DEPARTMENT OF
COMPUTER
SCIENCE
FACULTY OF COMPUTING & ARTIFICIAL INTELLIGENCE

Course Guide

Information Security (CS-415)
Spring 2023
BSIT – II (A, B), VI

Instructor:

1. **Sibgha Tahir BSIT – II (A, B), VI**

Email:

1. sibgha.tahir@mail.au.edu.pk

Air University Islamabad

Course Summary:

This is an introductory course where students will be introduced to the fundamentals of information security. Basic concepts related to both technical as well as managerial aspects of information security will be introduced. The topics covers include: 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.

Course Objectives

Upon completion of this course, students will be able to do the following:

The objective of this course is to provide an introduction to the field of information security. Students will learn the basics of information security management, threats and risk assessment, use of appropriate security controls, cryptography, network, Cyber Crimes, computer security, pentesting, and ethical hacking (practical approaches) etc. This course will make students prepare for their future journey with advanced information security-related courses.

Pre-requisites

- NA

Program Learning Outcomes:

Following are the relevant PLOs:

2. **Knowledge for Solving Computing Problems:**
   Apply knowledge of computing fundamentals, knowledge of a computing specialization, and mathematics, science, and domain knowledge appropriate for the computing specialization to the 16 abstraction and conceptualization of computing models from defined problems and requirements.

8. **Computing Professionalism and Society:** Understand and assess societal, health, safety, legal, and cultural issues within local and global contexts, and the consequential responsibilities relevant to professional computing practice.

9. **Ethics:** Understand and commit to professional ethics, responsibilities, and norms of professional computing practice.

10. **Life-long Learning:** Recognize the need, and have the ability, to engage in independent learning for continual development as a computing professional.

Course Learning Outcomes:

After completion of the course, the student shall be able to:

1. **Demonstrate** fundamentals concepts of information security.
2. **Analyze** security risks, threats, and vulnerabilities to the organization.
3. **Apply** cybersecurity tools to analyze and mitigate different attacks.

Mapping of CLO to PLO

CLO	Domain	PLO
1	C2 (understand)	2
2	C4 (analyze)	2,8
3	C3 (apply)	9,10

Course Outline with Week Breakdown (tentative):

Week	Lecture Details	Activity	CLO
Week 1	• Course Introduction, format & grading • Data & Information, Information System(IS), components of IS (data, people, procedures, technology) • Desired security properties of IS • Why is Information Security important?	**Q/A**	1
Week 2	• Nations engaged in information warfare: a few instances from recent past • Case study of SLS company & it's business • First instance of security problem & reporting in SLS Company History of Information Security • Key Information security concepts	**Q/A**	1
Week 3	• Information security at present • Information security life Cycle • Legal, Ethical, and Professional Issues • Cyber Security Laws: Laws in Pakistan • Two well-known models of information security ◦ The C.I.A Triangle	**Assignment 1**	1

Week 4	• CNSS model of information security • Access, Asset, Attack • Safeguard, or countermeasure • Exploit, Exposure, Loss • Threat, Threat agent • Increased threats with the emergence of the Internet of Things (IoT) • VulnerabilitiesSoftware security	**Quiz 1**	2

Week 5	•
	• Case study of buybay.com for reviewing key concepts
	• **Security vs. Access**
	  • Balancing Information Security and Access
	  • Approaches to Information Security Implementation
	  • Top-down approach
	  • Bottom-up approach
	• Privacy: *Concepts*
	• Authentication and Privacy
	• Privacy on the Internet
	• Aspects: *Social Media, Email*
	• Anonymity & Onion Routing
	•
		Q/A	2

Week 6	• Ten steps to building a secure organization
	  o Evaluate the Risks and Threats
	  o Beware of common misconceptions
	  o Security Training of IT Staff
	  o Identify and Use Built-in
	• Security Features of OS & applications
	• Do Not Forget the Basics
	• Database security
	• Information Security: Is It an Art or a Science?
	• What Information Security does for an organization?
	• The four main functions
	• Planning for security,
	• Information security governance,
	• Policy, Standards, and Practices,
	• Different types of Policies
	• Categories of Attacks
		Q/A	2

Week 7	• Firewalls • Virtual private networks (VPNs) • Intrusion Detection / Prevention (IDS/IPS) • Digital Watermarking • Internet Content Filtering • Data Interception Techniques	**Q/A**	2
Week 8	**Mid Exam**		

Week9	• Information gathering and reconnaissance (PracticalApproach)
	  o Port enumeration
	  o Service enumeration
	  o Bypass Firewalls
		Q/A	1

Week 10	• Zombie attack Vulnerability Assessment using Practical Approach
	  ○ Web site vulnerabilities
	  ▪ XSS, CSRF, HTML Injection
	  ▪ SQL Injection and Mitigation
	  ○ System Level vulnerabilities
	• Most Critical vulnerabilities
		Q/A	3

