University of the West of Scotland

Module Descriptor

Session: 2021/22

Last modified: 09/02/2021 14:40:51

Title of Module: Malware Analysis & Reverse Engineering

Code: COMP11090	**SCQF Level: 11** (Scottish Credit and Qualifications Framework)	**Credit Points: 20**	**ECTS: 10** (European Credit Transfer Scheme)
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Sean Sturley		

Summary of Module

This module develops a deep understanding of low-level aspects of processors and code for analysing security vulnerabilities and malware. Through an initial examination of assembly language programming and machine-level instruction sets, the module will explore in detail reverse engineering methods to understand malware functionality, advanced static and dynamic analysis methods,

Anti-disassembling, anti-debugging and de-obfuscation methods. The ethical and professional issues/requirements of the professional practitioner are incorporated throughout the syllabus.

This module will work to develop a number of the key **'I am UWS' Graduate Attributes** to make those who complete this module:

Universal

- Critical Thinker
- Ethically-minded
- Research-minded

Work Ready

- Problem-Solver
- Effective Communicator
- Ambitious

Successful

- Autonomous
- Resilient
- Driven

Module Delivery Method

Face-To-Face	Blended	Fully Online
	✓	

Face-To-Face
Term used to describe the traditional classroom environment where the students and the lecturer meet synchronously in the same room for the whole provision.

Fully Online
Instruction that is solely delivered by web-based or internet-based technologies. This term is used to describe the previously used terms distance learning and e learning.

Blended
A mode of delivery of a module or a programme that involves online and face-to-face delivery of learning, teaching and assessment activities, student support and feedback. A programme may be considered "blended" if it includes a combination of face-to-face, online and blended modules. If an online programme has any compulsory face-to-face and campus elements it must be described as blended with clearly articulated delivery information to manage student expectations

Campus(es) for Module Delivery

The module will **normally** be offered on the following campuses / or by Distance/Online Learning: (Provided viable student numbers permit)

Paisley:	Ayr:	Dumfries:	Lanarkshire:	London:	Distance/Online	Other:

					Learning:	
			✓			

Term(s) for Module Delivery					
(Provided viable student numbers permit).					
Term 1	✓	Term 2		Term 3	

Learning Outcomes: (maximum of 5 statements)
On successful completion of this module the student will be able to: L1. Comprehensively understand the key attributes and behaviour of malware, malicious code implementation and the methods of malware analysis. L2. Critically evaluate the design, code and implementation of a malicious components and the steps required to reverse engineer the process. L3. Employ low level techniques and system-monitoring to examine and assess how malware interacts with the file system, registry, network and other processes, and utilise memory techniques to examine, predict and compare capabilities. L4. Identify, select and critically evaluate techniques at the forefront of the discipline used in detection strategies and the defence of systems against malicious software and software based attacks. L5. Demonstrate critical awareness of the techniques to isolate an infected system and perform malicious code analysis and reverse engineering in line with advanced professional practice.

Employability Skills and Personal Development Planning (PDP) Skills	
SCQF Headings	During completion of this module, there will be an opportunity to achieve core skills in:
Knowledge and Understanding (K and U)	SCQF Level 11. Critical and systematic knowledge and understanding of low level techniques and tools (such as assembly language programming and machine-level instruction sets) in the context of malicious code implementation.
Practice: Applied Knowledge and Understanding	SCQF Level 11. Use specialised and advanced skills, techniques and practices.
Generic Cognitive skills	SCQF Level 11. Critically identify, define, conceptualise and analyse complex problems; Demonstrate some originality and creativity; Critically review and consolidate knowledge, skills, practices and thinking in the discipline; Make judgements where data/information is limited or comes from a range of sources.
Communication, ICT and Numeracy Skills	SCQF Level 11. Use a wide range of advanced and specialised skills in support of established practices. Interpret, use and evaluate a wide range of data.
Autonomy, Accountability and Working with others	SCQF Level 11. Exercise autonomy and initiative in activities. Manage complex ethical and professional issues.

Pre-requisites:	Before undertaking this module the student should have undertaken the following:	
	Module Code:	**Module Title:**
	Other:	
Co-requisites	**Module Code:**	**Module Title:**

* Indicates that module descriptor is not published.

