2024 / 25

School of Science and Computing
+353 (0)51 302037
Eleanor.Reade@setu.ie
www.wit.ie/schools/science_computing

Ollscoil Teicneolaíochta an Oirdheiscirt

South East Technological University

Module Descriptor

Computer Security (Computing and Mathematics)

Computer Security (A13623)

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

Description of Module / Aims

This module provides the essentials of computer security. Topics covered include the various security threats and vulnerabilities and the services available to address these threats. Cryptographic foundations that underpin many security mechanisms are covered. Issues relating to network and application security, including web applications, are also explored. Best practice in secure programming is also covered.

Programmes

		stage/semester/status
COMP-0628	BSc (Hons) in Creative Computing (WD_KCRCO_B)	4 / 7 / M
COMP-0628	BSc (Hons) in Multimedia Applications Development (WD_KMULM_B)	4 / 1 / M

Indicative Content

- Introduction to computer security: security threats; attack methods; common vulnerabilities; security services
- Cryptography: symmetric encryption; modern encryption; block vs stream ciphers; public key cryptography
- Message authentication and integrity: hash functions; collisions; MACs; digital signatures; digital certificates
- Network security: TLS/SSL; wireless security, SSH, firewalls
- Secure Web Application development: SQL Injection; Cross Site Scripting, CSRF
- Security policy and procedures
- Steganography, Digital watermarking and Digital rights management

Learning Outcomes

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

1. Assess the various security threats and attack methods to which an organisation may be susceptible.
2. Appraise the role of cryptography in computer security, including its benefits and limitations.
3. Test and use cryptographic software and set up network and system security.
4. Evaluate the specific security concerns pertinent when developing web applications.
5. Appraise the role of steganography, digital watermarking and digital rights management within multimedia environments.

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%	
In-Class Assessment	50%	1,2,3
Assignment	50%	1,4,5

Assessment Criteria

<40%: Unable to describe key network and system security technologies. Unable to distinguish between different types of application vulnerabilities or present instances of them in a clear manner. 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. Able to present instances of vulnerabilities and carry out threat modelling on a basic system.

50%–59%: In addition to the above, can reason about the various approaches to security and their benefits and limitations. Able to explain in context and present instances of web application vulnerabilities. Able to model threats in a software system with multiple usage scenarios and actors.

60%–69%: In addition, can explain basis of a variety of cryptographic schemes. Can competently make use of security tools and technologies and carry out effective penetration tests. Able to present and explain how to address web application vulnerabilities.

70%–100%: All of the above to an excellent level. Can demonstrate an understanding of some the trade-offs involved in providing security. Able to demonstrate in detail how to address web application vulnerabilities.

Essential Material(s)

- "Open Web Application Security Project (OWASP)." https://www.owasp.org
- "OpenSSL, Cryptography and SSL/TLS Toolkit.." https://www.openssl.org/

Supplementary Material(s)

- "Computer Emergency Response Team, CERT." https://www.cert.org
- "Security Focus." http://securityfocus.com/
- "The SANS Institute." https://www.sans.org
- McGraw, G. *Software Security: Building Security In.* NY: Addison-Wesley, 2006.
- Stallings, W. *Computer Security: Principles and Practices.* 3rd ed. England: Pearson Higher Education, 2014.

Requested Resources

- Computer Lab: BYOD Lab