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

Introduction to Computer Security (Computing and Mathematics)

Introduction to Computer Security (A13203)

Short Title: Intro to Computer Security
Department: Computing and Mathematics
Credits: 5 **Level:** Introductory

Description of Module / Aims

This module will provide an introduction to computer security. The emphasis is on the fundamentals of security, including the nature of security threats and attack methods. It will also include the services that can be put in place to address these threats. Cryptographic techniques, that underpin many security mechanisms, are also covered. This module will introduce the student to the foundations of modern cryptography, with a focus on practical applications. The importance of security policy and procedures will also be explained.

Programmes

		stage/semester/status
COMP-0607	BSc (Hons) in Software Engineering (WD_KDEVP_BI)	2 / 4 / M
COMP-0607	BSc (Hons) in Software Systems Development (WD_KDEVP_B)	2 / 4 / M
COMP-0607	BSc in Applied Computing (WD_KCOMP_D)	2 / 4 / M
COMP-0607	BSc in Information Technology (WD_KINFT_D)	2 / 4 / M
COMP-0607	BSc in Software Systems Development (WD_KCOMC_D)	2 / 4 / M

Indicative Content

- Vulnerabilities, types of attack, security services
- Overview of encryption and authentication
- Randomness & entropy
- Symmetric block & stream ciphers, public key cryptography
- Authentication and hash functions
- Key management & digital certificates
- Security policy & procedures
- Applications

Learning Outcomes

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

1. Describe and categorise potential computer security threats and attacks and the security services that can be implemented to address them.
2. Explain the role played by both technology and security policy in supporting security services.
3. Describe various cryptographic approaches and techniques for the provision of secrecy, authentication, integrity and non-repudiation.
4. Use commercial encryption software for secrecy of data and authentication purposes.
5. Communicate technical information effectively.

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 student will be encouraged to participate in class discussions and ask questions to support their learning process.
- 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	12
Practical	24	12
Independent Learning	87	111

Assessment Methods

	Weighting	Outcomes Assessed
Final Written Examination	50%	1,2,3
Continuous Assessment	50%	
Lab Report	20%	4,5
Practical	30%	4,5

Assessment Criteria

<40%: Unable to interpret and describe key concepts of computer security. Unable to interpret and describe computer security threats, vulnerabilities and security services. Unable to interpret and describe key concepts of cryptography.

40%–49%: Be able to interpret and describe key concepts of computer security. Be able to interpret and describe computer security threats, vulnerabilities and security services. Be able to interpret and describe key concepts of cryptography.

50%–59%: All of the above and the ability to distinguish between the various security services necessary to mitigate against a range of security threats and attacks. Ability to explain various cryptographic approaches and techniques required to implement each security service.

60%–69%: All of the above and be able to evaluate different cryptographic approaches and techniques.

70%–100%: All the above to an excellent level. Be able to analyse and design solutions to a high standard for a range of existing security problems.

Essential Material(s)

- "OpenSSL, Cryptography and SSL/TLS Toolkit." https://www.openssl.org/

Supplementary Material(s)

- "Computer Emergency Response Team, CERT." http://www.cert.org/
- "Security Focus." http://www.securityfocus.com/
- "The SANS Institute." http://www.sans.org
- Stallings, W. *Network Security Essentials.* 5th ed. England: Pearson, 2014.
- Stalllings, W. *Cryptography and Network Security, Principles and Practice.* 6th ed. England: Pearson, 2013.

Requested Resources

- Computer Lab: BYOD Lab