River Valley Community College
One College Place
Claremont, NH 03743

March 2012

PRINCIPLES OF INFORMATION ASSURANCE

CURRICULUM AND COURSE NUMBER: CYBS 101R
DEPARTMENT: Business/Computer Technology
CREDIT HOURS: 3
SEMESTER HOURS: **CLASS:** 2   **LAB:** 2
PREREQUISITES/COREQUISITES: CSCI 101R or POI

COURSE DESCRIPTION

Students will be introduced to basic security principles, giving the student an understanding of the current threats and vulnerabilities of the cyber landscape, plus other topics relating to the information assurance field.

Course Competencies:
Upon successful completion of this course, the student will be able to:
1. Ethics: In this topic, students learn the importance of recognizing and practicing ethical behavior in computer security and its related fields. A score of 100 percent is required before moving on to the next module. The student signs an ethical behavior agreement.
   a. Gain an insight into what makes up computer ethics
   b. Examine and discuss the hacker mentality through a review of a hacker's manifesto
   c. Review the "Ten Commandments of Computer Ethics"
   d. Read and sign a computer ethics statement
2. Security Concepts: In this topic, students explore the core concepts and components of computer, network, and physical security
   a. Examine and understand the general security concepts and relationships outlined in the Common Criteria
   b. Identify and describe each component of the security "CIA" triad
   c. Distinguish between the roles of identification, authentication, and nonrepudiation
   d. Define and explain the operational model of security
   e. Compare and contrast host and network security
   f. Describe the concept of least privilege in security
   g. Explain the importance of layered and diversified security with minimal complexity
   h. List and describe the three methods of access control
   i. Compare and contrast the confidentiality and integrity security models, providing examples of each
   j. Explain the roles of security policies, standards, guidelines, and procedures
   k. List and describe six security concerns associated with people
   l. Identify two components of physical security and discuss the implications presented by wireless networks

m. Explore security issues related to the physical environment
n. Explain the importance of business continuity planning and disaster recovery
o. Research, define and describe security risks associated with several common categories of malware and scripting languages
p. Research, define and explore common cryptographic terms and concepts

3. Physical Security: In this topic, students identify the physical security measures used to secure not only automated information systems hardware and software, but also those used to secure the facilities in which those systems are housed.
   a. Identify the principles of physical security
   b. Learn ways to mitigate risk as concerned with physical security
   c. Complete a physical security checklist in regards to your own facility

4. Identifying Security Threats and Attack Techniques: In this topic, students discover the common threats to which automated information systems are exposed, and the countermeasures used to mitigate those threats. Given examples, students learn how to map networks, identify network operating system types, and scan for potential holes in those operating systems. The concepts behind viruses, worms, and Trojan Horses are examined. Students will identify password-cracking techniques, and explore and discuss basic scripting techniques.
   a. Explore, discuss, and identify social engineering attack techniques
   b. Describe audit attacks
   c. Identify hardware attacks
   d. Identify the major categories of network threats
   e. Differentiate between a virus, a worm, and a Trojan horse
   f. Identify the elements of a virus protection plan
   g. Identify the components of local network security
   h. Identify network authentication methods
   i. Identify major data encryption methods and technologies
   j. Identify the primary techniques used to secure Internet connections
   k. Define the process of network reconnaissance
   l. Map, sweep, and scan a network
   m. Perform local and remote Vulnerability Scanning
   n. Gain control over a network system
   o. Record keystrokes with software and hardware
   p. Crack encrypted passwords on Linux and Microsoft machines
   q. Investigate potential ways that unauthorized administrator access can be achieved
   r. Hide the evidence from an attack
   s. Perform a Denial of Service on a target host

