BSc in Computer Engineering

CMP4103
Computer Systems and Network Security

Eng Diarmuid O'Briain, CEng, CISSP

Department of Electrical and Computer Engineering,
College of Engineering, Design, Art and Technology,
Makerere University

Author

Diarmuid is a Chartered Engineer (CEng) with over 25 years experience in Telecommunications, Information Networking and Security. He has designed and implemented next-generation networks and information security solutions for major multi-national communications companies as well as serving as Chief Technical Officer for an Irish Internet Service Provider for over 5 years. Since 1999 he has also lectured on Telecommunications and Computing programmes at both the Dublin Institute of Technology (DIT) and the Institute of Technology, Carlow (ITC) in Ireland.

Table of Contents

This page is intentionally blank

1. Module Aims

The aim of this course is to discover what is computer security, especially as it relates to the protection of information stored on the computers and exchanged between computers The Computer Engineering student will be equipped with knowledge and skills in advanced cryptography, access control, distributed authentication, TCP/IP security, firewalls, IPSec, Virtual Private Networks, intrusion detection systems, and advanced topics such as wireless security, identity management.

2. Objectives

- To familiarise the student with the concept of system security analysis.
- To introduce access control methods and various security models.
- To equip the student with skills of identification and authentication in the security domain.
- To introduce the various security concerns associated with the most popular operating systems – GNU/Linux, UNIX and Windows.
- To introduce the concept of communication security.
- To equip the student with various cryptography systems.
- To introduce the student to the security concerns applicable to the Internet.
- To introduce the student to the various e-commerce security protocols.

3. Learning Outcomes

On completing this course the student should be able to:

- Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
- Enumerate set programming techniques that enhance security.
- Explain the various controls available for protection against internet attacks, including authentication, integrity check, firewalls, and intruder detection systems.
- Describe the different ways of providing authentication of a user or program.
- Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
- Describe the background, history and properties of widely-used encryption algorithms such as DES, AES, and RSA.
- Describe legal, privacy and ethical issues in computer security.
- List and explain the typical set of tasks required of a system security administrator.

4. Teaching and Learning Strategies

Formal lectures, group-based activities, class discussion, case studies and laboratory sessions may be used in the presentation of this module. Typically the lectures will include practical sessions providing students with the immediate opportunity to implement and reinforce the material presented in the lectures.

5. Module Lectures

Lecture 1	Information Security, Governance and Risk Management
Lecture 2	Security Architecture and Design
Lecture 3	Cryptography
Lecture 4	Physical Security and Access Control
Lecture 5	Virtualisation
Lecture 6	Systems: Threats, Vulnerabilities and Risks
Lecture 7	Secure Software Development
Lecture 8	Project Management
Lecture 9	Network Security and Penetration Testing
Lecture 10	Legal, Regulations, Investigations and Compliance
Lecture 11	Business Continuity and Disaster Recovery Planning
Lecture 12	Operations Security

6. Assignments

All assignments will be submitted in both Open Document Format (ODF) and Portable Document Format (PDF). Assignments will be typed in FreeSans or Arial font size 12 single spaced with the text paragraphs justified. The header on each page must include on a single line the title of the assignment in bold type FreeSans or Arial font, size 10.5 while the footer should include the authors name, e-mail address and the page number, all again in font size 10.5 FreeSans or Arial. A coversheet will also be included which will have the assignment title and author's name in font FreeSans or Arial, size 14 bold typeface centred on the page both horizontally and vertically. Header and footer will be separated from the body text by a horizontal line.

Assignments will NOT be accepted after the deadline.