# Introduction to Information Security

## INFSYS 3848 / INFSYS 6891 (Combined Section) Fall-2014

## Wednesday 6:55pm to 9:35pm – Room ESH 103

**Instructor:** *Dr. Shaji Khan* (Ph.D. Business Administration, M.S. Computer. Science, B.A., B.Com)
**Office location:** Room 234, Express Scripts Hall
**Office Hours:** Wednesday 4:30 to 6:30pm
**Email address:** shajikhan@umsl.edu
**Cell phone:** (314) 489-9733

**Note**: If anyone has a health condition or disability which may require my attention, please contact me and the **Disability Access Services Office at 144 Millennium Student Center (ph: 314-516-6554)**

**Course Materials**

- **There is no required text-book**
- Considerable material in the form of notes, PowerPoint slides, and web links will be assigned and available through MyGateway
- ***Recommended (but not required) books***:
  - Anderson, Ross (2007) *Security Engineering, 2nd Edition*, Wiley (Free and available online at: http://www.cl.cam.ac.uk/~rja14/book.html)
  - Harris, Shon (2012) *CISSP All-in-One Exam Guide, 6th Edition*, McGraw-Hill (ISBN-13: 978-0071781749)
  - Whitman, M.E. and Mattord, H.J. (2014), *Principles of Information Security*, Cengage (ISBN-13: 978-1285448367)

**Course Description**

***Prerequisites:*** Junior/Senior standing or permission of department chair.

***Student background:*** This is an introductory course and open to students from all majors. A background in data networking, programming, and web application development will be very beneficial but is not required. However, the course does get technical and I encourage you to get in touch with me if you have any concerns. It will also be very helpful if students have their own laptops with at least 4GB of RAM (memory).

***Motivation***: Arguably, Information Security (InfoSec) is currently one of the most critical issues facing individuals, organizations, governments, and society. Media reports are replete with breaches of information security and the adverse consequences for all stakeholders involved. Thus, demand for InfoSec professionals who understand the managerial and technical aspects of InfoSec is growing. However, InfoSec is a rather vast field and includes a plethora of management and technical areas. Students or professionals seeking an entry into this field are often overwhelmed by its vastness. In a broad sense, InfoSec is both a management issue and a technological issue. Thus, it is critical that students think about it from both perspectives and develop their skills at their intersection.

***Course objectives***: The purpose of this course is to two-fold. First, it provides an overview or a survey of the vast field of InfoSec. The goal is to make students aware of the fundamentals of InfoSec and the various facets represented under this umbrella term. Specifically, the course enables students to apply principles of InfoSec to organizational settings. Second, the course provides students a foundation in the

technical aspects related to InfoSec. Specifically, the course provides basic technical knowledge and background that should enable students to continue developing their InfoSec skills beyond this course. Thus, this course provides a foundation in the management of information security and at the same time provides a technical introduction to InfoSec with the hope that students will pursue both areas vigorously and practice at the intersection of management and technology.

***Learning Outcomes**:* Upon completion of the course, students will have a basic understanding of at least the following:

- InfoSec terminology
- Fundamental principles of InfoSec
- The vastly complex threat environment
- The variety of sub-specialties within the InfoSec field
- Management of InfoSec including
    - security planning
    - identifying information assets and their associated security requirements
    - establishing risk criteria
    - risk analysis and risk evaluation
    - risk treatment
        - security controls
    - InfoSec security management standards/models (and the organizations that develop these)
- Information Security Technologies and Tools
    - Access control and associated technologies/tools
    - Data Networking fundamentals from an InfoSec perspective
    - Firewalls (various types of filtering and overview of current trends in "firewalling")
    - Intrusion Detection/Prevention Systems
    - Virtual Private Networks
- Basics of Cryptology/Cryptography
    - Terminology relevant to InfoSec
    - Symmetric and Asymmetric Ciphers – key differences and uses
    - Cryptographic Hash Functions
    - Applications of Cryptographic Techniques in InfoSec
    - InfoSec Management issues associated with cryptographic techniques
- Overview of Secure Software Development
- The need for Web Application Security
    - Overview of web based applications and common architectures
    - Overview of most common vulnerabilities within web applications

***Technical learning outcomes**:*

- Overview of Linux
- Understanding of virtualization (using VirtualBox)
    - Setting up a virtualized and sandboxed penetration testing lab using a Linux distribution known as Kali Linux. The Kali virtual machine acts as the "attack" machine. We will also setup intentionally vulnerable "target" machines such as "metasploitable".

