1. **Title of the module**

COMP8760 (CO876) Computer 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 7

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

15 credits (7.5 ETCS)

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

Autumn

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

None.

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

Portfolio of Taught Postgraduate Programmes in Computing

1. **The intended subject specific learning outcomes.
On successfully completing the module students will be able to:**
2. Demonstrate an understanding of some basic concepts of the state-of-the-art in symmetric and asymmetric key cryptography;
3. Demonstrate a systematic understanding of the mathematical and computational principles used in cryptography and how they relate to real world applications;
4. Demonstrate an understanding of the various techniques used in authentication, authorisation and accountability (AAA);
5. Make informed choices of the appropriate cryptographic primitives and AAA security measures to put into place for a given application.
6. **The intended generic learning outcomes.
On successfully completing the module students will be able to:**
7. Undertake individual tasks as well as work effectively in a group;
8. Demonstrate self-direction and originality in tackling and solving problems, and act autonomously in planning and implementing tasks;
9. Communicate effectively with specialist and non-specialist audiences;
10. Present ideas, arguments or results in the form of a well-structured written report;
11. Demonstrate the independent learning ability required for continuing professional development.
12. **A synopsis of the curriculum**

This module starts with the fundamental mathematical concepts to build cryptographic primitives. A key objective is to learn to implement the primitives without using programming libraries, learn the formal security notions and models for the primitives, and the use of the primitives in practical applications like blockchains.

The second part of the module covers the key application areas of authentication, authorisation and accountability (AAA). Included here are foundational topics of user and non-user authentication (including issues with password and biometric authentications), as well as access control and authorisation, along with matters related to accountability.

1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**
* Nigel P. Smart. “Cryptography Made Simple”, 2016, Springer. Available at: [https://link-springer-com.chain.kent.ac.uk/content/pdf/10.1007%2F978-3-319-21936-3.pdf](https://link-springer-com.chain.kent.ac.uk/content/pdf/10.1007/978-3-319-21936-3.pdf)
* Jonathan Katz and Yehuda Lindell. “Introduction to Modern Cryptography”, 2nd edition, 2015, CRC Press.
* Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography, 1997, CRC Press. Available at: <http://cacr.uwaterloo.ca/hac/>
* Arvind Narayanan, Joseph Bonneau, Edward W. Felten, Andrew Miller, Steven Goldfeder, Jeremy Clark. Bitcoin and Cryptocurrency Technologies. http://bitcoinbook.cs.princeton.edu/
* Charles P. Pfleeger and Shari Lawrence Pfleeger, "Security in Computing", 5th ed., 2015,
Prentice Hall
* Dieter Gollmann, "Computer Security", 3rd Edition. 2011. John Wiley and Sons.
1. **Learning and teaching methods**

Contact hours: 40

Private study hours: 110

Total hours: 150

1. **Assessment methods**

13.1 Main assessment methods

Programming assessment (30%)

Practical report (20%)

Written examination (50%)

13.2 Re-assessment methods

Like for like.

1. **Map of module learning outcomes (sections 8 & 9) to learning and teaching methods (section 12) and methods of assessment (section 13)**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Module learning outcome** | **8.1** | **8.2** | **8.3** | **8.4** |  |  | **9.1** | **9.2** | **9.4** | **9.5** |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |  |
| **Lectures** | **x** | **x** | **x** | **x** |  |  |  |  |  |  |
| **Classes** | **x** | **x** | **x** | **x** |  |  | **x** | **x** |  |  |
| **Private study** | **x** | **x** | **x** | **x** |  |  |  | **x** | **x** | **x** |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |
| **Report** |  |  |  |  |  |  | **x** | **x** | **x** | **x** |
| **Programming** | **x** | **x** | **x** | **x** |  |  | **x** | **x** |  |  |
| **Examination** | **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**

Most of the curriculum in this module is universal in its scope. The module focuses on technologies and international standards which apply worldwide. Where the module touches on legal aspects, care is taken to specify which issues apply solely to the UK or EU, and which apply more universally.

**DIVISIONAL 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) |
| 09/05/2018 |  | September 2018 | 6, 12, 13 |  |
| 03/08/20 | Major | September 2020 | 8,9,10,11,13,14 | No |
| 24/01/22 | Major | September 2022 | 7, 8, 10, 11, 12 | No |