MODULE DESCRIPTOR

Module Title

Software Security & Malware Analysis

Reference	CM3148	Version	1
Created	November 2023	SCQF Level	SCQF 9
Approved	April 2024	SCQF Points	15
Amended		ECTS Points	7.5

Aims of Module

This module aims to equip students with a comprehension of software security concepts and the ability to identify code vulnerabilities and malware through various techniques.

Learning Outcomes for Module

On completion of this module, students are expected to be able to:

1	Make judgements on code vulnerabilities in software systems.
2	Demonstrate proficiency in various methods of software code analysis.
3	Demonstrate proficiency in secure software life cycle and secure coding practices.
4	Explain techniques for malware analysis and detection.
5	Draw on expertise in implementing various methods to prevent vulnerabilities and malware.

Indicative Module Content

Categories of vulnerabilities, Common Weakness Enumeration (CWE) and Common Vulnerability Exposure (CVE), memory management vulnerabilities, structured output generation vulnerabilities, race condition vulnerabilities, API vulnerabilities, side-channel vulnerabilities, static analysis, dynamic analysis, hybrid analysis, detection and prevention of vulnerabilities, secure coding practices, secure software lifecycle, malware taxonomy, malware response, types of malware, malware analysis and detection, analysis environments, anti-analysis and evasion techniques, application of Artificial Intelligence (AI) and non-AI methods to detect vulnerabilities and malware.

Module Delivery

Key concepts are introduced and illustrated through lectures. The necessary practical skills are developed through a series of laboratory exercises.

Module Ref:	CM3148 v1

Indicative Student Workload	Full Time	Part Time
Contact Hours	30	N/A
Non-Contact Hours	120	N/A
Placement/Work-Based Learning Experience [Notional] Hours	N/A	N/A
TOTAL	150	N/A
Actual Placement hours for professional, statutory or regulatory body		

ASSESSMENT PLAN

If a major/minor model is used and box is ticked, % weightings below are indicative only.

Component 1

Type:	Coursework	Weighting:	100%	Outcomes Assessed:	1, 2, 3, 4, 5
Description:	This is a coursework in which students will demonstrate their understanding on the core concepts and various software security and malware analysis applications taught in classroom and practical sessions.				

MODULE PERFORMANCE DESCRIPTOR

Explanatory Text

The calculation of the overall grade for this module is based on 100% weighting of Component 1. An overall minimum grade of D is required to pass this module.

Module Grade	Minimum Requirements to achieve Module Grade:
A	The student needs to achieve an A in Component 1
B	The student needs to achieve a B in Component 1
C	The student needs to achieve a C in Component 1
D	The student needs to achieve a D in Component 1
E	The student needs to achieve an E in Component 1
F	The student needs to achieve an F in Component 1
NS	Non-submission of work by published deadline or non-attendance for examination

Module Requirements

Prerequisites for Module	CM1131: Cybersecurity Fundamentals or equivalent prior learning
Corequisites for module	None.
Precluded Modules	None.

INDICATIVE BIBLIOGRAPHY

1. Ransome, J. and Misra, A., 2018. Core software security: Security at the source. CRC press.
2. Gerardus Blokdyk., 2021. Software Security Vulnerability A Complete Guide, 5STARCooks
3. Bultan, T., Yu, F., Alkhalaf, M. and Aydin, A., 2017. String analysis for software verification and security (Vol. 10, pp. 978-3). Cham: Springer.
4. Senanayake, J., Kalutarage, H., Al-Kadri, M.O., Petrovski, A. and Piras, L., 2023. Android source code vulnerability detection: a systematic literature review. ACM Computing Surveys, 55(9), pp.1-37.
5. Mohanta, A. and Saldanha, A., 2020. Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware. New York, NY, USA: Apress.
6. Stamp, M., Alazab, M. and Shalaginov, A. eds., 2021. Malware analysis using artificial intelligence and deep learning (Vol. 1). Berlin/Heidelberg, Germany: Springer.