



GRADUATE COLLEGE OF MANAGEMENT

MIS 7233 NETWORK SECURITY COURSE SYLLABUS 100% Online COURSE

Course Information

*MIS 7233-01
CRN 5150
Summer Semester - 2007*

This course will satisfy general elective requirements for DMIT, MSIS, BSCS, MSECE, MSCE, and BSCE.
THREE (3) Graduate Level Credit Hours

Instructor Information

Name and Title: Dr. Kamal Kakish, Adjunct Professor, Graduate College of Management

Cell Phone w/Voice Mail: (248) 703-6882 *for emergencies only please; otherwise please use email.*

E-mail: profkakash@gmail.com
Office Hours: Online

Texts and Assigned Readings

Required Text

- ["Principles of Computer Security – Security + and Beyond"](#), by Conklin et al., McGraw Hill Technology Education, 2004. ISBN: 0-07-225509-9
- ["Readings and Cases in the Management of Information Security"](#), by Michael Whiteman and Herbert Mattord, Thomson Course Technology, 2006, ISBN 0-619-21627-1.
- ["Pocket Guide to APA Style"](#), by Robert Perrin, Houghton Mifflin Publishers, ISBN 0-618-30820-2.

Supporting Texts (Optional)

- ["Fundamentals of Network Security"](#), by Eric Maiwald., McGraw Hill Technology Education, 2004. ISBN: 0-07-223093-2

- “Guide to Network Defense and Countermeasures”, by Greg Holden., Thomson Course Technology, 2003. ISBN: 0-619-13124-1
- “Guide to Computer Forensics and Investigations”, by Bill Nelson, et. al., Thomson Course Technology, 2004. ISBN: 0-619-13120-9
- “Guide to Disaster Recovery”, by Michael Erbschloe., Thomson Course Technology, 2003. ISBN: 0-619-13122-5

Additional Resources

- ISO/IEC 17799 – Information Technology – Code of practice for Information Security management
- NSAI/IS 17799-2 – Information Security Management Systems – Part 2: Specification with Guidance for Use

Instructions on how to obtain copies of the standards from the LTU Library will be given online.

Supplementary Readings

1. The instructor will periodically provide the students with articles, web sites, etc.

Course Overview

Purpose of Course

This course offers an in-depth exploration of security issues and related challenges for any organization. It is highly technical, and focuses on Information and Computer Security technologies, tools, techniques and approaches. This course addresses emerging technologies and best practices that are state-of-the-art. It can yield significant value to the student during the implementation phase of an enterprise information security plan.

The course is designed to take a deep dive in today’s technologies of computer security. It will discuss the following topics in depth:

- Cryptography
- Security Standards and Protocols
- Infrastructure Security
- Internet and Web Security
- Intrusion Detection and Prevention
- Wireless security and remote access
- Disaster Recovery and Business Continuity
- Computer Forensics
- Risk Management
- Patch Management

- Privilege Management
- Auditing
- And more

Students who attend this course will have had some background knowledge in computer networks, enterprise computer security policy, and an overall understanding for the need to implement an information security plan.

Course Objectives

This course is designed for students working toward a degree in MSIS, MSECE, MSCE, and other disciplines with focus on Information and Computer Security. This course may be considered as one of several courses required to satisfy that emphasis. Students can gain a greater advantage if they come into this course having had:

- An enterprise information security type course
- A data telecommunication course, or
- A networking / infrastructure course.

This course is NOT intended to be an introduction to information security and assumes that the students already understand the importance of developing an enterprise information security plan and policy.

The objective of this course is to equip the students with the knowledge necessary to address tactical and strategic business issues by selecting and recommending the appropriate technologies and tools necessary to solve a business problem related to the security of information and computers.

Ideally, the student will be prepared to provide an optimal solution to a real-life information security business problem upon successful completion of this course. Understanding the pros and cons of the various technologies and techniques that are available for use in order to secure and protect intellectual property and the infrastructures that contain it, the student should be able to apply the appropriate tools, techniques, and technologies to the situation at hand effectively.

