BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS 3310 Designing for Security

3 Semester Hours

Student Learning Outcomes & Enabling Objectives

1. Explain information network security fundamentals
    a. Explain the fundamentals of TCP/IP
    b. Explain the Defense in Depth Strategy
    c. Explain Common Attacks and Defenses
    d. Explain security solutions for wireless networking
    e. Explain basic concepts in wireless security
    f. Explain basic VPN concepts

2. Explain how cryptography works
    a. Explain the components of cryptographic protocols
    b. Explain modern-day techniques like 3DES, RSA, hashing, and the use of certificates
    c. Explain Public vs Private keys

3. Interpret the fundamentals of computer network defense including knowledge of TCP/IP packets and subnetting, workstation security and Web based security concerns.
    a. Assess common attack threats to a computer network.
    b. Analyze intrusion signatures
    c. Assess a network defense system including knowledge of network security components in a layered defense configuration
    d. Identify security activities and integration of an Intrusion detection system.
    e. Recognize IPv4 vs IPv6

4. Evaluate the management of security using security tools, auditing and defense upgrades and improvements
    a. Recognize firewall components including hardware and software.
    b. Identify create a risk analysis process to perform ongoing risk analysis.

Big Ideas and Essential Questions

Big Ideas

- Examine common security vulnerabilities and the defenses used to protect network resources
- Evaluate the nuances of secure network design
- Understand the purpose of security
- Understand wireless communication concepts
- Learn how to design, adopt, and enforce security policies
- Explain common cryptography standards
- Explain the fundamental concepts of risk
- Understand what firewalls do and how to implement them to maximum effect

Essential Questions

1. Explain the Goals of Network Security
2. What is a Firewall? Host? Network?
3. What is a VPN? What are the benefits?
4. What is the purpose of Cryptography?
5. What is risk? How is risk calculated?
6. Explain how network security defenses affect your organization?
7. What are risky ports?
8. Explain IDS vs IPS? Host vs Network? Benefits?
9. Explain methods for hardening Web and Internet resources

These SLOs are approved for experiential credit.

Effective: Fall 2017