

TCOM 5233 / MSIS 4233 Applied Information Systems Security Spring 2008

Instructor: Prof. JinKyu Lee, Ph.D.

Classrooms: NCB 226, Tulsa or
CLB 106A, Stillwater

Office: 380 North Hall, OSU-Tulsa Phone: (918) 594-8254
426 Business, OSU-Stillwater Phone: (918) 812-0600 (Cell)

Office hours: Tue. 5:00-7:00 pm @ originating campus (see class schedule)
or by appointment

E-mail: jinkyu.lee@okstate.edu

* *Please include your course code (TCOM5233 or MSIS4233) and section number (001, 603, 604, or 801) in the subject field of every email.*

Course Web: Online Classroom and Community (a.k.a. OC, Desire2Learn or D2L) at
<http://oc.okstate.edu> for all materials and assignments

Textbook:

Required: *Corporate Computer and Network Security*, by R. Panko, from Prentice Hall (ISBN: 0-13-038471-2)

Optional: *Hacking Exposed* by S.McClure, J.Scambray, G.Kurtz, from Osborne

The class schedule and assignments will change throughout the semester. Check the online schedule and message board often for changes as the semester progresses. You are responsible for all information disseminated through various channels. Important and useful university info can also be found at <http://osu.okstate.edu/acadaffr/aa/syllabus.htm>. An addendum for Tulsa students is attached at the end of this document.

Course Objectives

The course will explore various technical aspects of managing security, protecting information technology assets, attacking and guarding against attacks, and failures in various types of information systems. Topics covered in the course will include (but not limited to) various information security threats and cyber attack methods (e.g., hackers, viruses, worms, sniffers, identity spoofs, DoS, etc.) as well as computer, network, and data protection technologies (e.g., firewalls, IDS/IPS, authentication, etc.)

Grading Scheme

Grading: Your final grade will be determined by the weighted average of all grading items, according to the grading scheme table below. Each of the 4 grading categories will have one or more grading items (e.g., Term project has 2 items: presentation and report). Every item within one category will have the same weight within the category.

| Grading Category | Weight |
|--|-------------|
| Participation (Attendance & Online discussions) | 10% |
| Examinations (Exam I & II) | 20% |
| Assignments (TBD) | 30% |
| Term Project (I. Presentation & II. Report) | 40% |
| Total | 100% |

Letter Grades will be assigned as:

- A: ≥ 90.00
- B: ≥ 80.00
- C: ≥ 70.00
- D: ≥ 60.00
- F: ≤ 59.99

- * All scores will be automatically rounded to hundredths by D2L grade book, and no manual adjustment will be considered.
- * Depending on the overall class average, the instructor reserves a right to adjust the scale. The decision to adjust the scale will be made only after grades for all items are in, at the end of the semester.

Course Requirements

1. You **MUST** participate in a group project that requires you to **invest your time IN ADDITION to class hours**. * For the project, you may need an Internet connection (preferably hi-speed) and physical access to a TCOM lab (or remote desktop).
2. You are also responsible for completing all readings, written assignments, and oral presentations by the assigned due dates, all of which require an additional time investment.
3. The class/exam schedules, assignments, and other information included in this syllabus may be changed during the semester, and all such changes will be announced in class, emailed, or posted on the course web site. It will be your own responsibility to **keep track of such announcements, regardless of the channel**. You are also responsible for securing access to all necessary materials covered in lectures, class discussions, textbook chapters, class handouts, and assigned outside readings.
4. You are required to **sign & submit the Legal/Ethical/Moral Code of Conduct form** (attached) before the 3rd class to the D2L digital drop-box.

Lectures: You are expected to read the textbook (Panko) chapters **BEFORE they are covered in the class**. Lecture notes will be uploaded to the D2L course web site. Class time will include a lecture and discussions of the week's material, as well as other relevant classroom activities (e.g., lab demonstrations by the instructor, student presentations).

* There will be NO hands-on lab activity during the scheduled lecture hours.

Class Attendance/Participation: Class attendance (resident sections only) and participation in online discussions are encouraged and required.

Assignments/Quizzes: Completion of all assignments (e.g., online quizzes, lab experiments, Internet research) is expected by the due date.

Examinations: Two in-class (resident sections only), open-book, multiple-choice examinations will be given. Students are responsible for their own OMR answer sheets (Scantron bubble sheet). Distance Learning students will be required to take an online exams on the SAME DAY.

No makeup exam will be given except under extremely unusual circumstances, and the instructor will be the sole judge of the nature of such circumstances.

Term Project Report & Presentation: Students are required to complete a term project (options listed on the next page), of which final deliverables will include an in-class presentation and a written project report. This is a team project that has to be done in group. Recommended group size is 4, with minimum 2 and maximum 6 students in a group. Group size will be factored in when evaluating the results.

* Students enrolled in a Distance Learning section (603 & 604) will be assigned to resident section groups by the instructor and required to work together using the Internet connection.

