IY5512: Coursework 2

If feedback is required, coursework solutions must be submitted electronically via the course Moodle page. The deadline for receipt of submissions is 23:59 UK time on Friday 23/10/15. Coursework submissions should normally be in the form of a single pdf file. If you use Word, a free add-on to enable you to save a document in pdf format can be obtained from the Microsoft web site. Take care to ensure that you include your full name on the first page of your submission, the course number (IY5512), and the coursework number.

These questions are designed to test and extend your understanding of Part 2 of the course material.

1. 'Open design', one of the Saltzer-Schroeder security design principles, is often paraphrased as 'do not reply on security by obscurity'. The phrase 'security by obscurity' has become a term of abuse that is used whenever design aspects of a system are kept secret. Is this justified, i.e. are there any circumstances under which keeping aspects of a design secret might be reasonable?

2. The following quote is taken (in slightly edited form) from the Wikipedia article on 'Principle of least privilege' (as of 15/10/11):

   > The principle of least privilege is widely recognised as an important design consideration in enhancing the protection of data and functionality against faults (fault tolerance) and malicious behaviour (computer security).

   Describe a practical example of a use of this principle.

3. Look at a set of security design principles other than that of Saltzer and Schroeder (e.g. the 2005 report of Benzel et al.)[1]. Give a security principle in this set that is distinct from the eight Saltzer-Schroeder principles and explain its key idea. Why is this not already covered by the Saltzer-Schroeder principles?

4. Security evaluations can be performed by government agencies (as in the US) or by commercial evaluation facilities (as in Europe). Discuss the relative advantages and disadvantages of the two approaches.

5. Discuss the difference between products and systems, as defined in ITSEC. Describe how evaluation of both products and systems is made possible through the notion of a Target of Evaluation (ToE), and, in doing so, describe what might be contained in a ToE.

[1] This report is available at: http://cisr.nps.edu/downloads/techpubs/nps_cs_05_010.pdf