Information Assurance Specialization
College of Technology, University of Houston

Course Description

Course:	Introduction to Information Systems Security
Course Number:	ITEC 5321
Credit Hours:	3 hours
Department:	Information and Logistics Technology

Catalog Description
ITEC 5321
Introduction to Information Systems Security
3 credit hours
Overview of contemporary information systems security issues for technology professionals from an applied perspective.

Course Overview
This course introduces the student to the principles of enterprise information systems security. These principles are examined within operational, technical, and administrative contexts. Specific operational issues include continuity planning, physical security and operations management. Specific technical issues include networking, cryptography and trusted computing. In addition to policy, specific administrative issues include, risk assessment, evaluation and management. Security standards and models as well as certification and accreditation are also examined here. Related issues include the legal and regulatory context of enterprise security.

Class lectures are augmented by laboratory and group activities. Laboratory activities are facilitated by the use of Open Source Tools and Live CD based security toolkits. These activities provide students the opportunity to apply security principles. Laboratory activities focus on several areas: system and network monitoring, applied cryptography as well as enterprise security assessment and evaluation.

Learning Objectives
At the end of this course, the student will be able to:

1. Draw and explain major enterprise security models
2. Define and explain the relationship between vulnerability, asset, threat, and risk.
3. Explain the relationship between security and an organization's mission.
4. Define three access control models.
5. Describe security policy and differentiate it from related constructs such as guidelines, procedures and standards.
6. Explain how risk analysis and risk management relate to Information Assurance.
7. Articulate possible risk responses.
8. Draw and explain OSI/ISO and TCP/IP layered communication models

9. Define telecommunication/LAN vulnerabilities, threats, risks and countermeasures (controls).
10. Define, compare, and contrast Disaster Recovery and Business Continuity Planning
11. Identify and discuss security issues related to personnel decisions.
12. Articulate and explain basic enterprise security assessment and evaluation methodologies.
13. Within an IA context, define and explain ethics. Identify two established IT security codes of conduct.

Subject Matter Modules *

Module#	Topic
Mod 1	Risk, Modeling and Management
Mod 1A	Open Source Security Toolkits
Mod 2	Enterprise Risk Management
Mod 2A	Security Toolkit Introduction
Mod 3	Information Assurance Framework (Policy, Procedures, and Guidelines)
Mod 3A	Foot-printing, Scanning, and Enumeration
Mod 4	Networking Security Basics
Mod 4A	Introduction to Packet Analysis (Wireshark)
Mod 5	Cryptology
Mod 5A	Introduction to Cryptography
Mod 6	Access Control
Mod 6A	Hands on Free and Open Software Tools
Mod 7	Continuity Planning and Disaster Recovery, Physical Security
Mod 7A	Malware and Software Vulnerabilities
Mod 8	Law, Investigations, and Ethics, Physical Security
Mod 8A	Risk Analysis Case Study Group Activity
Mod 9	Assuring against Software Vulnerabilities, Security Architecture
Mod 9A	System and Network Monitoring
Mod 10	Project Preparation and Preliminary Poster Presentation
Mod 11	Final Exam
Mod 11A	Project Presentations

* Note that each subject matter module consists of 4 contact hours. Note also that each module includes a lecture component as well as an active learning component. In the active learning component the students work either on 'Hands-On" laboratory assignments or on group projects.

Detailed Course Outline

1. Risk, Modeling and Management
   1.1. Computer Crime
   1.2. Computer Crime Laws
   1.3. Security Goals
   1.4. Security's Relationship to Enterprise's Mission

1.5. Confidentiality, Integrity, Availability, Authentication, and Non-repudiation
1.6. Risk Primitives
1.7. Assets, Information in Transit, Information in Storage, Information in Processing, and Information Criticality
1.8. Vulnerabilities including people, processes, and technology
1.9. Threats Natural and Man Made including Disasters, Social Engineering and Malware
1.10. Countermeasures
1.11. Risk Models
1.12. Risk Assessment
1.13. Risk Management
1.14. Defense in Depth (DID)
1.15. Ethics

1A Open Source Security Toolkits
1A.1 Introduction to Live Linux CDs
1A.2 Interactive Demonstration
1A.3 System and network mapping, Vulnerability Scanning
1A.4 Protocol Analysis
1A.5 Class activity: Students burn their own Live CDs

