MSIS4233/TCOM 5233 Applied Information Systems Security

Course Syllabus - Spring, 2015 (Jan. 12-May 8)

Oklahoma State University
Spears School of Business, Management Science & Information Systems

The class schedule and assignments outlined in this syllabus may change as the semester progresses. You must stay current by paying attention to in-class and online (e.g., D2L, email) announcements. The grading scheme and other general guidelines will remain constant once the semester starts.

Section(s): Resident: Stillwater (001), Tulsa (801) & Distance Learning (583)

Class Hour/Location: STW: Tue. 7:20-10:00 PM @ CLB106B
TUL: Tue. 7:20-10:00 PM @ T-NCB 226
DL: Video link posted on OC before 5PM the next day (Wed).

Course Website: http://oc.okstate.edu (a.k.a. Online Classroom/OC, Desire2Learn/D2L)

DL Support: spearsdistance@okstate.edu / Phone: 405-744-4048

Instructor: Dr. JinKyu Lee, *Ph.D., Assoc. Prof. of MSIS, SSB.*

Instructor Office: Tulsa: NCB 317, Stillwater: BUS 426

Office Hours: Tue. 5-7PM @ originating location, or by appointment.

Contact Channels: E-mail: AppliedIA@live.com
* Mandatory email protocol:
1. Always include your **course code** (MSIS4233 or TCOM 5123), **section** (STW, TUL, or DL) and **first & last name**.
2. DON'T send/cc emails to my okstate.edu address.
3. DON'T attach any file to your email.

Phone: (918) 594-8254 (Office) / (918) 200-9072 (Google #)
Google Plus: google.com/+JinLeeOSU
Facebook: www.facebook.com/groups/OSUInfoSec

Required Textbook: *Corporate Computer Security*, 4th Edition, Randall Boyle & Raymond Panko, Prentice Hall. (ISBN-13: 978-0133545197 / ISBN-10: 0133545199)
* The 3rd edition is acceptable.
* You are expected to acquire the book before the 2nd class.

Additional References: Wikipedia, Google, YouTube

Course Prerequisites: TCOM5123 (TCP/IP Upper Layers) or equivalent w/ a solid understanding of TCP/IP (v4) networking.

Other Requirements:

- Access to a PC (physical or virtual) with admin privileges and a reliable/high-speed Internet connection. The standard PC platform for this course is Windows 7. If you use a different OS, it is your responsibility to resolve incompatibility issues, if any.
- Basic multi-media authoring tools (e.g., web-cam, smart phone, Camtasia Studio, Windows Movie Maker) and skills.
- Familiarity with virtualization technologies (e.g., VMware vSphere/ESXi, VMware Workstation/Fusion)
- Willingness to put (a lot of) extra time & effort **in addition** to the regular class work.

Course Description & Objectives:

In MSIS4233/TCOM5233, students explore various technical aspects of managing information security and protecting IT assets. Topics covered in the course will include, but are not limited to, various information security threats and cyber attack methods (hackers, viruses, worms, sniffers, scanners, exploits, etc.), as well as security countermeasures (firewalls, IDS/IPS, authentication, etc.) to protect computers, networks, and data from such threats/attacks.
Accordingly, students are guided to develop a comprehensive understanding of security architectures and their practical implications through hands-on labs and term projects.
In addition, students are expected to develop their soft skills (e.g., presentation, communication, time management) while working with others in groups.

Course Objectives & Learning Goals

Course Objective *By the end of the course, the students are expected to be able to…*	**Learning Goals** *, which will help the students achieve a higher level of…*
• Identify major security threats and describe recent trends in the threat environments.	✓ Information Assurance Competence ✓ Critical and creative thinking
• Explain the threat vectors of major threats and suggest security countermeasures/architectures for such threats.	✓ Information Assurance Competence ✓ Technology Skills – Telecommunications and Security
• Develop & implement security assessment plans. • Design & build a safe test environment using virtualization technologies. • Identify technical solutions for identified security vulnerabilities.	✓ Information Assurance Competence ✓ Critical and creative thinking ✓ Business knowledge and competency ✓ Technology Skills – Telecommunications and Security
• Effectively present the findings of a security assessment project. • Effectively exchange technical information, questions, instructions, and suggestions online.	✓ Critical and creative thinking ✓ Communication Skills

Attendance Policy

Initial attendance: Students must attend (resident section) or review the first video (DL section) and complete all required tasks (to be announced in the class) before the end of the 2nd week. Students who have not completed the tasks within the first two weeks, unless arranged a different schedule with the instructor, will be reported as not having attended class, and the instructor will recommend the student to drop the course.
On-going attendance: This course is a concurrent course where both the resident section and the DL section follow the same course schedule and work together. Thus every student must keep up with the progress. Accordingly, students are required to attend every class/watch the video in a timely manner.
* If you foresee a difficulty in attending/promptly reviewing the lectures in this semester, you may consider taking this course later when your schedule allows.

