NCEAC.FORM.001-D

**COURSE DESCRIPTION FORM INSTITUTION** \_National University of Computer & Emerging Sciences

(FAST-NUCES) Karachi\_

**PROGRAM (S) TO BE EVALUATED**

A. **Course Description**

BS (Computer Science) / BS (Software Engineering) / BS (Artificial Intelligence) / BS

|  |  |
| --- | --- |
| **Course Code** | **CS3002** |
| **Course Title** | Information Security (Fall 2024) |
| **Credit Hours** | 3 |
| **Prerequisites by**  **Course(s) and Topics** | CS3001 Computer Networks |
| **Assessment Instruments with Weights** (homework, quizzes, midterms, final, programming assignments, lab work, etc.) | Labs / Assignments / Quizzes – 10% (minimum 4) Project – 10%  Mid-Term 1 Exam – 15% Mid-Term 2 Exam – 15% End-Term Exam – 50% |
| **Course Coordinator** | Dr. Sufian Hameed |
| **URL (if any)** |  |
| **Current Course**  **Description** | Information security foundations, security design principles; security mechanisms, symmetric and asymmetric cryptography, encryption, hash functions, digital signatures, key management, authentication and access control; software security, vulnerabilities and protections, malware, database security; network security, firewalls, intrusion detection; security policies, policy formation and enforcement, risk assessment, cybercrime, law and ethics in information security, privacy and anonymity of data. |
| **Textbook** (or **Laboratory Manual** for Laboratory Courses) | 1– Computer Security, Principles and Practice, William Stallings, 4th Edition, Pearson  Publication, 2018 (Main Textbook for Theory)  2- Computer and Internet Security, A Hands-On Approach, Wenliang Du, 3rd Edition, Create Space Publications, 2022 (for Labs) |
| **Reference Material** | 1- Cryptography and Network Security: Principles and Practice, William Stallings, 8th  Edition, Pearson Publication, 2020.  2- Principles of Information Security, M. Whitman and H. Mattord, 7th Edition, CENGAGE Learning Inc., 2022 |
| **Course Goals** | In this course, students learn basics of information security, in both management aspect and technical aspect. Students understand of various types of security incidents and attacks, and learn methods to prevent, detect and react incidents and attacks. Students will also learn basics of application of cryptography which are one of the key technologies to implement security functions. In the last session, teams of students will make presentation of their study project for a topic related to information security. |

NCEAC.FORM.001-D

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | | | | | | | | | | |
|  | **CLO** | | **Course Learning**  **Outcome (CLO)** | **Domain** | **Taxonomy**  **Level** | **PLO** | **Tools** | | |  |
| **01** | | **Explain** key concepts of information security such as design principles, cryptography, risk management, and ethics | Cognitive | C2  (Explain) | **1** | **A1, A2, M1, M2, P, F** | | |
| **02** | | **Discuss** legal, ethical,  and professional issues  in information security. | Affective | A2 (Discuss) | **6** | **A3, A4, P, M2, F** | | |
| **03** | | **Analyze** real world scenarios, model them using security measures, and apply various security and risk management tools for achieving information security and privacy | Cognitive | C4  (Analyzing) | **2** | **A3, A4 M2, P, F** | | |
| **04** | | **Identify** appropriate techniques to tackle and solve problems of real life in the discipline of information security | Cognitive | C4 (Identify) | **3** | **A1, A2, M1, M2, P, F** | | |
| **05** | | **Understand** issues related to ethics in the field of information security | Cognitive | C2  (Understanding) | **8** | **A4, P, F** | | |
| ***Tool****: A = Assignment, P = Project, M = Mid-term (M1 and M2), F=Final (End-term)* | | | | | | | | |
|  | **B. Program Learning Outcomes** | | | | | | |  |
|  | For each attribute below, indicate whether this attribute is covered in this course or not. Leave the cell blank if the enablement is little or non-existent. | | | | | | |  |
| 1.Computing Apply knowledge of mathematics, natural sciences, Knowledge: computing fundamentals, and a computing  specialization to the solution of complex computing problems. | | | | | | | ⏺ | |
| 2.Problem Identify, formulate, research literature, and analyse Analysis: complex computing problems, reaching substantiated conclusions using first principles of  mathematics, natural sciences, and computing sciences. | | | | | | | ⏺ | |
| 3.Design/Develop Design solutions for complex computing problems and Solutions: design systems, components, and processes that meet specified needs with appropriate consideration for  public health and safety, cultural, societal, and environmental considerations. | | | | | | | ⏺ | |
| 4.Investigation & Conduct investigation of complex computing problems  Experimentation: using research-based knowledge and research-based methods. | | | | | | |  | |

