Computer Security Techniques Course Specifications

Course Specifications

Program(s) on which the course is given: Bachelor of Computers and Information Sciences

Major or Minor element of programs **:** Computer Systems / Computer Science

Department offering the program **:** Computer Science

Department offering the course **:** Computer Systems

Academic year / Level **:** 4th Year/B.Sc.

Date of specification approval **:** 1/03/2010

Basic Information

Title: Computer Security Techniques **Code:** CHW 464

Lecture: 3 hrs/week **Tutorial:** 2 hrs/week **Practical:** ---

Credit Hours: --- **Total:** 5 hrs/week

Professional Information

1. Overall Aims of Course:

The "Computer Security Techniques" course is a fourth year undergraduate course that introduces students to the subject of Information Security from the technical point of view. The purpose of this course is to help students in learning the principles of computer information security in general and of constructing secure systems in particular. It familiarizes students with the aspects of information security: security attacks, security mechanisms, and security services. Since cryptographic techniques underlie many of the security mechanisms in use, this course covers the development, use and management of such techniques. It also introduces authentication techniques, access control mechanisms, and how security assurance is achieved on computer networks.

2. Intended Learning Outcomes of Course (ILOs):

a. Knowledge and Understanding:

a1- Articulate the principles of computer and information security.

a2- Describe the types of attacks and malicious code that may be used against a computer system; threats and countermeasures.

a3- Describe similarities and differences among various symmetric and public key cryptographic techniques.

a4- Explain discretionary , mandatory, and role-based access control models.

a5- Technologies and concepts used for providing secure communications channels, secure internetworking devices, and network medium;

a6- Describe the risk assessment techniques and the types of security policies.

a7- Describe the role and types of intrusion detection systems, firewalls, and physical security concepts

b. Intellectual Skills:

b- Appraise and appreciate the information security needs of an organization

b2- Interpret how to evaluate and select various information security encryption techniques

b3- Appraise security threats to networked systems and make decisions regarding network security practice.

c. Professional and Practical Skills:

c1- Implement cryptography algorithms and techniques.

c2- Describe and apply security protocols for securing networked system data and access.

d. General and Transferable Skills:

d1-Discuss high awareness of how to protect data and resources from disclosure, to guarantee the authenticity of data and messages and to protect computer systems from network-based attacks.

d2- Develop research skills and extend professional knowledge to clarify problems and take responsibility for furthering own learning.

3. Contents:

Topic	No. of hours	Lecture	Tutorial/Practical
Overview of Information Security	5	3	2
Attackers and their attacks	5	3	2
Security Basics	5	3	2
Traditional Symmetric-Key Ciphers	5	3	2
Modern Symmetric-Key Ciphers	5	3	2
Asymmetric Key Cryptography	5	3	2
Message Integrity and Authentication	5	3	2
Hash Functions and Digital Signature	5	3	2
Entity Authentication	5	3	2
Key Management	5	3	2
Securing the Network Infrastructure	5	3	2
Operational Security	5	3	2
Security Policies and Procedures	5	3	2