University of the West of Scotland

Module Descriptor

Session: 2022/23

Last modified: 30/09/2020 09:43:20

Title of Module: Security for the Mobile Web

Code: COMP11057	**SCQF Level: 11** (Scottish Credit and Qualifications Framework)	**Credit Points: 10**	**ECTS: 5** (European Credit Transfer Scheme)
School:	School of Computing, Engineering and Physical Sciences		
Module Co-ordinator:	Zeeshan Pervez		

Summary of Module

This module provides an overview of how the security of information in modern computing environments is assured. The approach taken starts from the position that much of the architecture, design, management, risks and controls developed to protect information in the context of distributed corporate information systems remain applicable in the world of cloud computing and the mobile web. However, the proliferation of new platforms, and recent trends such as bring-your-own-device, necessarily gives rise to new threats and the module reviews some of these and the responses to them.

The module explores each of the areas in the 2012 body of knowledge defined by the Certified Information Systems Security Professional (CISSP), emphasising those of most importance to cyber security and mobile computing. These are organised under the headings: identification and authentication, authorisation and access control, auditing and monitoring, cryptography, operations security, physical (environmental) security, network security, operating systems security and application security. As each of these areas are covered, recent threats targeting new platforms are reviewed and assessed.

- 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	HybridC	HybridO	Work-based Learning
✓					

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.

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

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.

HybridC
Online with mandatory face-to-face learning on Campus

HybridO
Online with optional face-to-face learning on Campus

Work-based Learning
Learning activities where the main location for the learning experience is in the workplace.

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 Learning:	Other:
✓						

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. Demonstrate a critical understanding of the principles of design, management and control of security on distributed computing systems.

L2. Demonstrate a critical awareness of current security issues in one or more mobile web technologies.

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. To understand the principles of design, management and control of security on distributed computing systems. To know the security threats arising in the context of cloud computing and the mobile web.
Practice: Applied Knowledge and Understanding	SCQF Level 11. To use a range of techniques, practices and policies related to the assurance of security in corporate computing systems.

Generic Cognitive skills	SCQF Level 11. To apply critical analysis and evaluation to research material on emerging issues in computer security.
Communication, ICT and Numeracy Skills	SCQF Level 11. To communicate using appropriate written and oral methods to a range of audiences.
Autonomy, Accountability and Working with others	SCQF Level 11. To deal with complex professional issues relating to responding to emerging security threats in the context of cloud computing and the mobile web.

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

The learning and teaching activities are composed by a series of lectures and laboratory sessions. The lectures are used to deliver the core knowledge and key technologies of security for modern computing systems. Details of the lectures are listed below:

1. Identification and authentication,
2. Authorisation and access control,
3. Auditing and monitoring,
4. Cryptography,
5. Operations security,
6. Physical (environmental) security,
7. Network security,
8. Operating systems security
9. Application security

The laboratory part will be used to demonstrate the applications of technologies relating to security and provide opportunities for students to research on a given aspect of security issues and produce an evaluative report of the current state of the art about the security issues.

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	18
Laboratory/Practical Demonstration/Workshop	6
Work Based Learning/Placement	24
Independent Study	52
	100 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:

Module “handbook”, lecture materials, reading lists, and assessment instruments are published on the module’s Moodle site.

Core Text (see Moodle site for the most up-to-date information):
Paperback edition:
Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. Waltham: Elsevier.
e-book edition:
Andress, J. (2011). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. [Hand-Held device, Kindle] Syngress.
Available: http://www.amazon.co.uk

Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). Available: https://www.isc2.org/CIB/CISSP-CIB.pdf

Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). https://www.isc2.org/CIB/CISSP-CIB.pdf

Sophos (2012). Security Threat Report 2013: New Platforms and Changing Threats. Available:
http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx

Students will be referred to articles in current journals on security issues. Illustrative examples:

Mansfield-Devine, S. (2013). Security review: the past year. Computer Fraud and Security. Vol.2013(1), pp.5-11.

Paessler, D. (2012). Monitoring private clouds. Network Security. Vol.2012(11), pp.8-12.

Mansfield-Devine, S. (2012). Android malware and mitigations. Network Security. Vol.2012(11), pp 12-20.

Journals (all accessible via http://www.sciencedirect.com with a UWS Athens login):

Computer Fraud and Security. Elsevier
Computers and Security. Elsevier
Network Security. Elsevier

(**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)

Engagement Requirements

In line with the Academic Engagement 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 the relevant learning platform, and complete assessments and submit these on time. Please refer to the Academic Engagement Procedure at the following link: Academic engagement procedure

Supplemental Information

Programme Board	Computing
Assessment Results (Pass/Fail)	No
Subject Panel	Business & Applied Computing
Moderator	Tom Caira
External Examiner	C Luo
Accreditation Details	
Version Number	2.08

Assessment: (also refer to Assessment Outcomes Grids below)
The presentation will assess the student's understanding of the core principles and concepts covered in the module. In the presentation, student will discuss the details of the proposed solution to a specific web and mobile security problem. (Weighted at 20%).
A laboratory notebook. Students will research the literature in a given aspect of security and produce an evaluative report of the current state of the art in that area. Generally the lab report should follow the structure: Title, Introduction, Purpose of the report, Literature review, Findings and discussion, Conclusion and References, and be written in the academic writing style. (Weighted at 80%).
(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)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Presentation	✓		20	0

Component 2

Assessment Type (Footnote B.)	Learning Outcome (1)	Learning Outcome (2)	Weighting (%) of Assessment Element	Timetabled Contact Hours
Laboratory/ Clinical/ Field notebook		✓	80	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
The University policies on equality and diversity will apply to this module: the content and assessment are based on the ability to communicate in English but are otherwise culture-neutral. When a student discloses a disability an enabling support advisor will agree the appropriate adjustments to be made, consulting with the module coordinator if necessary. 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)