Grading Policy

Your final grade will be determined by the weighted sum of all grading items, according to the grading scheme below. Each of the grading categories will have one or more grading items. Grading items within one category may or may not have the same weight within the category.

Grading Category	Weight
Attendance Check (pop quizzes/labs)	**10%**
Online Discussions (on D2L Discussion Boards)	**10%**
Assignments (3~5 lab or research reports)	**40%**
Group Project	**40%**
Total	**100%**

Letter grades will be assigned according to the following scale.

Total Weighted Score	Grade
>= 90.00	**A**
>= 80.00	**B**
>= 70.00	**C**
>= 60.00	**D**
< 60.00	**F**

* The instructor reserves the right to adjust the scale. A decision to adjust the scale will be made only after all grades are in at the end of the semester. Individual adjustment for a better grade may NOT be requested.
* The total weighted scores will be rounded to the nearest integer at the end of the semester. The calculated total weighted scores will not be manually adjusted. You will be able to check your raw & weighted scores of graded item on the OC Grade book.

Description of Course Requirements and Grading Rubric

- **Attendance Check** (pop quizzes and pop labs)
  Resident section students are required to (physically) attend every class, and *DL section* students are required to watch the lecture video by the end of the weeks (Sunday night). If it is not possible for you to attend or watch a lecture in time, you must inform the instructor of the situation and your backup plan to catch up the class ASAP.
  Attendance will be randomly checked by a pop quiz or pop lab announced during a lecture. You will need to complete each pop quiz/lab within 7 days from the lecture day unless specified otherwise.

- **Online Discussions**
  Every student is required to closely monitor & contribute to online discussions on D2L Discussion Boards. Online discussions, in addition to in-class discussions, add depth and context to your understanding of course topics. Therefore, participation in online discussions is an important learning activity in this course.
  Participation in online discussions will be randomly checked and graded several times throughout the semester. In order to earn full credit for this grading category, you need to read all messages on the graded discussion boards and post at least one value-adding messages.

  A value-adding message would have the following characteristics:
  1. Theoretical or technical information relevant to a course topic.
  2. Help readers improve their understanding of an infosec issue/topic.
  3. Self-contained message: Readers do not need to refer to another online/offline resource to understand the message.
  4. Original: The message must be written by you in your own language. The source of the info (e.g., URL, journal article reference info) should be clearly cited. You can quote a line or two from a cited material, but you should not copy & paste a whole block of other's writing even with a citation.

  Some ways to earn extra Online Discussions points:
  1. Include business/practical implications (e.g., why does it matter to some organizations, societies, or consumers? Who can do what in order to benefit from the information in the message?).
  2. Ask a well composed question message. When you ask a question, elaborate your question (i.e., clearly specify what you already understand and what is that you don't know) and provide all necessary info (e.g., the organizational or technical context of the issue in question such as business process, network design, error message/screenshot, system specification, etc.).
  3. Provide a comprehensive answer to a posted question (from others or your own). The answer may not work for the particular question instance but may solve a similar instance. The answer should include some explanation of the suggested solution and boundary conditions (i.e., what was the underlying problem/issue of the questioned situation, how would the solution resolve the problem, what are the conditions for the solution to work)

Some ways to lose Online Discussions points:

1. Post a redundant question or answer – If your question or answer is substantively similar to a previously posted question/answer, you will be considered as not having monitored the discussion boards.
2. Show an inappropriate behavior – If your message includes any element that is unprofessional (e.g., use of slangs, disclose classified info), unethical (e.g., copying others' work without acknowledging it, accessing unauthorized systems to answer a question), or offend others (see Internet Netiquette Guidelines section), you will be considered as not having learned the integrity and soft skills expected from business-major students.
3. Post a one-liner like "hey, check out this webpage", "This is interesting!", "Thank you for the info", etc. Keep in mind that everyone in the class is supposed to read every message on the graded discussion boards. Don't add your tweets in their reading list.
4. Ask a question that lacks info needed to answer the question IF such info need could be easily anticipated and provided earlier. If you don't bother to help others answer your question, others won't bother to help you solve your problem. Also, any unnecessary message traffic will cause a wasteful distraction to each and every other student in the class.

