

COURSE OUTLINE for MGS 650 Information Assurance

**** Dr. H.R. Rao (mgmtrao@buffalo.edu)**

Comments and feedback are welcome

Monday Evening, 6.30 to 9.10 pm Jacobs 320, SUNY Buffalo

Office Hours: 5:15pm – 6:15 pm Monday and by Appointment

Office: 325 C Jacobs Center; Ph: 645-3425, e-mail: mgmtrao@buffalo.edu

TAs: Insu Park insupark@buffalo.edu & Teju Herath tcherath@buffalo.edu, PhD students, MSS Department, SOM, SUNY Buffalo

Motivation

The IT security specialist was named the hottest job, according to Challenger, Gray & Christmas, a Chicago-based international outplacement firm. An IT security manager came in ninth on the list of high-paying hot jobs according to Datamation. According to the Certification Magazine's (CertMag.com) 2005 Salary Survey, Certified Information Systems Security Professionals (CISSP's) can earn on average \$ 93,000 - \$ 116,000 a year while Cisco Certified Security Professionals (CCSPs) can earn on average \$ 91,000 a year. And the post of chief privacy officer got the nod for the highest-paying hot job, bringing in an average salary of \$122,360. Clearly the discipline of Information Assurance is an important one and it is expected that it will become even more important in the near future.

Objective

This is an interdisciplinary course in Information Assurance (IA). It has two primary objectives:

1. To introduce students to fundamental concepts, terminologies, IA models and practices.
2. To view how different fields of disciplines interact in this area. The course will familiarize students with the technical, legal, socio-political, and managerial issues of IA.

Broadly, the issues that we will cover in this course include:

1. Security investigation and analysis
2. Ethical, legal, and professional aspects of Information assurance
3. Risk management
4. Implementation and maintenance of information assurance

Design

This course has been designed to integrate theoretical concepts with their practical applications so as to teach both the theory and the practice of information assurance. The emphasis on practice is important because in many areas of information systems theory lags practice. In fact, it is the

attempt of this course not only to understand current practice but also to contribute to it. Teamwork is a required component of the course. (Each team will consist of two to four students).

There will be a variety of approaches undertaken to assist the integration process. In addition to traditional lectures there will be guest lectures, case analyses and a final project. There will be an opportunity to do some lab exercises, though this course is **not** a hand – on lab course. Note: Case preparation and what it entails are outlined in the attached **memorandum "Case Preparation Guideline."**

Texts

1. (Primary textbook) Title: Principles of Information Security; Author: Michael E. Whitman & Herbert J. Mattord; Publisher: Thompson Course Technology, Boston, MA;
2. (Primary textbook) Title: Information Security: Contemporary Cases; Authors: Marie Wright and John Kakalik. Jones and Bartlett, 2007;
3. Wall Street Journal, (Required) Dow Jones, Inc. (In particular look out for the special issues on Telecommunications, Electronic Commerce etc that deal with IT)
4. Electronic banking and information assurance issues: survey and synthesis. : An article from: Journal of Organizational and End User Computing by Manish Gupta, Raghav Rao, Shambhu Upadhyaya: Available on MGS 650 course website ("Available on "Course Documents" section at UBLeans (<https://ublearns.buffalo.edu/>)")

Recommended Book

5. Managing Information Assurance in Financial Services (eds H. R. Rao, M. Gupta, S. Upadhyaya, Idea Group, 2007)

<http://books.google.com/books?id=7OqtfAiA9LEC&dq=rao+gupta+upadhyaya&printec=frontcover&source=web&ots=6NfcCCR54p&sig=pRpJRB0mdJpNdAW-V-resjDJ1cQ#PPA332,M1>

or http://www.amazon.com/gp/product/customer-reviews/1599041715/sr=1-1/qid=1188069463/ref=cm_cr_dp_all_top/103-8598455-2603002?ie=UTF8&n=283155&s=books&qid=1188069463&sr=1-1#customerReviews

Prerequisites

1. Some knowledge of Networking. (MGS 602 – corequisite or equivalent)

Grading

Case Position Statements (2	10pts (Note: Six cases will be covered in class, but each
-----------------------------	---

points per statement)	individual is responsible for five cases during the semester)
Mid Term:	15 points multiple choice (One page cheat sheet)
Homeworks/Labs:	20 points
Final Exam:	25 points (15 pts multiple choice (Two page cheat sheet)+ 10 pts open book)
Final Project:	25 points ((ind-10 pts, team- 10 pts, Web and in-class Presentation – 5 pts)
Class Participation & Discretionary:	5 points

Grades

This is a required SOM option course. This means that S/U or P/F grading is not permitted if you are using it in the option or as part of your MBA work. Final grades will be given in the form of A, A-, B+, B, B-, etc. Incomplete grades will only be considered for extenuating circumstances. You must be passing the course, as evidenced by your work, to receive, via written (typed) request, an "I" grade.

