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

Application Security (Computing and Mathematics)

Application Security (A13401)

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

Description of Module / Aims

This module equips the student with knowledge of security vulnerabilities of application software taking into account both web and native applications. Methods used to solve these vulnerabilities are investigated. Intrusion Detection/Prevention Systems and Malicious Software are also presented. Students will be given a grounding in the area of Secure Software Development. This module also explores issues pertinent to Incident Response and Recovery.

Programmes

		stage/semester/status
COMP-0612	BSc (Hons) in Software Engineering (WD_KDEVP_BI)	4 / 7 / M
COMP-0612	BSc (Hons) in Software Systems Development (WD_KCSDV_B)	4 / 2 / M
COMP-0612	BSc (Hons) in Software Systems Development (WD_KDEVP_B)	4 / 8 / E
COMP-0612	BSc (Hons) in Software Systems Practice (WD_KSOFP_B)	1 / 2 / M
COMP-0612	BSc in Applied Computing (WD_KCOMP_D)	3 / 6 / M
COMP-0612	BSc in Information Technology (WD_KINFT_D)	3 / 6 / M

Indicative Content

- Web application security
- Native application security (mobile apps, desktops apps etc.)
- Intrusion detection/prevention systems
- Malicious software
- Secure software engineering
- Incident response and recovery

Learning Outcomes

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

1. Assess a variety of security issues, vulnerabilities and fixes that arise in applications and categorise them by using information from CERT, OWASP and other trusted services.
2. Compare the capabilities and limitations of intrusion detection systems and intrusion prevention systems.
3. Appraise different threats posed by various categories of malware and explain different techniques to defend against them.
4. Justify the need for appropriate incident response and recovery measures.
5. Assess how security can be integrated into the software development process.
6. Formulate a variety of security attacks in a simulated environment.

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
Continuous Assessment	100%	
Assignment	30%	5
Practical	40%	6
In-Class Assessment	30%	1,2,3,4

Assessment Criteria

<40%: Unable to describe typical security vulnerabilities of application software. Unable to explain the operation of IDS/IPS. Unable to describe the different categories of malware. Unable to describe how security can be incorporated into the software engineering process.

40%–49%: Be able to describe typical security vulnerabilities of application software. Be able to explain the operation of IDS/IPS. Be able to describe the different categories of malware. Be able to describe how security can be incorporated into the software engineering process. Be able to explain the need for appropriate incident response and recovery.

50%–59%: All of the above and the ability to discover and review contemporary knowledge of application software vulnerabilities, secure software development techniques, IDS/IPS, malicious software and incident response and recovery techniques.

60%–69%: All of the above and be able to solve problems within application software security by experimenting with the appropriate skills and tools.

70%–100%: All the above to an excellent level and the ability to analyse and design application software security solutions to a high standard for a range of security threats through the use and modification of appropriate skills and tools.

Essential Material(s)

- "Open Web Application Security Project (OWASP)." https://www.owasp.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. *Cryptography and Network Security, Principles and Practice.* 6th ed. England: Pearson, 2014.
- Stallings, W. *Network Security Essentials.* England: Pearson, 2014.

Requested Resources

- Computer Lab: BYOD Lab