Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4008	Advanced Security 2

8.8.2. Advanced Security 2

Module author: Dr. Fredrick Mtenzi.

Module Description:

In the last few decades, computers, mobile devices, networks and the Internet have become an integral part of our social fabric. As computer, networks and the Internet are used for communication and for varieties of online interactions and transactions, security has become the key issue in today's information technology world. Information security is required at all levels – the personal level, corporate level, and country level. There is a steady rise in the occurrence of security attacks. Security is a broad issue which is becoming increasingly important as computer networks become more widespread. It encompasses computer- and network-related crime, privacy issues, trust and confidence, and dependability of critical infrastructures. The evidence of the security threat is growing and new vulnerabilities are found each day. Those interested in exploiting these vulnerabilities are becoming a well-organized. Security threats are taking a variety of forms, including espionage, hacking, identity theft, crime, and terrorism. The level of sophistication and speed of development of the tools being used to create security breaches and attacks are growing exponentially.

With the increasing concern for safety and integrity of information against security attacks, it has become mandatory that organizations follow strict guidelines and security framework to assure the safety and protection of data and systems. To address these needs this module has will provide a detailed understanding of the issues involved in providing systems security. Further, the module will examine and critically analyze the security challenges faced by the society and the computing industry. It will elaborate and demonstrate the role of security in design, implementation and deployment of secure systems.

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 knowledge of provision of an enterprise secure systems, security audit and compliance,
- to provide them with an in-depth practical enterprise security.

Learning Outcomes:

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

- Define and explain the components of network security,
- Discuss, relate and organise the fundamental concepts of Security,

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4008	Advanced Security 2

- Classify and analyse the nature and threat from malware,
- Design and develop best practice techniques of mitigating security threats,
- Critically analyze different aspects of security such as security testing, evaluation, auditing and policies,
- Assess security compliance of an organisation
- Compare and contrast international and regional security standards, legislations and laws.
- Asses and rank different systems security approaches according to the protection they provide in real-life applications.
- Recognise and justify the different scenarios of deploying systems security approaches.

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:

- Authentication Applications,
- Electronic Mail Security,
- Internet Protocol Security,
- Web security,
- Intruders, Crimeware, Firewalls
- Security Policies, Standards, Compliance
- Security Metrics and Auditing
- Penetration Testing
- Defences to security attacks
- The effect of Technological developments on 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.

Pre-Requisite Modules code(s)	Co-Requisite Modules code(s)	ECTS credits	Module Code	**Module Title**
		5	CMPU4008	Advanced Security 2

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.

Andrew Lockhart, 2004, Network Security Hacks 100 Industrial-Strength Tips & Tools, O'Reilly

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

Ed Skoudis and Tom Liston, 2006, Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and Effective Defences, Prentice hall

Bruce Schneier, 2004, Secrets and Lies: Digital Security in a Networked World, Hungry Minds Inc

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 ……