Systems security	M817

Presentation pattern: Annually May to October

Module description

The proliferation of digital systems that impact on many aspects of our daily lives, have brought with them a range of challenges, including those relating to ensuring the security of these systems. Securing these systems above requires qualified technical cyber security professionals who have the knowledge and skills required to analyse the threats against the security of these systems, evaluate suitable solutions that minimise the risk of these threats being realise, and implement these solutions and monitor their efficacy. Within the broader field of cyber security, these activities fall into the domain of **systems security**, which is the focus for this module. Students who complete M817 Systems Security will be able to:

- Analyse cyber security threats for different digital systems, using systematic methods (e.g., STRIDE);
- Evaluate the role of authentication, authorization and audit mechanisms, cryptographic techniques, methods for securing distributed systems, and techniques securing operating systems & virtualisation technologies; and
- Implement appropriate security mechanisms to mitigate the threats posed in different systems contexts.
- Assess the effectiveness of different security solutions.

The module will be organised into five blocks covering an introduction to systems security; cryptography; authentication, authorisation and accountability; operating systems and virtualisation security and distributed systems security. The main assessment component of the module will allow students to develop their own case study, enabling them to apply their learning to solve a problem that is important to their professional or personal context.

Person specification

The person specification for this module should be read in conjunction with the generic person specification for an associate lecturer at The Open University.

As well as meeting all the requirements set out in the generic person specification, you should have:

- experience of designing and developing systems security solutions, drawing on knowledge of some combination of applied cryptography, authentication, authorisation and accountability techniques, operating systems, virtualisation and distributed systems security.
- an understanding of the underlying social, professional and technical issues relevant to systems security;
- the ability to assist students in developing their knowledge in this topic and in setting this knowledge in the wider context of cyber security.
- a relevant postgraduate degree or equivalent experience.
- awareness of current Standards and legislation
- experience of teaching at postgraduate level

It would be an advantage to have:

- experience of teaching systems security at postgraduate level
- industry certifications in cyber security (e.g., CASP+, CISSP, CRTSA, etc)

Additional information

The minimum computer specification for the module is insufficient for marking assignments electronically. A large monitor (17-inch, 256 colour) would be preferable, and you may need significantly more free disk space than is recommended for students.

Module related details - a full explanation can be found on the website

Credits awarded to the student for the successful completion of a module:	30
Number of assignments submitted by the student:	2
Method of submission for assignments:	eTMA
Level of ICT requirements:	Web Intensive
Number of students likely to be in a standard group:	20
Salary band:	4
Estimated number of hours per teaching week:	6