

A18866

Calculators may be used in this examination but must not be used to store text. Calculators with the ability to store text should have their memories deleted prior to the examination.

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Final Year – Degree of MEng with Honours
Computer Science/Software Engineering

Degree of MSc
Advanced Computer Science
Computer Security
Intelligent Systems Engineering
Internet Software Systems

Undergraduate Occasional
Computer Science/Software Engineering

06 17417

Computer Security

Summer Examinations 2009

Time Allowed: 1 ½ hours

[Answer THREE out of Four Questions]

[Answer THREE Questions]

1. Access control

- (a) In access control systems, what is a *capability*? [10%]
- (b) (i) Explain an advantage of access control lists over capability lists. [5%]
(ii) Explain an advantage of capability lists over access control lists. [5%]
- (c) A hospital patient record system provides login accounts for nurses. It is desired to implement the following policy:
- (i) When a nurse registers a new patient, the nurse is granted access to the patient's records for a period of 90 days.
- (ii) A nurse possessing the right to access a patient record can give that right to another user (this facilitates staff shift changes). This may be done offline.

To implement this policy, the system works as follows. When a nurse registers a new patient, a capability to access the patient record for the following 90 days is generated. The nurse stores it on a USB stick, and may copy it onto other USB sticks to give to other users. When a user attempts to access patient records, she is prompted to upload the relevant capability. The capability has the following format:

patient-id, issue-date, hmac(K, (patient-id, issue-date))

where $\text{hmac}(K, \dots)$ denotes a suitable keyed hash function with key K . The key K is a secret key known only to the patient record system. Any user in possession of this capability is able to access the records of the patient with patient-id, provided the date is within 90 days after issue-date.

- (i) Suppose nurse A registers a patient and receives such a capability. A passes it to B, B passes it to C, and C passes it to D. Is D able to use the capability? [4%]
- (ii) In order to stop long-lived capabilities being distributed widely, the hospital decides to adopt the policy that the nurse that initially registers the patient will have access to the records for 90 days, as before, but if she passes the capability to any other user, the validity should be 10 days from the issue date. Explain a new format for capabilities which would support this new policy. [10%]

2. Trusted computing

- (a) What is the purpose of a *platform configuration register* (PCR) in the TPM? [10%]
- (b) Explain how a PCR p is updated with new data d . [10%]
- (c) The command TPM_Seal is used to encrypt data and bind it to some PCR values. Suppose TPM_Seal is called with arguments including the usual arguments concerning keys and authorisation data, and also the PCR p and associated value v . The command runs successfully and returns a blob.
- (i) Explain the conditions under which the blob can later be decrypted. [7%]
- (ii) Explain a scenario in which TPM_Seal might be useful. [7%]

3. Electronic voting

(a) Explain the meaning of the following properties as used in the context of electronic voting systems.

- (i) individual voter verifiability [5%]
- (ii) vote-privacy [5%]

(b) For each of the following voting systems, does it provide individual voter verifiability? Does it provide vote privacy? Explain your answers.

(i) Ballot papers such as the ones shown below are distributed, and voters mark with an X their chosen candidate. (A ballot marked in any other way will be considered invalid.) Then an upturned hat is handed around the room. Each voter puts her ballot paper into the hat. At the end of this procedure, someone pins all the ballot papers on a publicly viewable noticeboard, and counts the votes.

<i>Candidate</i>	
C. Baldwin	
B. Barr	
J. McCain	
C. McKinney	
R. Nader	
B. Obama	

[8%]