A group representative must submit, by the specified due date, a one-page proposal stating which option his/her group has selected and describing project ideas. The proposal must also provide a list of the group members – (name, course code, section, and CWIDs) and coordination plan for group work.

* Groups choosing Option 1 must obtain preliminary approval from their sponsoring organization and include the organization's name and the title of the contact person in the proposal.

Project Options

Option 1: Examination and Analysis of a Real Organization's Security Vulnerability.

You need to **find a REAL organization** that allows you to examine their security vulnerabilities. You will need to interview appropriate individuals within the sponsor organization for guidance and permissions, create a **plan for a penetration testing**, which specifies the scope and detailed procedure of the testing, and then actually **conduct the test**.

* This option will *require a written permission* and cooperation of the sponsoring organization.

A typical option 1 project report will include (but not limited to) the following components: executive summary, intro to the organization, purpose/scope of the project, testing plan, step-by-step descriptions of all actions that you took, findings, suggested solution(s), and a copy of the written permission from the sponsoring organization (as an appendix). Your written report should be delivered to the appropriate individual at the sponsoring organization as well as to me.

SPECIAL NOTE: A special care must be taken to conform all applicable laws and not to compromise the sponsor's sensitive information.

Option 2: Hands-on Experiment of Hacking & Security Techniques in a Controlled Lab Environment.

Your goal is to **identify vulnerabilities of target systems**, which will be given, **and come up with solutions to eliminate, protect, or minimize such vulnerabilities**. In order to achieve the project goal, you will need to actively investigate hacking/security techniques (from hacking/infosec websites and books), conduct a penetration testing (remotely penetrate or disrupt the targets), and find out solutions.

You will be given access to a network where you can safely try some hacking tools as well as security tools.

A typical option 1 project report will include (but not limited to) the following components: executive summary, purpose/scope of the project, attack plan, step-by-step descriptions of all actions taken, test results, and suggested solution(s).

SPECIAL NOTE: A special care must be taken not to infringe the privacy of other network users.

Option 3. Research on a Current Topic in Information Security.

A group of students will choose a **CLASS of security technologies** (as opposed to a specific technique, product, or brand) and **research the technology over and beyond the coverage of the textbook**. Students are expected to enrich their technical knowledge by actively searching for relevant information from various sources, including the Internet (e.g., www.wikipedia.org, www.insecure.org), news/magazines, academic/practitioner journals, etc.

A typical option 3 project report will include (but not limited to) the following components: executive summary, functional mechanism of the chosen class of information security technologies, related information security threats/risks, strengths and weaknesses of the technologies at the current stage, current market situation (brand, model, price) and the trends of different sub-classes technologies.

Project Final Deliverables:

On a presentation day (to be determined), 10 -30 minutes (will be allocated by the instructor depending on number of groups and the type/topic of the project) will be allocated for each group to present the findings and demonstrate the team members' understanding on the chosen topic. Following each presentation, 5-10 minutes may be allotted for questions and answers. The presenting group needs to submit the ppt file to me and hand-outs to the class on the assigned presentation day.

Each group needs to submit one final project report by the specified due date, but regular interaction with the instructor through out the semester is strongly recommended. The project report should be typed, double-spaced, and use 12 point Times New Roman font with one-inch side, top, and bottom margins. The length of the final report should not exceed 40 pages, regardless of the project type. The general expectation will be 25-30 pages, including summary, figures/tables, reference lists, and appendix.

Your report must be properly referenced. APA style is preferred, but any standard citation style will be acceptable. If you are not familiar with citation styles, refer to a style guide (e.g., <http://www.apastyle.org/styletips.html>, <http://www.mla.org/style>)

The presentation and written report have the same weight on the final grade (20% each), and all members in a group will receive the same grade for the project.

- ***Overdue final reports*** will be subject to penalty at the rate of 5 points per day.
- ***Overtime presentations*** will be subject to penalty at the rate of 1 point per minute.

Important Notes:

* For all types of written submissions, proper citation with a references list is required. Any use of others' work without explicit acknowledgement of the source of the work will be considered as **plagiarism**. Make sure that the work you submit is original and properly documented as to the sources of your information. Any direct quotes, including but not limited to factual assertions (numeric information, statistical information, costs, etc.) and ideas/opinions of others from any source should be properly cited. Failure to do so will **result in a grade of "F" for the submission and possibly for the entire course, at the sole discretion of the instructor.**

TCOM 5233 / MSIS 4233 Applied Information Systems Security
Spring, 2008 Course Schedule (Tue. 7:20 - 10:00pm)
 Classrooms: TUL NCB 226 or STW CLB 106A

Note: Schedule may be altered during the semester. Check the course web site for changes and updates.

