

CS458 – Information Security

Last Updated - 2/3/04

Course Manager - Dr. David Grossman, Associate Professor

3 credit hours; elective for CS & CPE; 150 min. lecture each week

Catalog Description - An introduction to the fundamentals of computer and information security. This course focuses on algorithms and techniques used to defend against malicious software. Topics include an introduction to encryption systems, operating system security, database security, network security, system threats, and risk avoidance procedures. Prerequisites: CS 425 and CS 450. (3-0-3)

Textbook - Security in Computing, 2nd edition. Charles P. Pleegeer. Prentice Hall, 1997.

References - Relevant security engineering papers are provided to students to supplement text material.

Course Goals - Students should be able to:

- Provide an introduction to the security engineering discipline
- Expose students to contemporary risks and attack procedures.
- To provide students with an appreciation of the historical perspective in information assurance research.
- Describe security engineering processes – particularly those being used in industry .
- Students will be familiar with fundamental encryption algorithms
- Students will be able to design an architecture to defend a specific system from attack.
- The student will be able to apply standard, accepted security engineering techniques to protect a system with respect to a specific organizational security policy.
- The student will demonstrate an ability to document their work to an acceptable standard.

Major Topics Covered in Course

1. Security Engineering Perspectives	3 hours
2. Security Historical Perspectives	3 hours
3. Operating System Security	4.5 hours
4. Database Security Algorithms	4.5 hours
5. Network Security	4.5 hours
6. Security Administration	4.5 hours
7. E-Commerce Security	4.5 hours
8. Encryption types and techniques	6 hours
9. Prevention, Detection, and Response	6 hours
10. Legal and Ethical Issues	4.5 hours
	45 hours