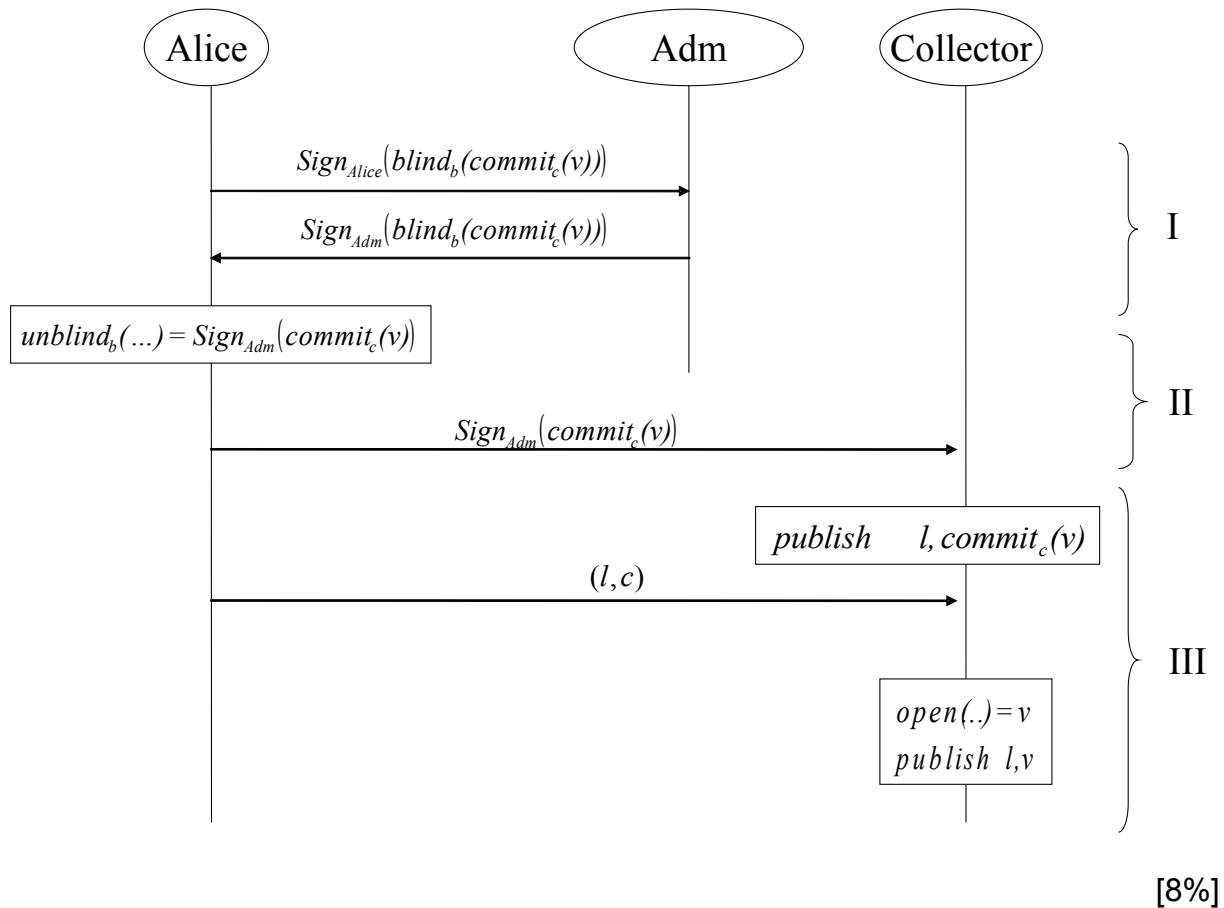
(ii) PGP and email are used. An administrator creates a PGP key for the purpose of running the election. We may assume that each voter has an authentic copy of this key (it has been given to each voter in person). To vote, a voter sends an email to the administrator containing her name and her chosen candidate. The email is encrypted with the administrator's key. At the end of this procedure, the administrator publishes the list of voters and their selected candidates on a web page, like this:

[8%]

(Question 3 continues over the page)

(Question 3 continued)

- (iii) The protocol by Fujioka, Okamoto and Ohta (studied in lectures) is used. To help you remember the details, a figure illustrating the protocol is given below.



4. Short notes.

Write short notes (maximum 100 words) on each of the following topics.

- (a) Web application penetration testing [10%]
- (b) ISO 27001 Information Security Management System [10%]
- (c) How could Alice surf the web without her activity being logged by her ISP? [7%]
- (d) In what way is the encryption scheme known as DES considered weak? [7%]