

INF 741: Security Policies
University at Albany, State University of New York
NYS Center for Information Forensics and Assurance
Spring 2007 Syllabus

Instructor Information

Name: Sanjay Goel
Email: goel@albany.edu
Phone: (518) 442-4925
Office Location: BA 310b, University at Albany
Office Hours: Monday 12:30-2:00 or by Appointment

Class Information

Location: NA
Dates: March 19-30, 2007
Credit(s): 1
Call #: 8944
Available Lab(s): CIFA Teaching Laboratory

Resources

Course Website: The course website is located at: <http://ecourses.purdue.edu>. You must click on "West Lafayette Open Campus" to access the proper site. Click on "Log In" and sign in using the User name and Password assigned to you via email.

Readings: Reference readings will be posted at the end of each presentation. Available readings will be accessible via <http://eres.ulib.albany.edu>. You must click on "Electronic Reserves & Reserve Pages" and then type in "INF741" in the empty box. Click under the Course Number section (which is hyperlinked) you will be asked to input a password. The password to access this information will be provided via email and is case-sensitive. All of the readings is divided by Unit and contains readings in pdf format or web links to readings.

Reference Books:

Writing Information Security Policies by Scott Barman

Course Overview

This course provides students with an introduction to information security policies. Students will be introduced to sociological and psychological issues in policy implementation in general and then provided a focused dialogue on information security specific policies. The class discusses the entire lifecycle of policy creation and enactment and presents the students with issue specific policies in different domains of security. The structure of the policy is also discussed to assist the students design and modify policies. Several examples from different domains are incorporated in the curriculum to assist the students learn in context of real life situations.

Course Format

The class is taught in an online format where the students can learn at their own pace. The learning environment is very interactive containing, instructor video, discussion groups, and interactive quizzes. Students learn the basic elements of security policies as well as the process of enacting security policies. It is assumed that the students have a good understanding of risk analysis, which will assist the students in understanding security policies. To illustrate the concepts context is build through use of examples and case studies. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value. Even though the course is spread over 2 weeks, it is important that students stay on schedule so that they can participate with other students in discussions. The class should require approximately 40 hours of work. This should work out to roughly 15 hours of video and lecture material, 2 hour worth of quizzes, 4 hours for discussion postings, 12 hours for the final project, and 7 hours of readings.

Each class comprises of theoretical elements as well as case analysis. Please come prepared with the readings since the class will move at a brisk pace. Readings will be announced

approximately a week before class. All the information will be posted on this webpage. Students are expected to use critical thinking skills as they go through the material rather than accepting facts at face value.

Course Prerequisites

The prerequisite or co-requisite is the INF 710: Information Security Risk Assessment course. It is assumed that students will have a general background of computer security. It would be helpful if students have some knowledge of the following topics:

1. Computer Networks
2. Computer Architecture
3. Software Design
4. Risk Analysis (assets, threats, vulnerabilities, and controls)

Learning Objectives

Students should be able to:

1. Understand the lifecycle of policy enactment
2. Create and modify security policies
3. Create a dissemination plan for the policy
4. Critique the security policy for its effectiveness and completeness

Grading

Quizzes: 20%

Discussion Postings: 30%

Project: 50%

Quizzes

Please work individually on all quizzes. A quiz will be offered after each Unit is completed through a link.

Discussion Postings

Even though this is an online course, it is expected that students will be able to learn from each other and participate in a discussion. To promote this, you will be assigned discussion postings. Discussion postings will generally be due on Wednesday and a response to someone else's posting should be up by the Sunday of that week.

Project

The students will get a project to complete at the end of the class. Students need to complete and submit this via email to the instructor. More details will be given during the class.

Course Schedule

Unit	Topics	Readings
1	General Overview of Policies & Security Policy Lifecycle	TBD
2	Network, Communications, Web, Policies	TBD
3	Security Policies for Software and Data	TBD
4	Security Policy: Audit and Compliance	TBD
5	Case Study	TBD