- Basics of a variety of penetration testing tools, such as "nmap", "dig", "metasploit" etc., especially those built into Kali Linux
- Data Networking fundamentals
    - *Hybrid TCP/IP Model*
    - A good understanding of HTTP, TCP, IP, and SSL/TLS protocols
- Use of network protocol analyzers such as WireShark™
- Basic understanding of Web Application architectures

**Expectations of performance**
I expect all students to prepare for, **attend**, and contribute to the classes on a regular basis. Students will lose up to 10% of the course grade for poor attendance (see Attendance section below). Another forum for you to demonstrate your learning is through assignments or quizzes, which together account for 25% of the course grade. We will also perform "hands-on" lab assignments to better appreciate InfoSec concepts. Given the importance of practical experience in InfoSec, lab assignments are worth 40%. Finally, we will learn and explore InfoSec through a group research project worth 35%. This course does not have exams. Thus, your grade will be calculated as follows:

| **Course Component** | **Weight** |
|---|---|
| Quizzes/Non-lab Assignments (Individual work) | 25% |
| Lab Assignments (Individual work) | 40% |
| Research Project (Team work, undergrads only) OR Individual Research Papers (Graduate Students only) | 35% |
| Maximum Possible Final Score: | 100% |
| **NOTE**: Up to 10% **loss** in final score for poor attendance | |

*Grading Policy***:**
Letter grades will not be assigned to individual components of the course. Only points (numeric scores) will be assigned. These scores will be combined into a 'Weighted Total' out of 100, rounded to one decimal place. Depending on this final score, your overall letter grade for this course will be determined as follows:

| **Final score ranges and corresponding letter grades** | | | | |
|---|---|---|---|---|
| >=94 | A | | 70-73.9 | C |
| 90-93.9 | A- | | 66-69.9 | C- |
| 86-89.9 | B+ | | 62-61.9 | D+ |
| 82-85.9 | B | | 58-57.9 | D |
| 78-81.9 | B- | | 54-49.9 | D- |
| 74-77.9 | C+ | | <54 | F (fail) |

**Attendance (Possibility of losing 10% of overall grade due to poor attendance)**
It is extremely important you attend all class periods. This material becomes unwieldy when a student has missed a class or two. Overall, I will allow TWO (2) excused absences. For every additional class period missed, you will lose 2% of your overall grade for a maximum of 10%. I will take attendance each class period.

**Quizzes / Non-lab assignments (25% of your overall grade)**

During this semester, I will assign up to four (4) quizzes / non-lab assignments combined.

1. Some quizzes carry more weight toward your final grade than others.
2. Quizzes will be either in-class or through MyGateway. Some in-class quizzes may be ***un*announced**
3. Online quizzes will be turned in through MyGateway. Submission deadlines will be listed on each online quiz. Late submissions will receive deductions of 10% for each 24 hour period after the due date until no points remain.

**Lab Assignments (40% of your overall grade)**

It is imperative that we get as much "hands-on" exposure to InfoSec fundamentals as possible. We will be able to devote only limited class-time for lab exercises. Thus, I will assign up to six (6) lab assignments during this semester to be completed as homework.

1. Students will work individually on lab assignments
2. Some lab assignments could be completed on the student's personal computer
3. Some lab assignments are to be completed within the dedicated Management Information Systems (MIS) lab. Access to this lab is contingent upon acceptance of lab usage policies.
4. I will provide detailed descriptions of the lab tasks on MyGateway and make relevant announcements. In some instances, I will also provide demonstrations. However, the goal is to let students "get their hands dirty" and "figure things out"!
5. Lab assignment reports will be turned in through MyGateway. Submission deadlines will be listed on each assignment. Late submissions will receive deductions of 10% for each 24 hour period after the due date until no points remain.

***VERY IMPORTANT NOTE: Please be mindful that the tools and techniques we will learn are NOT TO BE USED OUTSIDE the MIS Lab and the "sandboxed" environment created in it. Most of these techniques are illegal when carried out in the "real world" without explicit permission from the entity you are "hacking" for penetration testing purposes. PLEASE READ AND SIGN the "White-hat" agreement provided on MyGateway during the first week of this course. When in doubt, please contact me beforehand.***

**Undergraduate Students Only - Team Research Project (35% of your overall grade)**

A team-based research project will be another important aspect of this course. As mentioned earlier, InfoSec is a vast field. This course essentially surveys this field and "scratches the surface". However, it is important that students explore a particular / specific topic in depth. Toward this end, students will engage in a focused research project on a particular topic of interest. I will provide guidance on potential topic areas based on the backgrounds and future plans of students. I will also provide guidance on conducting research.

