CS-480/585I: Information Systems Security (INFOSEC), Spring 2003 Semester

Course Syllabus

Summary Course Description:

This course provides a solid theoretical foundation in Information Systems (INFOSEC) Security, including both Computer Security and Communications Security. In addition, Various terms used in the field will be defined, and the basic principles underlying INFOSEC will be laid out. Subjects to be covered include Identification and Authentication, including not just Username and Password but also other techniques, such as biometrics, and also a survey of techniques used by attackers to reveal users' passwords. Principles of access control will be discussed, including subject-oriented, object-oriented, and hybrid techniques, and also several security models, including the Bell-LaPadula (BLP) model, the Biba and Clark-Wilson models, and the Chinese Wall model. Techniques for assuring that the system enforces the stated security policy will be covered, as well as the practical implementation of security in several representative systems. Problems often encountered in system security will be discussed, as well as the evaluation of a system to determine the level of soundness with which security has been implemented.

Security will also be discussed in a distributed environment, wherein several systems must cooperate to provide an operationally secure computing environment. Both cryptography and network security are important in such an environment, and therefore will both be discussed, as well as the problems encountered in the context of the world-wide web. Database security will be examined in depth, including both the notorious inference problem and the special problems associated with implementing Mandatory Access Control in a database environment, and the problems of both concurrency control and transaction control in a secure database.

Required Textbooks and Materials:

(1) GOLLMANN, DIETER (1999). *Computer Security.* New York, NY: John Wiley & Sons. ISBN 0-471-97844-2.

Suggested Supplementary Materials:

Grammar and Writing:

(2) GORDON, KAREN ELIZABETH (1993). *The Deluxe Transitive Vampire: The Ultimate Handbook of Grammar for the Innocent, the Eager, and the Doomed.* New York, NY: Pantheon Books. ISBN: 0679418601. [This book is a concise, wittily written tutorial on the fine points of grammar and punctuation.]

(3) DUPRE, LYN (1998). *Bugs in Writing Revised. A Guide to Debugging Your Prose.* Reading, MA: Addison-Wesley. ISBN: 0-201 37921-X. [The author specifically addresses the needs of computer professionals and other technical people to write clearly.]

(4) STRUNK, WILLIAM, JR.; & White, E.B. (2000). *The Elements of Style. With Revisions, an Introduction, and a Chapter on Writing. Fourth Edition.* New York, NY: Longman. PE1408.S772 1999; 808'.042—dc21; 99-16419; ISBN 0-205-30902-X (paperback) or 0-205-31342-6 (casebound). [A classic on clarity in writing.]

Learning Objectives:

By the end of this course, the student should be able:

(1) to define a precise security policy for a computer system that will meet the security needs of the organization in which the system is sited.

(2) to choose and implement an appropriate means of identification and authentication to be used within the computer system.

(3) to make use of all security models appropriate to the security needs of the organization.

(4) to implement properly the security features of any of the commonly-found operating system, and to study the technical literature pertaining to an unfamiliar operating system and implement its security features, as well.

(5) to understand the principal avenues used to attack computer systems, and to implement appropriate defensive measures.

(6) to evaluate the security features of both commercial off-the-shelf and custom-built products to determine whether they meet the security needs defined for a particular system.

(7) to implement security in a distributed computer system, including installation and effective use of cryptographic mechanisms and network security.

(8) to understand and implement security in a database, including a multi-level secure database environment.

(9) to serve either as a System Security Officer, controlling security in the day-to-day operational environment, or as a System Security Engineer, supervising the design of a new system so that it will incorporate a level of security appropriate for the needs of the environment in which it must operate.

Instructor:

Dr. Charles Abzug

Course Practices.

Grading Policy.

Homework.

Philosophy Regarding Classes Missed by Students.

Class Meetings:

Classes meet during the Spring 2003 semester on Tuesday evenings in ISAT/CS Room 243 from 1800 to 2030 hrs.