Southeast Missouri State University

Department of Industrial and Engineering Technology — Course No. CY510

Title of Course: Information Security and Assurance — Revision

New Fall 2012

I. Catalog Description and Credit Hours of Course:

System security principles, Components of system security, Information assurance with high assurance software design, Cryptographic principles to design secure systems, Data protection at rest and in motion and evolution of challenges in information security. 3 credit hours.

II. Prerequisite (s): CY201 or consent of instructor.

III. Purposes or Objectives of the Course:

A. Understand system requirements for information assurance.

B. Understand high assurance security design principles.

C. Understand how secure systems are built around software, hardware, and networks.

IV. Student Learning Outcomes:

A. Students will be able to identify critical components in system security of a cyber-infrastructure.

B. Students will be able to demonstrate usage of cryptographic primitives in design of information security systems.

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. Embedded Systems Security: Practical Methods for Safe and Secure Software and Systems Development, David Kleidermacher, Mike Kleidermacher, ISBN-10: 0123868866, ISBN-13: 978-0123868862

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.