



National Computing Education Accreditation Council NCEAC



NCEAC.DOC.001-E

COURSE DESCRIPTION

NAME OF INSTITUTION	Lahore Garrison University
PROGRAM (S) TO BE EVALUATED	Computer Science , Spring 2022

Course Description : Provides an introduction and overview of information security/assurance for incoming students. This course will enhance technical, communication, problem solving and teaming skills, as students relate to the study of Information Security and Information Assurance. This course will cover an introduction to cryptography, intrusion detection systems, data firewalls, malicious software, information operations and warfare, and denial of service attacks, regulations, law and governance.

Course Code	CSC736																		
Course Title	Network Security																		
Credit Hours	3																		
Prerequisites by Course(s) and Topics	N/A																		
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	SESSIONAL (Quizzes, Assignments, Presentations) =25 % Midterm Exam =25 % Final Exam = 50%																		
Course Coordinator	Dr. Ishtiaque Mahmood																		
URL (if any)																			
Current Catalog Description																			
Textbook (or Laboratory Manual for Laboratory Courses)	Principles of Information Security Michael E. Whitman, Herbert J. Mattord																		
Reference Material	Computer Security: Art and Science, Matthew Bishop • Principles of Information Security 3rd E by Michael E. Whitman and Herbert J. Mattord • Corporate & Network Security, Raymond R. Panko																		
Course Goals	At the end of this course, students will be able to: Explain key concepts of information security such as design principles, cryptography, risk management, and ethics Discuss legal, ethical, and professional issues in information security. Apply various security and risk management tools for achieving information security and privacy. Identify appropriate techniques to tackle and solve problems in the discipline of information security.																		
Course Learning Outcomes (CLOs):	<table><tr><td>At the end of the course the students will be able to:</td><td>Domain</td><td>BT Level*</td></tr><tr><td>Examine and apply the fundamental techniques of computer security.</td><td></td><td></td></tr><tr><td>Identify and explain risk and potential security issues.</td><td></td><td></td></tr><tr><td>Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society.</td><td></td><td></td></tr><tr><td>Demonstrate foundation knowledge of information security/assurance within the organization.</td><td></td><td></td></tr><tr><td>* BT= Bloom's Taxonomy, C=Cognitive domain, P=Psychomotor domain, A= Affective domain</td><td></td><td></td></tr></table>	At the end of the course the students will be able to:	Domain	BT Level*	Examine and apply the fundamental techniques of computer security.			Identify and explain risk and potential security issues.			Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society.			Demonstrate foundation knowledge of information security/assurance within the organization.			* BT= Bloom's Taxonomy, C=Cognitive domain, P=Psychomotor domain, A= Affective domain		
At the end of the course the students will be able to:	Domain	BT Level*																	
Examine and apply the fundamental techniques of computer security.																			
Identify and explain risk and potential security issues.																			
Demonstrate responsible computer use as it deals with social, political, legal and ethical issues in today's electronic society.																			
Demonstrate foundation knowledge of information security/assurance within the organization.																			
* BT= Bloom's Taxonomy, C=Cognitive domain, P=Psychomotor domain, A= Affective domain																			

Topics Covered in the Course, with Number of Lectures on Each Topic (assume 15-week instruction and one-hour lectures)	Week	Lecture	Topics Covered
	Week 1	1	Objective and Motivation, Introduction,
		2	Course Contents. History of Secure Systems
	Week 2	3	Basic Principles (Information Security, Confidentiality Integrity, Availability).
		4	Authentication Models (Authentication, Authorization),
	Week 3	5	Access Control Models (MAC, DAC, RBAC, TBAC), Formal Security Models
		6	Security Kernels including History of Kernels Security, OS Protection Principles, OS Protection Objects, Trusted OS Concepts
	Week 4	7	Cryptography Algorithms (Symmetric vs. Asymmetric Algorithms)
		8	Digital Signature, CAs
	Week 5	9	Symmetric Algorithms including Data Encryption Standard (DES)
		10	3DES (Triple DES) Blowfish, Two fish
	Week 6	11	IDEA (International Data Encryption Algorithm)
		12	RC4, RC5, RC6
	Week 7	13	AES (Advanced Encryption Standard)
		14	Asymmetric Key Algorithms (Diffie- Hellman), RSA (Rivest-Shamir-Adleman)
	Week 8	1 hours	Mid Term
	Week 9	15	El Gamal Elliptic curve cryptosystem (ECC)
		16	Digital Signature Algorithm (DSA)
	Week 10	17	Message Digest
		18	Secure Hash Algorithm
	Week 11	19	Stateless Protocol, Network-based, Host- based, Network Behavior Analysis (NBA), Wireless IDPS, IDPS
		20	Host and Network Security Requirements, Types of Threats, Interruption
	Week 12	21	Host and Network Security Requirements
		22	Policy Formation and Enforcement including Information Security Policy Standards and Practices
	Week 13	23	Policy Management, Military Security Policy, Commercial Security Policies,
		24	Software Security Issues, Handling program input safely, Writing safe program code, Interacting with O/S and other programs
	Week 14	25	Database Security, Database Policy Formulation and Enforcement, Database Administration, Database Policies, Access Privilege Policies
		26	Prevention of unauthorized access, Intentional or accidental to database
	Week 15	27	Legal and Social Security Issue including Law and Ethics in Information Security, Relevant U.S. Laws (General), Privacy of Customer Information
		28	Digital Millennium Copyright Act (DMCA), United Nations Charter, Policy Versus Law
	Week 16	29	Information Security and Human Aspects (Social Engineering)
		30	Phishing Techniques
	Week 17	2 hours	Final Term
Laboratory Projects/Experiments Done in the Course			
Programming Assignments Done in the Course			

Instructor Name Dr. Ishtiaque Mahmood

Instructor Signature

Date

