The George Washington University
School of Engineering and Applied Science
Department of Engineering Management and Systems Engineering

EMSE 6540 Management of Information and Systems Security

Fall 2010

Instructor:

The instructor for this course is Julie J.C.H. Ryan. Office hours are by appointment only. Contact outside of class is preferred through email: jjchryan@gwu.edu. A brief introduction: Dr. Julie Ryan currently serves as Associate Professor and Chair in the Engineering Management and Systems Engineering Department at The George Washington University. Prior to joining the faculty at GWU, she worked for many years in industry and in government gaining both practical and theoretical knowledge in the field of information security. Current research interests include knowledge security, measuring the effectiveness of security measures, the role of governance in the information age, and information warfare. Her academic degrees are from the US Air Force Academy, Eastern Michigan University, and The George Washington University.

General Course Information:

This course meets every other week on Wednesdays and Thursday evenings over ten (10) weeks at SAIC. The course begins at 5:30 pm and runs until 8:30 pm. The first night of class is October 6, 2010. The last night of class is December 2, 2010. The precise schedule of classes is provided in the plan at the end of this syllabus.

Summary Course Description:

This course presents a systems engineering approach to implementing and managing effective information security in contemporary highly networked enterprises. The course provides an overview of the security challenges faced by individuals and organizations in the information age and introduces the complex and dynamic state of information assurance in cyberspace. It is intended to sensitize managers and computer professionals to the pitfalls and dangers of doing business in an interconnected world, and to familiarize the student with various organizations and materials that can be turned to for assistance in understanding how to operate and use modern computer systems and networks securely.

Disclaimer

This course examines *inter alia* ethical and legal dimensions of on-line behavior. However, it is not intended to turn information technology professionals or managers into lawyers. One or more of the course lecturers may be lawyers and many of the topics to be discussed will be concerned with the law and the legal implications of certain behavior. Every effort will be made to provide accurate and complete information. Please note, however, that at no time during this course will legal advice be offered. Any student or attendee needing legal advice should seek the services of a lawyer authorized to practice in the appropriate jurisdiction.

This class will explore both technology and management issues related to managing the elements of holistic information security. Specific technologies and techniques used by hackers, crackers, spies and thieves to obtain access to sensitive, private information are discussed and explored.

Students are reminded that it is a violation of Federal and some states' laws to attempt to gain unauthorized access to information assets or systems belonging to others, or to exceed authorized on systems to which they have been granted access.

At no time in this class should any student violate either laws or confidences.

This class is not about pushing the envelope or hacking, and any violation of legal boundaries in the course of this

class will be considered a violation of the class trust and will be subject to sanctions in grading and may result in dismissal from the Program.

Eligibility for NSTISSI 4011

Completion of this course with a grade of B or better entitles the student to the award of a certificate of completion of NSTISSI-4011, National Training Standard for Information Systems Security (INFOSEC) Professionals. In order to get the certificate, students should provide a self-addressed large envelope (larger than 8.5 x 11 inches) to Dr. Julie Ryan in the EMSE department. (It may be mailed to her. The address is on the website noted above in the very first paragraph of this syllabus.) The envelope does **not** need to be stamped. Upon completion of the course, Dr. Ryan will mail the certificates in the provided envelopes.

Course Objectives:

Upon completion of this course, the student should be able to:

a. Identify and critically assess issues and concepts related to the protection of information and information systems.

b. Define security attributes confidentiality, integrity, and availability. Describe confidentiality requirements for an enterprise environment. Describe integrity requirements for an enterprise environment. Describe availability requirements for an enterprise environment.

c. Analyze and evaluate proposed or extant information security policies, practices and procedures in order to assess potential advantages and disadvantages that might flow from implementing them. Describe how confidentiality can be protected. Describe how integrity can be protected. Describe how availability can be protected. Describe how failures of protections can be detected. Describe how attacks can be detected. Describe how impacts from an attack can be mitigated.

d. Use risk management principles to assess threats, vulnerabilities, countermeasures and impact contributions to risk in information systems. Perform a risk analysis for an environment. Create a management plan for security in an environment.

e. Evaluate policies, strategies and standard operating procedures for securing information and communication systems.

f. Identify and critically assess the legal, moral and ethical implications of behavior in an on-line world.

g. Describe and use a systems engineering approach to define a security architecture for a given operational environment.

Textbooks and Other Source Materials:

There are two required textbooks for this class. There are many other books that could prove useful to a fuller understanding of the subject matter, two of which are listed as optional for this class. No test material will be derived from either of the optional texts. Additionally, there are many valuable resources on line that students are encouraged to take advantage of. Three of these are listed below, each of which is free.

