IY5512: Coursework 3

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 30/10/15. 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 3 of the course material.

1. What is the difference between paging and segmentation? Briefly indicate their respective advantages and disadvantages.

2. Modern processor architectures typically support two or more privilege levels for programs. What is the purpose of these privilege levels, and how are they used by the processor?

3. Describe the use made by Windows of the four privilege levels provided by the Intel x86 family of processors. How does this contrast with the intended use of these levels? What problems does this cause?

4. What security issues arise from interrupts? Find and briefly describe an example of a security vulnerability arising from misuse of interrupts.

5. Explain the difference between a virtual address and a physical address. Discuss the advantages of the use of virtual memory management.

6. Memory management is fundamental to the operation of virtual memory management (VMM) systems.

   a. Give two primary objectives for a memory management system.

   b. Outline how a paged VMM system operates and indicate how it meets the two primary objectives you have given.

7. What security threats can Direct Memory Access (DMA) devices pose?

8. Outline the operation of a real-life example of malware that attacks the system BIOS (e.g. mebromi).

9. Briefly describe the mechanism provided within Intel TXT to provide protection against the threats posed by DMA.