- **Assignments**

There will be 3-5 assignments. Most assignments will be either a lab report or research report.

1. Lab report: Perform specified hands-on lab tasks and document the process and findings.
2. Research report: Conduct a short online research on a given topic and summarize the findings.
3. Some assignments may include different sets of tasks for different levels (i.e., undergrad vs. grad). Make sure you complete the tasks for your level.
4. Some assignments may involve group work.
5. Different assignments may carry different weights within the Assignments category

- **Group Project**

All students are required to work in groups for a term project. The term project is to **build a shared virtual lab environment for the group** and **perform a set of infosec experiments** while **documenting and presenting the activities**. Note that the shared virtual lab environment will also be used for other coursework (e.g., infosec lab assignments).

Each group will consist of 2-5 students (3-4 ideal) including at least one resident section student and at least one DL section student. Students may request to form a group with preferred group members, but the instructor reserves the right to adjust the membership. Each group will **submit a project proposal, bi-weekly (individual) project logs and a (written) final report, and deliver two presentations (i.e., interim & final).**

An individual student's group project score will be a function of 1) the quality of the group work and 2) the individual's contribution to the group work.
The quality of group work will be assessed on the following dimensions:

1. Comprehension of the presented hacking/security technologies, which should be evident in the final report and presentations.
2. Effective written communication (proposals, logs, reports) – Think about the purpose of the written deliverable (e.g., project proposal, log, final report, ppt slides, etc.) and use the best format/style, strategy, techniques for the deliverable.
3. Effective presentation (professionalism, instructional value).

The contribution to the group work will be assessed in terms of
1. Contribution to the group's knowledge and deliverables, and
2. Efforts to improve the group performance & dynamics

, which should be evident in the project logs and peer-assessment reports.

Group Project Requirements

- ***Build a shared virtual lab for the group (Group Lab):*** Design & implement a virtual lab that includes the following minimum components:
  1. Two subnets connected to one of the TIA lab VLANs (e.g., OpenLab, VILab)
  2. VM * the # of group members
  3. 1 virtual router firewall/UTM appliance (VA)
  4. 4 of the VMs/VAs should be running on different OSs (e.g., WinXP, Win7, WinSrv2008R2, CentOS) with some known vulnerabilities (e.g., missing patch/insecure config for the OS or Apps)

- ***Perform a set of infosec experiments:*** Using the Group Lab, conduct a series of infosec experiments. Such experiments should include, but not be limited to:
  1. Active scanning from a hacker's perspective (NW scan, host scan, and OS/service scan from an external network
  2. Automated vulnerability scanning from an infosec admin's perspective (form internal NW w/ admin privilege)
  3. Additional infosec experiment * the # of grad-level group members.

  * An infosec experiment may be based on an in-class demo or an assignment, but in such a case, the project group must demonstrate a deeper understanding of that component.
  * Each and every group member must perform the activity #1 & #2. Doing #3 is optional.
  * Each grad-level member should produce a short video demo/tutorial for his/her #3 activity for other group members. The video clip may be used in the final presentation (or create a new video if desired).
  * Each activity should have a designated activity manager. An activity manager is responsible to check who has completed the activity and combine the findings/outcomes for the final report & presentation. Each grad-level member is the default activity manager for his/her own #3 activity.
  * Appointing a project manager to keep track of the overall progress of the whole project is recommended (but not required).

- ***Document & present the activities:*** Each group should submit two written documents and perform two group presentations. In addition, each individual should submit bi-weekly project logs. Below are guidelines for these deliverables.
  1. Proposal: Submit the design of the group lab and activity plan. The proposal should include:
     a) The NW design (including the IP addressing plan)
     b) VM/VA specification (OS, apps, NW connection, etc.)
     c) Activity schedule (list of experiments & scheduled dates, VMs to be used). Grad-level student should propose at least 3 alternative experiments, from which the instructor will select one that does not overlap with other groups' proposals.
     d) Collaboration plan (Meeting/communication methods & schedules)
     e) Workload distribution plan (who builds what VM, who takes up the activity manager/other admin roles, who do the research on the experiment, who is responsible for what deliverable, etc.)

