Southeast Missouri State University

Department of Industrial and Engineering Technology — Course No. CY501

Title of Course: Introduction to Cybersecurity — Revision

New Fall 2012

I. Catalog Description and Credit Hours of Course:

Broad introduction to the field of Cybersecurity. Information assurance terminology and issues. Computer forensics investigation and methodology. 3 credit hours (2 hours lecture and 2 hours lab).

II. Prerequisite (s): CS155 or consent of instructor.

III. Purposes or Objectives of the Course:

A. Understand basic information assurance terminology.

B. Understand ethical and legal issues in computing.

C. Understand computer security policies and how they are implemented in organizations.

D. Understand privacy concerns in computing.

E. Understand how secure computer systems are designed.

F. Understand basic computer forensic terminology.

G. Understand the basic methodology of a computer forensic investigator.

H. Perform some basic forensic investigation using up-to-date software tools.

IV. Student Learning Outcomes:

A. Students will be able to correlate information assurance terminology to relevant aspects of a computing system.

B. Students will be able to identify proper cryptographic choices to suit the need of a computing system within the ambit of privacy concerns.

C. Students will be able to demonstrate ability to perform basic computer forensic investigation using software tools in an ethical way.

V. Expectations of Students:

A. Students are expected to read assigned materials.

B. Students are expected to complete all assignments. Assignments will ONLY be accepted on the due dates provided, unless previous arrangements are made or student provides a written medical doctor's excuse.

C. Students are expected to participate in class and group discussions.

D. Student work will be completed in accordance with Code of Student Conduct (http://www6.semo.edu/judaffairs/code.html).

E. In a professional environment, work areas are kept clean. In keeping with a professional attitude towards fellow students, always clean your area before leaving.

F. All laboratory work must be completed during the regularly scheduled lab time.

VI. Course Content or Outline: (*4 contact hours per week*)

A.

1.	Overview of Security in Cyber Infrastructure	2 Weeks
2.	Legal and Ethical Issues in Computing	2 Weeks
3.	Threats to Cyber Infrastructure	2 Weeks
4.	Privacy In Computing	1 Week
5.	Security policies	1 Week
6.	Elementary Cryptography	1 Week
7.	Secure Programs, Malware, Anti-Virus etc.	1 Week
8.	Security In Operating Systems	2 Weeks
9.	Networking/Database Security	1 Week
10.	Tools for Forensic Analysis	2 Weeks

VII. Textbook(s) and/or Other Required Materials or Equipment:

A. Security in Computing by Charles P Pfleeger, Shari Pfleeger (Prentice-Hall, Fourth Edition). Supplemental materials will be provided by the instructor.

VIII. Basis for Student Evaluations

A.

Homework	15%
Labs	10%
Class Participation*	5%
Mid-term Exam	25%
Final Exam	30%
Project	15%

B. Grading Policy:

90-100	A
80-89.9999	B
70-79.9999	C
<70	F

C. The weight of evaluation criteria may vary at the discretion of the instructor and will be indicated at the beginning of each course.

D. *Participation to class discussions, taking labs, homework, and exams on the assigned time slots. The instructor reserves the right, acting within the policies and procedures of the university, to make changes in course content or instructional techniques without notice or obligation. No late assignments will be accepted. “Emergencies” require that YOU contact the instructor ASAP. Request for a late submission after the due time will not be granted.