COURSE DESCRIPTION FORM

INSTITUTION National University of Computer & Emerging Sciences

PROGRAM (S) TO BE EVALUATED Computer Science

A. Course Description

(Fill out the following table for each course in your computer science curriculum. A filled out form should not be more than 2-3 pages.)

Course Code	**CS 3002**
Course Title	**Information Security**
Credit Hours	3
Prerequisites by Course(s) and Topics	CS 3001 Computer Networks, CS 2006 Operating Systems
Assessment Instruments with Weights (homework, quizzes, midterms, final, programming assignments, lab work, etc.)	1. 5-6 Assignments/ In-class labs (10%) 2. 3-4 Quizzes (10%) 3. Course Project (10%) 4. 1-2 Midterm Exam(s)(25-30%) 5. Final Exam (40-45%)
Course Coordinator	Dr. Haroon Mahmood
URL (if any)	
Current Catalog Description	
Textbook (or **Laboratory Manual** for Laboratory Courses)	• Computer Security: Principles and Practice, 3rd edition by William Stallings • Principles of Information Security, 6th edition by M. Whitman and H. Mattord
Reference Material	• Official (ISC)2 Guide to the CISSP CBK, 3rd edition • Computer Security, 3rd edition by Dieter Gollmann • Computer Security Fundamentals, 3rd edition by William Easttom • Research papers (provided)
Course Goals	This course serves as a comprehensive overview to the field of information security at senior undergraduate level. At the end of the

<table>
<tr><td></td><td>course the students will be able to:
1. Explain key concepts of information security such as design principles, cryptography, risk management, and ethics.
2. Discuss legal, ethical, and professional issues in information security.
3. Apply various security and risk management tools for achieving information security and privacy.
4. Identify appropriate techniques to tackle and solve problems in the discipline of information security.

The course will broadly cover the following topics: 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.</td></tr>
<tr><td>Topics Covered in the Course, with Number of Lectures on Each Topic (assume 15-week instruction and one-hour lectures)</td><td>
<table>
<tr><th>Timeline</th><th>Content Covered</th></tr>
<tr><td>Lecture 1</td><td>Course Introduction
• Introducing syllabus, policies, and projects.
• Setting the course context: recent cyber threats overview, the field of information security in industrial and academic context.</td></tr>
<tr><td>Lecture 2</td><td>Information Security Foundations
An overview of basic information security principles (with practical examples): confidentiality, integrity, availability, authentication, authorization and non-repudiation.</td></tr>
<tr><td>Lecture 3</td><td>Security Design Principles
Discussion and evaluation of following primitives: Least-privilege, fail-safe defaults, complete mediation, separation of privilege.</td></tr>
<tr><td>Lecture 4</td><td>Security Mechanisms
Access Controls, Authentication
(Access control theory, access control matrix, information flow)</td></tr>
<tr><td>Lecture 5</td><td>Security Mechanisms –II
Introduction to Cryptography: symmetric and asymmetric, block and stream ciphers – (continued).</td></tr>
<tr><td>Lecture 6</td><td>Security Mechanisms –III
• Cryptography: Hash functions, message</td></tr>
</table>
</td></tr>
</table>

	authentication codes. • Encryption: Message digests. Approximate strength of ciphers
Lecture 7	**Security Mechanisms –IV** • Digital Signatures: Authenticity, signing algorithms. • Key Management: Public and private key systems
Lecture 8	**Network Security –I** • TCP/IP security issues • DNS security issues and defenses
Lecture 9	**Network Security –II** • TLS/SSL • Firewalls
Lecture 10	**Revision**
Lecture 11	**Network Security –III** Advanced network intrusion detection and prevention systems: traffic profiling, anomaly detection, honeypots, mitigation and best-practices.
Lecture 12	**Software Security** • Vulnerability auditing, penetration testing • Sandboxing • Control flow integrity
Lecture 13	**Threat Classification** • Computer virology – overviewing state of the art • Threat taxonomy and classification • Recent types of malware and mitigation techniques
Lecture 14	**Database & Web Security** • User authentication, authentication-via-secret and session management Cross Site Scripting, Cross Site Request Forgery, SQL Injection)***(in-lecture lab/practice)***
Lecture 15	**System Security** • TCB and security kernel construction. • System defense against memory exploits.
Lecture 16	**System Security - II** • UNIX security and Security-Enhanced Linux (SELinux) • Windows security***(in-lecture lab/practice)***
Lecture 17	**Security Policies**

	• Confidentiality policies (BLP model) • Integrity policies (Biba Model)
Lecture 18	**Security Policies – II** • Integrity policies (Clark-Wilson model) • Hybrid policies (Chinese Wall model, role-based access control)
Lecture 19	**Human Aspects of Information Security** • Hardening the weakest-link: end-user • End-user awareness and knowledge • Social Engineering ***(in-lecture lab/practice)***
Lecture 20	**Revision**
Second Mid-term Examination	
Lecture 21	**Auditing & Risk Assessment** • Sarbanes-Oxley (SOX) Act • Corbit framework
Lecture 22	**Cybercrime Laws and Ethics** Pakistan cybercrime act and the role of investigative agencies.
Lecture 23	**Cybercrime Laws and Ethics - II** • Ethical perspective of research studies and experimentation (data privacy and anonymization techniques). • Intellectual property, copyright, patent, trade secret.
Lecture 24	**Digital Forensics** Introduction to forensics, gold standards, evidentiary source identification, artefact acquisition and evidence provenance.
Lecture 25	**Digital Forensics - II** Introduction to open source forensic toolkits.***(in-lecture lab/practice)***
Lecture 26	**Digital Forensics – III** Contemporary issues in digital forensics: network, cloud and IoT/big data forensics.
Lecture 27	**Limitations and Future Challenges** • Issues in big data, IoT and software defined infrastructures. • Applications of blockchaining in information security.
Lecture 28 - onwards	**Revision & Project Evaluations**

	Final Examination
Laboratory Projects/Experiments Done in the Course	In-class labs on Malware analysis will be conducted!
Programming Assignments Done in the Course	

Class Time Spent on (in credit hours)	**Theory**	**Problem Analysis**	**Solution Design**	**Social and Ethical Issues**
	45	20	30	5

Oral and Written Communications	Every student is required to submit at least **1** written report of typically **10-15** pages and to make 1 oral presentations of typically **20** minute's duration. Include only material that is graded for grammar, spelling, style, and so forth, as well as for technical content, completeness, and accuracy.

Instructor Name: Dr. Haroon Mahmood

Instructor Signature: 

Date: 22-08-2022