

IT 428: Introduction to Information Security (exists as MSIS 428)

Course Description: An introduction to the various technical and administrative aspects of Information Security and Assurance. This course provides the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system, with appropriate intrusion detection and reporting features.

The purpose of the course is to provide the student with an overview of the field of Information Security and Assurance. Students will be exposed to the spectrum of Security activities, methods, methodologies, and procedures. Coverage will include inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of the Information Security Planning and Staffing functions.

Prerequisites: IT 110 Introduction to Computers or approval of the MSIS Department

Textbook and Resources: M. Whitman and H. Mattord. Principles of Information Security, 2nd Edition (Course Technology, 2005).
COBIT Student Book (Electronic Format from ISACA)
Software used in lab: Provided by Instructor.

Instructor: Jean-Pierre Kuilboer

Office: M 5-246

Email Address: Jeanpierre.kuilboer@umb.edu

Phone: 617 287-7868

Instructor Website Address: <http://boston.umassonline.net> Using WebCT

Course ID: _____ **Course Password:** _____

Course Objectives: After completing the course, students will be able to:
Identify and prioritize information assets.
Identify and prioritize threats to information assets.
Define an information security strategy and architecture.
Plan for and respond to intruders in an information system
Describe legal and public relations implications of security and privacy issues.
Present a disaster recovery plan for recovery of information assets after an incident.

POLICIES

Attendance:

The Instructor expects your attendance at each and every class; however, actual attendance is up to the student. Grade performance is a demonstrated function of attendance, preparation and participation. You can get behind very easily by skipping classes, resulting in a poor understanding of the material, which will show up as a poor grade for the class. Any class sessions missed by the student are the student's responsibility to make up, not the instructor's. Late arrival that causes disruption, early departure that causes disruption, excessive conversation among students (a disruption in its own right), inappropriate use of electronic devices that cause disruptions and other actions that disrupt the classroom are unacceptable.

Assessment:

Quizzes	10%
Exams	30%
Final Exam	20%
Lab Assignments	10%
Other Assignments	10%
Semester Project	20%
	100%

Grade Evaluation:

A	90% - 100%
B	89% - 80%
C	79% - 70%
D	69% - 60%
F	59% or below

Evaluation criteria explained:

Students are expected to be active participants in each class meeting. Full credit for participation will be extended to students who regularly ask questions, share observations, and contribute relevant personal experiences.

The mid-term examination will consist of objective questions and will require a technological comprehension that covers the lecture material and assigned readings.

The assignments will consist of a number of individual in class and homework tasks. Students will be given specific guidance on the amount of collaboration permitted for each assignment. Unless otherwise specified, all assignments are individual assignments, and thus must be completely the original work of the student submitting them and include proper citations to the published work of others.

Quizzes:

Quizzes will be given throughout the semester, at a rate of approximately 1 per chapter. Quizzes will always cover the material covered since the last Quiz or Exam. The quizzes will be combinations of objective and short-answer questions. Quizzes will be administered online via WebCT. Makeup quizzes will not be given. However, the lowest quiz grade will be dropped. Any class material missed by the student is the student's responsibility to acquire.

Exams:

There will be two (2) non-cumulative examinations – a midterm and a final exam. The content will come from the text and other material presented in lecture sessions as well as labs. Note that material presented in class and in lab will supplement the assigned reading. Therefore, class attendance and good note taking are essential tactics for success.

There will be no make-up examinations. It is the student's responsibility to arrange for an excused absence **before** the exam. A grade of zero will be assigned for all exams missed without an excused absence. If an emergency arises on the day of the midterm, and the instructor deems that the absence is excused, then the weight of the final exam may be increased to replace the midterm.

Guidelines for submitting work:

All homework assignments are to be submitted by email to the instructor's email address at the top of this syllabus. See individual assignment requirements in WebCT. Be sure you receive an acknowledgement from the instructor for each assignment. Every assignment the instructor receives will have an acknowledgement sent. If you did not get the acknowledgment, the instructor did not get the assignment.

All email submissions must be received prior to the stated deadline. The following format must be used when submitting assignments via email.

Subject: MSIS428-hw/01 yourname LAB# Example: msis428-hw/01 *Surname Lab 1*

Late assignments will not be accepted!

Withdrawal Policy:

The last day to withdraw without academic penalty is 04-06-06. Ceasing to attend class or oral notice thereof DOES NOT constitute official withdrawal from the course. Students who simply stop attending classes without officially withdrawing usually are assigned failing grades. Students wishing to withdraw after the scheduled change period (add/drop) must obtain and complete a withdrawal form from the Academic Services Department in the Registrar's Office.

Enrollment Policy:

Only those students who are enrolled in the class may attend lectures, receive assignments, take quizzes and exams, and receive a grade in the class. If a student is administratively withdrawn from this course, they will not be permitted to attend class nor will they receive any grade for the class.

Electronic Devices:

In order to minimize the level of distraction, all watches, beepers and cellular phones must be on quiet mode during class meeting times. Students who wish to use a computer/PDA for note taking need prior approval of the instructor since key clicks and other noises can distract other students. Recording of lectures by any method requires prior approval of the instructor.

Email Messages:

Remember to put the course name and section number in the subject field of every e-mail message that you send me. E-mail messages that are missing this information are likely to be automatically redirected to a folder the instructor will seldom check.

Lab Assignments:

Four lab sessions and accompanying assignments are due throughout the term. Details and due dates are available from WebCT. Each of these lab assignments is weighted equally.

No lab make up sessions are available, and late assignments will not be accepted! If you are unable to arrive at the lab on time on the day of the lab session and must then perform the lab work on your own, you are responsible for turning on the lab assignment on time. You may turn the assignment in early. Assignments are submitted via email unless specified otherwise.

General Assignments:

Five general assignments are due throughout the term. Details and due dates for these assignment are available from WebCT. Each of these assignments is weighted equally.

Late assignments will not be accepted! You may turn the assignment in early. Assignments are submitted via email unless specified otherwise.

Semester Project:

A group multimedia project will be performed with delivery during the last two class days. Details of this group project assignment are available from WebCT.

Internet Services Account:

Servername is the name of the server used to provide students with an e-mail account and space for a Web page. Accounts may be applied for online. You are responsible for knowing and following all policies that are posted on the servername site. A very useful introduction to servername is also available.

If you established a servername account prior to registering, make sure that your account is active and that you know your password before the second week of class.

Your e-mail address on servername will be important as it will used for class communication of important announcements.

Computer Labs:

Please be aware of and follow all computer lab user policies.

Campus red Lab

The labs on the Healey Library Building are open 7 days each week as follows:

M-Th 7:45am - 11pm

Friday 7:45am - 5pm

Sat 10am - 6pm

Sun noon - 8pm

The Campus Red Lab lab is open most holidays. Be prepared to show your current student ID card upon entering the lab. The telephone number of the Campus Computing service is 770-555-6110.

Campus (Purple) Lab

The lab in HL of the Library Building is open for this class as follows:

Wed 4:00-5:15

The telephone number of the Campus is .

Disability Statement:

Any student with a documented disability needing academic adjustments is requested to notify the instructor as early in the semester as possible, and must do so before the mid-term exam. Verification from disabled Student Support Services is required. All discussions will remain confidential.

Academic Integrity Statement:

Every University student is responsible for upholding the provisions of the Student Code of Conduct, as published in the Undergraduate and Graduate Catalogs. The Student Code of Conduct addresses the University's policy on academic honesty, including provisions regarding plagiarism and cheating, unauthorized access to University materials, misrepresentation/falsification of University records or academic work, malicious removal, retention, or destruction of library materials, malicious/intentional misuse of computer facilities and/or services, and misuse of student identification cards. Incidents of alleged academic misconduct will be handled through the established procedures of the University Judiciary Program, which includes either an "informal" resolution by a faculty member, resulting in a grade adjustment, or a formal hearing procedure, which may subject a student to the Code of Conduct's minimum one semester suspension requirement.

Students are encouraged to study together and to work together on class assignments and lab exercises; however, the provisions of the STUDENT CONDUCT REGULATIONS, II. Academic Honesty, Undergraduate Catalog will be strictly enforced in this class.

Frequently students will be provided with "take-home" exams or exercises. It is the student's responsibility to ensure they fully understand to what extent they may collaborate or discuss content with other students. No exam work may be performed with the assistance of others or outside material unless specifically instructed as permissible. If an exam or assignment is designated "no outside assistance" this includes, but is not limited to, peers, books, publications, the Internet and the WWW. If a student is instructed to provide citations for sources, proper use of citation support is expected. Additional information can be found at the following locations.

<http://www.apa.org/journals/webref.html>
<http://www.lib.duke.edu/libguide/citing.htm>
<http://bailiwick.lib.uiowa.edu/journalism/cite.html>
<http://www.cas.usf.edu/english/walker/papers/copyright/ipdummie.html>
<http://www.indiana.edu/~wts/wts/plagiarism.html>
<http://plagiarism.phys.virginia.edu/links.html>
<http://www.arts.ubc.ca/doa/plagiarism.htm>
<http://alexia.lis.uiuc.edu/%7ejanicke/plagiaryv.htm>
<http://webster.comnet.edu/mla/plagiarism.htm>
<http://www.virtualsalt.com/antiplag.htm>
http://www.engr.washington.edu/~tc231/course_info/plagiarism.html
<http://quarles.unbc.edu/lsc/rpplagia.html>

Week	Textbook Assignment	Other Assignments and Notes
1		Introduction to the course
	Chapter 1 IS	Introduction to Information Security
2	Chapter 2 IS	The Need for Security
	Chapter 1 IS-lab	Footprinting
3	Chapter 3 IS	Legal, Ethical, and Professional Issues in Information Security
	Chapter 6 IS-Lab	Information Security Management
4	Chapter 4 IS	Risk Management
	Chapter 3 IS-Lab	Operating System Vulnerabilities and Resolutions
5	Chapter 5	<i>President's day</i>
	Chapter 5	Planning for Security
6		First Exam
	Chapter 2 IS-Lab	Scanning and Enumeration
7	Chapter 6	Technology: Firewalls & VPNs
	Chapter 4 IS-Lab	Network Security Tools and Technologies
8	Chapter 7	Technology: IDS and Access Control
	Chapter 8 IS-Lab	Computer Forensics
9	Chapter 8	Cryptography
	Chapter 7 IS-Lab	File System Security and Cryptography
10	Chapter 9	Physical Security
		Introduction to COBIT
11	Chapter 10	Implementing Security
		Second Exam
12		<i>Patriots Day</i>
		Catch-up lab (exam review)
13	Chapter 11	Security and Personnel (Private/Public/Task Force)
		Introduction to COBIT (2)
14	Chapter 12	InfoSec Maintenance
	Chapter 5 IS-Lab	Security Maintenance
	Presentation of Group Projects	
	Presentation of Group Projects	
15	Final Exam	

Special Dates:

Holidays/No Class

Last day to withdrawal without penalty

Last day of class

Final Exam

White Hat Agreement And Code of Ethics

This is a working document that provides further guidelines for the course exercise. If you have questions about any of these guidelines, please contact one of the course instructors. When in doubt, the default action should be to ask the instructors.

- 1) The goal of the project is to search for technical means of discovering information about others with whom you share a computer system. As such, non-technical means of discovering information are disallowed (e.g., following someone home at night to find out where they live).
- 2) ANY data that is stored outside of the course accounts can be used only if it has been explicitly and intentionally published, (e.g. on a web page), or if it is in a publicly available directory, (e.g. /etc, /usr).
- 3) Social engineering for information about individuals from anyone outside of the course is disallowed.
- 4) Impersonation, e.g. forgery of electronic mail, is disallowed.
- 5) If you discover a way to gain access to any account other than your own (including root), do NOT access that account, but immediately inform the course instructors of the vulnerability. If you have inadvertently already gained access to the account, IMMEDIATELY exit the account and inform the course instructors.
- 6) All explorations should be targeted specifically to the assigned course accounts. ANY tool that indiscriminately explores non-course accounts for vulnerabilities is specifically disallowed.
- 7) Using the web to find exploration tools and methods is allowed. In your reports, provide full attribution to the source of the tool or method.
- 8) If in doubt at all about whether a given activity falls within the letter or spirit of the course exercise, discuss the activity with the instructors BEFORE exploring the approach further.
- 9) You can participate in the course exercise only if you are registered for a grade in the class. ANY violation of the course guidelines may result in disciplinary or legal action.

