UNIVERSITY OF LONDON | INTERNATIONAL PROGRAMMES

Royal Holloway University of London

University of London International Academy
MSc/PG Dip in Information Security
Lead College – Royal Holloway

Computer Security IYM004 (Core)

Aims

This course deals with the more technical means of making a computing system secure. This process starts with defining the proper security requirements, which are usually stated as a security policy. Security models formalise those policies and may serve as a reference to check the correctness of an implementation. The main security features and mechanisms in operating systems will be examined as well as security related issues of computer architecture. Specific well-known operating systems are then studied as case studies. Other areas investigated include the security of middleware, software protection and web security

Pre-requisites

None

Essential Reading

- Computer Security 3rd Ed. (Gollman)

Included as study material once registered on the course.

Assessment

This module is assessed by a two hour unseen written examination.

Learning Outcomes

On completion of this course students should be able to:

- Demonstrate an understanding of the importance of security models with reference to the security of computer systems.
- Describe the features and security mechanisms which are generally used to implement security policies.
- Provide examples of the implementation of such features and mechanisms within particular operating systems.
- Display a breadth of knowledge of the security vulnerabilities affecting computer systems.
- Demonstrate an understanding of the main issues relating to Web security in the context of computer systems.

Syllabus

Part 1 - Your computer:

Before looking at the theory of computer security, you are invited in Unit 1 to examine the security of your own computer. This unit is primarily intended as an introductory unit for those of you who are not already familiar with types of security features incorporated in a typical PC operating system.

***Part 2 – Computer Security theory**:*

Units 2 to 5 contain the core computer security theory of this module

In Unit 2 you are introduced to the fundamental design principles of computer security. These will be referred to throughout the rest of this module.

Unit 3 investigates the important topic of access control. You will be introduced to different ways of defining and administering access control operations. Security models are investigated in Unit 4. The usefulness of security models will be explained and several security models will be examined in some detail.

In Unit 5 we look at protection mechanisms, both those that can be implemented in hardware and those designed for implementation at operating system level. In order to understand these security controls we need to describe some background material on how computers manage memory and processes.

Part 3 – Operating system case studies

In Part 3 we illustrate the theory behind computer security by closely examining three different types of operating system:

- Unix and Linux security is examined in Unit 6;
- z/OS security is examined in Unit 7;
- Windows 2000 security is examined in Unit 8.

Part 4 - Software and application security

The last part of this module deals with security issues that affect software and applications.

In Unit 9 we look at general software security issues. We will look at the problems of designing secure software and in particular at Java security. In Unit 10 we look at web security.

This is a rather general topic, but is a good environment within which to discuss a number of important application security issues.