Introduction to Information Assurance

M. E. Kabay, PhD, CISSP-ISSMP, Prof of Information Assurance & Statistics
School of Business & Management, Norwich University

1 Course Description

This course provides an overview of design considerations involved with the security of site design. The course will also provide an understanding of the Levels of Trust and system accreditation/certification processes. Life cycle management of software, hardware, and physical plant, from planning through destruction will be examined and reinforced using case studies. Additionally understanding of the variety of security systems involving computers and networks and an ability to evaluate vulnerabilities will be discussed. Prerequisite IS228 or permission of instructor. (3 Credits)

2 Course Objectives

By the end of this course, students will be able to discuss the following issues at a management level:

- Recognize, define and use the technical terminology of information assurance (IA).
- Name and define the fundamental concepts of IA.
- Describe models and key elements of information warfare.
- Recognize, name, define and discuss computer crime techniques; present countermeasures.
- Describe and discuss criminal-hacker subculture.
- Recognize, name, define, and discuss techniques of denial-of-service (DoS) attacks and countermeasures.
- Recognize, name, define, and discuss physical (facilities) security vulnerabilities and defenses.
- Recognize, name, define, and discuss identification and authentication techniques.
- Discuss specific security issues pertaining to voice and data networks.
- Recognize, name, define, and discuss fundamentals of firewalls and of intrusion-detection systems.
- Recognize, name, define, and discuss fundamentals of modern cryptography.
- Evaluate requirements and techniques for backing up, archiving, storing, managing, and destroying electronic records.

3 Course Schedule & Location

- Mondays and Wednesdays from 15:00:03 to 16:14:57 in Dewey 211 and using NUoodle.

4 Text

- Bosworth, S., M. E. Kabay & E. Whyne (2009), eds. *Computer Security Handbook,* 5th Edition. Wiley (New York). ISBN 0-471-71652-9. Two volumes; 2040 pp. Index.
  Volume **1** is used for **IS340**; Volume **2** is used for **IS342**.
  AMAZON < http://www.amazon.com/Computer-Security-Handbook-2-Set/dp/0471716529/ >
- Additional readings are provided on the course Web pages and in class handouts.

5 Course Web Site

Course materials are posted at < http://www.mekabay.com/courses/academic/norwich/is340 > and also on the IS340 section of NUoodle.

 Updated 2011-08-26 09:25:00.

6 Methods of Assessment

All assignments and quizzes are submitted using NUoodle. Deadlines for each assignment are posted in NUoodle and on the class syllabus.

Responding punctually to professional responsibilities is part of the maturation of students. To encourage promptness, late submissions for any of the essay exams and assignments will result in reduction of grades by 10% per day from the total score allotted. However, because of the constraints on NUoodle quizzes, the time limits on quizzes have to be definite; therefore, quizzes close at their deadlines and cannot be taken or retaken after closure.

6.1 Preliminary Written Assignment: 5% of final grade

Students will write a 500 ± 50 word research paper on an assigned topic. This essay will provide an opportunity for detailed commentary and correction that will support better research and writing of the term papers. Your instructor has been a professional editor since 1970, so this is a good opportunity to get some practical guidance that can improve your work in later essays. Pick anything interesting to you and relating to anything mentioned in the syllabus and upload via NUoodle by the deadlines indicated.

6.2 Term Paper #1: 10% of final grade

Students will write a 1,000 ± 100 word research paper on a suitable topic to be selected in conjunction with the instructor. Instructor approval helps to avoid the problem of discovering that you have picked a topic worthy of a textbook! Don't hesitate to work with your instructor to review draft versions before you prepare your final version. Submit your final version via NUoodle no later than the deadline listed there.

6.3 Quizzes: 20% of final grade

Using NUoodle, there will be 13 sets of weekly quizzes (each individual quiz will cover a single chapter in the readings). These open-book, automatically graded quizzes will test for concepts and technical vocabulary and must be completed in 30 minutes or less. These quizzes open on Thursday mornings (00:05) a week after the material being tested and will close at the end of Sunday night (23:55). There are three attempts possible for each quiz with 24 hours minimum delay between attempts. The final grade for each quiz will be the average of the grades for the quizzes attempted. For example, if a student tries the quiz at 09:00 on Thursday and gets 80%, and tries again at 13:30 on Friday and gets 100%, the recorded final grade for that quiz will be 180%/2 = 90%. If the student continues and takes the quiz again on Saturday at 14:00 and achieves 100%, the final recorded grade for that week's quiz will be 280%/3 = 93.3%.

6.4 Mid-term Exam: 15% of final grade

The mid-term exam will be an open-book take-home essay exam with four management-level 500-word memoranda responding to realistic questions raised by managers querying a CISO about security issues. Exam coverage is the first four weeks of the course.

6.5 Term Paper #2: 20% of final grade

Students will write a second research paper in 2,000 ± 200 words on a suitable topic to be selected in conjunction with the instructor. The topic is to be approved on or before the posted deadline. Late submissions for topic selection or for final drafts will result in reduction of grades by 10% per day from the total score allotted to the assignment.

6.6 Final Memo Questions: 10% of final grade

Towards the end of the course, once all the chapter readings are completed, students will complete an open-book take-home assignment with five management-level 500-word memoranda responding to realistic questions raised by managers querying a CISO about security issues. Exam coverage is Weeks 5 through 11 of the course.

6.7 Final exam: 15% of final grade

The final exam will be an open-book multiple-choice exam similar to the weekly quizzes but covering all the material in the course. The exam will be scheduled in the official exam period of the University and will use ScanTron bubble sheets.

