

COURSE DESCRIPTION

Dept., Number	CS458	Course Title	Information Security
Semester hours	3	Course Coordinator	Dr. David Grossman, Associate Professor

Current 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. Pleege. Prentice Hall, 2007

References

Introduction to Computer Security, Matt Bishop, Addison Wesley, ISBN: 0-321-24744-2
Exploiting Software - How to Break Code, Greg Hoglund and Gary McGraw, Addison Wesley, ISBN: 0-201-78695-8

Course Outcomes

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.

Relationship between Course Outcomes and Program Outcomes

The following Program Outcomes are supported by the above Course Outcomes:

- c. An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs

- e. An understanding of professional, ethical, legal, security, and social issues and responsibilities
- f. An ability to communicate effectively with a range of audiences.
- g. An ability to analyze the local and global impact of computing on individuals, organizations and society
- i. An ability to use current techniques, skills, and tools necessary for computing practices.
- j. An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices

Prerequisites by Topic

Operating Systems, Databases and Programming Knowledge

Major Topics Covered in the 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

Assessment Plan for the Course

End of every semester Course Objective Assessments by CS department. End of semester Course Evaluations by IIT. Reviewed every Spring semester by CS Undergraduate Studies Committee for possible updates in the following Fall. Once every 4-5 years a detailed review of all materials for the course is made by the CS Undergraduate Studies Committee.

How Data in the Course is Used to Assess Program Outcomes (unless adequately covered already in the assessment discussion under Criterion 4)

See the assessment discussion under Criterion 4

For a computer science program

Estimate Curriculum Category Content (Semester hours)

Area	Core	Advanced	Area	Core	Advanced
Algorithms		1.5	Software design		
Data structures			Concepts of programming languages		1.5