SE TU

Ollscoil
Teicneolaíochta
an Oirdheiscirt

South East
Technological
University

Module Descriptor

Network and System Security (Computing and Mathematics)

Short Title: Network and System Security
Department: Computing and Mathematics
Credits: 5   **Level:**   Advanced

Description of Module / Aims

The objective of this module is to equip students with the necessary skills to evaluate the security of systems and networks and implement appropriate solutions. Network security is covered at all layers of the TCP/IP protocol suite and system security is considered with respect to operating system, applications, virtualisation and cloud technologies.

Programmes

	stage/semester/status
COMP-0651 BSc (Hons) in Applied Computing (International) (WD_KACCM_BI)	4 / 7 / M
COMP-0672 BSc (Hons) in Applied Computing (WD_KACCM_B)	4 / 7 / E
COMP-0672 BSc (Hons) in Applied Computing (WD_KCOMP_B)	4 / 7 / E
COMP-0672 BSc (Hons) in Computer Forensics and Security (WD_KCOFO_B)	4 / 7 / M
COMP-0672 BSc (Hons) in Computer Science (WD_KCMSC_B)	4 / 7 / E
COMP-0672 BSc (Hons) in Information Technology Management (WD_KITMA_B)	1 / 7 / M
COMP-0651 BSc (Hons) in Information Technology (WD_KINTE_B)	4 / 1 / M

Indicative Content

- Auditing and assessment
- Communications & network security - link layer, network layer, transport layer
- Mobile & wireless security
- Cloud security
- Identity and access management
- Access control models; firewalls
- Malware and intrusion detection

Learning Outcomes

On successful completion of this module, a student will be able to:

1. Evaluate Internet and cloud security technologies.
2. Evaluate a selection of leading Internet security protocols.
3. Compare and describe the roles of firewalls, intrusion detection and malware protection.
4. Develop security policies (for example firewall rules) for a given scenario.
5. Deploy popular network security technologies (e.g. TLS in various configurations).
6. Set up test systems and evaluate their security.
7. Assess the challenges with securing wireless communications and the main solution approaches.

Learning and Teaching Methods

- This module will be presented by a combination of lectures and practicals.
- The lectures will be used to introduce new topics and their related concepts.
- The practical element allows the student to put into practice the theoretical concepts covered in the lectures.

Learning Modes

Learning Type	F/T Hours	P/T Hours
Lecture	24	
Practical	24	
Independent Learning	87	

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
Practical	50%	4,5,6
Assessment	50%	1,2,3,4,7

Assessment Criteria

<40%: Unable to describe key network and system security technologies. Unable to effectively use relevant tools.

40%–49%: Can describe in detail key security threats and technologies. Can carry out basic configuration of technologies to implement security policies for access control, encryption and authentication.

50%–59%: All of the above and in addition can reason about the various approaches to security and their benefits and limitations.

60%–69%: In addition, be capable of discussing the relative merits of securing at all layers or just at one layer. Also, can competently make use of security tools and technologies and carry out effective penetration tests.

70%–100%: All of the above to an excellent level. Be able to describe a variety of new developments in security. Demonstrate an understanding of some the trade-offs involved in providing security.

Essential Material(s)

- "The SANS Institute." http://www.sans.org/

Supplementary Material(s)

- "Computer Emergency Response Team." http://www.cert.org/
- "Security Focus." http://www.securityfocus.com/
- Gollmann, D. *Computer Security.* 3rd ed. Chichester: Wiley, 2011.
- Stallings, W. and L. Brown. *Computer Security: Principles and Practice.* 3rd ed. Harlow: Pearson, 2014.

Requested Resources

- Computer Lab: BYOD Lab