Saint Leo University

COM 355
System Security

Course Description:

Securing the systems which run our computers is the key to ensuring that our essential information remains safe and available. This course provides the essentials to understanding the threats to systems security, the methods to counter those threats, and some practical work in systems security. A computer system with appropriate software will be required.

Prerequisite: COM 309
COM 416

Textbooks*:*

Student Note: Students ordering from our online bookstore will access the materials from the links in the course. There is nothing to receive from the bookstore once the order has been placed. This class has direct digital access within the course.

Kim, D., & Solomon, M. *Fundamentals of Information Systems Security* (3rd ed.). (eBook with virtual lab access). Jones & Bartlett. ISBN: 9781284146035 (Custom for Saint Leo)

Created from the National lab package:

Kim, D., & Solomon, M. Fund of Information Security 3.0 (Nav2 Access Code) (3rd ed.). Jones & Bartlett. ISBN: 9781284141825

Learning Outcomes:

1. Describe and explain the terminology and software threats to systems security and the methods required for maintaining security;
2. Explain and demonstrate policies, programs and procedures for prevention of unauthorized internal access;
3. Explain and demonstrate methodologies to prevent unauthorized external access;
4. Describe and explain systems security management policies and procedures for dealing with wireless, web, remote access, VPN and email security;
5. Describe and explain systems security through disaster planning, monitoring and auditing.

6. VALUES OUTCOME: Students will demonstrate an understanding of the Saint Leo University core value Personal Development including the criticality of Ethical Behavior, in using
computers in an organizational environment.

Core Value:
Personal Development: Saint Leo University stresses the development of every person's mind, spirit, and body for a balanced life. All members of the Saint Leo University community must demonstrate their commitment to personal development to help strengthen the character of our community.

Evaluation:

Tests (4) 40%
Lab Assignments (9) 50%
Discussion (8) 10%

Tests—There will be 4 multiple choice tests. Complete each test no later than Sunday 11:59 PM EST/EDT of the module in which it is due.

Lab Assignments— Assignments from the accompanying manual (online) will be assigned to reinforce techniques and concepts taught. Lab assignments will be assigned after every module and will consist of hands-on activities. Note that the lab can only be accessed through some browsers. Each assignment must be submitted as a single MS Word document and **not** submitted as multiple files.

Discussion—Each module will include a discussion assignment (Module 1 will also include an additional "Introduction" topic). Participation in class discussions is expected to be thoughtful and well-informed. For each module, respond to a discussion question posted on the Discussion Board no later than Thursday 11:59 PM EST/EDT of the respective module. Finally, post responses to at least two classmates no later than Sunday 11:59 PM EST/EDT. Be certain to review the requirements for each discussion question within the module pages.

Assessment of the Learning Outcomes

Learning Outcome	Assessment Method(s)
1	Test, Homework
2	Test, Homework
3	Test, Homework
4	Test, Homework

5	Test, Homework
6	Test, Homework
7	Homework, Discussion

Grading Scale:

Grade Score (%)

A	94-100
A-	90-93
B+	87-89
B	84-86
B-	80-83
C+	77-79
C	74-76
C-	70-73
D+	67-69
D	60-66
F	0-59

Course Schedule:

Module 1 **Information Systems Security Fundamentals**

Objectives **When you complete this module, you should be able to:**

- Describe the concepts of information systems security (ISS) as applied to an IT infrastructure.
- Describe the threats and vulnerabilities common within the seven domains.
- **Describe the Internet of Things (IoT)**
- **Describe how IP mobility is helping to drive an IoT world**
-
- Explain:

Confidentiality, integrity, and availability (C-I-A) concepts.
Layered security solutions implemented for the seven domains of a typical IT infrastructure.

- Common threats for each of the seven domains.

IT security

- policy framework.
- Impact of data classification standard on the seven domains.

Assignments

Items to be Completed:	**Due No Later Than:**
Post an introduction to the class	Thursday 11:59 PM EST/EDT
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 1	Sunday 11:59 PM EST/EDT

Module 2 Security Countermeasures to Mitigate Malicious Attacks Objectives

When you complete this module, you should be able to:

- Identify malicious code and attacks, and implement countermeasures.
- Implement system auditing, logging, and scanning.
- Describe how organizations can manage risk.
- Explain:
  - Attacks, threats, and vulnerabilities in a typical IT infrastructure.

