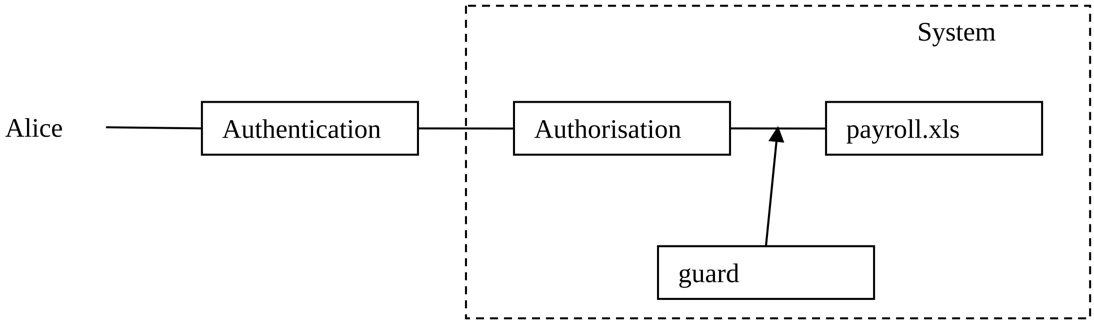
A. There are three security goals in the common "CIA" taxonomy: Confidentiality, Integrity, Availability. Some authors, including Butler Lampson in his article "Computer Security in the Real World", include a fourth goal of Accountability. Lampson identifies three basic mechanisms for implementing security: Authentication (of principals), Authorisation (of access), and Auditing (of the guard's decisions).

1. Draw a picture to illustrate the operation of the three basic security mechanisms in a computer system, when an end-user named Alice attempts to make a read-access to a file named "payroll.xls". To obtain full credit, your picture must clearly show the interactions between its elements, which must include the security mechanisms, Alice, the guard, and the file. Your picture must also have an appropriate caption of approximately 50 words, in which you very briefly explain each of its elements and their interactions. [10 marks]

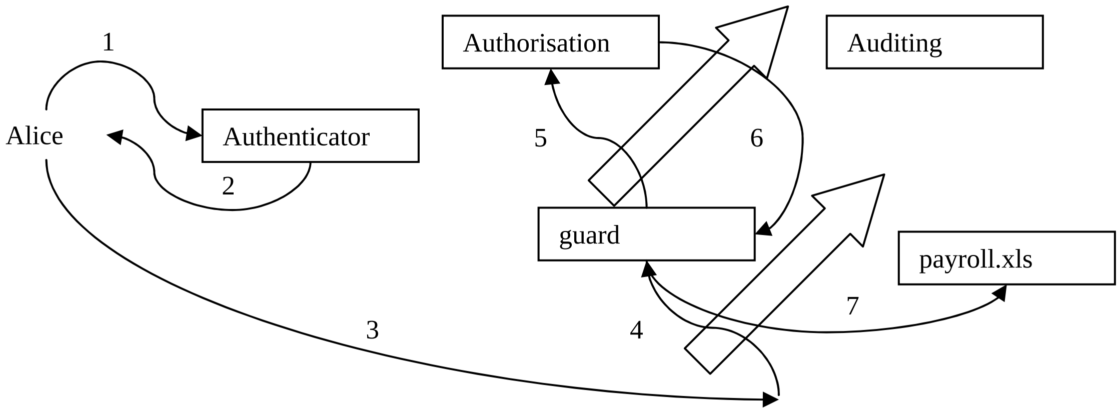
<u>Authentication:</u> to make sure you are "who you are". The purpose of Authentication is to use several ways (e.g. username, passwords, etc.) to identify a user.

<u>Authorisation:</u> to make sure "what you can do". The purpose of Authorisation is, after Authentication, the identity of a valid user has been proved, in this stage, the system need to know what operations of this particular [user] can be allowed. For example, a valid user may have right to access a file by read-only Authorisation, that means that user cannot modify or delete this file.

<u>Auditing:</u> this one works like a "double-check" or evaluation of how security system works.



5/10: The student shows understanding of authentication and authorisation in their definitions and diagram. Their definition of auditing does not indicate what is examined during an audit. Their picture does not show an auditing process. No caption is provided for the picture, and no explanation of what the guard is supposed to be doing.



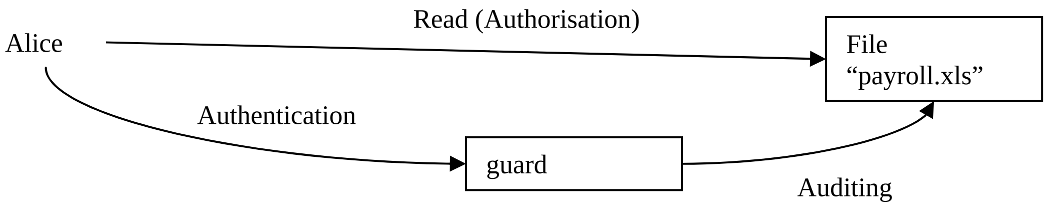
1. Alice tries to authenticate herself.
2. Authenticator gives back some kind of token (which can be passed to the guard).
3. Alice tries to access the payroll.xls.
4. The guard blocks here and checks whether she should have access.
5. – 6. The guard communicates with the authorisation server and checks if Alice has the permission to read the payroll.
7. If Alice has permission, she will have read-only access to the payroll. If not, she will be denied access by the guard.
8. An auditor can pick up the logs and perhaps can compare whether the guard relayed the "permission granted" or "denied" to Alice from the Authorisation server honestly.