Homework

Through the semester, I shall assign several homeworks / labs. The homeworks will be assigned at least one week before they are due. Some will be individual and others will be team-based assignments. Typically team-based assignments will require more time and may be substantially more complex than individual assignments. Late home works will be penalized.

Some of the home works will be done in the Information Assurance (Sleiman) **lab**: These are tentatively listed below in random order and are to be done as teams. Details will be handed out during the course of the semester. In addition there will be a couple of other homeworks.

Lab 1: Security with Security Center and Firewall Security Policy Configuration:

Lab 2: Password Cracking

Lab 3: Footprinting

Lab 4: Sniffing Packets with Ethereal and Stack Fingerprinting (OS Scanning) with NMap

Lab 5: Enumeration and Vulnerability Scanning

Lab 6: To be announced

Lab 7: To be announced

Exams

Mid-term Exams

There will be one mid-term exam on Oct 29. No make-ups will be administered.

- Multiple choice exam which will be closed book and no notes but one cheat sheet will be allowed. This part of the exam will closely follow the CISSP certification exam and is worth 15 points)

Final Exam

The final is during the week of December 11, finals week. This will be in two parts

- (1) Multiple choice comprehensive exam which will be closed book and no notes but two cheat sheets will be allowed .(worth 15 out of 25 points of the exam grade) This part of the exam will closely follow the CISSP certification exam and is worth 15 points)
- (2) Essay (open book)- based on Wall Street (or equivalent) technology readings, cases, guest lectures and your current knowledge of IT assurance innovations (worth 10 out of 25 points of the final exam grade)

Final Project

There will be several teams in class. This is a term paper that you have to work on as a team. It has an individual component (one person); and a larger team component.

As individuals you have to work as loosely coupled teams, and as a larger team you have to work as a strongly coupled team (where you will actually be making a contribution to the state of practice in the IT arena). Specifically each team will be focusing on Information Assurance (IA) in the government. You can choose any one of the following topics (or a topic in the general area with Instructor's permission). A maximum of two teams can choose the same topic.

Topics in Information Assurance in Electronic Government

"E-Government: Information technology continues to trigger disruptive change in the US economy. Many business processes can be incrementally improved but, many need to be completely transformed to capture the full benefits. Areas of interest include: electronic delivery of information, programs, and services; web 2.0, and the expansion of social networking, blogging, wikis, etc.; electronic communications to increase citizen engagement; and the use of new cross servicing arrangements" (IBM).Other sample topics include:

Legal and Regulatory

1. Regulatory Framework in Electronic Gov: Information Assurance Perspective

People, Policies and Processes

2. Privacy, Fraud and Identity Theft Issues in e-Gov
3. Consumer and End User view of Information Assurance Issues in e-gov
4. IA issues with People, Policies, Processes and Governance

Technology

5. Trends in Electronic Government and Infrastructure for Enhanced IA posture

6. Cross Organizational Communication Issues for Disaster Management or Anti Terrorism Management

Environment

7. Environmental and Institutional factors that affect IA in Electronic Government
8. Cutting edge states, localities, other countries, and private industry in the context of e-government.

Deliverables

PART A: Individual deliverable (a subset of the team deliverable – each individual has to submit a writeup that is self contained and that falls under the team topic umbrella):

A 5 page web based "white-paper" hypertext document (per individual) with an extra reference section. Make sure that the citations are correct, and be sure to **cite** EVERY reference you use. The paper should flow logically and be broken into subsections.

PART B: Team deliverable: This is a 5 page hypertext document (one per team) that should have some added value in addition to the collection of individual deliverables. (It can compare and contrast, analyze, inform, benchmark, etc. It can be for example, a mini- case study of Information Assurance Practices in an organization, or a checklist for a vulnerability assessment in an organization.) Note: A 1 page executive summary PLUS team deliverables tied together in a coherent format with a TABLE OF CONTENTS for the final report. PLUS any exhibits, figures, tables. Is the final deliverable

Note: You must meet the following milestones:

