SECURE ELECTRONIC COMMERCE (W/LAB)
Course Syllabus

Course Number: NTWK-0010  OHLAP Credit: Yes
OCAS Code: 8133
Course Length: 130 Hours
Career Cluster: Information Technology
Career Pathway: Network Systems
Career Major(s): Cyber Security Forensics Specialist

Pre-requisite(s): Enterprise Security Management

Course Description: Students will learn about the history, present, and future of electronic commerce in the world. They will also learn about the threats, vulnerabilities, and policies when dealing with commerce in the electronic age.

Textbooks: *Electronic Commerce* - 7th Edition; Schneider; Course Technology

Course Objectives:

1. Secure E-Commerce Concepts & Practices: In this topic, the core concepts that comprise secure e-commerce are explored. The most common practices used today are examined.
   **Objectives:**
   a. Define E-Commerce and identify the key components.
   b. Examine the history of E-Commerce and how E-commerce integrates into the economy.
   c. Examine the common methods used in E-Commerce.
   d. Explore the security risks associated with E-Commerce.
   e. Examine how E-Commerce is included in security policies.

2. Trusted Network Implementation: In this topic, you will examine and identify the transition towards the implementation of trusted networks, including their requirements and critical components.
   **Objectives:**
   a. Examine reasons for migrating networks from defense to trust.
   b. Analyze the requirements of a trusted network.
   c. Define the fundamentals of cryptography.
   d. Define the role of strong authentication.
   e. Define the role of a public key infrastructure.

3. Planning a Trusted Network: In this topic, you will be introduced to the concepts and documents required in planning a trusted network. You will examine trusted network architectures, certificate paths, certificate policies, certification practice statements, and the certificate policy framework.
   **Objectives:**
   a. Examine the components required for a trusted network implementation.
   b. Analyze certificate paths.
   c. Analyze trusted network planning documents.
   d. Examine the certificate practices framework.
4. Microsoft Trusted Networks: In this topic, you will examine the requirements for Certificate Authorities (CA) in general and the various models of CAs that are implemented in practice. You will study the key elements that have to be in place in order for a Certificate Authority to have any meaning for the organization it is designed to serve.

Objectives:
   a. Examine the requirements surrounding the implementation of a CA.
   b. Examine the critical function that trust plays between CAs in a network built on trust.
   c. Examine the types of certificates in a trusted network.
   d. Implement a standalone Microsoft Certificate Authorities hierarchy.
   e. Implement a Microsoft Enterprise Root CA.

5. Linux Certificate Authorities: In this topic, you will examine the basics of certificate authorities on Linux.

Objectives:
   a. Examine the requirements for implementing Certificate Authorities on a Linux platform.
   b. Examine multiple CA options on Linux.
   c. Prepare a Linux server for a CA implementation.
   d. Examine the fundamentals of LDAP.
   e. Install and configure a Linux CA package.

6. Managing Certificates: In this topic, you will examine issues related to the management of certificates. Depending upon the size of the organization and depending upon whether the CA is hosted internally or not, certificate issuance policies may vary.

Objectives:
   a. Examine the management of certificates base on end entity needs.
   b. Create certificate requests and use a CA to generate the certificates for computers and users.
   c. Issue multiple types of digital certificates.
   d. Assign the issued certificate to the entity that requested it.
   e. Implement certificates on smart cards.

7. Local Resource Security: In this topic, you will examine multiple systems and technologies available to secure data stored locally on your computer.

Objectives:
   a. Examine how Windows operating systems function.
   c. Configure a system to prevent users from using EFS.
   d. Implement EFS to protect files.
   e. Implement data security using biometrics.

8. Secure Email: In this topic, you will examine the current vulnerabilities of email and the reasons that plaintext is a serious security risk for any enterprise.

Objectives:
   a. Examine the benefits and challenges of secure email.
   b. Implement PGP (Pretty Good Privacy) to secure email.
   c. Implement S/MIME to secure email.
   d. Explore other options to secure email.

9. Building Trusted Networks (Lab Only): In this topic, you will take the different pieces that you have worked with through the course and tie them together in a simulated environment.

Objectives:
   a. Implement a multi-platform CA structure.
   b. Configure the CA hierarchy.
   c. Configure the Linux CA.
d. Implement trusting CAs.
e. Implement multi-platform secure email.
f. Revoke certificates and verify revocation.

ODCTE Objectives

TTC Additional Objectives for SEC

A. Concepts and Practices

B. Trusted Network Implementation
   1. Define the need to develop trusted networks.
   2. Identify the function of both authentication and identification.
   3. Examine the components of a Public Key Infrastructure (PKI).
   4. Identify the applications of PKI.

C. Planning a Trusted Network

D. Microsoft Trusted Networks

E. Linux Certificate Authorities

F. Managing Certificates
   1. Digital Certificates
      a. Examine the various ways that identities are established in the world.
      b. Examine the role of an authority that thoroughly examines applications
         and then issues some form of identity document, such as a certificate.
      c. Examine issues surrounding the protection of the sanctity of a Certificate
         Authority.
      d. Distinguish between the purposes of certificates issued in the physical
         world versus the digital world.
      e. Examine key standards specified for digital certificates.
      f. Examine the X.509 authentication standard as defined by the ITU and
         the information contained in an X.509 certificate.
      g. Perform a case study of one of the leading Certification Authorities.
   2. Digital Signatures
      a. Compare digital signatures with real world signatures.
      b. Examine the features of digital signatures and their requirements for use
         in e-commerce.
      c. Describe how digital signatures function.
      d. Examine the various types and emerging standards for digital signatures.
      e. Examine the digital signature applications and protocols used.

G. Local Resource Security

H. Secure E-mail

I. Building Trusted Networks
   1. Implement PKI and certificate management.
Teaching Methods: The class will primarily be taught by the lecture and demonstration method and supported by various media materials to address various learning styles. There will be question and answer sessions over material covered in lecture and media presentations. Supervised lab time is provided for students to complete required projects.

Grading Procedures: 1. Students are graded on theory and shop practice and performance.
2. Each course must be passed with seventy (70%) percent or better.
3. Grading scale: A=90-100%, B=80-89%, C=70-79%, D=60-69%, F=50-59%.

Description of Classroom, Laboratories, and Equipment: Tulsa Technology Center campuses are owned and operated by Tulsa Technology Center School District No. 18. All programs provide students the opportunity to work with professionally certified instructors in modern, well-equipped facilities.

Available Certifications/College Credit: The student may be eligible to take state, national or industry exam after completion of the program. College credit may be issued from Oklahoma State University-Okmulgee, Rogers State University or Tulsa Community College. See program counselor for additional information.

College Credit Eligibility: The student must maintain a grade point average of 2.0 or better.