Manchester Metropolitan University

Unit Details & Outline

Unit Title	Introduction to Computer Forensics and Security		
Unit Code	6G7Z1009		
Occurrence(s)	MMU Science & Engineering		
Unit Abbreviation	Intro CF & Sec		
Level of Study	7		
Credit Value	30	**ECTS Value**	15
Home Department	School of Computing, Mathematics and Digital Technology Division of Computer Science and Information Systems		
Home Faculty	Faculty of Science and Engineering		
Unit Co-ordinator	Majdi Owda		
Key Words	Introduction to Computer Forensics, Introduction to Computer Security, File Systems Forensics, Recent Developments and Advances in Digital Forensics, Information Security.		

Unit Description

Brief Summary	This unit will introduce both computer security and digital forensics concepts.
Indicative Content	**Forensic Process [10%]:** Types of investigations, role of investigator, processes, and legal aspects. **File System Analysis [30%]:** Data acquisition,volume analysis, write blockers, signatures, file systems artefacts, locating and restoring deleted content. **Recent Developments and Advaces in Digital Forensics [10%]:** Topics such as mobile forensics, memory forensics and forensic data mining. **Overview of security [15%]:** The need for security; Types of security; Threats; Security mechanisms and security services. **Introduction to Cryptography [10%] :** Attacks on conventional and public key cryptography; Integrity (hash functions and message authentication codes). **Access control [25%]:** Goals of protocols (Authentication and Authorisation; Key distribution and confirmation); Fiat-Shamir protocol; PKI; Digital certificates; Mediated authentication (Needham-Schroeder protocol); Access control lists and capabilities; Multilevel Security; Multilateral Security; Covert channels; Kerberos.

Learning Outcomes

Unit Learning Outcomes	On successful completion of this unit students will be able to: 1. Critical analysis and evaluation of the digital forensic process in terms of technical and legal aspects. 2. Analyse and evaluate volatile and non-volatile data. 3. Explain, critically analyse, compare basic cryptographic algorithms and propose appropriate uses for them. 4. Explain, critically analyse a variety of security attacks, basic security protocols and propose corrections to simple defective security protocols.

Assessment

Summative Assessment

Element	Type	Weighting	Learning outcomes assessed
1	Coursework	50%	1-4
2	Exam	50%	1-4

Employability and Sustainability Outcomes	**Outcomes**	**Element of Assessment**
	Apply skills of critical analysis to real world situations within a defined range of contexts.	1, 2
	Demonstrate a high degree of professionalism.	
	Express ideas effectively and communicate information appropriately and accurately using a range of media including ICT.	
	Develop working relationships using teamwork and leadership skills, recognising and respecting different perspectives.	
	Manage their professional development reflecting on progress and taking appropriate action.	
	Find, evaluate, synthesise and use information from a variety of sources.	2
	Articulate an awareness of the social and community contexts within their disciplinary field.	
	Use systems and scenario thinking.	1,2
	Engage with stakeholder/interdisciplinary perspectives.	

Description of each element of Assessment	**Summative** **Element 1: Portfolio** which will have of the following two components: Component 2: An expert wittness report to be produced based on an imitated crime evidence files. The students will be given evidence files to investiage/analyse in order to find the evidence inside them and then they will create an expert witness report to present their findings. Component 2: the implementation of a cryptographic algorithm or protocol or an attack on a cryptographic algorithm/protocol along with appropriate analysis and design documents. **Element 2:** Formal Examination (**Seen Examination**). Three hours exam, students have to answer 4 questions out 6. The exam will assess the selected learning outcomes. **Formative** Students receive formative feedback during supported weekly laboratory sessions.	
Mandatory Learning & Teaching Requirements	N/A	
Minimum Pass Mark	N/A	

Learning Activities

Breakdown of Student Learning Activity	**Type of Activity**	**%**
	Summative Assessment	25%
	Directed Study	25%
	Student-centred Learning	50%

Learning Resources

Books recommended for purchase by students	None
Essential Reading/ Resources	**Nelson,B., Phillips, A. and Steuart C. (2016), Guide to computer forensics and investigations: processing digital evidence, Cengage Learning, Fifth Edition, ISBN-13:9781285060033** Carrier B. (2005) *File System Forensic Analysis*, Mass, Addison-Wesley, ISBN 13-978-0321268174 C. Prosise, K. Mandia, et al. (2003) *Incident Response & Computer Forensics*,

	McGraw-Hill/Osborne, 2nd Ed. ISBN 13-978-0072226966 Jones K. Bejtlich R. et al. (2005) *Real Digital Forensics: Computer Security and Incident Response*. Addison-Wesley, ISBN 13-978-0321240699 Stallings W. (2013) *Cryptography and Network Security: Principles and Practice* Prentice Hall, 6th Ed. ISBN 13-978-0273793359 Stamp M. (2011), *Information Security. Principles and Practice,* John Wiley, 2nd Ed. ISBN 13-978-0470626399 D. Gollmann D. (2011), *Computer Security*, John Wiley, 3rd Ed. ISBN 13-978-0470741153
Further Reading/ Resources	Bunting S. (2012) *EnCase Computer Forensics: the Official EnCE : EnCase Certified Examiner Study Guide*, John Wiley, ISBN 13-978-0470901069 Casey E. (2011) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, 3rd Ed. ISBN 13-978-0123742681 Ferguson N. Schneier B. , Kohno T. (2010) *Cryptography Engineering: Design Principles and Practical Applications*, John Wiley, ISBN 13-978-0470474242 Pfleege C. P. Pfleeger S. L. (2006) *Security in Computing*, Prentice Hall , 4th Ed. ISBN 13-978-0132390774 Trappe W. Washington L. C. (2005) *Introduction to Cryptography with Coding Theory,* 2nd Ed. ISBN 13-978-0131981997 J. Erickson J. (2008) *Hacking: The Art of Exploitation,* 2nd Ed. ISBN 13-978-1593271442 MMU's VLE will be used to deliver course materials, assessments, support blende learning and enhance communication.
Specialist ICTS Resources	None
Additional Requirements	Hardware and software requirements decided annually and communicated to specialist technical support.

Administration

JACS Code	I100
HESA Academic Cost Centre	121 IT, Systems Sciences and Computer Software Engineering (C1)
Date of Approval	18 February 2016
Date of Most Recent	18 February 2016

Consideration	
Unit External Examiner	Prof. Reinhold Behringer
Unit Assessment Board	CMDT Tier 1