University: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

College/Faculty: \_\_\_\_\_\_\_\_\_\_\_\_

Course title: Computer Security

Course code: COSC4035

Credit hours: 3 ECTS: 5 Contact hrs: 2 Lab hrs: 3 Tutorial hrs: 1

Prerequisite: CoSc2032-Data Communications and Computer Networks

Course category: compulsory

Year: IV Semester: I

**Course Description**

To familiarize students with the security issues and technologies involved in modern information systems, including computer systems and networks and the various ways in which information systems can be attacked and tradeoffs in protecting networks.

**Course objectives**

By the end of this course, students will be able to:

* Understand the basic concepts in information security, including security attacks/threats, security vulnerabilities, security policies, security models, and security mechanisms
* Understand the concepts, principles and practices related to elementary cryptography, including plain-text, cipher-text, the four techniques for crypto-analysis, symmetric cryptography, asymmetric cryptography, digital signature, message authentication code, hash functions, and modes of encryption operations.
* Understand issues related to program security and the common vulnerabilities in computer programs; including buffer overflow vulnerabilities, time-of-check to time-of-use flaws, incomplete mediation.
* Explain and compare security mechanisms for conventional operating systems, including memory, time, file, object protection requirements and techniques and protection in contemporary operating systems.
* Understand the basic requirements for trusted operating systems, and describe the independent evaluation, including evaluation criteria and evaluation process.
* Describe security requirements for database security, and describe techniques for ensuring database reliability and integrity, secrecy, inference control, and multi-level databases.
* Describe threats to networks, and explain techniques for ensuring network security, including encryption, authentication, firewalls, and intrusion detection.
* Explain the requirements and techniques for security management, including security policies, risk analysis, and physical threats and controls.

**Course outline**

**Chapter 1: Introduction to Computer Security (3 hrs)**

* 1. Basic concepts of computer security
	2. Threats, vulnerabilities, controls, risk
	3. Goals of computer security
	4. Security attack
	5. Security policies and mechanisms
	6. Prevention, detection, and deterrence
	7. Software security assurance

**Chapter 2: Computer Threat (4 hrs)**

* 1. Malicious code
		1. Viruses
		2. Trojan horses
		3. Worms
		4. Spy-wares, etc.
	2. Class of Attacks
		1. Reconnaissance
		2. Access
		3. Denial of Service, etc.
	3. Program flaws
		1. Buffer overflows
		2. Time-of-check to time-of-use flaws
		3. Incomplete mediation
	4. Controls to protect against program flaws in execution
		1. Operating system support and administrative controls
	5. Program Security Defenses
		1. Software development controls and Testing techniques
		2. Database management systems security

**Chapter 3: Cryptography and Encryption Techniques (13 hrs)**

* 1. Basic cryptographic terms
	2. Historical background
	3. Cipher Techniques
		1. Transposition Cipher
		2. Substitution Cipher
	4. Conventional encryption algorithms
	5. Cryptanalysis
	6. Cryptographic Systems
		1. Symmetric key cryptography
			1. DES
			2. 3DES
			3. AES
			4. Block Cipher Modes
		2. Public key cryptography
			1. Diffie-Hellman
			2. RSA
		3. Digital Signature
			1. Using Public Key
			2. Using Message Digest
				1. MD4family
				2. SHA family
				3. RIPEMD
		4. Public key Infrastructure (PKI)
			+ 1. Trusted Third Party
				2. Certification
				3. Key Distribution
				4. PKI Topology
				5. Enrollment and Revocation Procedures

**Chapter 4: Network Security (4 hrs)**

* 1. Network security basics
	2. Threats on network
	3. Trust, Weaknesses, Risk and Vulnerabilities
	4. TCP/IP Suit Weaknesses and Buffer Overflows
	5. Network security protocols
		1. Application layer security
			1. Web security
			2. E-mail security
		2. Transport layer security
		3. Network layer security
		4. Link layer security
		5. Physical security
	6. Wireless security

**Chapter 5: Security Mechanisms (3 hrs)**

* 1. Firewall
	2. Proxy server
	3. IDS/IPS
	4. Virtual Private network

**Chapter 6: Authentication and Access control (3 hrs)**

* 1. Authentication basics
		1. Password and Passphrase
		2. Biometrics
			1. Fingerprint
			2. Palm Scan
			3. Hand Geometry
			4. Iris Scan
			5. Signature Dynamics
			6. Voice Print
			7. Facial Scan
			8. Hand Typography
		3. AAA server
		4. Smart card and memory cards
		5. Kerberos
	2. Access control basics
	3. Access control models
		1. Discretionary Access Control (DAC)
		2. Mandatory Access Control (MAC)
		3. Role-Based Access Control (RBAC)

**Chapter 7: Administering security (2 hrs)**

* 1. Security planning
	2. Risk analysis
	3. Security policies
	4. Cyber security
	5. Ethics

**Lab content: using OpenSSL**

Lab 1: Installing and configuring OpenSSL

Lab 2: Introduction and commands used in OpenSSL

Lab 3: Encryption using conventional algorithms

Lab 4: Symmetric encryption with OpenSSL

Lab 5: Encrypting file using DES

Lab 6: Asymmetric encryption with OpenSSL

Lab 7: Encrypting file using RSA

Lab 8: Combination of DES and RSA

Lab 9: Digital Certification with OpenSSL

Lab 10: Digital Signature

**Assessment methods**

|  |
| --- |
| Assignment/quizzes 10 % |
| Mid semester examination 20% |
| Project ` 20% |
| Final examination 50% |

**Text books:**

* Security in Computing, Charles P. Pfleeger and Shari L. Pfleeger. (3rd edition), Prentice-Hall, 2003

**References:**

1. Computer Security, Dicter Gouman, John Wiley & Sons
2. Computer Security: Art and Science, Mathew Bishop, Addison-Wesley
3. Principles of Information Security, Whitman, Thomson.
4. Network security, Kaufman, Perl man and Speciner, Pearson Education
5. Cryptography and Network Security, 5th Edition William Stallings, Pearson Education
6. Introduction to Cryptography, Buchmann, Springer.