2. Enterprise Risk Management Overview
2.1. People, Processes, and Technology Enterprise Model
2.2. Enterprise Information Assurance
2.3. Risk Assessment
2.4. Vulnerability, Threat, and Control (Countermeasure) Analysis
2.5. Impact and Risk (Threat-Vulnerability Pair) Analysis
2.6. Evaluation, Assessment, and Audit
2.7. Enterprise Education, Training, and Awareness
2.8. Ethics
2.9. ISC2 Code of Ethics
2.10. IAB Ethics and the Internet RFC 1087

2.0A Security Toolkit Introduction
2A.1 Orientation
2A.2 Boot Environment
2A.3 Interface Features
2A.4 TCP/IP Foot-printing Utilities
2A.5 TCP/IP Networking Utilities
2A.6 Software Licenses (GNU GPL)
2A.7 Software Piracy

3. Policy, Procedures, and Guidelines
3.1. Define and document an information assurance framework
3.2. Differentiate between policies, procedures, and guidelines
3.3. Security Policy

3.4. Roles, System Owner, Data Owner, Custodian, User
3.5. Identify role of IA policy
3.6. Define IA Framework major components
3.7. Operational Security
3.8. Create dependable operational security process
    3.8.1. Electronic Records Management
    3.8.2. System impact concerning records management
    3.8.3. Record Retention Policy
3.9. Ensure operational incident response
3.10. Personnel Security
3.11. Ensure secure behavior
3.12. State the role of human resources in ensuring personnel security
3.13. Define contractor control
3.14. Physical Security
3.15. Manage dispersion and diversity problems
    3.15.1. Secure Media Disposal And Destruction Policy
3.16. Construct a security process using a security plan
3.17. Mitigate physical security threats

3.0A Foot printing, Scanning, and Enumeration
    3A.1 Demonstrate and Explain Foot printing
    3A.2 Foot printing, Scanning, And Enumeration Tools
    3A.3 From publicly available information, identify an organization's internal components.
    3A.4 Ascertain an organization's assigned IP range
    3A.5 Within a local area network, map active host machines
    3A.6 Scanning and Enumeration

4. Networking Security Basics
    4.1. Define layered protocol models including: ISO/OSI and TCP/IP
    4.2. Identify major telecommunication and network components for both peer to peer and client/server networks
    4.3. Explain packet orientated communications
    4.4. Analyze TCP/IP
    4.5. Define firewall architectures
    4.6. List communication related security issues including electronic emanations
    4.7. List major attacks types
    4.8. Network Auditing and Monitoring
    4.9. Intrusion Detection

4.0A Introduction to Packet Analysis (Wireshark)
    4A.1 Wireshark/Ethereal (packet analysis) Interactive Demonstration.
    4A.2 Capture Ethernet Packets.
    4A.3 Identify and Explain the Packet Header for each TCP/IP layer.
    4A.4 Identify Three Way Handshake.
    4A.5 Reassemble a visited web page from the captured packet stream.

5. Cryptology
    5.1. Cryptography
    5.2. Articulate cryptology's history, purpose, and function
    5.3. Describe fundamental encryption elements and services
    5.4. Differentiate among symmetric, asymmetric and one way encryption
    5.5. Key management and key management problems
    5.6. Key Escrow
    5.7. Cryptanalysis
    5.8. Cryptanalysis Demonstration
    5.9. Define Public Key Architecture
    5.10. Identify PKI Components

5.0A Introduction to Cryptography
    5A.1 Random Numbers and Random Number Generation
    5A.2 Symmetric Cryptography with DES
    5A.3 Asymmetric RSA Key Pair Generation

6. Access Control, Applications and Systems Development
    6.1. Access Control MAC, DAC, RBAC, and NDAC
    6.2. Access Control Models
    6.3. Authentication Policy
    6.4. Authentication Procedures
    6.5. Authentication Methods Passwords, Tokens, Biometrics
    6.6. Kerberos and other SSOs
    6.7. Principles: Need to Know
    6.8. Software Development Life Cycle
        6.8.1. Secure Media Disposal
    6.9. Development Process
    6.10. Software Maintenance and Change Control
    6.11. Configuration Management
    6.12. Database and Data Warehousing Systems
    6.13. Aggregation and Inference
    6.14. Database Security Issues
    6.15. Data Mining
    6.16. Object Orientated Systems

