SWRE C7007: Security for Software Developers

Module Details

Module Code:	SWRE C7007
Full Title:	Security for Software Developers APPROVED
Valid From:	Semester 1 - 2019/20 (June 2019)
Language of Instruction:	English
Duration:	1 Semester
Credits:	5
Module Owner::	Caroline Sheedy
Departments:	Unknown
Module Description:	Students completing this module will have an understanding of the importance of secure development from the design stage, develop an understanding of the most common threats and vulnerabilities, and will be aware of how to select appropriate security controls and defences.

Module Learning Outcome	
On successful completion of this module the learner will be able to:	
#	**Module Learning Outcome Description**
MLO1	Illuminate the need for security at the design phase of an application and identify risk.
MLO2	Discuss the legislation and ethical issues relating to privacy and confidentiality, specifically when holding user data.
MLO3	Analyse the OWASP top 10 vulnerabilities.
MLO4	Design and incorporate appropriate software development practices.

Pre-requisite learning
Module Recommendations *This is prior learning (or a practical skill) that is strongly recommended before enrolment in this module. You may enrol in this module if you have not acquired the recommended learning but you will have considerable difficulty in passing (i.e. achieving the learning outcomes of) the module. While the prior learning is expressed as named DkIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
No recommendations listed

Module Indicative Content
Introduction Program security flaws, OWASP, malicious and non-malicious.
Secure Development Principles Identify security issues at the design phase.
Data Security Principles Almost any source of data can be an injection vector, environment variables, parameters, external and internal web services, and all types of users.
Privacy Privacy-Enhancing and Privacy-Aware methodologies and technologies, relevant legislation.
Cryptography Symmetric and asymmetric encryption, hashing algorithms, digital signatures.

Module Assessment

Assessment Breakdown	%
Course Work	50.00%
Final Examination	50.00%

Module Special Regulation

Assessments

Full Time

Course Work

Assessment Type	Continuous Assessment	**% of Total Mark**	30
Marks Out Of	0	**Pass Mark**	0
Timing	Week 7	**Learning Outcome**	2,3,4
Duration in minutes	0		

Assessment Description
Show understanding of the importance of implementing good security practices with developing software applications

Assessment Type	Continuous Assessment	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	Week 12	**Learning Outcome**	1,4
Duration in minutes	0		

Assessment Description
Develop a small piece of software to specified security requirements

No Project

No Practical

Final Examination

Assessment Type	Formal Exam	**% of Total Mark**	50
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	1,2,3,4
Duration in minutes	120		

Assessment Description
End-of-Semester Final Examination

Part Time

Course Work

Assessment Type	Continuous Assessment	**% of Total Mark**	30
Marks Out Of	0	**Pass Mark**	0
Timing	Week 7	**Learning Outcome**	2,3,4
Duration in minutes	0		

Assessment Description
Show understanding of the importance of implementing good security practices with developing software applications

Assessment Type	Continuous Assessment	**% of Total Mark**	20
Marks Out Of	0	**Pass Mark**	0
Timing	Week 12	**Learning Outcome**	1,4
Duration in minutes	0		

Assessment Description
Develop a small piece of software to specified security requirements

No Project

No Practical

Final Examination

Assessment Type	Formal Exam	**% of Total Mark**	50
Marks Out Of	0	**Pass Mark**	0
Timing	End-of-Semester	**Learning Outcome**	1,2,3,4
Duration in minutes	120		

Assessment Description
End-of-Semester Final Examination

Reassessment Requirement

A repeat examination
Reassessment of this module will consist of a repeat examination. It is possible that there will also be a requirement to be reassessed in a coursework element.

Reassessment Description
The case assignment(s) will be repeatable

Module Workload

Workload: Full Time

Workload Type	*Contact Type*	*Workload Description*	*Frequency*	*Average Weekly Learner Workload*	*Hours*
Lecture	Contact	The lecture will outline the theories of software security	Every Week	2.00	2
Practical	Contact	Implement the theories outlined in the lecture	Every Week	2.00	2
Directed Reading	Non Contact	Carry out further reading on the topics covered in lectures and labs	Every Week	2.00	2
Independent Study	Non Contact	Carry out further reading on relevant topics which have not been addresses during lectures and labs	Every Week	2.00	2
				Total Weekly Learner Workload	8.00
				Total Weekly Contact Hours	4.00

Workload: Part Time

Workload Type	*Contact Type*	*Workload Description*	*Frequency*	*Average Weekly Learner Workload*	*Hours*
Lecture	Contact	The lecture will outline the theories of software security	Every Week	2.00	2
Practical	Contact	Implement the theories outlined in the lecture	Every Week	2.00	2
Directed Reading	Non Contact	Carry out further reading on the topics covered in lectures and labs	Every Week	2.00	2
Independent Study	Non Contact	Carry out further reading on relevant topics which have not been addresses during lectures and labs	Every Week	2.00	2
				Total Weekly Learner Workload	8.00
				Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

Gollman, Dieter. (2013), Computer Security, Wiley, [ISBN: 9780470741153].

O'Reilly. (2009), Beautiful Security, [ISBN: 978059652748].

Michael Howard, David LeBlanc. (2004), Writing Secure Code, Second Edition.

Merkow, Mark S., and Lakshmikanth Raghavan Auerbach Publications. (2010), Secure and resilient software development..

Long, F., Mohindra, D., Seacord, R. C., Sutherland, D. F., & Svoboda, D. Addison-Wesley Professional.. (2011), The CERT Oracle Secure Coding Standard for Java..

Michael Goodrich Roberto Tamassia Pearson. (2018), Introduction to Computer Security, 2nd. [ISBN: 0133575470 97].

Fred Long. (2013), Java Coding Guidelines: 75 Recommendations for Reliable and Secure Software, Pearson.

This module does not have any article/paper resources

Other Resources

[website], SANS Institute,
http://www.sans.org

[Website], OWASP. (2017), OWASP Top 10,
https://www.owasp.org/index.php/Top_10-2 017_Top_10