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 and Forensics (Computing and Mathematics)

Computer Security and Forensics (A13744)

Short Title: Security and Forensics
Department: Computing and Mathematics
Credits: 10 **Level:** Advanced

Description of Module / Aims

This module provides the essentials of computer security and forensics. Topics covered include 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. Students will explore the area of digital forensics through file system forensics, network/online forensics and media forensics.

Programmes

		stage/semester/status
COMP-0620	Higher Diploma in Science in Computer Science (WD_KCOSC_G)	1 / 2 / E

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
- Secure coding best practice
- Introduction to computer forensics, the forensic process
- File systems and recovery of data
- Live response
- Network data, types of data, collecting and analysing data from a network
- Web forensics, HTTP headers, cookies, browser / server log analysis, proxy servers, capturing web pages, web form server-side data, web activity reconstruction, DNS
- E-mail forensics, e-mail activity reconstruction, message headers, message attachments, tracing online e-mail
- Mobile device forensics

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 configure network and system security tools.
4. Evaluate the specific security concerns pertinent when developing web applications.
5. Recommend security measures when developing code.
6. Utilise forensic tools to analyse a file system and recover deleted data.
7. Perform a live response and gather network data.
8. Investigate web based services/applications.
9. Trace and analyse email data.
10. Collect electronic evidence from modern devices such as smart phones or tablets.

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	48	
Practical	48	
Independent Learning	174	

Assessment Methods

	Weighting	Outcomes Assessed
Continuous Assessment	100%	
In-Class Assessment	25%	1,2,3
Assignment	25%	1,4,5
Assignment	25%	6,10
Assignment	25%	7,8,9

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. Unable to differentiate stages of the forensic process.

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. Can conduct basic computer forensic investigations.

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. Can conduct computer forensic investigations and recover deleted data.

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. Can interpret evidence extracted during a forensic investigation and corroborate it with other sources of evidence.

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. Can evaluate the appropriateness of different forensic tools and approaches.

Essential Material(s)

- "Open Web Application Security Project." https://www.owasp.org
- "The OpenSSL project." https://www.openssl.org

Supplementary Material(s)

- "Computer Emergency Response Team." https://www.cert.org
- "The SANS Institute." https://www.sans.org
- Carrier, B. *File System Forensic Analysis.* Boston: Addison-Wesley, 2005.
- Casey, E. *Handbook of Digital Forensics and Investigation.* Burlington, MA: Elsevier Academic Press, 2010.
- Jones, K., R. Bejtlich and C. Rose. *Real Digital Forensics: Computer Security and Incident Response.* Boston: Addison-Wesley, 2005.
- Jones, R. *Internet Forensics.* Sebastopol, CA: O'Reilly, 2005.
- McGraw, G. *Software Security: Building Security In.* Boston: Addison-Wesley, 2006.
- Stallings, W. and L. Brown. *Computer Security: Principles and Practices.* 3rd ed. Harlow: Pearson, 2014.

Requested Resources

- Computer Lab: BYOD Lab