1. **Title of the module**

COMP8990 (CO899) - System 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 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 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:**

8.1 Demonstrate knowledge of a broad variety of advanced topics related to computer systems security.

8.2 Demonstrate awareness of the importance of taking a systems wide approach to achieving and maintaining information security.

 8.4 Apply modern principles to model, test and develop security solutions for complex systems .

8.5 Select and employ appropriate tools for modern secure systems.

8.7 Undertake an investigation into areas covered by this module 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 (in writing and verbally).

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 computer and systems security that are important for understanding, finding and assessing security solutions .

* D igital steganography and watermarking, and its increasing role in modern malware;
* CAPTCHAs and other mechanisms to distinguish bots from humans remotely;
* The fundamental role which Deep Learning and adversarial examples is taking in Cybersecurity;
* Random number generators and their testing and certification, with their relevance in password and nonce generation and how a bad RNG could compromise the security of entire systems, with examples on Bitcoin and e-Passports;
* Operating Systems hardening, for improved security, with recommendations to increase the security of popular OS’s such as Linux and Windows;
* Advanced malware threats such as ransomware, covering its evolution over the last 20 years and providing some insights into its likely future evolution.
1. **Reading list (Indicative list, current at time of publication. Reading lists will be published annually)**

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

Gregory Kipper. 2003. Investigator’s Guide to Steganography. CRC Press, Inc., USA.

Ingemar Cox, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. 2007. Digital Watermarking and Steganography (2nd. ed.). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA.

Solving CAPTCHAs, Machine Learning vs. online services

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

M. Osadchy, J. Hernandez-Castro, S. Gibson, O. Dunkelman and D. Pérez-Cabo, "No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples, With Applications to CAPTCHA Generation," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 11, pp. 2640-2653, Nov. 2017, doi: 10.1109/TIFS.2017.2718479.

Breitner, J., & Heninger, N. (2019, February). Biased nonce sense: Lattice attacks against weak ECDSA signatures in cryptocurrencies. In the International Conference on Financial Cryptography and Data Security (pp. 3-20). Springer, Cham.

Nemec, Matus, Marek Sys, Petr Svenda, Dusan Klinec, and Vashek Matyas. "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. 2017.

Turnbull, James. Hardening Linux. Apress, 2006.

Jonathan Hassell. Hardening Windows, 2004, Apress

Mohurle, S. and Patil, M., 2017. A brief study of wannacry threat: Ransomware attack 2017. International Journal of Advanced Research in Computer Science, 8(5).

Nieuwenhuizen, D., 2017. A behavioural-based approach to ransomware detection. Whitepaper. MWR Labs Whitepaper.

Hernandez-Castro, Julio, Edward Cartwright, and Anna Stepanova. "Economic analysis of ransomware." Available at SSRN 2937641 (2017).

Cartwright, Edward, Julio Hernandez- Castro, and Anna Cartwright. "To pay or not: game theoretic models of ransomware." Journal of Cybersecurity 5, no. 1 (2019): tyz009.

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* |   | *8.4* | *8.5* |   | *8.7* | *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 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) |
| 03/08/20 | Major | January 2021 | 8,10,11,14 | No |
|  |  |  |  |  |

Revised FSO July 2020