Upon successful completion of this course, each student should have a deep understanding of both business and technical issues related to:

- Adopting/developing and implementing information security Best Practices
- Managing risk and protecting against network attacks and malware (DoS, spoofing, hijacking, viruses, worms, Trojan horses, zombies, logic bombs, etc)
- Understanding various types of devices that construct the infrastructure, the variety of media that carry network signal, the diversity of storage devices, and how the use of security zones and other topologies provide network/web-based security.
- Defending the infrastructure with techniques, technologies and approaches such as authentication, digital signatures, digital watermarking, digital certificates, public and private keys, intrusion detection, intrusion prevention, standards and

protocols (PKIX/PKCS, X.509, SSL/TLS, ISAKMP, CMP, S/MIME, PGP, HTTPS, IPSec, FIPS, WTLS, WEP, ISO 17799) and cryptography

- Understanding the vulnerabilities of Wireless LAN's, WAN's, Protocols and Instant Messaging, and how Remote Access methods can be effectively applied to maximize security and privacy (WAP, WTLS, WEP, AAA, VPN, SSH, Telnet, Tunneling L2TP, PPTP, IEEE 802.11, 802.1X, RADIUS, etc)
- Hardening various operating systems, network devices, and applications (with special emphasis on e-mail transmissions), and establishing the system's security state (baselining process)
- Understanding hacking threats & the importance of trustworthy code
- Securing and protecting Web Components (SSL/TLS suite, LDAP, FTP, Web Services, plug-ins, directory services, dynamic content, applets, servlets, malicious cookies, etc)
- Incorporating security best practices into the software development process in order to prevent/minimize future/production attacks.
- Understanding the importance of auditing, what should be audited, and how to conduct an effective and timely audit.
- Understanding Disaster Recovery and the different strategies and alternatives that can maintain Business Continuity (of course, the subject of Disaster Recovery is so broad and diverse, and deserves to have a course on its own).
- Applying Privilege Management using the advantages of single sign-on and other techniques
- Understanding the rules of Computer Forensics and how various types of evidence can be used to prevent future computer crime
- Legal and ethical aspects of network security

Attaining the Course Objectives

To pursue the course objectives effectively, students will engage in the following activities:

- Read assigned material prior to the online sessions;
- Complete individual assignments and submit them on time;
- Participate in online class discussions (via BB Discussion Board); Online Participation
- Complete a midterm examination;

Unless specifically authorized by the professor, all work assignments should be solely the student's own individual work.

Course Policy

General Policies:

- Individual Assignments must be completely finished to pass the course. On time delivery of complete documentation is expected. Specific criteria for the deliverables will be provided prior to the work assignments.
- The topics listed in the syllabus are only an estimate of the material, which can be covered during the semester. Some topics might be deleted and some others might be added at the discretion of the instructor.
- Teamwork and collegiality are encouraged but everyone must understand and be responsible for their work, actions and work products; observations of the Honor Code Policy are mandatory. http://www.ltu.edu/currentstudents/honor_code.asp
- All other University policies regarding incomplete grades, etc. apply.

Academic Integrity:

This course falls under the provisions of the policies on academic integrity of LTU. Any violations of this policy will result in failure.

Online Participation:

Students are expected to actively participate online using the BB Discussion Board. The due date for each discussion thread is ONE week after the associated chapter(s) is scheduled according to the class calendar below. Discussions will be “locked” typically 2 weeks after participation is due for the particular module; therefore, the most any student could be behind in participation is one week. Once a module is locked, students cannot participate online for that module.

Assignments:

All assignments should be delivered electronically via the Black Board *View/Submit Assignment* function located under “Assignments”. If technical difficulties are encountered, you can send the assignment via e-mail to the address provided above, but only as a last resort. Assignments are due on or before the date assigned. *Late assignments will cause a 10% per day deduction from the value of the assignment.*

Technology:

Students are expected to utilize the following types of technology during this class.

- Internet data retrieval and research
- Use of Black Board (Access provided by LTU)
 - Group collaboration and Communication
 - Announcements and Updates
 - Course Material
 - Grades Posting
- Use of the following software:
 - Word Processing Software
 - Email System

- Web Browser Software
- Presentation Software
- A variety of Software Tools relating to IT Security Management Systems (ex: cryptographic tools). Most can be downloaded from the internet for free for a limited period of time.

Course Calendar / Schedule

10-week Course starts 5/14/08 and ends 7/24/2008

Module	Date	Topic/Activity	Readings
1	5/19/2008	Introduction/Syllabus Review Student data sheets Course Expectation Online Discussion Board	Ch. 1-4 <i>Students read the first 4 chapters on their own.</i>
2	5/26/2008	Cryptography <i>Crypto Demo – put in View/submit assignment Due by 11:59pm on Friday 5/30/08</i> Online Discussion Board	Ch. 5
3	6/2/2008	Public Key Infrastructure Impact of Physical Security on Network Infrastructure Security <i>Assignment #1 Due by 11:59pm on Friday 6/6/08</i> Online Discussion Board	Ch.6 Ch. 8 Ch. 10
4	6/9/2008	Standards and Protocols Network Fundamentals Online Discussion Board	Ch. 7 Ch. 9
5	6/16/2008	Wireless and Instant Messaging Remote Access <i>Assignment #2 Due on Friday 6/20/08 by 11:59pm</i> Online Discussion Board	Ch. 12 Ch. 11
	6/23/2008	<i>Midterm Exam (Selected Topics)</i> Exam available on Monday 6/23/08 from 6:00 am to 11:00 pm Online Discussion Board	
6	6/30/2008	Intrusion Detection Systems Online Discussion Board	Ch. 13
7	7/7/2008	Attacks and Malware Software Development Best Practices <i>Assignment #3 Due on Friday 7/11/08 by 11:59pm</i> Online Discussion Board	Ch. 15 Ch. 18

8	7/14/2008	Securing Web Components Security of E-mail Transmissions Online Discussion Board	Ch. 17 Ch. 16
9	7/21/2008	Security Baselines Online Discussion Board <i>Assignment #4 Due on Thursday 7/24/2008 by 11:59pm</i> Online Discussion Board	Ch. 14

Summary of Grading Scheme

What	Content	Weight
Crypto Demo	Report on a Cryptography SW Package	5%
Individual Assignment 1	CISSP, Security+, SSCP, CISM, CCSP, Other Exams and CNSS, US-CERT Research Report	10%
Individual Assignment 2	Activity – Security Situation – Select any TWO of the 4 activities	10%
Individual Assignment 3	Infrastructure Security Case - Proposal	15%
Individual Assignment 4	Intrusion Detection System	10%
Midterm Exam	Chapters Covered to date	25%
Online Participation	Online Forum Discussions on BB & GP	15%
Online Facilitation	Facilitate assigned online discussions	10%
	Total	100%

Course Assignments, Instructions, and Grading Guidelines

All assignments and project work must adhere to the following:

- Course#, Semester, Student Name, and assignment number must be contained in the assignment file name. For example, if this assignment 2 for John Smith, the file name would look like this:

MIS7233Summer08JohnSmithA2.doc/xls/ppt/etc.

- Please use APA Style format for all your documents. For more information, refer to the APA Pocket Guide listed above and visit <http://www.apastyle.org/>. **References should be cited within the body of your document, ex: (Kakish, 2004), and at the end under a section titled “References”, sorted alphabetically.**
- No handwritten assignments allowed.

Here are some guidelines for figuring out where or why points may get deducted from your assignment score. To maximize your score, please adhere to the instructions above and avoid the common mistakes below. The following deductions may be applied as follows:

Reason	Point Deduction
Not answering a question	% question worth out of entire assignment
Assignment turned in late	10% per each late day
References Missing	10 points
References in document body don't match reference list	5 to 10 points
Document Name submitted in Digital Drop Box inconsistent with above naming convention	5 points
Document Format submitted in Digital Drop Box inconsistent with APA Style	5 points
Elaboration on each question is shallow	1 to 10 points
Overall quality of the assignment report	1 to 50 points
Cheating or using someone else's work	Both students get ZERO
Quoting someone's work or idea without proper citation	10 points per occurrence
Copying and pasting from the Internet without rephrasing in your own words. Assignments will be randomly checked for copying from the Internet via "Safe Assignment" automated tool.	20 points per occurrence.

Crypto Demo

For this exercise, once you finish chapter 5 (Cryptography), search the internet to find a FREE demo of a Cryptographic software package of your choice (there are tons of them out there). Download and install the demo or free product on your machine and play with it. Then write a 500 word report describing the product, what protocols it uses, how it works, what you learned from it, and if you would recommend it and why. Submit your report to BB under View/submit Assignment. Also, put a PowerPoint presentation for your demo in the BB Discussion Board so other students see it. Finally take a look at what the other students submitted for their demo.

Assignment # 1

Security Certification Research

"Some certifications are hot, some not"

Security Certification has increasingly become an important consideration among business managers and technical professionals alike. With the advent of 9/11 terrorism and the progressive threats and attacks on computer and data systems worldwide, governments and businesses have sharply increased their requirements for information security certified professionals.

Students should research information on the various types and classifications of Security Certifications from a variety of sources. At minimum students should contrast, compare, and report on the following certifications:

1. CISSP (from ISC2)
2. CompTIA Security+
3. SSCP

4. CISM
5. CCSP, and
6. Other relevant Certifications and Exams.
7. Your personal observations and conclusions on certification

In addition, students should visit the Center for National Security Studies (CNSS), US-CERT <http://www.us-cert.gov/>, and other cyber-terrorism and counter-terrorism websites including the Whitehouse and the Department of Homeland Security (DHS), and summarize their findings, assessments, and personal opinions regarding the US readiness in combating information threats and attacks, and the degree to which Information Technology is able to address national and global information security issues.

The length of the report should be a minimum of 1,200 words but should not exceed 2,000 words, using APA style format with references (both within and at the end) and a font of "Arial 12".

Assignment # 2

Security Scenario

For the 2nd assignment, you may select ANY TWO of the 4 following activities – the choice is yours. Remember: you should answer ONLY TWO of the 4 activities:

Activity 1: E-mail memo to customer regarding Melissa virus incident

Situation:

Recently, a workstation in the Engineering Department was infected with a virus delivered through e-mail. You investigate and discover that the virus did not penetrate your normal security protections, which would have detected and cleaned the e-mail arriving through the company's mail servers. An engineer had, however, in addition to the normal company mail, established a Hotmail account and had downloaded an e-mail unaware of the virus that was attached. When the engineer opened the attachment, the virus installed itself. The Hotmail account was not being used for work purposes; however, everybody knows that employees access web mail for personal reasons on a regular basis. You need to solve the problem, and then prepare an incident report that describes the incident and what you did to resolve the problem.

1. Write an informal incident report as an e-mail memo to your supervisor.
2. In the memo, describe in your own words what happened, and the corrective action taken. The corrective action should include the steps to prevent further attacks of this kind. The steps should list how to find the virus, how to get rid of it, and finally, what you recommend the company to do about user education and policies for use of e-mail.

Criteria for Success:

1. At least two solutions to the problem including (1) user education and (2) the regular use of antivirus software. Your solutions will be read for reliability and effectiveness of the proposed solutions. For instance, how reliable will user education be in preventing users from using non-secure e-mail services at work? When you suggest installing and keeping antivirus software up-to-date, discuss the most reliable strategy for doing this. Finally, suggest a company policy to warn employees about the security risks of non-secure e-mail services and the possible consequences if they choose to ignore this warning.
2. Appropriate and correct language for the intended audience, in this case a technical audience. The language should be accurate, spell-checked, and grammatically correct.

Activity 2: Factory worker doing eBay business on company's computer

Situation:

Acme allows employees to use their computers for personal use such as checking bank statements and personal Web searches. An employee has requested that he be able to use his laptop at work and home for checking his eBay store during lunch breaks and at home for doing other eBay activities. Your boss has asked you to study the issue and recommend a company policy regarding eBay. Determine if there are any security issues associated with eBay. Choose a position and develop pros and cons in the policy. Draft the policy in a memo format.

Criteria for Success:

1. Display knowledge of security issues as relevant to the requirement.
2. Develop position developed logically and with general security policies in mind.
3. Use accurate and appropriate language that is spell-checked and grammatically correct.

Activity 3: Engineer is not allowing his workstation to be updated with the most recent patches

Situation:

An engineer is not allowing his workstation to be updated with the most recent patches because the updates cause problems. His workstation is used to run large computations and many computations may run for days. Updates, especially automated patches and virus fixes, often require reboots. These unplanned reboots interrupt the computation, which forces the engineer to restart the computation from the beginning. Unscheduled reboots have direct impact on his schedule to support his projects. The results of the computations and many graphics files created are used by other engineers. They are stored in JPG format on his workstation, so his system must be on the network that

exposes it to virus infections. Company security policy requires virus updates and security patches to be kept up-to-date. Explain the importance of following the Company security policy and let him know that you will be providing him a solution. Then type a memo to your manager in which you suggest three solutions with their pros and cons, and recommend the best solution.

Criteria for Success:

1. Memo to engineer regarding the security policies and reasons for the need to comply with the security policies.
2. Memo to your supervisor describing alternative plans to solve the problem.
3. Spell-checked and grammatically correct language.

Activity 4: A company executive is concerned about company's confidential data being compromised

Situation:

Acme has recently begun work on a new product that requires the engineers to collaborate with another firm located in another state. In order to collaborate, the engineers are using shared design software on Acme's server. They also plan to co-develop technical documentation, which will be stored on Acme's server. An Acme executive is concerned that the company's confidential data will be compromised on the project, if outsiders are allowed to access proprietary information. You have been asked to give a presentation on the security aspects of remote access and how the security procedures such as VPN and cryptography will protect Acme's confidential information. A short PowerPoint presentation on how VPNs and cryptography will protect Acme's network should be appropriate for Acme's high level managers.

Criteria for Success:

1. Detailed information regarding VPN, how it works, and why it is more secure than a normal network.
2. Description of cryptographic techniques and the one, which is most secure.
3. A suggested solution with justifications for the solution being a best practice.
4. PowerPoint presentation with title page, table of contents, purpose, body, and conclusion charts.
5. Spell-checked and grammatically correct language.

Assignment # 3 Infrastructure Security

To complete this assignment, you need to read “Reading 2”, which can be found on page #8 in the Readings and Cases in the Management of Information Security Textbook, AND, “Case A”, which can be found on page A-1 of the same book.

Here, you are presented with a fictitious computer gaming company (CGT, Inc.) that has put out a Request for Proposal (RFP) relative to a variety of security needs and objectives that will align with and support the company’s goals, if implemented effectively.

The proposal you prepare in response to the RFP has a well-structured **format that you should follow**. This case study will expose you to a number of security topics, but most importantly, I’d like you to focus the bulk of your efforts on the logical and physical security design, and implementation strategies which can be found under sections III and IV of the RFP on page A-9. These 2 sections will provide ample opportunity to leverage the Infrastructure Security knowledge you gained from chapters 6, 8, 9, 10, 17, and 18 of your main textbook – Principles of Computer Security.