10/10: The student shows excellent understanding of the situation, using all terms correctly. The diagram differs substantially from the one in Lamport. It doesn't clearly indicate that the guard is in charge of keeping the logbook, as in Lamport's diagram, but it does show an excellent understanding of how token-based authentication systems (e.g. Kerberos) operate. The student might believe that the main purpose of auditing is to check up on the guards, which would be incorrect in general; however this is a minor defect and no points were deducted.

Confidentiality: An unauthorised user can not read / secrecy.

Integrity: An authorised user can write.

Availability: An authorised user can read and write.



Alice should be authorised to this file. The guard has to decide whether Alice can read this file. Alice has to accept the principals in the security mechanism. Both of the conditions decide whether Alice can read the file.

3/10: This student shows understanding of authorisation and the role of the guard, but it seems unlikely that they understand either authentication or auditing. Neither their picture nor their caption use the term "auditing" correctly. They don't give any indication, in their caption, of what the guard might do to authenticate Alice. The student misuses the technical term "security principal", confusing it with "principle". The student included some extraneous information by defining confidentiality, integrity and availability; however no points were deducted for this.

2. **Consider the article by Crampton and Loizou entitled "Administrative Scope: A Foundation for Role-Based Administrative Models". Write a brief (25-word) synopsis of this paper. For full credit, your synopsis should indicate which *one* of the basic security goals or mechanisms is the primary focus of this article. [5 marks]**

(Only about 2/3 of the students answered this question.)

This paper is about the roles and defines a direction that allows us to define roles to certain groups of people. One security goal of the article is to define each role to a user of a certain trust band, and limit access to those roles accordingly.

1/5: The student discusses role-based authorisation but without using the term "authorisation". They don't show any evidence of having understood role-based administration.

The role-based administrative model is designed to distribute the authorisation (which include policy of what they can do to whom) to each group of users in the system.

2/5: The student discusses role-based authorisation. They don't show any evidence of having understood that Crampton and Loizou were proposing a way to allow users limited rights (based on their role) to adjust the authorisation policy on a system.

Administrative Scope tries to define the boundaries that each role in an administrative model has. The structure presented paper has shown a way to manage the right each player in the system has.

1/5: The student might understand that Crampton and Loizou were proposing a way to allow principals to administer an authorisation policy. However they might just be making reasonable guesses about what Crampton and Loizou were writing about, based on the title of their paper. The student hasn't defined what an administrative model is, and they haven't identified any of Lampson's security goals or mechanisms.

The primary focus of the Administrative Scope paper is to define a flexible hierarchy for determining permissions. So it provides a method for designating who should be responsible for assigning authorisations when two members of the hierarchy wish to share this.

5/5: This student has shown good understanding of the Crampton-Loizou paper, pointing out (correctly) that it allows flexibility in authorisation.

3. **Briefly describe how Administrative Scope (as described in the Crampton-Loizou article) could be constructively applied to the LOCK system (as described in the O'Brien-Rogers article); alternatively, briefly describe a fundamental conflict in these two approaches to computer security which would make it difficult – or even impossible – to use Administrative Scope in a LOCK system. The first part of your answer should be a very brief synopsis of the O'Brien-Rogers article. [5 marks]**

(Only a few students answered this question.)

2 and 3. I honestly have to admit that I haven't read any of these two articles. I assume the LOCK system emphasises confidentiality while Role Based Administrative Models emphasises more Integrity and Availability…

0/0: full marks for honesty, however LOCK ensures integrity as well as confidentiality, and Role Based Administration is about authorisation, not about integrity and availability. In any event, an unsupported guess won't get any credit.

The LOCK system is based in the UNIX platform. The LOCK system could be applied to the LOCK system by verifying if people are misusing the system. If they are, then their level of access into the system is either scaled down or removed entirely. A conflict in these two approaches arises when a user is scaled down by mistake. This person may have a certain amount of access but when they are mistakenly "locked out" of the system, the system has failed.

2/5: This student seems to have understood that the O'Brien-Rogers article described a security-enhanced variant of Unix. However they did not clearly relate it to the Crampton-Loizou article.

The LOCK system is a highly secure OS platform. Different roles have different levels of trust, however it is inevitable that failures in the role based system will occur, exposing features that otherwise should not be accessible to that role. Therefore this invites exploitation of the OS functions which a system like LOCK cannot afford.

5/5: This student clearly understands the LOCK system, and gives a plausible use for role-based adminstration of authorisation when responding to security breaches in a LOCK. Another acceptable answer would have pointed out the ongoing requirement (in most systems) to update roles and role definitions when systems and requirements are changed. Another approach to a full-credit answer would point out that one of the admitted defects of LOCK is that it is very difficult to design an appropriate set of authorisations. Thus it would seem difficult – and perhaps even infeasible –to design user roles in a LOCK system with enough flexibility that user authorisations can be adjusted by the Crampton-Loizou approach.

B. (Other questions…). **[80 marks]**