Miami Dade College

Course Description

CIS3360 | Principles of Information Security | 4.00 credits

This upper division course, for students majoring in Information Systems Technology, provides an overview of information systems security principles, practices, methods, and tools for organizational and institutional computing. Students will learn about the relationship between policy and security, the mechanisms used to implement policies, and the methodologies and technologies for assurance and vulnerability analysis and intrusion detection. Students will be required to perform security analyses, and set up protection schemes. Prerequisites: CTS1134 or CTS1650.

Course Competencies:

Competency 1: The student will demonstrate an understanding of the information security concepts by:
1. Distinguishing among the main security goals (confidentiality, integrity, and availability)
2. Interpreting the authenticity and accountability security goals
3. Applying the generally accepted security principles (including defense-in-depth, least privilege, economy of mechanism, open design, and separation of privilege)
4. Categorizing countermeasures (technical vs. administrative, and preventive vs. detective vs. corrective)

Competency 2: The student will demonstrate an understanding of the diversity of potential attacks against an organization by:
1. Analyzing social engineering techniques
2. Researching eavesdropping attacks
3. Investigating spoofing and man-in-the-middle attacks
4. Discussing session hijacking attacks
5. Comparing the different types of password attacks
6. Evaluating Denial of Service (DOS) attacks and Distributed Denial of Service (DDOS) attacks
7. Comparing and contrasting software exploitation attacks (buffer overflow, SQL injection, Cross-Site Scripting (XSS) attacks)
8. Describing traffic analysis
9. Categorizing malware (viruses, worms, bots, Trojan Horse, rootkits)
10. Discussing the typical cyber-attack phases (Reconnaissance, Scanning, Gaining Access, Maintaining Access, Covering Tracks)

Competency 3: The student will demonstrate an understanding of cryptographic techniques by:
1. Implementing security controls using hashing algorithms
2. Implementing security controls using secret key cryptographic primitives
3. Implementing security controls using various modes of encryption
4. Implementing security controls using public key cryptographic primitives
5. Comparing various cryptographic algorithms (DES, 3DES, AES, Diffie-Hellman, RSA, HMAC)
6. Assessing key distribution and management techniques (Public Key Infrastructures, Kerberos, x.509 certificates, PGP certificates)

Competency 4: The student will demonstrate an understanding of authentication methods by:
1. Using passwords as an authentication method
2. Using biometrics as an authentication method
3. Using cryptography primitives to implement authentication methods
4. Using authentication devices
5. Designing multi-factor authentication techniques

Competency 5: The student will demonstrate an understanding of access control systems by:

1. Employing various models of access control (Discretionary access control (DAC), Mandatory Access Control (MAC), Role-based Access control (RBAC), the access matrix, and multilevel models)
2. Designing and implementing a file systems access control policy
3. Examining network access control techniques

Competency 6: The student will demonstrate an understanding of various network security controls by:
1. Explaining the role of firewalls and the demilitarized zone (DMZ)
2. Contrasting different types of intrusion detection systems
3. Describing honeypots and honeynets
4. Describing virtual private networks

Competency 7: The student will demonstrate an understanding of the legal, ethical, and professional issues in information security by:
1. Distinguishing between unethical and illegal behavior in information security
2. Identifying major national laws that relate to the practice of information security
3. Discussing legal, ethical, and professional issues in information security

Learning Outcomes:
- Solve problems using critical and creative thinking and scientific reasoning
- Use computer and emerging technologies effectively