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 2	Sunday 11:59 PM EST/EDT
Complete Test 1	Sunday 11:59 PM EST/EDT

  - Common security countermeasures typically found in an IT infrastructure.
  - Risk assessment approach to securing an IT infrastructure.
  - Risk mitigation strategies to shrink the information security gap.

Module 3 Access Controls for Systems, Applications, and Data Access Objectives

When you complete this module, you should be able to:

- Describe the formal models of access controls.
- Describe how identity is managed by access controls.
- Describe access control concepts and technologies.
- Explain:
  - Authorization policies that apply access control to systems, application, and data.

- The role of identification and authentication in granting access to information systems.
- Authentication factor types and the need for two- or three-factor authentication.
- The pros and cons of the formal models used for access controls.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 3	Sunday 11:59 PM EST/EDT

Module 4 **Security Operations and Administration**

Objectives **When you complete this module, you should be able to:**

- Describe how to manage the security infrastructure.
- Develop and maintain security programs.
- Describe how to promote user awareness of security.
- Explain:
  - Role of IT governance and security administration to implement security policy.
  - Components of an IT security policy
  - infrastructure.
  - Change management and configuration management.
    Secure system development life cycle (SDLC).

Module 5 **Access Controls for Systems, Applications, and Data Access Objectives**

When you complete this module, you should be able to:

- Describe the practices and principles of system audits.
- Describe how to define metrics for system performance.

- Describe different methods for assessing security compliance.
- Explain:
  - The role of an audit in effective security base-lining and gap analysis.
  - The importance of monitoring systems throughout the IT infrastructure.
  - Security logs for normal and abnormal traffic patterns and digital signatures.
  - Security countermeasures of auditing, testing, and monitoring test results.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 4	Sunday 11:59 PM EST/EDT
Complete Test 2	Sunday 11:59 PM EST/EDT
Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 6	Sunday 11:59 PM EST/EDT
Complete Test 3	Sunday 11:59 PM EST/EDT
Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 5	Sunday 11:59 PM EST/EDT

Module 6 **Security Operations and Administration**

Objectives **When you complete this module, you should be able to:**

- Describe the principles of risk management.
- Describe how to respond to and analyze incidents.
- Describe how to develop a business continuity plan.
- Explain:

- Quantitative and qualitative risk assessment approaches.
- Business impact analysis (BIA).
- Business continuity plan (BCP).
- Disaster recovery plan (DRP).

Module 7 **Access Controls for Systems, Applications, and Data Access**

Objectives **When you complete this module, you should be able to:**

- Demonstrate how to encrypt and decrypt messages using the transposition method.
- Demonstrate how to encrypt messages using the substitution method.
- Explain the differences between symmetric and asymmetric cryptography.

Explain:

- Secret key and public key cryptography.
- Encryption mechanisms and techniques.
- Business applications of cryptography.
- Impact of compliance laws on maintaining confidentiality of privacy data.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 7	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 8	Sunday 11:59 PM EST/EDT

Module 8 **Security Operations and Administration**

Objectives **When you complete this module, you should be able to:**

- Classify the International Standards Organization/Open Systems Interconnection layers and characteristics.
- Analyze the Transmission Control Protocol/Internet Protocol (TCP/IP).
- Distinguish among wide area networks (WANs), local area networks (LANs), and the Internet, intranets, and extranets.
- Describe incident-detection and attack-prevention tools and techniques.

Explain:

- Physical and logical network topologies.
- Characteristics of a secure network.
- The impact of malicious code and malware on public- and private-sector organizations.
- The security awareness training to harden User domain and the correct use of IT assets.

Assignments

Items to be Completed:	**Due No Later Than:**
Read the assigned materials	
Post an initial response to the discussion question	Thursday 11:59 PM EST/EDT
Post responses to at least two classmates	Sunday 11:59 PM EST/EDT
Submit Lab Assignment 9	Sunday 11:59 PM EST/EDT
Complete Test 4	Sunday 11:59 PM EST/EDT