Miami Dade College

Course Description

CIS2010C | Introduction to Internet of Things Networking and Security | 4.00 credits

This course explores Internet of Things (IoT) networks' design, implementation, and security, providing a well-rounded understanding of protocols and standards governing the Internet and IoT. Students gain experience performing security assessments and vulnerability testing of IoT systems using industry-standard tools, focusing on identifying and mitigating risks to build secure and resilient IoT solutions.

Course Competencies:

Competency 1: The student will demonstrate understanding of networking and security fundamentals by:

1. Explaining the basic principles and architecture of computer networks, including the OSI and TCP/IP models
2. Identifying common networking devices such as routers, switches, and firewalls, and their roles in a network ecosystem
3. Describing the functions of network protocols and services in data communication and network operations
4. Understanding fundamental security concepts, common security threats, and essential security protocols

Competency 2: The student will demonstrate the ability to install and configure IoT devices and networks by:

1. Setting up IoT devices and integrating them into existing network infrastructures
2. Configuring wireless communication technologies like Wi-Fi, Bluetooth, and Zigbee for IoT applications
3. Implementing appropriate network topologies (star, mesh, etc.) for IoT deployments
4. Understanding basic network concepts such as IP addressing, subnetting, and routing as they apply to IoT
5. Configuring network devices like routers, switches, and access points to support IoT connectivity
6. Troubleshooting common connectivity issues within IoT networks

Competency 3: The student will demonstrate understanding of IoT networking protocols and data communication by:

1. Comparing and contrasting various IoT communication protocols and their use cases
2. Understanding the role of network layers and how data is transmitted in IoT systems
3. Analyzing data flow in IoT networks to identify potential bottlenecks or security issues
4. Exploring the use of IPv6 in IoT and its advantages over IPv4

Competency 4: The student will demonstrate understanding of IoT security fundamentals by:

1. Recognizing common security threats and vulnerabilities specific to IoT devices and networks
2. Applying basic security measures such as strong authentication and secure communication protocols
3. Understanding the importance of firmware updates and secure configurations
4. Discussing the impact of unsecured IoT devices on network security

Competency 5: The student will demonstrate the ability to perform basic security assessments on IoT systems by:

1. Using essential tools to assess the security of IoT devices and networks
2. Identifying potential vulnerabilities and weaknesses in IoT setups
3. Implementing recommended practices to mitigate identified security risks
4. Understanding network security measures such as firewalls and intrusion detection systems in IoT networks

Competency 6: The student will demonstrate the ability to implement and maintain secured IoT networks by:

1. Configuring encryption and authentication settings on IoT devices and network equipment
2. Managing firmware updates and applying security patches to devices and network components
3. Ensuring secure deployment and decommissioning of IoT devices following best practices
4. Implementing network segmentation and access controls to enhance security

Competency 7: The student will demonstrate understanding of best practices and standards in IoT networking by:

1. Summarizing key IoT networking standards and industry guidelines
2. Applying best practices in the installation and maintenance of IoT networks and devices
3. Understanding basic regulatory compliance requirements relevant to IoT network deployments
4. Exploring network scalability and interoperability challenges in IoT systems

Competency 8: The student will demonstrate understanding of incident response procedures in IoT by:

1. Using network monitoring tools to oversee IoT device performance and data flows
2. Identifying and resolving common operational issues in IoT networks
3. Maintaining logs and documentation for IoT devices and network configurations
4. Implementing network performance optimization techniques for IoT applications
5. Recognizing signs of security incidents affecting IoT devices and network
6. Following established incident response steps for IoT-related issues
7. Assisting in recovery efforts to restore normal IoT system and network operations after incidents

Competency 9: The student will demonstrate awareness of emerging trends in IoT networking by:

1. Discussing current developments in IoT network technologies and infrastructure
2. Understanding the role of edge computing and its impact on IoT network design
3. Examining the potential of 5G networks in enhancing IoT applications

Learning Outcomes:

- Solve problems using critical and creative thinking and scientific reasoning
- Use quantitative analytical skills to evaluate and process numerical data
- Use computer and emerging technologies effectively