**Note:**

1. Students will work in (self-selected) groups of four.
2. Students will finalize group membership by the second class-period at the latest.
3. In full consultation with the instructor students should ideally finalize a topic area by the end of third week of class.
4. Each team will make a comprehensive presentation to the class during the last two weeks of class.
5. Each team will provide a written research paper
6. I will provide a detailed Research Project Description and Guidelines document

**Graduate Students Only – Individual Research Papers (35% of your overall grade)**
While undergraduate students work in teams, graduate students will have the opportunity to engage in individual research on a topic germane to their particular backgrounds and interests with respect to information security. The outcome will be a well written and methodologically sound research paper. **Note**: This will not be a "simple term paper" but hopefully a well designed and implemented research project that draws on primary or secondary data. The goal is to submit each student's paper to an academic or practitioner journal for publication. It is important that graduate students learn how to conduct and publish basic research. I will provide very detailed guidelines and help to each student and do my best to develop each student's research paper into something that is publishable. Graduate students must see me early in the semester and preferably every week to work on their projects.

**Academic Honesty Guidelines:** (from Academic Affairs website, Updated April, 27 2010)
Students at the University of Missouri-St. Louis are expected to exhibit the highest standards of academic integrity. An act of academic dishonesty is an offense against the university. For that reason, university rules prescribe disciplinary consequences for academic dishonesty administered by the Office of Academic Affairs, as well as academic consequences assessed by the faculty member. For a description of what constitutes "Academic Dishonesty" and for procedures followed by the University and by faculty members, please refer to: http://www.umsl.edu/services/academic/policy/academic-dishonesty.html

**Be sure to sign the on-line academic integrity statement**: Please go to your "My Academic Toolbox" in MyGateway and find "My Academic Integrity." After reading the statement, please check the "I accept this agreement" box (if you want to) and then click on the accept button.

**Other notes:**

1. I will make announcements on MyGateway. I strongly encourage you to visit this course under MyGateway regularly for important updates and documents.
2. Please check your UMSL email account regularly for information/updates regarding this course.

**COURSE SCHEDULE**
**The schedule below is tentative. Please refer to MyGateway for the most updated weekly topics, assigned readings, tasks, and assignments.**

| Wk. | Date | Topic | Assigned Readings / Tasks/Assignments |
|---|---|---|---|
| 1 | 8/27 | Course introduction, syllabus, course preparation.<br>Introduction to Information Security | Read syllabus |
| 2 | 9/3 | (contd.) Introduction to Information Security<br>The need for security, examining the threat environment | MyGateway Week 2<br>*(finalize group membership)* |
| 3 | 9/10 | (contd.) The need for security, examining the threat environment<br>Information Security Management | MyGateway Week 3<br>*Lab Assignment 1 Due*<br>*(finalize topic areas for group research project)* |
| 4 | 9/17 | (contd.) | MyGateway Week 4-6 |
| 5 | 9/24 | (contd.) | *Lab Assignment 2 Due* |
| 6 | 10/1 | Fundamentals of data networking for InfoSec | *In-class quiz on topics from Weeks 1 to 6* |

| Wk. | Date | Topic | Assigned Readings / Tasks/Assignments |
|---|---|---|---|
| 7 | 10/8 | (contd.) | MyGateway Week 7<br>*Non-Lab Assignment 1 Due* |
| 8 | 10/15 | (contd.) | MyGateway Week 8 |
| 9 | 10/22 | Information Security Technologies and Tools - Access Control | MyGateway Week 9<br>*Lab Assignment 3 Due* |
| 10 | 10/29 | Information Security Technologies and Tools - Firewalls | MyGateway Week 10 |
| 11 | 11/5 | Information Security Technologies and Tools - Intrusion Detection/Prevention Systems | MyGateway Week 11<br>*Lab Assignment 4 Due*<br>*Online quiz on topics from weeks 7 to 11* |
| 12 | 11/12 | Cryptography/Cryptology | MyGateway Week 12 |
| 13 | 11/19 | (contd.)<br>Secure Software Development<br>Web Application Architectures | MyGateway Week 13-14<br>*Lab Assignment 5 Due* |
| **14** | **11/26** | **NO CLASS, FALL BREAK** | |
| 15 | 12/3 | Overview - major vulnerabilities of Web Applications<br>Authentication / Session Management Issues<br>SQL Injection<br>Cross Site Scripting (XSS) | MyGateway Week 15<br>*(possible lab sessions with instructor)* |
| 16 | 12/10 | Web Application Security continued<br>**Research Project presentations (second half of class)** | **All students (including graduate students) must attend all presentations** |
| 17 | 12/17<br>Exam Week | Wednesday, December 17 – 07:45 to 09:45PM<br>**Research Project presentations continue** | *All Research Papers Due December 18 by 11:59pm Central Time* |

--End Syllabus--