CS 4243: Introduction to Computer Security

Required Course: Elective
Course Number: CS 4243
Course Name: Introduction to Computer Security
Credit Hours: 3
Lecture Hours: 3
Lab Hours: 0
Instructors: Dr. Johnson P Thomas

Book Title: Computer and Internet Security: A Hands-on Approach 2nd Edition
Book Author: Wenliang Du
Book Year: 2019

Book Title: Computer Security: Art and Science, 2nd Edition
Book Author: by Matt Bishop Wesley, 2019
Book Year: 2019

Course Description: Overview of the components of computer and network security. Discussion of external processes required in secure systems, information assurance, backup, business resumption. Detailed analysis of security encryption, protocols, hashing, certification, and authentication.

Course Prerequisites: CS 3443 (Computer Systems) with a grade of 'C' or better.

Course Goals:

Student Outcomes:

Student Outcome	Course Outcome
1	• Understand that every that every component of a complex computing system, including software, operating system, network has security vulnerabilities and weaknesses. • Analyze the different components to identify security vulnerabilities and weaknesses.
2	• Gain knowledge and understand the principles of building a secure computer system based on: - secure design - access control matrix

	- policies including security policies and confidentiality policies
3	• Learn and understand the theory of cryptography in the implementation of secure systems: - Basic cryptographic techniques - Key Management - Authentication
4	• Learn the techniques and tools used to attack computer systems, that is, malware. • Write malware code to exploit vulnerabilities in software and database/web systems, and network protocols.
5	• Learn and understand measures to counteract malware attacks and thereby protect computer systems • Write code to counteract malware attacks
6	• Apply computer science theory, software development fundamentals, computer system models to produce secure computing systems and software

---

Course Topics:

Knowledge Area: Information Assurance and Security

Knowledge Unit	Topics Covered	Hours
Foundational Concepts in Security	Tier 1: Confidentiality, Integrity, Availability, Concepts of risk, threats, vulnerabilities, and attack vectors, Authentication and authorization, access control (mandatory vs. discretionary), Concept of trust and trustworthiness	7
Principles of Secure Design	Tier 1: Least privilege and isolation OS/Security, Protection/Policy/mechanism separation and SF/Virtualization, Defense in depth, Security by design, Tensions between security and other design goals	3
Defensive Programming	Tier 1: Input validation and data sanitization - methods/ Program Correctness and SE/Software construction/Coding practices, Buffer overflows, Integer errors, SQL injection, Race conditions	5
Threats and Attacks	Tier 2: Attacker goals, capabilities, and motivation, examples of malware - viruses, worms, spyware, botnets, Trojan horses or rootkits, Denial of Service, Social engineering (e.g., phishing)	6
Network Security	Tier 2: Network specific threats and attack types (denial of service, spoofing, sniffing and traffic redirection, man-in-the-middle, message integrity attacks, routing attacks, and traffic analysis), cryptography for data and network security, Architectures for	6

	secure networks (secure channels, secure DNS) Defense mechanisms and countermeasures (intrusion detection, firewalls)	
Cryptography	Tier 2: Basic Cryptography Terminology, encryption, decryption, keys and their characteristics, signatures, Cipher types (Caesar cipher), Public Key Infrastructure support for digital signature and encryption Elective: block ciphers (pseudo-random permutations)., AES, pseudo-random functions, hash functions, e.g., SHA2, message authentication codes, Symmetric key cryptography, Public key cryptography:, Public key encryption, RSA encryption, EI Gamal encryption, Digital signatures, Public-key infrastructure (PKI) and certificates, Message integrity (HMAC)	9
Web Security	Elective: SQL injection	1.5
Secure Software Engineering	Elective: Building security into the software development lifecycle	1.5