CS140-15 Computer Security

24/25

Department
Computer Science
Level
Undergraduate Level 1
Module leader
Ligang He
Credit value
15
Module duration
10 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

This module covers basic theory and practice of computer security, and comes in two parts.
Part 1: Introduction to Basic Computer Security
Part 2: Detailed Investigation of Security in Practice

Module aims

This module aims to introduce this very important discipline at an introductory level. It fits very well with the aim of our degrees to equip students to become successful professionals.

Outline syllabus

This is an indicative module outline only to give an indication of the sort of topics that may be covered. Actual sessions held may differ.

- First five weeks: Introduction to basic computer security. This will cover a number of important concepts in the area of security. For example a brief history, security and security threats, practical measures (eg: identification, authentication, authorization), security models, basics of cryptography, network security.
- Second five weeks: Detailed investigation of security in practice. In this part of the course an

area, which can be used to provide specific examples and practical exploration, will be selected for more detailed investigation. This will incorporate an introduction to some of the relevant security technologies. It is likely that the specific topic under consideration will vary from year to year. As an example, the area of secure email might be considered, investigating the challenges posed, the actual threats and attacks that have occurred, what can be done/has been done to secure email, aspects of use of cryptography in securing email, etc.

Learning outcomes

By the end of the module, students should be able to:

- - Understand what is meant by computer security and be able to display knowledge of the challenges to computer security. They should understand what computer security encompasses and know the basic concepts in the field.
- - Demonstrate an appreciation of the practical aspects of computer (in)security, understand common security threats and have a basic understanding of measures to combat them.
- Demonstrate improvement in the following skills: IT, numeracy, study skills, communication.
- Demonstrate critical analysis with respect to the evaluation of system security.
- Demonstrate skills appropriate to the computer science professional in the assessment and design of secure systems.

Indicative reading list

(a) Stallings W, Cryptography and Network Security, Pearson/Prentice Hall (4th ed) 2006.
(b) Mollins R, Introduction to Cryptography, (2nd ed) 2007.
(c) Kaufman C, Network Security, Perlman and Speciner (2nd ed) 2002.
(d) Schneier B, Secrets and Lies, Wiley 2004.
(e) Anderson, R, Security Engineering, Wiley (2nd ed) 2008.
(f) Gollman, D, Computer Security, Hoboken (3rd ed) 2011.

Research element

Lecturer and students will discuss and analyse some of the knowledge points from the perspective of conducting the research, namely, not just imparting the face value and fact of a knowledge point or a technique, but teaching the students to understand the underlying principle and logic of why they exist and why the technique is designed this way.

Subject specific skills

Analytical skills by applying the security knowledge learned in this module to analyze the security-related events in daily lives
Mathmatical thinking skills by linking rigour in math with the design of the security mechanisms
Problem solving and IT skills by applying the learned knowledge to do practical lab sesssions and the courseworks Presentation and communication skills by discussing and presenting the topic issues in the seminars

Critical thinking skills by analyzing and comparing the pros and cons of different security-related techniques.

Transferable skills

Communication and presentation skills

Study

Study time

Type	Required
Lectures	20 sessions of 1 hour (13%)
Practical classes	6 sessions of 1 hour (4%)
Private study	124 hours (83%)
Total	150 hours

Private study description

- Private study for preparing the seminar discussions and presentations.
- Reading further materials given in the lectures
- Independent studies for doing the practical lab sessions
- Private studies for doing the coursework
- Revision for the final exam

Costs

No further costs have been identified for this module.

Assessment

You do not need to pass all assessment components to pass the module.

Students can register for this module without taking any assessment.

Assessment group D2

	Weighting	Study time	Eligible for self-certification
Lab sheet.	15%		No
Group Work. This assignment is group work and is not, therefore, eligible for self-certification.			
Problem solving coursework	25%		No

	Weighting	Study time	Eligible for self-certification

Group Work. This assignment is group work and is not, therefore, eligible for self-certification.

	Weighting	Study time	Eligible for self-certification
In-person Examination CS140 Exam	60%		No

- Answerbook Pink (12 page)
- Students may use a calculator

Assessment group R

	Weighting	Study time	Eligible for self-certification
In-person Examination - Resit CS140 Resit Exam	100%		No

- Answerbook Pink (12 page)
- Students may use a calculator

Feedback on assessment

Written feedback on coursework
Verbal feedback in seminars and lab sessions

[Past exam papers for CS140](#)

Availability

Courses

This module is Optional for:

- Year 1 of UCSA-G500 Undergraduate Computer Science
- UCSA-G503 Undergraduate Computer Science MEng
  - Year 1 of G500 Computer Science
  - Year 1 of G503 Computer Science MEng
- Year 1 of UCSA-I1N1 Undergraduate Computer Science with Business Studies
- Year 1 of UCSA-G406 Undergraduate Computer Systems Engineering
- Year 1 of UCSA-G408 Undergraduate Computer Systems Engineering

This module is Option list B for:

- Year 1 of UCSA-G4G1 Undergraduate Discrete Mathematics
- Year 1 of UCSA-G4G3 Undergraduate Discrete Mathematics