1. **Title of the module**

COMP8990 (CO899) - Advanced Topics in Cyber Security

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

Division of Computing, Engineering, Mathematical Sciences (CEMS)

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 ECTS)

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

Spring

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

Pre-requisites: COMP8760: Computer Security,

COMP8740: Networks and Networks Security

(or equivalent knowledge of subject, e.g. gained from another degree course)

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

Portfolio of Taught Postgraduate Courses in Computing

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

8.1 Demonstrate a systematic understanding of knowledge of a broad variety of advanced topics related to cyber security research and development.

8.2 Demonstrate critical awareness of the importance role of human factors for addressing cyber security problems.

8.3 Demonstrate knowledge and a comprehensive understanding of modern principles in modelling, developing and evaluating in cyber security systems.

8.4 Select, use and evaluate critically appropriate tools for developing and evaluating cyber security systems.

8.5 Undertake a research investigation in order to have a conceptual understanding into areas covered by this module, to evaluate critical the current research, and report on their findings.

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

9.1 Demonstrate the ability for critical thinking, reasoning and reflection.

9.2 Produce a specification of the operation of a complex system based on an understanding of the component parts.

9.3 Undertake critical appraisal of a candidate system design and reflect upon its merits.

9.4 Study independently and make appropriate use of relevant resources.

9.5 Demonstrate personal and interpersonal skills, and work as a member of a team.

9.6 Communicate effectively.

9.7 Learn effectively for the purpose of continuing professional development.

9.8 Manage time and resources within a potentially complex problem domain.

9.9 Make effective use of general IT facilities including information retrieval skills.

1. **A synopsis of the curriculum**

The module looks at a number of advanced topics in cyber security that are important for understanding, finding, researching and assessing security solutions. Example topics include:

* Digital steganography and watermarking, and its increasing role in modern malware;
* CAPTCHAs and other mechanisms to distinguish bots from humans remotely;
* AI in security, for example, the role of deep learning and adversarial examples in cyber security;
* Security in AI, for example, the protection of machine learning techniques against cyber threats;
* Random number generators and their relevance in password and nonce generation;
* Advanced malware threats such as ransomware, covering their evolution and providing some insights into likely future trends, including economic aspects.
* Advanced topics in research related to human factors and usable security, e.g., user behaviour and their relationship to cybercrime, positive security, user profiling and modelling;
* Quantum cyber security and the development of quantum-resistant cyber security systems based on quantum mechanics;
* Advanced topics in IoT security, covering new developments and trends, threats and mitigations.

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

More recommended readings will be provided with each week’s teaching material. Some examples are:

Fridrich, J. (2009). “Steganography in Digital Media: Principles, Algorithms, and Applications”. Cambridge: Cambridge University Press. doi:10.1017/CBO9781139192903.

Kipper, G. (2003). “Investigator’s Guide to Steganography”. CRC Press, Inc., USA.

Solving CAPTCHAs, Machine Learning vs. online services

<https://towardsdatascience.com/solving-captchas-machine-learning-vs-online-services-3596ad6f0137>

Parisi, A. (2019). “Hands-On Artificial Intelligence for Cybersecurity: Implement smart AI systems for preventing cyber attacks and detecting threats and network anomalies”. Pack Publishing.

Nemec, M., Sys, M., Svenda, P., Klinec, D. and Matyas, V. (2017). "The return of coppersmith's attack: Practical factorization of widely used rsa moduli" In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1631-1648.

Sikorski, M. (2012). “Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software”. No Starch Press.

1. **Learning and teaching methods**

Total contact hours: 34

Private study hours: 116

Total study hours: 150

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

Presentation (10%)

Written assessment (40%)

Examination, 2 hours (50%)

13.2 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* | *9.5* | *9.6* | *9.7* | *9.8* | *9.9* |
| **Learning/ teaching method** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Lectures | x | x | x | x | x | x | x | x | x |  | x |  | x | x |
| Presentations | x | x |  | x | x | x |  | x |  | x | x | x | x | x |
| Private Study | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| **Assessment method** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Presentation | x | x |  |  | x | x |  | x | x | x | x | x | x | x |
| Written assessment | x | x |  |  | x | x |  | x | x | x | x | x | x | x |
| Exam | x | x | x | x |  | x | x | x |  |  | x |  |  |  |

1. **Inclusive module design**

The Division 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.

**DIVISION 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) |
| 04/12/2020 | Major | September 2021 | 1,8,10,11 | No |
|  |  |  |  |  |