CS435-15 Advanced Computer Security

26/27

Department
Computer Science
Level
Undergraduate Level 4
Module leader
Feng Hao
Credit value
15
Module duration
10 weeks
Assessment
Multiple
Study location
University of Warwick main campus, Coventry

Description

Introductory description

The module aims to provide students with a thorough grounding in computer security from a system wide perspective, including language-based security, operating system security and network security, and to provide an enhanced and detailed understanding of selected advanced topics of current importance, such as quantum cryptography, proof-carrying code, etc.

Module aims

The module aims to provide students with a thorough grounding in computer security from a system wide perspective, including language-based security, operating system security and network security, and to provide an enhanced and detailed understanding of selected advanced topics of current importance, such as quantum cryptography, proof-carrying code, etc.

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.

Threats and Security policy models.
Security automata, edit automata
Network security: Firewall design.
Distributed system security.
Fair exchange.
Bitcoin.
Source location privacy.

Learning outcomes

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

- Understand the various security concepts such as confidentiality, privacy etc.
- Understand various security models.
- Understand the notion of security policy enforcement and classes of policies that runtime enforceable.
- Understand the workings of firewalls.
- Understand security in distributed systems.
- Understand notions of security in E-commerce.
- Understand the technologies and techniques that support bitcoin.
- Understand source location privacy in wireless sensor networks.

Indicative reading list

Reading lists can be found in Talis

Specific reading list for the module

Subject specific skills

CIA, threat modelling, authentication, security models, access control, symmetric cryptography, asymmetric cryptography, software security, web security, OS security, hardware security

Transferable skills

Able to critically analyze security systems identifying flaws, and able to build secure systems theoretically and practically

---

Study

Study time

Type	Required
Lectures	30 sessions of 1 hour (20%)
Practical classes	4 sessions of 1 hour (3%)
Private study	116 hours (77%)
Total	150 hours

Private study description

Background reading, secure programming practice, revision

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
Written Report	30%		No
Written Report. Roughly 2000 words, 6 page hard limit. This assignment is worth more than 3 CATS and is not, therefore, eligible for self-certification.			
Centrally-timetabled examination (On-campus)	70%		No
CS435 examination			

- Answerbook Pink (12 page)

Assessment group R2

	Weighting	Study time	Eligible for self-certification
In-person Examination - Resit	100%		No
CS435 resit exam			

	Weighting	Study time	Eligible for self-certification

- Answerbook Pink (12 page)

Feedback on assessment

Individual written feedback on each assignment

Past exam papers for CS435

Availability

Courses

This module is Optional for:

- Year 5 of UCSA-G504 MEng Computer Science (with intercalated year)
- Year 4 of UCSA-G503 Undergraduate Computer Science MEng

This module is Option list A for:

- Year 4 of UCSA-G408 Undergraduate Computer Systems Engineering
- Year 5 of UCSA-G409 Undergraduate Computer Systems Engineering (with Intercalated Year)

This module is Option list B for:

- Year 4 of UCSA-G4G3 Undergraduate Discrete Mathematics
- Year 5 of UCSA-G4G4 Undergraduate Discrete Mathematics (with Intercalated Year)