Title:	Embedded Software Security APPROVED
Long Title:	Embedded Software Security

Module Code:	COMP8053	**Duration:**	1 Semester

Credits:	5
NFQ Level:	Advanced
Field of Study:	Computer Science
Valid From:	Semester 1 - 2017/18 (September 2017)
Module Delivered in	1 programme(s)
Module Coordinator:	Sean McSweeney
Module Author:	VINCENT RYAN
Module Description:	The emerging Internet of Things (IoT) networked world of embedded systems presents a unique and increasingly important security challenge. Malicious actors will increasingly use these systems to perform a variety of undesired activites such as identity theft and illegal remote monitoring. As many of these devices by their nature are resource starved, may or may not have an operating system and are physically accessable securing these devices requires a different skillset to traditional software security. This module provides the learner with both the technical and theoretical skills to test and harden embedded software for this new threat landscape.

Learning Outcomes	
On successful completion of this module the learner will be able to:	
LO1	Appraise the current threat and security landscape for contemporary embedded systems.
LO2	Analyse the exploitation techniques used against embedded systems and means to mitigate against such attacks.
LO3	Evaluate secure software development approaches and techniques for contemporary embedded systems and platforms.
LO4	Utilise specialized tools for testing the security of embedded software.

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 CIT module(s) it also allows for learning (in another module or modules) which is equivalent to the learning specified in the named module(s).*
Incompatible Modules *These are modules which have learning outcomes that are too similar to the learning outcomes of this module. You may not earn additional credit for the same learning and therefore you may not enrol in this module if you have successfully completed any modules in the incompatible list.*
No incompatible modules listed
Co-requisite Modules
No Co-requisite modules listed
Requirements *This is prior learning (or a practical skill) that is mandatory before enrolment in this module is allowed. You may not enrol on this module if you have not acquired the learning specified in this section.*
No requirements listed

Module Content & Assessment

Indicative Content
Introduction to Embedded Software Security Microprocessor and micro-controller security considerations, system categorization.
Threats and Exploitation Buffer overflows, integrity overflow, heap overflow, return oriented vulnerabilities, Ret2ZP, ROP, format string attacks, TPM attacks, Exploitation techniques.
Secure Embedded Development Dynamic analysis, static analysis, manual code reviews, TPM, LSM for embedded systems, limiting kernel access, identifying security and non-secure functions, encryption.
Standards and Techniques Standards, CISQ, execution space protection, data handling, integrity checking.
Tools binwalk, OpenWrt in Qemu, Firmware Modification Toolkit, GDB, SamuraiSTFU.

Assessment Breakdown	%
Course Work	50.00%
End of Module Formal Examination	50.00%

Course Work

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Project	This project will evaluate the learner's practical skills in applying the tools and techniques detailed in this module to an embedded application for security vulnerabilities. This will require the use of tools and techniques and the patching of security vulnerabilities in embedded software.	1,2,3,4	50.0	Week 9

End of Module Formal Examination

Assessment Type	*Assessment Description*	*Outcome addressed*	*% of total*	*Assessment Date*
Formal Exam	End-of-Semester Formal Exam.	1,2,3,4	50.0	End-of-Semester

Reassessment Requirement
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.*

The institute reserves the right to alter the nature and timings of assessment

Module Workload

Workload: Full Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & directed learning.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Workload: Part Time				
Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Learner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Practical computer-based lab supporting learning outcomes.	2.0	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent & directed learning.	3.0	Every Week	3.00
			Total Hours	7.00
			Total Weekly Learner Workload	7.00
			Total Weekly Contact Hours	4.00

Module Resources

Recommended Book Resources

- **Konstantinos Markantonakis and Keith Mayes 2014, *Secure Smart Embedded Devices, Platforms and Applications*, Springer [ISBN: 9781461479147]**
- **Kleidermacher, David, and Mike Kleidermacher. 2012, *Embedded systems security: practical methods for safe and secure software and systems development*, Elsevier [ISBN: 9780123868862]**

Supplementary Book Resources

- **Fei Hu 2016, *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*, CRC Press [ISBN: 9781498723183]**
- **C. Warren Axelrod 2012, *Engineering Safe and Secure Software Systems*, Artech House [ISBN: 9781608074723]**
- **Will Arthur and David Challener 2015, *A Practical Guide to TPM 2.0: Using the Trusted Platform Module in the New Age of Security*, Apress Open [ISBN: 9781430265832]**

Supplementary Article/Paper Resources

- **Ebert, C. and Jones, C. 2009, *Embedded software: Facts, figures, and future.*, Computer, vol 42 issue 4**

This module does not have any other resources

Module Delivered in

Programme Code	Programme	Semester	Delivery
CR_KDNET_8	Bachelor of Science (Honours) in Computer Systems	7	Mandatory