1. Choose your individual topic **and** team topic by **September 10** and e-mail it to mgmtrao@acsu.buffalo.edu, with a cc to Insu Park: insupark@buffalo.edu. (In the subject heading mention Re: MGS 650 Term paper). Note that the individual topic must be a subset of the team topic.
2. A typed one page word document by **September 24** that details the subsections/ agenda (with two to three sentence description for each subsection/agenda point).
3. Submit your **full** individual deliverable by **October 22** to Prof Rao and Insu Park. (**Please also hand in a hard copy**).
4. Presentation of team term paper is on **December 3**. Every team member does not have to present but NOTE that any team member may be asked to answer questions from the audience. NOTE: Questions to ask for presentation: Is the presentation convincing? Does it have a logical flow and does it interest the audience?
5. Team deliverable (**a hard copy and a diskette containing the html files**) is due the week of **December 10** on the exam day. Also e-mail the url to mgmtrao@acsu.buffalo.edu, with a cc to Insu Park <insuparkbuffalo.edu>. (In the subject heading mention Re: MGS 650 Term paper).

Lecture	Topic	Cases	Reading	Homework Due
Session 1 Aug 27	Introduction		Witman & Mattord (WM) Ch 1	
Sept 3 Labor Day	Holiday	Holiday	Holiday	Holiday
Session 2 Sept 10	Security Investigation and Professional Issues I		WM 3	Individual and Team Paper Topic due by e-mail to Dr Rao:mgmtrao@buffalo.edu Lab 1 handed out
Session 3 Sept 17	Security Analysis Guest Lecture (Deloitte)		WM2,	Lab 1 due Lab 2 handed out
Session 4 Sept 24	Risk Management *Guest Lecture	Case 1: Kraft Foods	WM4,	Lab 2 due 1. One page case writeup of Case by every individual <u>A typed one page word document details the subsections/ agenda of Individual term paper deliverable</u> Lab 3 handed out Guest Lecturer: Matthew M. Speare Senior Vice President, Corporate Information Security Officer, M & T Bank
Session 5 Oct 1	Business Continuity Planning (Guest Lecture Chuck Dunn, CISO, UB tentative)			
Session 6 Oct 8	Blue print for Security	Case 2: Advo Inc	WM 5	1. One page case writeup of Case by every individual Lab 3 due Lab 4 handed out

Session 7 Oct 15	Security Technology	Case 3: Yale : Emergency Preparedness and Contingency Response	WM 6	1. One page case writeup of Case by every individual Lab 4 due Lab 5 handed out
Session 8 Oct 22	Physical Security	Case 5: SRA International	WM 8	1. One page case writeup of Case by every individual Lab 5 due Lab 6 handed out <u>Individual term paper deliverable by October 22</u>
Session 9 Oct 29	1. MidTerm Exam	Case 6: FBI		1. One page case writeup of Case by every individual MidTerm Exam Homework 7 and 8 handed out
Session 10 Nov 5	Implementing Security Guest Lecture (Bob Vail, EDS tentative)		WM 9	Lab 6 due
Session 11 Nov 12	Security and Personnel	Case 7: Aetna	WM 10	1. One page case writeup of Case by every individual
Session 12 Nov 19	Information Security Maintenance		WM 11,12	Homework 7 due
Session 13 Nov 26	Information Systems Ethics		WM 3	Homework 8 due
Session 14 Dec 3	Final Team Presentations			

Session 15 Week of Dec 10	1. Final exam (The Exam Date, Time, and Room will be announced) 2. Final Team Deliverable Due
---------------------------------	--

****NOTE:** The above is **tentative** and I reserve the right to change as per the dynamics of the situation. Please also note that the topics refer to the chapters in the book, however I may change the sequence of presentations/topics. So it is your responsibility to make sure that you know what has been covered in class.

Cases

1. The instructor will lead the cases. Each individual will be responsible for a **one-page typed, double-spaced position statement**. You are free to discuss among your team members but no duplication is allowed. **The focus of your statement must be highlighted in yellow**. The position statements must be handed in at the beginning of class. Late submissions will not be accepted.

Please take a look at the suggested questions regarding the cases below. You can use these to guide your position statement.

2. What is involved in a case analysis?

Objectives of Case Analysis:

1. To identify and define major problem(s) and subproblems.
2. Examine facts and evaluate evidence.
3. Apply knowledge / experience / understanding to analyze action choices, and consider feasibility of alternative courses of action.
4. Decide on a course of action, include specific steps for implementation.

Case Preparation Guidelines

Please note: Your one page writeup for each case has to be handed into Dr Rao as a hard copy at the beginning of the class.