5. Common Criteria: In this topic, students are introduced to the Common Criteria (CC), including its historical development, and terms and definitions. Students explore CC literature, including CC Parts 1, 2, and 3, and the CC Users Guide. Students identify the roles of Protection Profiles (PP), Security Targets (ST), and Targets of Evaluation (TOE) in the certification process. Security Functional Requirements and Security Assurance Requirements are reviewed in order to show how selected functional and assurance components are suitable to counter the threats in an intended environment. The seven Evaluation Assurance Levels (EALs) are examined, assessing the rising scale of assurance associated with the increasing rigor represented by each EAL.
   a. Understand the history and function of the Common Criteria
   b. Identify the terms and definitions used in the Common Criteria
   c. Define and identify the roles of Protection Profiles, Security Targets, and Targets of Evaluation in the certification process

d. Consider how the Common Criteria serves the interests of its target audience (TOE consumers, TOE developers, and TOE evaluators)
e. Identify and define the seven Evaluation Assurance Levels used in the Common Criteria
f. Identify the general purpose of each Functional Class and explore the families, components, and elements comprised therein
g. Identify the general purpose of each Assurance Class and explore the families, components, and elements comprised therein
h. Define system security architecture and determine the appropriate functional and assurance components for a given automated information system in a particular environment
i. Discuss how the Centralized Certified Products List (CCPL) allows for products, such as firewalls and operating systems, to be selected so as to provide an appropriate level of Information Assurance
j. Discuss the role of system custodians and system security officers as defined in Part 1 of the Common Criteria

6. Hardening Linux Computers: In this topic, students are introduced to the core operational principles of Linux. Students learn to manage users, groups, and file system permissions, and configure Pluggable Authentication Modules (PAMs). System information, services, and processes are examined such that students develop an understanding of how to manipulate them for security. Shell scripts, network protocols, and security tools are utilized to harden and manage Linux security.
   a. Perform fundamental Linux administrative functions
   b. Examine system information and investigate the management of processes in Linux
   c. Determine and implement appropriate Linux user and file system security
   d. Evaluate and utilize built-in and add-on services and network protocols to configure Linux network security
   e. Create and evaluate simple shell scripts executing Linux command strings
   f. Evaluate and implement various security tools, including Bastille and Tripwire, to improve Linux security

7. Hardening Windows Server 2003: In this topic, students investigate the concepts and procedures required to secure Microsoft Windows computers. Students examine an advanced range of security principles and management tools, including authentication, auditing and logging, group policy, security templates, the Registry, Encrypting File System (EFS), Active Directory, Windows Firewall, and various network security components and protocols.
   a. Study Windows 2003 infrastructure security concepts and create a custom Group Policy Object
   b. Examine the fundamentals of authentication in Windows 2003 and describe the local logon process
   c. Investigate and implement Windows 2003 security configuration tools, including security templates, secedit.exe, and the Security Configuration and Analysis snap-in
   d. Examine and configure security settings in the Registry
   e. Configure auditing and logging, and analyze Security Log Event IDs
   f. Examine the components of and implement the Encrypting File System on Windows 2003
   g. Study and configure the systems available to secure Windows 2003 network communications, including Windows Firewall and hardening TCP/IP

8. Security on the Internet and the WWW: In this topic, students learn how to identify the security issues associated with the Internet and World Wide Web. The major components of the Internet and their functions are explored. This is followed by an examination of techniques used to attack the Internet's components contrasted against those used to attack the Internet's users.
    a. Identify and describe the functions of the major components comprising the Internet
    b. Identify and explain the roles of the organizations governing the Internet
    c. Evaluate and discuss some of the major disruptions that have occurred over the last several years
    d. Identify the role of and risk mitigation techniques for Domain Name Services (DNS)
    e. Discuss areas of vulnerability associated with the Internet, and analyze where attacks have the highest probability of occurring and what those attacks are likely to be
    f. Identify the risks faced by Internet users and discuss ways in which to mitigate these risks

Course Outline:

Foundations of Network Security	Security on the Internet and the World Wide Web
Data Confidentiality, Integrity, and Availability	Physical Security Measures
Securing Windows and Linux Computers	Attack Techniques
Routing and Access Control Lists	Threats and Countermeasures
	Legal and Ethical Issues in Cyber Security

Learning/Instructional Methods:

Lectures	Discussions
PowerPoint Presentations	Term Papers
Lab and Reading Assignments	

Performance Evaluation:

Midterm and Final Exams	Weekly written assignments
Term Paper	Discussion participation
Quizzes	

Suggested Text(s):   Please refer to syllabus

Origination date: March 2012

Revisions: