Course Title: ITAP 3431: Network Security

Semester Credit Hours: 3 (2,3)

I. Course Overview

This course examines the basic principles, techniques and technologies associated with securing local area networks. Topics covered include security threats, data protection including cryptography and authentication, a review of network security applications and techniques for the management of intruders, malicious software and other internal and external threats to the network

II. PMU Competencies and Learning Outcomes

This course is highly practical in nature. Effective management of network security is a matter of practical skill and effective management and oversight as much as it is academic. This course primarily addresses two of the PMU competencies, critical thinking and teamwork. Network security requires the examination of network activity and response to potential threats as they arise. Team-based responses are essential to ensure that security is not dependent upon a single individual and so the course models the professional environment.

III. Detailed Course Description

ITAP 3431: Network Security examines the techniques used by network administrators and network security technicians in protecting and securing local area networks. Techniques for ensuring the confidentiality of messages are examined, including public and private key encryption, message and target authentication, digital signatures and key management issues. Network security applications are discussed in detail including authentication, email and web security, IP security and network management security. Techniques for detecting and defending against intruders, malicious software and other forms of attack are also covered.

IV. Requirements Fulfilled

This course satisfies three hours of the requirements for degrees in Information Technology and Computer Engineering. It is an available elective for the degree in Computer Science. It should be taken no earlier than the junior year.

V. Required Prerequisites

ITAP 2431 Network Management

VI. Learning Outcomes

In this course, students learn:

- To develop an understanding of the available techniques for securing communication through cryptography and authentication techniques and to apply them in a practical environment.
- To develop skills and establish techniques in securing networks from external and internal integrity threats.
- To enhance professional adaptability and performance in reacting to new and unexpected security threats
- To develop improved communication and collaborative skills in meeting security threats as a team member or team leader.

VII. Assessment Strategy

This course is designed to introduce students to the concepts and practical skills and techniques involved in securing local area networks from internal and external threats. With this in mind, the course grade involves an assessment of their performance on, and understanding of the threats, the application of techniques for minimizing risk associated with those threats and to the solution of security problems and the communication of designed solutions to those problems to an audience. Course grades are be based on

- Weekly assigned homework to motivate students to do the work and earn credit accordingly.
- Weekly structured laboratory exercises designed to guide students through specific course topics.
- Two in-class exams to assess students' accumulative mastery of content covered prior to time of exam.
- A comprehensive final exam to assess students' accumulative mastery of course material.

Students' final grades are based on 20% credit for homework, 10% for presentations and participation in classroom discussion, 30% for weekly lab exercises, 20% on in-class exams and 20% for the final examination.

Students are required to maintain a journal of thoughts and commentaries during the course. The journal contains daily entries including the identification of areas of interest and concern, notes on the preparation of presentation and comments and analysis of classmate's presentations. The journal is reviewed weekly by the instructor to provide feedback to the students.

Final grades and the student and instructor observations from reflective notebooks are included in the student's portfolio for use in the final assessment capstone course. The intent is to document the student's maturation as he proceeds through the curriculum.

VIII. Course Format

This course utilizes both lecture/discussion and laboratory exercises. Students are expected to attend two hours of lecture/discussion per week and three hours of laboratory per week. At least once per week students should be prepared to make presentation on the design and implementation of a solution to a problem selected by the instructor and to take part in a discussion based on that presentation. Once a week students should have at least 30 minutes of collaborative problem solving activity.

Classroom Hours (5 hours per week) **Class: 2**
Lab: 3

Web supplement: Course home page (the university's Web tool, WebCT or Blackboard) should contain the following:

- Course syllabus
- Course assignments
- Sample solutions to examinations (after being graded and returned)
- Sample solutions to programming assignments (after being graded and returned)
- Course calendar (an active utility)
- Course e-mail (an active utility)
- Course discussion list (an active utility)
- Student course performance (an active utility)

IX. Topics to be Covered

A. Security Principles and Standards
   1. Basic Security Concepts
   2. OSI Security architecture
   3. ANSI Security Standards

B. Cryptography
   1. Symmetric encryption and message confidentiality
   2. Public Key Cryptography
   3. Authentication

C. Network Security applications
   1. Authentication
   2. Email and Web Security
   3. IP Security
   4. Network Management Security

D. System Security
   1. Intruder Management
   2. Malicious Software
   3. Firewall Management

X. Laboratory Exercises

This course requires a weekly 3-hour lab component. Topics to be covered in the laboratory sessions should include:

- Security overview – Using NTFS to secure local resources
- Device & System Management – Installing service packs and hotfixes. Protecting the systems account database. Configuring Network Settings
- Media – transferring NTFS encrypted files, NetMon, autocleaning applications
- Authentication – Setting access policies and techniques for bypassing access control
- Attacks & malicious code – at, DDOS attacks, Netbus Trojan horses
- Remote access – Configuring VPN's, remote access policy
- Email – PGP, passphrase caching, public key management and malicious file detection
- Web Security – IE security, Content filtering
- Directory and file Transfer Services – FTP configuration and restrictions
- Wireless and Instant Messaging – wireless security options, telnet management
- Network Security topologies – RRAS and NAT, Configuring I/O filters and VLAN's
- Intrusion Detection – Detection applications, honeypots
- Security Baselines –Defining security templates, IIS lockdown, Security analyzers
- Cryptography –certification management
- Physical Security – Physical Barriers, biometrics, Social Engineering
- Disaster recovery and Business continuity

XI. Technology Component

This course makes use of the university's wireless access infrastructure during the class/lecture sessions. The course relies on the university and the students having access to an isolated professional grade network environment for the students to use.

XII. Special Projects/Activities

Students are required to keep a "reflective notebook" in which, after each class, they enter their own assessments of what they learned, and what questions remain from the class. From each exercise set, each student selects one problem, which the student thinks best reflects the way the mathematical topic is used in a technical context. A detailed solution to the problem is included in the student's reflective notebook.

XIII. Textbooks and Teaching Aids

A. Required Textbook

Stallings, W. (2003) *Network Security Essentials: Applications and Standards*, Pearson Education, Inc., Upper Saddle River, New Jersey 07458
ISBN: 0-13-035128-8

B. Alternative Textbooks

None

C. Supplemental Print Materials

Cretaro, P. *Lab manual for Security+ Guide to Network Security Fundamentals* (2003) Thomson/Course Technology
ISBN 0-619-13104-7

D. Supplemental Online Materials

As available from publisher.