1. Case Outlines

1. Kraft Foods Inc.: *Protecting Employee Data*

Synopsis

Kraft Foods Inc. is the largest food and beverage company in North America and the second largest food and beverage company in the world. It employs a workforce of about 98,000 individuals; approximately 45,000 in the United States, and 53,000 in sixty-five countries around the world, including fourteen European Union (EU) states (Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, The Netherlands, Portugal, Spain, Sweden, and the United Kingdom).

When the EU Directive on the Protection of Personal Data became effective in 1998, Kraft needed to revise the means by which it collected, processed, transmitted, and stored employee data. Improvements were made to the Unified Personnel and Payroll System (UPPS) to better protect

North American human resources (HR) transactions. International HR systems were converted to the SAP HR system. A Data Transfer Agreement was legally established between Kraft and its operating entities in the EU member states, which specified restrictions on personal data and mandatory data protection principles. The position of Chief Information Security Officer was created, and stronger data security policies and practices were developed and implemented throughout the company.

1. How does the EU Directive on the Protection of Personal Data impose requirements on organizations in non-EU countries?
2. How does Kraft comply with EU data privacy regulations governing the protection of employee data?
3. The EU Directive requires “appropriate technical and organizational controls” to be in place to protect the confidentiality and integrity of personal data. How can an organization determine whether its security controls are appropriate?
4. What user access controls are in place for the UPPS and SAP HR systems?
5. How does Kraft implement the following access controls: need to know; least privilege; mandatory access control; and role-based access control?
6. Identify at least ten examples of specific HR data that are considered sensitive at Kraft Foods Inc.
7. What is the purpose of Kraft’s Code of Conduct for Compliance and Integrity? How is this information distributed to Kraft employees?
8. Why is Kraft moving away from the use of employee social security numbers for user identification on UPPS?
9. Through the UPPS, Kraft provides its employees online access to their own employee data. Why would Kraft do this?
10. Why would Kraft want to move all of its North American HR transactions from UPPS to SAP HR?

Case 2: Advo, Inc.: *Integrating IT and Physical Security*

Synopsis

Advo, Inc. is the largest provider of direct mail advertising services in the United States, and it is the largest commercial user of United States Postal Service standard mail. Advo processes and distributes printed advertising to more than 112 million consumer households in the United States and Canada. It operates twenty-one mail processing facilities located throughout the United States, and has approximately 3,900 employees.

For several years, security was considered a low priority. Physical security was minimal at corporate headquarters and practically nonexistent at the mail processing facilities. The security controls that were in place to protect Advo’s critical applications and databases were the result of a long-term outsourcing agreement with IBM Global Services. The terrorist attacks on September 11, 2001 triggered an abrupt change in executive attitudes toward security. Physical security was immediately given top priority. On September 21, 2001, the first bioterrorism-related anthrax attack occurred. For the next three months, public fears grew as media reports of anthrax-laced mail increased. For a company like Advo, whose clients rely on people opening their mail, the anthrax

attacks posed a significant threat to its existence. Advo responded by implementing stronger operational and procedural controls. Additional employees were hired in IT and physical security. Stronger physical security measures were implemented and enforced at corporate headquarters and all facilities. The facilities were connected to a Security Control Center at corporate headquarters, and all security applications were integrated within this security management system. Numerous policies and procedures were formulated. Disaster recovery plans were developed, and security audits were conducted regularly.

1. Traditionally, managing IT security and physical security have been treated as two separate domains. Why should they be integrated?
2. Why is top management's awareness and support essential for establishing and maintaining security?
3. Why should those responsible for leading the organization's security efforts be placed high in the organizational chart?
4. The first decision made by Advo's top management in the aftermath of the 9/11 attacks was to improve physical security. Why was attention focused on this particular aspect of security?
5. What are the advantages and disadvantages of using consultants and third-party organizations to provide security-related services? What reasons would a company have for hiring consultants to provide guidance for its security efforts?
6. Why is it a good security practice to have few visitors in a reception area?
7. Identify the security risks involved in allowing networked systems to be used by large numbers of temporary employees who do not need to log in. What password guidelines should be implemented for stronger user authentication?
8. How far away should a backup site be located from company headquarters? What factors should be considered in determining the location of a backup site?
9. Advo believes that frequent audits help to ingrain a security mindset among the company's employees. What other benefits are there to performing frequent security audits?
10. The vendor of Advo's security management system is Software House. Research the role of Software House in the Open Security Exchange (OSE). What is the purpose of the OSE?

