IY5512: Coursework 4

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 20/11/15. 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 4 of the course material.

1. Outline the ‘penetrate and patch’ approach to developing secure software, and describe three shortcomings of this approach.

2. Briefly describe two principles which can be used to aid in the development of secure software.

3. What is a buffer overflow and how can it give rise to vulnerabilities in software?

4. Outline two ways in which the risks from buffer overflows can be reduced.

5. What is type safety, and how can its use help to make software more secure?

6. Give an example of a piece of malware which exploits a failure to validate data input. Describe briefly how it operates.

7. Give an example of a piece of malware which exploits a data type error. Describe briefly how it operates.

8. Give an example of a piece of malware which exploits a buffer overflow. Describe briefly how it operates.

9. State three steps that a company could take to reduce the threat posed by worms and viruses.

10. In the context of computer malware, what is the main difference between a virus and a worm?

11. Give real-life examples of a worm and a virus, and briefly explain how these particular examples propagate themselves.

12. It is often argued that worms pose a more serious threat than viruses. Give two reasons why this might be true.

13. Scanners can be used to search for malware by looking for its signature. What is a signature? Describe three ways which can be used to try to hide or change the signature of malware.