1. **Title of the module**

COMP5580 (CO558 ) Introduction to Cyber Security

1. **School or partner institution which will be responsible for management of the module**

School of Computing

1. **The level of the module (Level 4, Level 5, Level 6 or Level 7)**

Level 5

1. **The number of credits and the ECTS value which the module represents**

15 credits (7.5 ECTS)

1. **Which term(s) the module is to be taught in (or other teaching pattern)**

Autumn or Spring

1. **Prerequisite and co-requisite modules**

Prerequisites:

CO320 Introduction to Object-Oriented Programming

CO3AA Computing and the Cloud

CO3BB Problem Solving with Algorithms

1. **The programmes of study to which the module contributes**

BSc Computer Science, including all variants, both with and without Year in Industry

1. **The intended subject specific learning outcomes.  
   On successfully completing the module students will be able to:**

8.1 understand the threats faced by computer operating systems, applications and networks and the various countermeasures that can be used;

8.2 make informed choices of the appropriate security measures to put into place for a given network and/or operating system;

8.3 understand the importance of putting security into the context of a larger system including hardware, software, and human users;

8.4 understand how cryptography can be used for providing security within applications;

8.5 understand and implement selected fundamental algorithms used in cryptography;

1. **The intended generic learning outcomes.  
   On successfully completing the module students will be:**

9.1 able to analyse a problem specification and to design and implement a solution.

9.2 aware of the relevant professional, ethical and legal issues in this subject area.

9.3 able to apply relevant fundamental mathematical techniques.

9.4 able to develop their own time management and organisational skills.

1. **A synopsis of the curriculum**

Cyber security has always been an important aspect of computing systems but its importance has increased greatly in recent years. The curriculum covers areas where cyber security is of major importance and the techniques used to secure computer systems. The areas looked at include computer operating systems (and increasingly, distributed operating systems), distributed applications (such as electronic commerce over the Internet) and embedded systems (ranging from smart cards to large industrial plant and telecommunications systems). Furthermore, the curriculum integrates the legal, ethical, and professional perspectives for instance to address concerns about data security, privacy, and societal impact of computing systems.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

Anderson, R., “Security Engineering: A Guide to Building Dependable Distributed Systems,” 2nd ed., 2010, Wiley.

BCS Code of Conduct, https://www.bcs.org.uk/

Pfleeger, C.P., “Security in Computing,” 2nd ed., 1996, Prentice Hall William.

Cranor, L.F. & Garfinkel, S., “Security and Usability: Designing Secure Systems that   
 People Can Use,” 2005, O’Reilly Media.

Sutton, D. “Information Risk Management: A practitioner's guide,” 2014, BCS.

Schneier, B., “Beyond Fear: Thinking Sensibly About Security in an Uncertain World,” 2003, Springer.

Stallings, W., “Cryptography and Network Security: Principles and Practice,” 2nd ed., 1998, Prentice Hall.

Summers, R.C., “Secure Computing: Threats and Safeguards,” 1997, McGraw Hill.

Schneier, B., “Applied Cryptography: Protocols, Algorithms, and Source Code in C,” 2nd ed., 1995, John Wiley & Sons

1. **Learning and teaching methods**

Total contact hours: 30

Private study hours: 120

Total study hours: 150

1. **Assessment methods**
   1. Main assessment methods

2 hour written exam (50%)

Two assessments (25% and approximately 15 hrs each)

* 1. Reassessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | *8.1* | *8.2* | *8.3* | *8.4* | *8.5* | *9.1* | *9.2* | *9.3* | *9.4* |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |
| Lectures | x | x | x | x | x | x | x | x | x |
| *Private study* | x | x | x | x | x | x | x | x | x |
| **Assessment method** |  |  |  |  |  |  |  |  |  |
| *Assessments* | x | x | x | x | x | x | x | x | x |
| *Examination* | x | x | x | x | x | x | x | x | x |

1. **Inclusive module design**

The School recognises and has embedded the expectations of current equality legislation, by ensuring that the module is as accessible as possible by design. Additional alternative arrangements for students with Inclusive Learning Plans (ILPs)/declared disabilities will be made on an individual basis, in consultation with the relevant policies and support services.

The inclusive practices in the guidance (see Annex B Appendix A) have been considered in order to support all students in the following areas:

a) Accessible resources and curriculum

b) Learning, teaching and assessment methods

1. **Campus(es) or centre(s) where module will be delivered**

Canterbury

1. **Internationalisation**

The topics addressed by this module relate to a field which is of international importance, given the global role of computers in today's technological innovation. The topics covered by this module are international in nature, being identical worldwide and independent of traditional spoken language.

**FACULTIES SUPPORT OFFICE USE ONLY**

**Revision record – all revisions must be recorded in the grid and full details of the change retained in the appropriate committee records.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date approved | Major/minor revision | Start date of the delivery of revised version | Section revised | Impacts PLOs (Q6&7 cover sheet) |
|  |  |  |  |  |
|  |  |  |  |  |

Revised FSO Jan 2018