Case 3: Yale New Haven Center for Emergency Preparedness and Disaster Response:
Contingency Planning

Synopsis

The Yale New Haven Center for Emergency Preparedness and Disaster Response was established by the Yale New Haven Health System (YNHHS) in 2002. The Center's mission is to develop and deliver services that improve healthcare planning, preparedness, and response for emergency events and disasters. It is responsible for identifying the status of emergency preparedness within the three YNHHS member hospitals (Yale-New Haven Hospital, Bridgeport Hospital, and Greenwich Hospital); preparing YNHHS to respond effectively to emergency preparedness and disaster response issues; providing leadership to healthcare delivery organizations (e.g., acute care hospitals, skilled nursing facilities, community health centers, home health agencies, urgent care centers, emergency medical service providers, and community medical practices) and their

workforce regarding emergency preparedness and disaster response issues; serving as a model for emergency preparedness and disaster response initiatives at the national and international levels; and advising statewide and national legislative and nongovernmental organizations on the development of standards and policies for emergency preparedness and disaster response in healthcare delivery organizations. These objectives are achieved through a complex web of partnerships with healthcare delivery organizations, professional health associations, and agencies on the local, state, regional, national, and international levels. This case study focuses on the intricacies of contingency planning and disaster recovery planning.

1. Contingency planning requires an understanding of the crises that are most likely to occur, the potential impacts of those events, the resources that are needed to address those situations, and the most efficient means of accessing those resources. How has the center addressed each of these concerns?
2. The center's contingency planning strategy is based on collaborative partnerships. List the center's local and state partners. What other organizations would you add to this list of partnerships?
3. Why is an integrated planning approach necessary for building healthcare capacity and providing a coordinated response to emergencies and disasters?
4. What is a needs assessment? What role did this play in the center's ability to provide disaster planning, education and training, clinical strategies, and logistical solutions to Connecticut's healthcare delivery infrastructure?
5. What is the difference between a tabletop exercise and a full functional disaster recovery drill? Identify the advantages and disadvantages of each.
6. What is a Hospital Emergency Incident Command System? Identify, and explain the functions of, the five sections of an HEICS. Explain how an HEICS provides unity of command and helps to improve the quality of communication during disaster response.
7. Why are education and training important parts of contingency planning?
8. Why are Strategic National Stockpile resources not available during the first seventy-two hours of a disaster? Why is a coordinated stockpiling strategy better than having each hospital stockpile enough equipment, supplies, and pharmaceuticals to meet its own needs?
9. How does redundancy improve the reliability of communication systems?
10. Why is surge capacity an important element of contingency planning for healthcare delivery organizations?

Case 4.: IBM: *The Embedded Security Subsystem*

Will **not** be done in MGS 650 class

Case 5.: SRA International, Inc.: *Automating Compliance with Federal Information Security Requirements*

Synopsis

SRA International, Inc., is a leading provider of information technology (IT) services and solutions to federal government clients in the national security, civil government, and health care and public health sectors. Since 2002, all federal agencies and their contractors have had to comply with the provisions set forth in the Federal Information Security Management Act (FISMA). FISMA requires each federal government agency to develop, document, and implement an agency-wide security program to protect the agency's information and information systems, including those provided or managed by another federal agency or contractor. Each information security program contains eight requirements: periodic risk assessments; risk-based policies and procedures; system security plans; information security training; periodic testing and evaluation of all security policies, procedures, and practices; remedial action plans; security incident procedures; and continuity of operations plans and procedures. To provide guidance for FISMA's information security program framework, the National Institute of Standards and Technology has published documents that detail the categorization standards and minimum security control requirements for federal information and information systems. SRA has incorporated these security categorizations and control requirements in its Web-based risk assessment software, ASSERT, which was developed to automate the FISMA compliance process. This case study highlights the complexities of federal government information security regulations.

1. Why do you think SRA has chosen to focus its efforts on federal government departments and agencies within the national security market? Explain why this has been a good strategy for SRA.
2. What is open source intelligence? What is the relationship between open source intelligence, national security, and text and data mining software? Why should businesses be concerned about open source intelligence?
3. What are critical infrastructures? List the U.S. critical infrastructure sectors and provide examples of each.
4. Why is improved interoperability between federal agency systems necessary for national security purposes?
5. FISMA replaced the Government Information Security Reform Act (GISRA). Provide an overview of GISRA. Do you think that there are significant differences between FISMA and GISRA?
6. Are the eight FISMA requirements a good model for business information security programs? Explain your answer.
7. In spite of FISMA's mandate to strengthen information security within the federal government, many federal agencies receive low grades on the Federal Computer Security Report Card because of the weaknesses in their information systems and information security programs. Explain why this has happened.
8. What are the differences, in terms of legal regulations and guidance for compliance, between the federal government and industry in managing the security of information and information systems?
9. Compare the classes and families of the minimum security control requirements, shown in Table 5-5, to the classes and control objectives of ASSERT's assessment questions, shown in Table 5-6. How do you explain the discrepancies?
10. Explain how ASSERT's questions could be used by a business to better control its IT systems and to mitigate its security risks.