Week 11	• Vulnerability Exploitation (Practical Approach)
	  ○ Gaining Access
	  DOS, DDOS attack and its Mitigations
	• Offensive and Defensive Mechanism
	Midterm Exam Review
		Quiz 2	3

Week 12	• Cyber Crime Tactics • Cyber Crimes: *Cyber Bullying, Cyber Harassment, Cyber Stalking, Cyber Fraud, Logic Bombs, Web Jacking, Cracking, Identity Theft*	**Assignment 2**	2
Week 13	• Cryptography & its Applications • Symmetric Cryptography: *Block Cipher, Stream Cipher* • *Modes of encryption*	**Q/A**	1
Week 14	• Asymmetric Cryptography: PKC • Hash Algorithms • Attacks & Threats: Cryptanalytic Attack, Brute force, Dictionary attack • Random Numbers, OTP	**Quiz-3**	1
Week 15	• Digital signatures • Key management • Introduction to Security Protocol • Threat model of Security Protocol	**Assignment-3**	1
Week 16	**Final exam**		

General Grading Policy:

Assignments, Quizzes and Project grade percentages are subject to change.

Evaluation Method	Theory (100)	
	Distribution	Marks
Quizzes (3)	10%	10
Assignments (3)	10 %	10
Practical Task / Semester Projects / Presentations	10%	10
Midterm Exam	25%	25
Final Exam	45 %	45
Total	100 %	**100**

Grading and General Course Policies:

- No makeup quizzes / assignments
- No late assignments will be accepted.
- All assignments and projects submitted should be the outcome of individual work only. Group work is explicitly prohibited (severe penalties for violation).
- **An 'F' grade will be allotted if projects/Assignments are found copied from internet or any other sources.**

Books / Reference Materials:

- **Textbooks**:
  - **Book1**: Principle of Information Security by Michael E. Whitman | Herbert J. Mattord, 6th or 5th Edition
  - **Book2**: Cryptography and Network Security by William Stallings7th or 6th Edition
  - **Book3**: Computer and Information Security Handbook 2nd Edition 2013
- **Reading Materials/Reference Books**
  - Lawrence C. Miller, *"**Cyber Security for Dummies***", Palo Alto Networks, 2nd Edition or Latest
  - William Stallings, ***"Network Security Essentials: Applications and Standards",*** 3rd Edition or Latest
  - Bruce Schneier, "***Beyond Fear: Thinking Sensibly About Security in an Uncertain World***", Latest Edition
  - Kevin D. Mitnick & William L. Simon, ***"The Art of Deception: Controlling the Human Element of Security"***, Wiley Publishing Inc.
  - Kevin D. Mitnick & William L. Simon, ***"The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers"***, Wiley Publishing Inc.
  - George Kurtz, Joel Scambray, and Stuart McClure***, "Hacking Exposed: Network Security Secrets and Solutions"***, 2nd Edition or Latest

Policy:

- To promote self-learning, the students will be introduced with online courses & self-learning websites
- To promote self-learning, the students may be assigned new topics to present in quick group presentations
- In case a topic is important, but the instructor realizes that students need instant practice of a concept e.g., Induction, Asymptote Analysis, etc., a related class task in last 5-10 minutes of the lecture may be conducted.

Program learning Outcomes (PLOs)

- **PLO 1: Academic Education :** Prepare graduates having educational depth and breadth knowledge and prepare Computing professionals.
- **PLO 2: Knowledge for Solving Computing Problems:** Apply knowledge of computing fundamentals, knowledge of a computing specialization, and mathematics, science, and domain knowledge appropriate for the computing specialization to the abstraction and conceptualization of computing models from defined problems and requirements.
- **PLO 3: Problem Analysis:** Identify, formulate, research literature, and solve complex computing problems reaching substantiated conclusions using fundamental principles of mathematics, computing sciences, and relevant domain disciplines.
- **PLO 4: Design/ Development of Solutions:** Design and evaluate solutions for complex computing problems, and design and evaluate systems, components, or processes that meet specified needs with appropriate consideration for public health and safety, cultural, societal, and environmental considerations
- **PLO 5: Modern Tool Usage:** Create, select, adapt, and apply appropriate techniques, resources, and modern computing tools to complex computing activities, with an understanding of the limitations.
- **PLO 6: Individual and Teamwork:** Function effectively as an individual and as a member or leader in diverse teams and in multi-disciplinary settings.
- **PLO 7: Communication:** Communicate effectively with the computing community and with society at large about complex computing activities by being able to comprehend and write effective reports, design documentation, make effective presentations, and give and understand clear instructions.
- **PLO 8: Computing Professionalism and Society:** Understand and assess societal, health, safety, legal, and cultural issues within local and global contexts, and the consequential responsibilities relevant to professional computing practice.
- **PLO 9: Ethics:** Understand and commit to professional ethics, responsibilities, and norms of professional computing practice.
- **PLO 10: Life-long Learning:** Recognize the need, and have the ability, to engage in independent learning for continual development as a computing professional.