| Week | Date | Topic | Items Due BEFORE the class |
|-----------|------------------|---|---|
| 1 TUL | 1/8 | Introduction and course overview A Framework (Chapter 1) | |
| 2 STW | 1/15 | Access Control and Site Security (Chapter 2) | |
| 3 TUL | 1/22 | Review of TCP/IP Internetworking (Chapter 3) | Project Proposal |
| 4 STW | 1/29 | Attack Methods (Chapter 4) | |
| 5 TUL | 2/5 | Firewalls (Chapter 5) | |
| 6 STW | 2/12 | Host Security (Chapter 6) | |
| 7 TUL | 2/19 | EXAM I | |
| 8 STW | 2/26 | The Elements of Cryptography (Chapter 7) | |
| 9 TUL | 3/4 | Cryptographic Systems (Chapter 8) | |
| 10 STW | 3/11 | Application Security (Chapter 9) | |
| 11 TUL | 3/18 | Spring Break | |
| 12 STW | 3/25 | Incident Response (Chapter 10) | |
| 13 TUL | 4/1 | Managing the Security Function (Chapter 11) | |
| 14 STW | 4/8 | Project Presentation I (for STW groups) | Term-Project Slides & Report |
| 15 TUL | 4/15 | Project Presentation II (for TUL groups) | Term-Project Slides & Report |
| 16 STW | 4/22 Pre-Fin | The Broader Picture (Chapter 12) | |
| 17 TUL | 4/29 Final W. | EXAM II | |



OKLAHOMA STATE UNIVERSITY – TULSA ADDENDUM TO SYLLABUS ATTACHMENT SPRING 2008

HOW TO CONTACT A FACULTY MEMBER

If you have questions regarding your class, talk to your instructor. Faculty members usually include their office hours and/or phone number(s) in the class syllabus. If you cannot locate this information, set a time to meet with the instructor prior to or following your class session. You may check with the Faculty Support Services office, 594-8276 or 594-8277 on when the instructor may be available.

SPECIAL ACCOMODATIONS FOR STUDENTS

According to the Americans with Disabilities Act, it is the responsibility of each student with a disability to notify the University of his or her disability and to notify the instructor and request verification of eligibility for accommodations from the Student Services Center, 103 North Hall, 594-8354. Please advise the instructor of such disability and desired accommodations at some point before, during, or immediately after the first scheduled class period.

WHERE TO GO FOR HELP

Academic Advisor – All admitted students have an assigned academic advisor. Although it is true that only certain categories of student's need an advisor's signature or approval on class registration, all students benefit by conferring with their advisor on a regular basis. The Academic Advisement Center is located on the first floor of North Hall, 594-8271.

Library – 594-8130

Library Hours:

| | |
|-------------------|------------------------|
| Monday – Thursday | 8:00 a.m. – 10:00 p.m. |
| Friday | 8:00 a.m. – 6:00 p.m. |
| Saturday | 9:00 a.m. – 5:00 p.m. |
| Sunday | 1:00 p.m. – 9:00 p.m. |

Martin Luther King Holiday Closed

Spring Break:

| | |
|-------------|-----------|
| March 15-22 | Hours TBA |
| March 23 | Closed |

Computer Lab – 594-8043

Computer Lab Hours:

| | |
|-----------------|------------------------|
| Monday – Friday | 8:00 a.m. – 12:00 a.m. |
| Saturday | 9:00 a.m. – 9:00 p.m. |
| Sunday | 1:00 p.m. – 9:00 p.m. |

A current student identification card is required.

HAVE A GREAT SEMESTER!

Ethical/Legal Code of Conduct for TCOM5233/MSIS4233 Students

The following is an understanding agreement on acceptable and/or restricted use of knowledge, techniques, and resources (including course material, tools, malicious code, and exploits) to which you may have access during your enrollment in TCOM5233 / MSIS4233. By providing your signature, you acknowledge that you have read and understand the following code of conduct set forth for TCOM5233/MSIS4233.

1. I will perform all educational activities and duties in accordance with all applicable laws and the highest ethical principles.
2. I will proactively maintain privacy and confidentiality of proprietary or otherwise sensitive information encountered in the course of activities in TCOM5233/MSIS4233. I acknowledge that my obligation to maintain privacy and confidentiality continues after my enrollment in TCOM5233/MSIS4233 ends.
3. Any tools, techniques, malicious code, and/or exploits presented in class shall only be used within the conduct of TCOM5233/MSIS4233.
4. Any tools, techniques, malicious code, and/or exploits presented in class shall only be used within a controlled environment, which will be defined and advised by the course instructor(s).
5. Under no circumstances, shall any of the class material, tools, techniques, malicious code, and/or exploits presented in class be used against the public on the Internet.
6. Under no circumstances, shall any of the class material, tools, techniques, malicious code, and/or exploits presented in class be shared with individuals and/or groups not enrolled in TCOM5233/MSIS4233.

Failure to comply with the above may constitute a violation of law and can result in potential civil and/or criminal legal penalties.

I have read the above and understand the acceptable and/or restricted use of knowledge, techniques, and resources expected to TCOM5233/MSIS4233 students.

PRINTED NAME _____

SIGNATURE _____ DATE _____