Case 6: FBI New Haven Field Office – Computer Analysis and Response Team: *Tracking a Computer Intruder*

Synopsis

Between April 24, 2001 and June 1, 2001, a student at the University of Akron gained unauthorized access to a Connecticut e-commerce company's Web server. The intruder stole confidential customer order information, including credit card numbers. He sent fraudulent e-mail messages to several customers, confirming their orders and credit card information, and requesting their credit card verification data and bank account information. The Connecticut e-commerce company contacted the FBI New Haven field office to locate the intruder.

A Special Agent/Computer Analysis and Response Team (CART) field examiner in the FBI New Haven field office began to track the e-mails back to their source. During his analysis, he discovered a directory traversal vulnerability in the e-commerce company's shopping cart software. The company's security breach was more serious than it realized: the directory traversal vulnerability had been exploited by intruders from around the world to gain unauthorized access to the company's daily order file, and to its customer order and credit card information. The CART field examiner continued to analyze Web log files and trace IP addresses until the sender of the fraudulent e-mail messages was finally identified. A University of Akron student was arrested, and data related to the e-commerce company's computer intrusion was recovered from his computer. On June 13, 2002, the student entered a guilty plea to one count of Title 18 US Code 1030 a(4) ("Fraud and related activity in connection with computers"). He served six months in jail and paid \$20,000 in restitution to the Connecticut e-commerce company. This case study focuses on the forensic processes used by the FBI New Haven field office to locate the intruder.

1. What should the Connecticut company have done to prevent the computer intrusion described in this case? What should it have done to detect this computer intrusion?
2. What security controls should be implemented by any organization to prevent, detect, and recover from a computer intrusion?
3. Why would someone want to use a forged e-mail address? Explain how this worked to the intruder's advantage in this case.
4. Numerous entries similar to the following were found in BoatingCT.com's Web logs. What does this entry mean?
5. spider-we084.proxy.aol.com - - [23/Apr/2001:02:04:14 -0400] "GET /cgi-bin/Web_store/web_store.cgi?keywords=803103&frames=yes&store=yes HTTP/1.0" 200 2164 "http://www.boatingct.com/" "Mozilla/4.0 (compatible; MSIE 5.5; AOL 6.0; Windows 98; Win 9x 4.90)"
6. What was the importance of having court orders immediately issued to Hotmail.com and Time Warner Cable?
7. When the FBI New Haven field office requested the log files from the University of Akron, none were available. Do you think it is typical for universities not to retain log files? What is the impact of this on the security of university computing environments?
8. The FBI New Haven CART field examiners imaged the hard drive and worked off of that. They did not use the original drive or the original evidence. Why?
9. When the Web logs from BoatingCT.com were analyzed, the CART field examiner discovered that intruders from around the world had gained unauthorized access to the

company's daily order file. The company was informed of this, but the CART field examiner's focus remained on identifying the sender of the suspicious e-mails to BoatingCT.com's customers, the reason given for the FBI's involvement in this case. What other reasons might the FBI have had for not pursuing these other intruders?

10. The computer intruder described in this case was a U.S. citizen who resided in Ohio. What would the FBI have done if he were a non-U.S. citizen who resided in a foreign country?
11. What types of Internet-related crimes should be reported to the FBI? At what point should a computer crime be reported to law enforcement?

Case 7: Aetna: Developing and Implementing a Successful Information Security Awareness Program

Synopsis

Aetna is one of the leading providers of health care, dental, pharmacy, group life, disability, and long-term care insurance and employee benefits in the United States. The company's line of work requires each of its 27,000 employees to follow good information security (InfoSec) practices and behaviors.

Aetna's organizational placement of InfoSec has been realigned many times. Prior to 1987, InfoSec was the responsibility of three corporate-level functions: computer security, information systems, and facilities risk management. In March 1987, these three functions were loosely consolidated to form a new corporate security/risk management group. In 1991, all of the business continuity and information technology security functions were merged within a centralized corporate organization called the Aetna Information Technology unit. In late 1994, responsibility for InfoSec was transferred from the Aetna Information Technology unit to the strategic business units. In February 1995, employee security awareness and education was transferred to the strategic business units, where, for the next three years, little was done to promote the understanding of InfoSec. In 1998, Aetna implemented a comprehensive InfoSec awareness program under the auspices of the Information Security Policy and Practices (ISPP) group.