6.0A Hands on Free and Open Software Tools
    6A.1 Account Management
    6A.2 File System Access Control
    6A.3 App Program Security and Configuration
    6A.4 Data Remanence

7. Continuity Planning/Disaster Recovery, Physical Security
    7.1. Backup and Restore
    7.2. Continuity Planning Scope

7.3. Business Impact Assessment (BIA)
7.4. Continuity Plans
7.5. Develop Effective Business Continuity Planning (BCP) Approaches
7.6. Organize and manage incident response
7.7. Disaster Recovery Planning (DRP)
7.8. Physical Access Control
7.9. Site Selection/Design Considerations
7.10. Man Traps, Guards, and Gates
7.11. Badges, smart and dumb cards
7.12. Biometrics
7.13. Detection Control with CCTV
7.14. Power and HVAC Considerations
7.15. Fire Detection and Suppression
7.16. Site Safety

7.0A Malware and Software vulnerabilities
7A.1 Trojans, Back doors, DoS, and Buffer Overflows
7A.2 Malicious Code Management and Hoaxes
7A.3 Malicious Code Policies and Protection
7A.4 Operating System Vulnerabilities and Analysis

8. Law, Investigations, Ethics
8.1. Computer Crime and Computer Laws
8.2. Computer Fraud and Abuse Act
8.3. HIPAA, GLB, and SOX
8.4. Federal Information System Management Act (FISMA)
8.5. Freedom of Information Act
8.6. Copyright Act and the Digital Millennium Copyright Act (DCMA)
8.7. USA Patriot Act
8.8. Civil and Criminal liabilities
8.9. Due Care and Due Diligence
8.10. Incident response and computer forensics
8.11. Crime determination
8.12. Investigation basics
8.13. Evidence preservation
8.14. Computer Ethics

8.0A Risk Analysis Case study Group Activity
8A.1 Information and System Criticality
8A.1.1 Hardware and Software Inventory
8A.2 Vulnerability Assessment
8A.3 Threat Assessment
8A.4 Controls Assessment
8A.5 Risk Assessment and Security Posture

9. Assuring against Software Vulnerabilities, Security Architecture and Models

9.1. Assure against software vulnerabilities
9.2. Evaluate commercial hacking attempts
9.3. Quantify the software assurance process
9.4. Software Licensing and Software Piracy
9.5. Security Architecture and Models, ISO 17799
9.6. Trusted Computer System Evaluation Criteria (Orange Book, TCSEC) and the Information Technology Security Evaluation Criteria (ITSEC)
9.7. Common Criteria for Information Technology Security Evaluation (CC)
9.7.1. NIAP Common Criteria Evaluation and Validation Scheme
9.8. Certification and Accreditation
9.9. Defense Information Technology Security Certification and Accreditation Process (DITSCAP)
9.10. National Information Assurance Certification and Accreditation Process (NIACAP)
9.11. Security Models
9.12. Access Control Models
9.13. Access Matrix
9.14. Bell LaPadula
9.15. Take Grant
9.16. Integrity Models
9.17. Biba, Clark Wilson
9.18. Information Flow Models
9.19. State Machine
9.20. Cover Channels

9.0A System and Network Monitoring
9A.1 Network Security Monitoring
9A.2 Firewalls
9A.3 Zone log analysis
9A.4 Making Good Passwords and Auditing Password Policy
9A.5 Log Analysis

Mod 10 Project Preparation

Mod 11 Final Exam

Mod 11.0A Project Presentations

Text Books

Title	Information Assurance for the Enterprise
Author	Schou and Shoemaker
Publisher	McGraw-Hill, Higher Education, ISBN: 978-0-07-225524-9
Year	2007

Title Hands-On Information Security Lab Manual; Second Edition

Author	Whitman, Mattord and Shackleford
Publisher	Thomson/Course Technology, ISBN:10: 0-619-21632-X, ISBN-13: 978-0-619-21631-3
Year	4 March 05

Required Readings

Title	Risk Management Guide for Information Technology Systems
Author	Stoneburner, Goguen, and Feringa
Publisher	NIST SP-800-30
Year	2002

Title	Generally Accepted Principles and Practices for Securing Information Technology Systems
Author	Swanson and Guttman
Publisher	NIST SP-800-14
Year	1996