| | |
|---|---|
| **Course number and name:** | **CS 07351: Cyber Security: Fundamentals, Principles and Applications** |
| **Credits and contact hours:** | 3 credits / 3 contact hours |
| **Faculty Coordinator:** | Vahid Heydari |
| **Text book, title, author, and year:** | Fundamentals of Information Systems Security, Third Edition, by David Kim and Michael G. Solomon, 2018 |

## Specific course information

**Catalog description:** This course exposes students to the principles of cyber-security and will introduce a wide range of security activities, methodologies, and procedures. The topics covered in the course include fundamental concepts of computer security, principles of cryptography, software security and trusted systems, network security as well as other topics.

**Prerequisites:** (MATH 03160 Discrete Structures ***or***
MATH 03150 Discrete Mathematics) ***and***
CS 06205 Computer Organization

**Type of Course:** ☒ Required ☐ Elective ☐ Selected Elective

## Specific goals for the course:

1. Describe the fundamental concepts of the cyber security discipline and use to provide system security.
2. Describe potential system attacks and the actors that might perform them.
3. Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
4. Describe appropriate measures to be taken should a system compromise occur.
5. Properly use the Vocabulary associated with cyber security.
6. Define the principles of cybersecurity.
7. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations and aversion to risk.
8. Describe the basic security implications of modern computing environments.

## Required list of topics to be covered:

1. Threats and Adversaries (threat actors, malware, natural phenomena)
2. Vulnerabilities and Risk management (include backups and recovery)
3. Common Attacks
4. Basic Risk Assessment
5. Security Life-Cycle

6. Applications of Cryptography and PKI
7. Data Security (in transmission, at rest, in processing)
8. Security Models
9. Access Control Models
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
11. Security Mechanisms (e.g., Identification/Authentication, Audit)
12. Malicious activity detection / forms of attack
13. Appropriate Countermeasures
14. Cybersecurity Principles
15. Endpoint protection
16. Storage Devices
17. System Architectures
18. Alternative environments (SCADA, real time systems, critical infrastructures)
19. Networks (Internet, LANs, wireless)
20. Software Security (secure coding principles, software issues by type)
21. Configuration Management
22. Patching
23. Vulnerability Scanning (core)
24. People and security (social engineering)
25. Physical and environmental security concerns
26. Internet Of Things (IOT)
27. Motivations and Techniques
28. The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access)
29. Types of Attacks (and vulnerabilities that enable them)
30. Events that indicate an attack is/has happened
31. Attack Timing
32. Attack surfaces / vectors, and trees
33. Covert Channels
34. Social Engineering
35. Insider problem
36. Threat Information Sources (e.g., CERT)
37. Access controls (models and mechanisms)
38. Creation and operation of virtualization technology