The ISPP group uses several mechanisms to convey and reinforce the importance of security: an intranet security portal (SecurNet), an InfoSec newsletter, promotional give aways, brown bag lunches, posters, the company's annual Customer Service Fair, and an InfoSec exam.

The InfoSec exam is Web-based and must be completed every year by all users, including managers. The exam is updated annually to incorporate security topics based on business needs, current industry practices, and government regulations. The security topics are directly focused toward different groups of users, and monitoring tools enable management to identify those employees who have not completed the annual exam for targeted follow-up.

Questions:

1. Many organizations have tried, but have not been able, to implement a successful information security awareness program. How was Aetna able to succeed with its program?
2. Most companies tend not to fund security awareness programs during financially difficult times. When Aetna implemented its first InfoSec exam in 1999, the company's stock price was \$99.87 per share. By February 2000, Aetna's stock price had fallen to \$40.75. Despite rising costs and declining profits, the company continued to support its internal security awareness program. What reasons might Aetna have had for doing this?
3. The ISPP group consists of only five employees. Each year, they design, develop, and implement a new version of the InfoSec exam for more than 27,000 Aetna employees. Explain how this small group has been able to accomplish such a task.
4. Most of the eight to ten users who are selected for usability testing have an entry-level understanding of computers and tend to be uncomfortable with Web-based applications. Why aren't more experienced users chosen for testing?
5. Research at least five security awareness solution providers. Summarize their similarities and differences.
6. Why is it important for a company's officers to be able to demonstrate due care? How is due care related to negligence?
7. Beginning in 2003, the InfoSec exam became integrated within Aetna's Business Conduct and Integrity training program. What are the advantages of doing this? What are the disadvantages?
8. Why is it considered good practice for an organization to have its users officially sign off on its security policy?
9. What factors should be considered in the development any information security awareness program?
10. It is often difficult to cost-justify an information security awareness program. What quantitative and qualitative factors should be considered when justifying the program's expense?

4. TEAM EVALUATION INSTRUCTIONS (due at the end of the semester)

General

You are to use the Rating Guidelines (below) and the Evaluation Form (below) to evaluate each of your team member's role in your meetings, including yourself. Please pay very careful attention to the guidelines. It is not intended or expected that all students will get an "A" rating.

Rating Guidelines

Attendance at the team meetings

1. Always attended
2. Almost always attended
3. Usually attended
4. Occasionally attended
5. Never attended

Contribution to ideas to the team effort

1. Made the major contribution in terms of ideas
2. Made an important contribution
3. Made reasonable contribution
4. Made little contribution
5. Made no contribution

Contribution to the overall process

1. Was the most helpful in encouraging others to participate, integrating the various ideas, in resolving disagreements and in keeping the team "on the track"
2. Was often helpful in several of the areas
3. Was moderately helpful, especially in selected areas as in report writing
4. Was occasionally helpful
5. Was rarely helpful

Evaluation Form

	Category (letter grades)		
Team Member's Name	Attendance	Contribution to Ideas	Contribution to Overall Process

August 29, 2007

Information Assurance Lab Assignments: MGS 650

Dr H. R. Rao

During the course of semester, you will be given 7 lab assignments. *The main objective of the labs is to give you hand on experience* in using some of the tools used in Information Assurance.

As you will see, the tools developed with the intent of aiding in maintenance and troubleshooting tasks can be used by hackers for the negative purposes. For example tool such as NMap which is used often by network administrators to see which servers (/services) are up and running can be used by hackers to see which ports are open to carry out the malicious activity. Similarly tools developed for remote assistance in case of troubleshooting can be used by malicious users to remotely control the machine to carry out their activities. Network administrators can in turn use the same tool to analyze the same information to find out whether the open resources pose any threat to the system and if so take necessary action.

All the labs are to be done in your teams. Provide name and person number of your team members when you submit the lab deliverables. You can choose to send a soft copy by e-mail to insupark@buffalo.edu or submit it as hard copy at the beginning of the class session on the date it is due.

Some of the exercises may need exclusive access to the resources used for particular lab. Please schedule well in advance so every team can complete the assignment without conflict with other teams.

If you need help, please e-mail: insupark@buffalo.edu (* Please put the keyword “[MGS650]” in the subject line in all your communication for MGS 650) or you can reach us during our office hours.