2. Interim Presentation: Present the proposed Group Lab environment and project plan. An interim presentation may consist of live presentation, recorded video clips, or a mixture of the two. Regardless of the format(s), the presentation must be facilitated by one or more resident section group members (play video clips, handle questions, etc.) in class.
   * MAX 15 minutes including Q & A

3. Final Report: Submit a written report that summarizes the group activities. The final report should include:
   a) A 0.5-1 page executive summary
   b) Report of performed activities
   c) Analysis and discussions of the outcomes/findings (* most important)
   d) A reference list (any format)

4. Final Presentation: Present the results of the project activities to the class. A final presentation may consist of live presentation, recorded video clips, or a mixture of the two. Regardless of the mode of the format(s), the presentation must be facilitated by one or more resident section group members (play video clips, handle questions, etc.) in class.
   * MAX 30 minutes including Q & A

5. Bi-weekly Project Logs: Record the progress of the project & share it with the instructor. This is an individual submission item. A project log should include the following information:
   a) Summary of group meetings/communication.
   b) Work done in the past 2 weeks & scheduled for the next 2 weeks.
   c) Analysis of group performance/dynamics and action plan. Each and every student is expected to find an issue and/or opportunity to improve group performance/dynamics and implement some managerial techniques. Such managerial techniques should be directed toward himself/herself (e.g., change the way **YOU** interact with others or the way your work), not toward others. You may ask other members to change their ways if necessary, but I don't want to see them in your project logs.
   d) Other thoughts to improve the group performance (e.g., information/communication systems design/functions that could improve group work if available).

Instructor Response

The instructor will try to respond to student emails within two business days, provided the student use the right email address (AppliedIA@live.com). Emails sent to elsewhere (e.g., okstate.edu), lacking required info (i.e., full name & section), or inappropriately written (use the same criteria as online discussions) may not be answered.
Students may expect grades for assignments to be posted to the D2L Gradebook within two weeks from the submission deadline.
Students with urgent issue should call or text the instructor @ +1-918-200-9072 for timely assistance. Please do not use Facebook or Google+ messaging.

Make-up Policy

Students/groups are expected to submit each assignment/project deliverable by the specified deadline. If for any reason a student/group cannot meet the deadline, the student/group rep must notify the instructor prior to the deadline and re-arrange the schedule. A late submission penalty may be applied to any late submissions, and some assignments/project deliverables cannot be accepted after a certain date.

University Policy

Drop Policy
Information about university drop policy and dates is at this website:
http://registrar.okstate.edu/
Click on "class schedules," and "short, internet, and outreach courses"
To drop this course, contact the Registrar's office, (405) 744-6876, or drop through SIS (Student Information Services).

Academic Integrity
Oklahoma State University is committed to the maintenance of the highest standards of integrity and ethical conduct of its members. This level of ethical behavior and integrity will be maintained in this course. Participating in a behavior that violates academic integrity (e.g., unauthorized collaboration, plagiarism, multiple submissions, cheating on examinations, fabricating information, helping another person cheat, unauthorized advance access to examinations, altering or destroying the work of others, and fraudulently altering academic records) will result in your being sanctioned. Violations may subject you to disciplinary action including the following: receiving a failing grade on an assignment, examination or course, receiving a notation of a violation of academic integrity on your transcript (F!), and being suspended from the University. You have the right to appeal the charge. Contact the Office of Academic Affairs, 101 Whitehurst, 405-744-5627, http://academicintegrity.okstate.edu/.

Accessibility
Any student in this course who has a disability that may prevent him or her from fully demonstrating his or her abilities should contact the instructor as soon as possible, so we can discuss accommodations necessary to ensure full participation and facilitate your educational opportunity. For more information about OSU Student Disability Services, please go to: http://sds.okstate.edu.

Internet Netiquette Guidelines

A melding of the words "network" and "etiquette", **netiquette** refers to the manner in which communication is conveyed in an electronic environment.

Here are some guidelines for communication within this course:

- REFRAIN FROM USING ALL CAPS. It is considered SHOUTING when communicating online.
- Do not post or forward offensive or racially insensitive jokes or comments.
- Be careful with humor and sarcasm.
- Don’t respond to personal attacks: Contact the instructor for action and referral.
- Always add in the subject line a concise statement describing the email or discussion post.
- Respect others' opinions. If you disagree with what another has said, post your thoughts in an objective, respectful manner. Do not make remarks that can be taken personally.
- Reflect upon the text you have entered before posting.
- Keep the discussion within the scope of the course material.
- Communication should be grammatically correct. Adhere to correct sentence structure, grammar, and spelling conventions. Proofread for errors before posting a message.
- Before you respond to a threaded message, read all the messages related to that message that have been previously posted.
- Send out an email to a group using the blind carbon copy field – BCC does not allow your recipients to view who was sent the email.