Your job is to prepare and present a proposal in response to CGT’s RFP which starts on page A-7. Again, please make sure you follow the proposal format with the following exceptions:

- In section I, you may skip the following items:
 - D. Feasibility Study. We will assume that the project is feasible.
 - F. Estimate of costs
 - H. Feasibility analysis
- In section II, you may skip the following:
 - D. Documentation of findings and updated feasibility analysis. **You should document your findings**, but ignore the updated feasibility analysis.
- In section III, you may skip the following:
 - H. Feasibility Recommendation for continuing and/or outsourcing the project
- In section IV, you may skip the following:
 - C. Documentation of the system
 - E. Updated feasibility analysis
- Section V maybe skipped all together.
- Appendix B: Copies of Pricing Sources maybe skipped in its entirety.

Assignment # 4 Intrusion Detection System

The objective of this assignment is to provide you an opportunity to do your own research in order to understand the various issues associated with recommending Intrusion Detection Systems (IDS) for a corporation.

To begin with, you received an e-mail from your boss informing you that your company has decided to invest in IDS. Your boss is asking you to **interview** the IT Security Manager at your place of work (if you can't find someone to interview, you may interview a professor) for the purpose of understanding the company's requirements for the IDS. During the interview, you must start with the business objectives then drill down to the specifics of the IDS needs. You must align the needs of implementing the IDS directly with the corporate goals and objectives regarding information security.

A logical sequence of events might flow like this:

1. Educate yourself all you can about IDS. Review chapter 13 in your textbook and research additional IDS topics beyond the textbook.
2. Compare and contrast the pros and cons of network versus host-based IDS solution. You want to make sure you understand the ins and outs of both solutions prior to the interview. You may potentially consider a hybrid solution, depending on the needs you gather from the interview.
3. Conduct the interview and identify the following (make sure you prepare your list of questions before you conduct the interview):
 - a. Business goals and objectives as they relate to information security
 - b. Specific corporate objectives for Intrusion Detection
 - c. Corporate Policy as it relates to Intrusion Detection
 - d. IT objectives for an IDS system
 - e. Security data requirements. They may include devices, topology, and intrusion detection
 - f. List of requirements for the ideal IDS solution
 - g. Criteria for selecting the appropriate IDS solution. • Requirements are analyzed relative to applicable time, technology, and cost constraints.
4. After the interview, document the requirements for the ideal IDS solution and draft a memo to the IT Security Manager to confirm your understanding of such requirements.
5. Research at least 3 IDS packaged solutions available in the market, based on the requirements and criteria provided by the IT Security Manager, and compare the pros and cons of each. This will help you finalize your decision for a recommendation. Hint: use the table below to help your research.
6. Draft a proposal to the IT Security Manager of your company explaining the following:
 - a. Your assessment of the company's needs for IDS.
 - b. Your findings relative to the IDS available on the market. For each IDS package list the pros and cons
 - c. Provide your best choice recommendation
 - d. Defend your rationale for making the best choice recommendation.

Name	Product	Where to Find More Information
Cisco Systems, Inc.	Cisco IDS	www.cisco.com
Computer Associates	eTrust	www.ca.com
Enterasys Network	Dragon	www.enterasys.com
Internet Security Systems, Inc.	RealSecure	www.iss.net
Intrusion, Inc.	SecureNet, SecureHost	www.intrusion.com
Intruvert Networks	IntruShield	www.intruvert.com
iPolicy Networks	ipEnforcer	www.ipolicynetworks.com
NetScreen	NetScreen IDP	www.netscreen.com
NFR Security, Inc.	NFR	www.nfr.com
Snort	Snort (free, open source)	www.snort.org
Symantec Corporation	Intruder Alert	www.symantec.com
TippingPoint Technologies	UnityOne	www.tippingpoint.com
Tripwire, Inc.	Tripwire	www.tripwiresecurity.com