Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS Credits	Module Code	**Module Title**
		5	CMPU3034	Security

8.3.5. Security

Module author: Dr. Fredrick Mtenzi.

Module Description:

Recent developments in the computing technology, mobile device technologies and the increasing broadband availability globally are shaping our lives in ways unimaginable a few years ago. While these developments have provided an unprecedented access to information and connectivity, they have also led to increased security concerns regarding the safety of our systems, data and wellbeing. The rush to market software which forms the trend of most of the modern technology has enhanced the release of insecure software.

This module provides an overview of the fundamental concepts of security. It will introduce students to the basic principles of securely using computers, wired and wireless networks and the internet. Emphasis will be placed on understanding issues which will lead to sensible security and an appreciation that security is the weakest link problem. The user security social responsibility which is becoming more important now will be covered in the legal and ethical aspects of security. Relevant concepts covered in the module will the subject of student experiments in the labs.

Module aim

The aim of this module is

- to introduce the students to the security principles,
- to give the students a thorough understanding of the network security issues,
- to provide them with sound practical knowledge of security tools, Operating Systems and Network security,
- to provide them with an in-depth practical security knowledge in real-life.

Learning Outcomes:

On completion of this module, the student will be able to:

- Define and describe network security,
- Discuss and relate the fundamental concepts of Security,
- Classify and analyse the nature and threat from malware,
- Design and deploy best practice techniques for securing Operating Systems and Networks,
- Compare and contrast different security tools and determine their appropriate use in a specific situation,
- Examine the trade-off of legal and ethical security issues in an organisation

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS Credits	Module Code	**Module Title**
		5	CMPU3034	Security

- Asses and rank different systems security approaches according to the protection they provide in real-life applications.
- Recognise and deploy the different hacking phases in systems.

Learning and Teaching Methods:

In this module a number of teaching methods may be employed including lectures, practical sessions, tutorials and case studies. At least one industrial seminar may be arranged. Focus should be placed on empowering the students to develop their skills independently of the presence of a tutor or lecturer.

Module content:

- Introduction to security
- Classical encryption techniques and stream ciphers
- User Authentication
- Access Control
- Physical and Infrastructure Security
- Operating Systems Security
- Network Security
- Security Tools
- Introduction to ethical hacking
- The role of people in security
- Legal and ethical aspects of security

Module Assessment

This module should have a 50% weighting for the examination and a 50% weighting for the continuous assessment. While it is important that the student can demonstrate their technical ability with coursework, it is equally important that they demonstrate an understanding of the theoretical aspects of security.

Essential Reading: (author, date, title, publisher)

William Stallings, 2005, Cryptography and Network Security: Principles and Practice, 5th ed, Prentice Hall

Supplemental Reading: (author, date, title, publisher)

Seymour Bosworth and M.E. Kabay, 2009, Computer Security Handbook, John Wiley & Sons. Inc.

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS Credits	Module Code	**Module Title**
		5	CMPU3034	Security

William Stallings and Lawrie Brown, 2008, Computer Security: Principles and Practice, Prentice Hall

Markus Jakobsson, Zulfikar Ramzan, 2008, Crimeware: Understanding New Attacks and Defences, Symantec Press.

Charles P. Pfleeger and Shari Lawrence Pfleeger, 2007, Security in Computing, Prentice hall

Michael Gregg, 2008, Certified Ethical Hacker, Que Publishing

Vincent Nestler, Gregory White, Wm. Arthur Conklin and Corey Schou , 2010, Principles of Computer Security CompTIA Security+ and Beyond Lab Manual, McGraw-Hill Companies

Web references, journals and other:

IEEE security & privacy

ACM Transactions on Information and System Security (TISSEC)

http://www.sans.org/rr/

Further Details:

The module will run over one semester, with three contact hours per week. Two hours for lectures and one hour for the laboratory.

Date of Academic Council approval …….