NCEAC.FORM.001-D

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | 5. Modern Tool Create, select, and apply appropriate techniques, Usage: resources and modern computing tools, including prediction and modelling for complex computing  problems. | | | | | | | | | | | | | | | ⏺ |  | |
| 6.Society Apply reasoning informed by contextual knowledge Responsibility: to assess societal, health, safety, legal, and cultural issues relevant to context of complex computing  problems. | | | | | | | | | | | | | | |  |
| 7.Environment Understand and evaluate sustainability and impact of and Sustainability: professional computing work in the solution of  complex computing problems. | | | | | | | | | | | | | | |  |
| 8. Ethics: Understand and commit to professional ethics, responsibilities, and norms of professional computing practice. | | | | | | | | | | | | | | | ⏺ |
| 9.Individual and Function effectively as an individual, and as a  Team Work: member or leader in diverse teams and in multi- disciplinary settings. | | | | | | | | | | | | | | |  |
| 10. Communicate effectively on complex computing  Communication: activities with the computing community and with society at large. | | | | | | | | | | | | | | |  |
| 11.Project Demonstrate knowledge and understanding of Management and management principles and economic decision Finance: making and apply these to one's own work as a  member or a team. | | | | | | | | | | | | | | |  |
| 12.Life-long Recognize the need for, and have the preparation Learning: and ability to engage in independent and life-long learning in the broadest context of technological  changes. | | | | | | | | | | | | | | |  |
| **C. Relation between CLOs and PLOs**  (CLO: Course Learning Outcome, PLOs: Program Learning Outcomes) | | | | | | | | | | | | | | | |
|  | | | **PLOs** | | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | |
| **CLOs** | 1 | | ● |  |  |  |  |  |  |  |  |  |  |  | |
| 2 | |  |  |  |  |  | ● |  |  |  |  |  |  | |
| 3 | |  | ● |  |  |  |  |  |  |  |  |  |  | |
| 4 | |  |  | ● |  |  |  |  |  |  |  |  |  | |
|  | 5 | |  |  |  |  |  |  |  | ● |  |  |  |  | |
| **Topics Covered in the Course, with Number of Lectures on Each Topic** (assume 15-week instruction and three one-hour lectures per week) |  | **Week**  **#** | | **Topic** | | | | | | | | | **Reference Text** | | | | | |  |
| 1 | | **Information Security Foundations**: Concepts, Threats and Attacks, Design Principles, Strategy and Standards | | | | | | | | | Main Textbook, Chapter 1  Sections 1.1, 1.2, 1.4, 1,6,  1,7 | | | | | |
| 2 | | **Cryptographic Tools**: Confidentiality with Symmetric Encryption, DES & AES, Message Authentication and Hash Functions | | | | | | | | | Textbook Chapter 2, Sections 2.1 and 2.2  Details in Chapter 20 & 21 | | | | | |

NCEAC.FORM.001-D

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | 3 | **Cryptographic Tools:** Public Key Encryption, RSA  **ASSIGNMENT # 1**  **ASSIGNMENT # 1** | Textbook Chapter 2, Section 2.3  Details in Chapter 21 |  |
| 4 | **Cryptographic Tools:** Digital Signatures and  Key Management | Textbook Chapter 2, Section 2.4 |
| 5 | **User Authentication:** Digital User Authentication Principles, Password based authentication  **ASSIGNMENT # 2** | Textbook Chapter 3, Sections 3.1 to 3.2 |
| **MIDTERM-I EXAM** | | |
| 6 | **User Authentication:** Token-based, and Biometric authentication and related security issues | Textbook Chapter 3, Sections 3.3 to 3.6 |
| 7 | **Access Control**: Principles, Discretionary Access Control, Role-based Access Control and Attribute based Access Control  **ASSIGNMENT # 3** | Textbook Chapter 4, Sections 4.1 to 4.7 |
| 8 | **Database Security:** Need, SQL Injection Attacks, Database Access Control and Database Encryption | Textbook Chapter 5, Sections 5.1 to 5.7 |
| 9 | **Malicious Software:** Types, Propagation, Payload, and Countermeasures  **ASSIGNMENT # 4** | Textbook Chapter 6, Sections 6.1 to 6.10 |
| **MIDTERM-II EXAM** | | |
| 10 | **Intrusion Detection**: Basics, Types and  Examples | Textbook Chapter 8, Sections 8.1 to 8.6 |
| 11 | **Firewalls and Intrusion Prevention**: Basics, Types, and Prevention Systems | Textbook Chapter 9, Sections 9.1 to 9.3 and 9.6 |
| 12 | **Software Security:** Software Vulnerabilities and Protection Mechanisms | Textbook Chapter 11, Sections 11.1 to 11.3 |
| 13 | **IT Security Management and Risk Assessment:** security policies, policy formation and enforcement, risk assessment | Textbook Chapter 14, Sections 14.1 to 14.3 |
| 14 | **Legal and Ethical Aspects:**  Cybercrime, Intellectual Property, Privacy and  Anonymity of Data and Ethical Issues.  **PROJECT SUBMISSION** | Textbook Chapter 19, Sections 19.1 to 19.4 |
| 15 | **Topics of Current Interests (Research**  **Topics)** | Research Papers (IEEE/ ACM and other digital libraries) |
| 16 | **PROJECT PRESENTATIONS** |  |
| **END-TERM EXAM** | | |

NCEAC.FORM.001-D

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  | | | |  |
| **Laboratory Projects/Experiments Done in the Course** | Students will be given assignments related to the theory concepts they learn in classroom lectures. A project (research / development) discussing issues related to the state-of-the-art information security concepts will also be assigned. | | | | | |
| **Programming Assignments Done in the Course** | A few programming labs are given to apply the key concepts of information security. | | | | | |
| **Class Time Spent on**  (in % credit hours) | **Theory** | | **Problem**  **Analysis** | **Solution**  **Design** | **Social and Ethical**  **Issues** | |
| 40% | | 25% | 25% | 10% | |
| **Oral and Written**  **Communications** | Every student group is required to submit at least 01 written report of typically 06 to 08 pages (IEEE Format) and to make 01 oral presentations of typically 15 minute’s durations. Include only material that is graded for grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy. | | | | | |
| **Late Submission & Plagiarism Policy**  **Policy** | Deadlines are meant to be strictly followed. Any late submission (without and valid reason and justification/ evidence) will be penalized. **The penalty will be 50%. Any delay of more than a week would mean ZERO credit in that particular assessment (assignments, labs, project). Plagiarized assignment will get you ZERO credit.** | | | | | |

**Instructor Name**  Dr. Sufian Hameed

**Instructor Signature**

**Date: August 15, 2024**