Security Risk Analysis, INF 766
University at Albany, State University of New York
Fall 2003

Instructor Information

Name: Sanjay Goel (Lecture Material)/ George Berg (Instructor)
Email: goel@albany.edu / berg@albany.edu
Phone: (518) 442 4925 / (518) 442-4267
Office Hours: (Berg) Tuesday 11:30-1:00, Wednesday 11:30-12:30

Class Information

Time: 8:30-11:30
Room: BA 222
Dates: 02/24-3/23
Credit(s): 1
Call #: 8932
Available Labs: BA222

Course Website:

http://www.cs.albany.edu/~berg/risk_analysis/

Course Overview

This course introduces concepts and methodology that information officers in public and private enterprises can use to analyze and mitigate the impact of security threats to the assets of their organizations. Work in information systems security risk analysis is very fluid, and standards are still evolving so this course draws from literature in different disciplines and security practices provided by National Institute of Standards and Testing (NIST). The course is designed to provide practical techniques and living cases that can be modified to work on the specific problems of different organizations. Theoretical concepts of risk analysis and system security will be covered at a high level with references for finer details. Two living cases are selected for risk analysis in addition to the case of the student's own organization. The class has three parts, the first part is security vulnerabilities, the second part is risk analysis and the third part is security policies.

Course Prerequisites

It is assumed that the students come in with varied background in information systems so the class starts with a general background of computer security. It would be helpful if the students have a general awareness of the following topics:

1. Computer Networks
2. Computer Architecture
3. Security
    a. Hacking Attacks
    b. Viruses and Worms
4. Basic Statistical Analysis
5. Database Architecture and System Administration

Learning Objectives (Programming Concepts)

Students will learn:

1. Various vulnerabilities of computers & network and the different modes of attack
2. Methodology for Risk Analysis
3. Application of risk analysis for security risk in their own organizations

Students should be able to:

1. Analyze the security risk of an organization
2. Create a security plan for the organization
3. Optimize the allocation of resources to security refinements

Class Structure

The first half of each class is going to be conducted in the class room and the second half of the class will be conducted in the computer lab. The students will learn the basic concepts in the first half of the class and go through an exercise in the second half. Please come prepared with the readings as the class will move at a brisk pace.

Assignments

There will be assignments after each class which you need to do to understand the subject material. Please work individually on all assignments. It is okay to discuss the concepts and questions with other colleagues but it is improper to copy each others work. All assignments will not be graded, however, please make sure that you complete all your assignments. The assignments must be submitted in the class one week after the assignment with your name and the assignment number clearly marked on the assignment sheet.

Project

In the project students are expected to work on security risk analysis of their organizations and submit the entire analysis as well as the security plan as projected for the next five years.

Text & Reference Books

Two books are listed in the syllabus, however, I expect students to purchase only the text book. The other book is only listed for students who would like additional material to increase their understanding. There is also a lot of material available on the web. Please check the NIST and CERT web sites for additional information.

Text: Security In Computing (Third Edition) by Charles P. Pfleeger & Shari Lawrence Pfleeger
Reference: Hackers Beware by Eric Cole

Grading

Project & Homework: 50%
Exam: 50%

Course Schedule

Lecture	Date	Topics	Readings
1	02/24	Introduction to Security, User Authentication & Password Based Attacks	Pfleeger Chapter 1
		Password Security Laboratory	
2	03/02	Network Based Attacks & Controls	Pfleeger Chapter 7
		Network Penetration Laboratory	
3	03/09	Security Risk Analysis - Qualitative	Pfleeger Chapter 8
		Case Study	
4	03/16	Security Risk Analysis - Quantitative	Pfleeger Chapter 8
		Case Study	
5	03/24	Security Policies	Notes
		Case Study + Take Home Exam	