

IY5512: Coursework 3

If feedback is required, coursework solutions must be submitted electronically, as an email attachment, to the following email address: me@chrismitchell.net.

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. 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?
3. What security issues arise from interrupts? Find and briefly describe an example of a security vulnerability arising from misuse of interrupts.
4. Explain the difference between a virtual address and a physical address. Discuss the advantages of the use of virtual memory management.
5. What security threats can Direct Memory Access (DMA) devices pose?
6. Briefly describe the mechanism provided within Intel TXT to provide protection against the threats posed by DMA.