Intro to Individual Practice Assignments:

(Detailed Directions will be distributed in class according to the assignment schedule.)

1. Firewall Security Policy Configuration (Group Project)

Firewall is a system or group of systems that enforces an access control policy between two networks or one host and the rest of the network. A firewall can utilize one or more mechanism to permit or block network traffic flowing through it. A basic and widely adopted mechanism is packet filtering that filters network traffic based on a set of rules. These rules are set according to the network user’s access control policy. By specifying protocols, ports, and (often) IP addresses to allow or drop, firewall can protect the network behind the firewall from outside nodes.

In this practice, you will be provided with a list of network services required by a hypothetical company. Your role will be developing a simple access control policy and add, modify, and remove access rules in a firewall according to the access control policy.

2. Password Cracking (Group Project)

Password cracking is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system, typically, by repeatedly verifying guesses for the password. The purpose of password cracking might be to help a user recover a forgotten password (though installing an entirely new password is less of a security risk), to gain unauthorized access to a system, or as a preventative measure by the system administrator to check for easily crackable passwords.

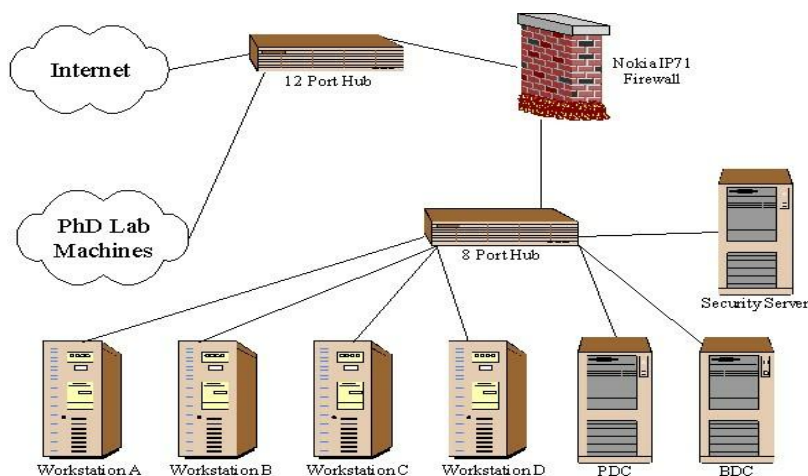
In this practice, you will experience how individual's password can be cracked by Cain and Abel software.

3. Foot Printing (Group Project)

Foot printing refers to activities that gather information about and gain knowledge of an organization's security posture. In the e-commerce security context, unauthorized users can develop an understanding or guess the network configuration, which can help them undermine information security of e-commerce systems. They can use a combination of tools and techniques in order to figure out various unknown or unexpected to be misused information (e.g., the size of a network, IP addresses and host names of servers/network devices, the email/postal address, the phone #, and the name of network administrators, etc.)

In this practice, you need to gather information about a public network of your choice (e.g., BestBuy, Adelphia, UB) and the Sleiman Lab network, using non-intrusive and stand-off methods to gain the information needed.

** An example of the Sleiman lab network structure diagram: (This is outdated and does not include all the information that you need to find out.)*



4. Sniffing Packets with Ethereal and Stack Fingerprinting (OS Scanning) with NMap (Group Project)

Ethereal relies on the WinPcap library, on the WinPcap device driver, and on the facilities that come with the OS on which it's running in order to do capture.

WinPcap is the industry-standard tool for link-layer network access in Windows environments: it allows applications to capture and transmit network packets bypassing the protocol stack. WinPcap is the packet capture and filtering engine of many open source and commercial network tools, including protocol analyzers, network monitors, network intrusion detection systems, sniffers, traffic generators and network testers. Some of these tools, like Ethereal, Nmap, Snort, WinDump, ntop are known and used throughout the networking community.

Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

In this practice, you will learn the mechanism of packet sniffing and how this malicious activity can be monitored by NMap

5. Enumeration and Vulnerability Scanning(Group Project)

SomarSoft's DumpSec is a security auditing program for Microsoft Windows® NT/XP/200x. It dumps the permissions (DACLS) and audit settings (SACLs) for the file system, registry, printers and shares in a concise, readable format, so that holes in system

security are readily apparent. DumpSec also dumps user, group and replication information. DumpSec (formerly known as DumpAcl) is software which dumps out the users' last logon information.

In this practice, you will learn how to extract remote information with DumpSec as well as how to find out your system's vulnerability with Nessus.

6. To be announced

7. To be announced