BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS2110 Introduction to Network Security
3 Semester Hours

Student Learning Outcomes & Enabling Objectives

1. Describe the concepts of confidentiality, integrity and availability (CIA).
    a. Describe the challenges of security, the threat actors, and legal considerations.
    b. Review fundamental principles and reference architectures.
2. Define cryptography, cryptographic algorithms, attacks and common use.
    a. Review open design.
    b. Describe cryptographic implementation considerations, digital certificates, PKI and Cryptographic Transport Protocols.
3. Examine security through: network devices, network architecture and network technologies (NAC, DLP).
    a. Describe secure network protocols.
    b. Examine security data from devices, software and tools.
    c. Review how to secure network platforms (documentation, virtualization, cloud, SDN).
    d. Describe wireless attacks, vulnerabilities and security solutions.
    e. Explain network attacks, server attacks and appropriate countermeasures.
    f. Discuss malware attacks and social engineering attacks
4. Explore client security (hardware, operating system and peripherals), physical/personnel security and application security secure coding and code testing).
    a. Investigate mobile device vulnerabilities, configuration and securing.
    b. Explore incident handling, authentication, and resilience
5. Describe types of authentication credentials, and account management.
    a. Describe access control models.
    b. Review account setup, applying restrictions and auditing.
    c. Describe best practices for access control and access control lists (ACLs).
6. Examine business continuity planning, business impact analysis, disaster recovery plans, incident response and forensics.
    a. Explore fault tolerance through redundancy (i.e. storage, servers, and data) and environmental controls.
    b. Examine the security posture through vulnerability assessment, and pen testing.
    c. Explore risk management, strategies for reducing risk and best practices through policies and training.

Big Ideas and Essential Questions

Big Ideas

- Network architecture and security
- Data and application security
- Threats and Vulnerabilities
- Access and Authentication

Essential Questions

1. How can organizations keep information in their network safe, including mobile devices?
2. How does the security triad relate to the administration of a network, including the significance of access control and cryptography?
3. What are the prevalent threats to network security and how can developers make applications more secure?
4. How does understanding risk and risk management relate to an information security plan and a business continuity plan?

These SLOs are approved for experiential credit.

Effective: Fall 2022