White Hat Agreement
University of Massachusetts Boston

Code of Ethics Preamble: (Source www.isc2.org Code of ethics)
Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
Therefore, strict adherence to this code is a condition of laboratory admission.

Code of Ethics Canons:
Protect society, the commonwealth, and the infrastructure.
Act honorably, honestly, justly, responsibly, and legally.
Provide diligent and competent service to principals.
Advance and protect the profession.

The following additional guidance is given in furtherance of these goals.

Protect society, the commonwealth, and the infrastructure
Promote and preserve public trust and confidence in information and systems.
Promote the understanding and acceptance of prudent information security measures.
Preserve and strengthen the integrity of the public infrastructure.
Discourage unsafe practice.

Act honorably, honestly, justly, responsibly, and legally
Tell the truth; make all stakeholders aware of your actions on a timely basis.
Observe all contracts and agreements, express or implied.
Treat all constituents fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession in that order.
Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide diligent and competent service to principals
Preserve the value of their systems, applications, and information.
Respect their trust and the privileges that they grant you.
Avoid conflicts of interest or the appearance thereof.
Render only those services for which you are fully competent and qualified.

Advance and protect the profession
Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
Take care not to injure the reputation of other professionals through malice or indifference.
Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

As part of this course, you may be exposed to systems, tools and techniques related to Information Security. With proper use, these components allow a security or network administrator better understand the vulnerabilities and security precautions in effect. Misused, intentionally or accidentally, these components can result in breaches of security, damage to data or other undesirable results.

Since these lab experiments will be carried out in part in a public network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this form, then you cannot participate in the lab exercises.

Student agreement form:

I agree to:

- only examine the special course accounts for privacy vulnerabilities (if applicable)
- report any security vulnerabilities discovered to the course instructors immediately, and not disclose them to anyone else
- maintain the confidentiality of any private information I learn through the course exercise
- actively use my course account with the understanding that its contents and actions may be discovered by others
- hold harmless the course instructors and University of Massachusetts Boston for any consequences of this course
- abide by the computing policies of University of Massachusetts Boston and by all laws governing use of computer resources on campus

I agree to NOT:

- attempt to gain root access or any other increase in privilege on any UMB workstation
- disclose any private information that I discover as a direct or indirect result of this course exercise
- take actions that will modify or deny access to any data or service not owned by me
- attempt to perform any actions or use utilities presented in the laboratory outside the confines and structure of the labs.
- utilize any security vulnerabilities beyond the target accounts in the course or beyond the duration of the course exercise
- pursue any legal action against the course instructors or University of Massachusetts Boston for consequences related to this course

Moreover, I consent for my course accounts and systems to be examined for security and privacy vulnerabilities by other students in the course, with the understanding that this may result in information about me being disclosed (if applicable).

The above agreement has been explained to me to my satisfaction. I agree to abide by the conditions of the Code of Ethics and of the White Hat Agreement.

Signed, _____ Date: _____

Printed name: _____

e-mail address _____

Acknowledgment and Acceptance of Academic Integrity Statement:

In any academic community, certain standards and ethical behavior are required to ensure the unhindered pursuit of knowledge and the free exchange of ideas. Academic honesty means that you respect the right of other individuals to express their views and opinions, and that you, as a student, not engage in plagiarism, cheating, illegal access, misuse or destruction of college property, or falsification of college records or academic work.

As a member of the University academic community you are expected to adhere to these ethical standards. You are expected to read, understand and follow the code of conduct as outlined in the graduate and undergraduate catalogs. You need to be aware that if you are found guilty of violating these standards you will be subject to certain penalties as outlined in the college judiciary procedures. These penalties include permanent expulsion.

Read the Academic Integrity Statement and then sign and date in the space below. You are required to abide by these ethical standards while you are a student. Your signature indicates that you understand the ethical standards expected of you in this academic community, and that you understand the consequences of violating these standards.

Course Name

Instructor Name

Print Name

Signature

Date