6.8 Term-Paper Presentation: 5% of final grade

Students will create a *narrated* PowerPoint lecture for the first or second term-paper topic for posting on NUoodle and will then lead a class discussion of their research (with or without their PowerPoint). Grading will include the quality of the content and the professionalism of the presentation.

6.9 Extra Work for Extra Points:

- Students may submit extra work for extra points on their final grade with permission of the instructor.
- For example, the instructor will agree to accept suitable short essays such as summaries of interesting incidents, articles or books relevant to the course materials.
- The rate granted for extra work is 1 point added to the final grade for 500 words of professional-grade writing. Thus a 1,000 word essay could improve the final grade by 2 points.
- Particularly good articles may be considered for publication in collaboration with the student author.
- Contributions to the online discussions can generate 0.1 pt on the final score per *good* contribution with references or an intelligent response to a posted message. (MAX 10 pts)

7 Cheating and Plagiarism

Students are graded on an individual basis and must therefore complete their own work. Students are reminded of the University's Policy against cheating and plagiarism:
< http://www.norwich.edu/about/policy/academic/appendix1.html >.

If in doubt as to what constitutes plagiarism, ask the instructor for a review of your work before submitting an assignment. All instances of cheating and of plagiarism must be reported to the Academic Integrity Committee by the instructor or by students who have observed the dishonesty. Penalties include expulsion from the University. Ignorance of the University's Rules is not a valid defense against accusations of academic dishonesty.

8 Additional Notes

- There will be no *grading on a curve*. There are no predetermined numbers of final letter grades. Students do not compete with each other for grades; if everyone gets A, great. If everyone fails, tough.
- Review questions (without answers) will be distributed to students throughout the term. These example questions will not limit the scope of actual exam questions, and are intended to help students review and in exam preparation.
- Students are encouraged to study together but may not collaborate during exams. Students are individually responsible for all assigned readings, lecture, and discussion material, unless otherwise noted (specifically, the case studies result in the same grade for each team member).
- Attendance Policy – no more than two unexcused absences. University regulations stipulate that "Unless stated otherwise, the maximum number of permitted absences is the number of times the course meets per week. When the student has reached the maximum number of permitted absences, the faculty member will warn the student of impending dismissal from class with a grade of 'F.' This warning letter will include the course number and section and dates(s) of absence(s). The letter will state that any future unexcused absences may result in recommendation to the Vice President of

Academic Affair through the course School Dean that the student be dismissed from the class with a grade of 'F.' A copy of the warning letter will go to the student's academic advisor and to the Commandant and Vice President of Student Affairs.' (See pp 69-70 of the PDF version of the *Academic Regulations* available online at < http://tinyurl.com/nuar2009 >.) Therefore, students may miss exactly two sessions of this course without explanation; the third and subsequent unexcused absences will be reported as stipulated in the academic regulations and may lead to dismissal from the course with an F grade. If you plan to be absent, discuss the absence with the instructor in advance.

9 Office Hours & Contact Information:

Students are welcome to call the instructor at **(802) 479-7937** at *any time* (that number rings in his office or his cell phone but cannot disturb him); leave a voice-mail message with a return number if necessary.

Students may also use Instant Messaging at any time using Skype (ID is **mekabay.**

Office hours are posted on the class Web site, on NUoodle, and on the instructor's office door (Dewey 209). The **Dewey 209** office door is almost always open when the instructor is present; all students are most welcome to drop in without having to make appointments – everyone is welcome at any time.

10 About your Instructor: M. E. Kabay, PhD, CISSP-ISSMP

M. E. Kabay began teaching his high school classmates how to use the slide rule in 1963 and began programming IBM 1401 computers in assembly language in 1965. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology and taught biology, statistics and programming as a university professor in Canada and overseas. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980 as an operating systems and database performance specialist, winning the *Systems Engineer of the Year* Award in 1982 and teaching primarily MPE operating system, IMAGE/3000 database and VPLUS/3000 GUI-design courses as well as serving as support engineer to HP's hospital and university customers and managing HP's call center *(Phone-In Consulting Service)* for Québec & the Maritime provinces.

He served as Director of Education for the National Computer Security Association (NCSA, later ICSA and then TruSecure) from 1991 to 1999 and then worked with AtomicTangerine where he supported the International Institute for Information Integrity® (I-4®). He collaborated in the committees defining the *Common Body of Knowledge* for the Certified Information Systems Security Professional (CISSP) designation in the mid-1990s and earned his CISSP in 1997.

Since 1986 (and as of mid-2011), he has published over 1,300 articles in operations management and security, written a college textbook on enterprise security (McGraw-Hill, 1996), and served as Technical Editor of the 4th (2002), 5th (2009) and 6th (2013) editions of the *Computer Security Handbook* (Wiley). He wrote two security-management columns a week distributed by *Network World* from February 2000 to September 2011.

He has been an invited lecturer at the United States War College, the Pentagon, NATO HQ in Brussels, and at NATO Counterintelligence training in Germany. He was inducted into the Information Systems Security Association (ISSA) *Hall of Fame* in December 2004 and earned his *Information Systems Security Management Professional* (ISSMP) designation in November 2005.

From 2002 to 2009, he was the Director of the *Master's Program in Information Assurance* (MSIA) in the School of Graduate and Continuing Studies (SGCS) at Norwich University, Northfield, Vermont where he was also the Chief Technical Officer of the SGS from 2007 to 2009.

From June 2001 to April 2011, Dr Kabay was Associate Professor of Information Assurance in the School of Business and Management from 2001 to 2011 and became Professor of Information Assurance and Statistics starting in May 2011. He was appointed Associate Chair of Computing and Program Director of the new Information Operations programs in July 2009.

Dr Kabay also serves as Acting Chief Technical Officer of a high-tech startup, Adaptive Cyber Security Instruments, Inc.