Computer Science and Engineering CSE 4243
Information and Computer Security

CREDIT/CONTACT HOURS: Credit Hours: 3, Contact Hours: 45

COORDINATOR:
Dr. David Dampier

   a. Supplemental Material: Handouts, lab exercises, and web site at http://www.cse.msstate.edu/~cs6243

SPECIFIC COURSE INFORMATION:
   a. Catalog Description: Three hours lecture. Topics include encryption systems, network security, electronic commerce, systems threats, and risk avoidance procedures.
   b. Prerequisites: Grade of C or better in CS 4733/6733
   c. Required/Elective:
      Computer Science – Elective
      Software Engineering – Selected Elective
      Computer Engineering – Elective

SPECIFIC GOALS OF THE COURSE
   a. Specific Outcomes of Instruction:
      1. Provide an introduction to the security engineering discipline
      2. Expose students to contemporary risks and attack procedures.
      3. To provide students with an appreciation of the historical perspective in information assurance research.
      4. Describe security engineering processes – particularly those being used in industry.
      5. Students will be able to apply generally accepted selection criteria to choose security products.
      6. Students will be able to design a defense in depth architecture to defend a specific system from attack.
      7. The student will be able to apply standard, accepted security engineering techniques to protect a system with respect to a specific organizational security policy.
      8. The student will demonstrate an ability to document their work to an acceptable standard.
   b. Criterion 3 Outcomes:
      Note: Parenthesized list indicates the ABET EAC and CAC outcomes addressed by each performance criteria.
      1. The student will be able to describe, discuss, and apply the security engineering discipline. (EAC: e; CAC: b)
      2. The student will be able to select the correct process for a given security requirement scenario. (EAC: c; CAC: c)
3. The student will be capable of discussing the historical perspectives of security engineering and apply lessons learned to contemporary problems. (EAC: g,i,j; CAC: f,h)

4. The student will be able to architect a defensive perimeter for an unprotected system. (EAC: c,e; CAC: b,c)

5. The student will demonstrate proficiency in selecting appropriate security products by using generally accepted security engineering practices. (EAC: a,b,e; CAC: a, b)

6. The student will be able to discuss the broad implication of risk to their system in a global, interconnected network and recommend solutions to mitigate that risk. (EAC: h, j, k; CAC: g, i)

7. The student will demonstrate an ability to consider ethics and law in application of security engineering. (EAC: f,h,j; CAC: e,g)

TOPICS COVERED:

1. Security Engineering Perspectives  2
2. Security Historical Perspectives  2
3. Operating System Security  3
4. Database Security  3
5. Network Security  3
6. Security Administration  3
7. Encryption types and techniques  2
8. Prevention, Detection, and Response  3
9. Guest Speakers  3
10. Legal and Ethical Issues  3
11. Exams  3