Module 8: Information and Network Security Technologies

Stage	1
Semester	2
Module Title	Information and Network Security Technologies
Module Number	8
Module Status	Mandatory
Module ECTS Credits	5
Module NFQ level	9
Pre-Requisite Module Titles	None
Co-Requisite Module Titles	None
Capstone Module?	No
List of Module Teaching Personnel	Dr. Faheem Bukhatwa Mr Alan Hannaway Dr Mark Scanlon

Contact Hours				**Non-contact Hours**			**Total Effort (hours)**
36				**64**			**100**
Lecture	**Practical**	**Tutorial**	**Seminar**	**Assignment**	**Placement**	**Independent Work**	
24		12		12		52	

Allocation of Marks (Within the Module)					
	Continuous Assessment	**Project**	**Practical**	**Final Examination**	**Total**
Percentage Contribution	**50**			**50**	**100**

Intended Module Learning Outcomes

On successful completion of this module the learner will be able to:

1. Discuss current challenges and problems relating to the field of network security and its deployment
2. Evaluate security technologies and demonstrate an understanding of skills, tools and mechanisms in network security
3. Conduct appropriate research about emerging technologies in network security
4. Understand best practise and principles in secure software development
5. Advise on the deployment of software security mechanisms in insecure systems
6. Produce industry standard reports on insecure systems

Module Objectives

This course aims to provide the learner with the knowledge of the techniques of attacks and protection of computer networks. This course of study gives the learner a mastery of a variety of methods used in attacking or protecting networks.

Module Curriculum

- **Introduction**
  Trends of network security and network attacks including penetration and access problems and malware and virus issues.

- **Wireless networks**
  Investigating the security issues relating to wireless networks.

- **Security techniques**
  A number of concept and techniques related to network security, such as firewalls, access lists and VPNs. Network analysis security tools.

- **Software security issues,**
  Concepts of secure software and potential problems and exploitation techniques. Analysis of methodologies used in secure coding. Problems such as buffer overflow, integer overflow, heap overflow, format String Attacks etc.

- **Insecure code**
  Software reverse engineering
  The concepts of secure software development, and the secure software development lifecycle

  Report on vulnerable code, learning to producing findings on why it is vulnerable, with real world examples from NIST's SAMATE database.

Reading Lists and other learning materials

Recommended Reading

Akhgar S, 2014, *Emerging Trends in ICT Security*, Elsevier
Warren Axelrod, 2012, *Engineering Safe and Secure Software Systems*, Artech House Publishers

Secondary Reading

Mark S. Merkow, Lashmikanth Raghavan, June 2010 *Secure and Resilient Software Development,* Auerbach Publications
David Kleidermacher and Mike Kleidermacher, 2012, *Embedded Systems Security: Practicle Methods for Safe and Secure Software and Systems Development,* Newnes

Additional reading as recommended by lecturer, appropriate to topic area of security.

Module Learning Environment

Lectures and tutorials are carried out in class rooms / lecture halls or labs in the College.

Library

All learners have access to an extensive range of physical and electronic (remotely accessible) library resources. The library monitors and updates its resources on an on-going basis, in line with the College's Library Acquisition Policy. Lecturers update reading lists for this course on an annual basis as is the norm with all courses run by Griffith College.

Module Teaching and Learning Strategy

Learners are taught using a combination of lectures and tutorials.

Module Assessment Strategy

Assessing the learners includes continuous assessment carrying 50% and a final exam carrying 50% of the overall mark of the course.

Learners are continually assessed on a combination of the following work, completed during the course of the module:

Element No.	Weighting	Type	Description	Learning Outcomes Assessed
1.	10%	Tutorials	This will involve a series of tutorials. These aim at enhancing the understanding of concepts and ideas. This may also involve a programming work or producing a written technical paper format report.	1,2,3,
2.	15%	Test	This will happen during the second half of the semester. This will cover most of the topics involved during the course.	1,2,3
3.	10%	Assignment	A take home assignment focusing on the secure software development processes, principles and best practices	4, 5
4.	15%	Practical Assignment	Learners will review real world insecure code from the NIST SAMATE Database. The assignment will challenge the learner to determine why the code is vulnerable, and what can be done to produce a secure equivalent. The findings will be written in a 2 page report.	4, 5, 6,
5.	50%	Examination	End of module examination	1,2,3,4,5,6