Learning and Teaching

Learning and teaching will take place through a variety of mechanisms, including lectures, seminars, with a collection of associated practical sessions, research into current developments and issues, and case studies. This module places an emphasis on active “hands-on” and an independent approach to learning, where students experience and develop capabilities through practical activities. Case studies will be used formatively in tutorials in order to promote application of knowledge to specific problems and encourage discussion. Topics will be introduced in lectures and discussed through guided inquiry learning activities. Additionally directed learning will reinforce essential theory and place understanding into context.

Learning Activities During completion of this module, the learning activities undertaken to achieve the module learning outcomes are stated below:	**Student Learning Hours** (Normally totalling 200 hours): (Note: Learning hours include both contact hours and hours spent on other learning activities)
Lecture/Core Content Delivery	24
Tutorial/Synchronous Support Activity	12
Laboratory/Practical Demonstration/Workshop	24
Independent Study	140
	200 Hours Total

****Indicative Resources: (eg. Core text, journals, internet access)**

The following materials form essential underpinning for the module content and ultimately for the learning outcomes:

Monnappa, K. A. (2018) Learning Malware Analysis. Packt Publishing

Elisan, C. (2015) Advanced Malware Analysis. McGraw-Hill Education

Oktavianto, D and Muhardianto, I. (2013) Cuckoo Malware Analysis. Packt Publishing

Wong, R. (2018) Mastering Reverse Engineering: Your Practical guide to master the art of Malware Reversing. Packt Publishing

Dang, B and Gazet, A. (2014) Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. John Wiley & Sons

(**N.B. Although reading lists should include current publications, students are advised (particularly for material marked with an asterisk*) to wait until the start of session for confirmation of the most up-to-date material)

Attendance Requirements

In line with the Academic Engagement and Attendance Procedure, Students are defined as academically engaged if they are regularly engaged with timetabled teaching sessions, course-related learning resources including those in the Library and on Moodle, and complete assessments and submit these on time. Please refer to the Academic Engagement and Attendance Procedure at the following link: Academic engagement and attendance procedure

Supplemental Information

Programme Board	Computing
Assessment Results (Pass/Fail)	No
Subject Panel	Business & Applied Computing
Moderator	Paul Keir
External Examiner	H Al-Khateeb
Accreditation Details	
Version Number	1.05

Assessment: (also refer to Assessment Outcomes Grids below)

Examination (50%) - The examination evaluates the students’ learning in all of the theoretical learning outcomes; students

can expect to utilise low level analysis tools, and be presented with malware/malicious documents or network flow traces similar to those introduced in the lessons.

Assignment: Report of practical work (50%) - The assignment will typically require either the analysis and/or reverse engineering of a malicious code sample; analysis/and or reverse engineering of malicious documents including memory analysis and reconstruction of artefacts.

(N.B. (i) **Assessment Outcomes Grids** for the module (one for each component) can be found below which clearly demonstrate how the learning outcomes of the module will be assessed.
(ii) An **indicative schedule** listing approximate times within the academic calendar when assessment is likely to feature will be provided within the Student Handbook.)

Assessment Outcome Grids (Footnote A.)

Component 1

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Learning Outcome (4)	Learning Outcome (5)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Unseen closed book (standard)	✓	✓		✓	✓	50	0

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Learning Outcome (3)	Learning Outcome (4)	Learning Outcome (5)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Report of practical/ field/ clinical work		✓	✓	✓	✓	50	0
					Combined Total For All Components	100%	0 hours

Footnotes
A. Referred to within Assessment Section above
B. Identified in the Learning Outcome Section above

Note(s):
1. More than one assessment method can be used to assess individual learning outcomes.
2. Schools are responsible for determining student contact hours. Please refer to University Policy on contact hours (extract contained within section 10 of the Module Descriptor guidance note).
   This will normally be variable across Schools, dependent on Programmes &/or Professional requirements.

Equality and Diversity

This module is suitable for any student. The assessment regime will be applied flexibly so that a student who can attain the practical outcomes of the module will not be disadvantaged. When a student discloses a disability, or if a tutor is concerned about a student, the tutor in consultation with the School Enabling Support co-ordinator will agree the appropriate adjustments to be made.
UWS Equality and Diversity Policy

(N.B. Every effort will be made by the University to accommodate any equality and diversity issues brought to the attention of the School)