[Answer THREE Questions out of Four]

[Marks indicated on this paper add up to 99%.
The final 1% is a bonus mark reserved for outstanding answers]
1. Malware
   
   (a) Explain in at most 120 words what is happening in the screenshot shown. [11%]

   (b) What is a polymorphic virus? Briefly state two ways in which viruses using polymorphic code can be detected. [11%]

   (c) Why is there less malware on GNU/Linux systems than on Microsoft Windows systems? [11%]
2. Biometric authentication

(a) State two advantages and two disadvantages that biometric authentication has compared with password authentication. [15%]

(b) Comment on the appropriateness of biometric authentication in the following situations, either as a replacement or in conjunction to the current system. For each situation, state two crucial issues, and then a conclusion on the appropriateness. (As an example of the sort of issues and conclusion you might describe, the first one is done for you. You just need to do ii, iii, iv).

(i) Payment for food and drinks in a university’s food outlets (a currently used system is payment by university ID smart cards).

   Issue 1 (disadvantage): the failure rate for biometric authentication may mean it is too unreliable and too slow for the purpose.
   Issue 2 (advantage): it could eliminate purchases made with lost or stolen ID cards currently usable for payment.
   Conclusion: It is too unreliable to be used on its own, and the security requirements do not motivate its usage in conjunction with other systems.

(ii) Authentication for module registration on a university’s web portal for students (the currently-used authentication system is login/password). [6%]

(iii) Authentication of students sitting university exams (the currently used system is visual inspection of the photograph on the student ID). [6%]

(iv) Authentication for voting by students in a university’s student union elections (the current system is manual counting of paper ballots). [6%]

-3- Turn Over
3. Access control

(a) What is a capability in access control? [5%]

(b) Explain one advantage of access control lists compared with capability lists, and one advantage of capability lists compared with access control lists. [12%]

(c) Nurses and home visitors have login accounts to the patient record system of a hospital. It is desired to implement these policies:

(i) a nurse has access to the records of all the patients who are currently on his ward, or who have been there in the last 90 days

(ii) a home visitor is assigned periodically to a district, covering one or more patient addresses. She is assigned to at most one district at a time. At any given time, she has access to the records of all the patients currently in her district.

Explain how to implement these policies, focusing particularly on the suitability of capability lists and access control lists for each one. [16%]

4. Trusted computing

(a) What is attestation? [6%]

(b) What is a platform configuration register (PCR) and how is it updated? [7%]

(c) Can trusted computing help solve these problems? Briefly explain your answer.

(i) A maker of on-line games wants to prevent its users from using automated bots which cheat at the game. [5%]

(ii) A user installed a driver for a printer and since then her computer freezes every few hours. [5%]

(iii) Attackers observe vulnerabilities in popular tools like web browsers and email clients, and write exploits for them. [5%]

(iv) The BBC wants to implement a “view again” service on its website which allows users to play content but not to record or copy it. [5%]