Required Texts:

National Institutes of Science and Technology (NIST) publications on computer security; available from the Computer Security Resource Center at http://csrc.nist.gov/ as identified in the course plan

McCumber, John (2004) Assessing and Managing Security Risk in IT Systems: A Structured Methodology. Auerbach Publications. ISBN 0849322324.

Conklin,W. Arthur, White, Gregory & Cothren, Chuck (2004) Principles of Computer Security: Security+ and Beyond. The McGraw-Hill Companies. ISBN 0072255099.

Optional Texts:

Turabian, Kate L. (1996) A Manual for Writers of Term Papers, Theses, and Dissertations (Sixth Edition). Chicago: The University of Chicago Press. ISBN 0-226-81627-3

Optional Podcasts and Other Material of Interest:

Bishop, Matt. Computer Science: Foundations of Computer and Information Security. http://deimos3.apple.com/WebObjects/Core.woa/Browse/ucdavis-public.1891962072.01891962085 (or simply go to iTunesU on the iTumes Store)

Science Friday by NPR

Planet Money by NPR

Grading:

The course grade will be in large part on completion of a group project. The group project is described in Appendix B to this syllabus. Please note the policy on groups. **Only part 4 of the group project will be graded.**

The final grade will be calculated based 75% on the group project and 25% on an in-class final exam. Grades are assigned on the letter basis and the final calculation will be conducted based on the 4 point scale as noted here:

Grade	Point Value		Grade	Point Value
A	4.0		C+	2.3
A-	3.7		C	2.0
B+	3.3		C-	1.7
B	3.0		F	0
B-	2.7			

Please note that in graduate school, the grade of D is not used.

As an example, the calculation of a final grade for a student who received an A- for the group project and a B- for the final exam would be as follows:

(3.7 * 0.75) + (2.7 * 0.25) = 3.45, which would result in the grade of B+ for the class.

Policy on Group Projects:

Group projects will be delivered electronically to the instructor not later than 11:59 pm East Coast US time on the date identified as the due date. The project will be downgraded by one half letter grade for every full or partial hour beyond that deadline. So, for example, if a project is received at 12:05 am following the deadline, half a letter grade will be deducted. If a project is received by the instructor at 1:05 am after the deadline, a full letter grade will be deducted from the grade. Obviously, any project received after 8 hours will be graded as an F.

For the purposes of adjudicating the time of delivery, the time stamp in the "received" field in the long email headers will be used.

Group projects are graded as a single entity and each group member is given the same grade. If a group project is found to include plagiarized material, academic integrity charges will be levied against all group members.

Every semester, one or more groups disintegrate in a cacophony of accusations and bad feelings. In the real world, this would be handled by either being forced (through contractual relationships or management decision) to continue to work together or by someone getting fired. If your group gets to the point where productive work is not possible, the following remedies are available:

1) the group can vote to "fire" a member. In this situation, the fired party may join another group, may form a new group with other disgruntled group members, or may elect to continue working alone.

2) a group member may elect to leave a group voluntarily. In this situation, the student may elect to join another group, may form a new group with other disgruntled group members, or may elect to work alone.

No group may have more than four (4) members, either originally or as reconstituted during the semester. In other words, the allowable size for any group is from one (1) member to four (4) members.

In any instance, due dates are fixed and will not be negotiated. The content of projects will not be lessened in any instance. Every turned-in project will be graded against the same criteria and held to the same standard.

Membership in the group must be clearly specified on the title page of the deliverable.

Because of the compressed nature of the semester, students are strongly advised to take action sooner rather than later to remedy a painful group situation.

Final Examination

The final examination will be a comprehensive exploration of the material. It will feature essay style questions and will require you to analyze situations and present solutions. It will be closed books, closed notes, and closed everything else. No external material, including dictionaries, calculators, or cell phones, may be used. Grading will be based on the comprehensiveness and appropriateness of answers provided. Imaginative and innovative solutions are especially valued. Students are encouraged to think "outside the box" in preparing their answers.

Class Attendance

Because the final exam is both closed everything and comprehensive, it should be obvious that attendance in class is valuable. Students have the responsibility to attend class and all material covered in class, whether part of the formal lecture material or not, is fair game to be included on the final examination.

Students may wish to make arrangements with classmates to review material to make sure all pertinent information was both heard and understood. Study groups are encouraged.

Make up classes will **not** be held for students who miss lecture sessions. If you need to miss a lecture for one reason or another, it is your responsibility to make arrangements with one or more of your classmates to take notes for you.

Academic integrity:

Academic integrity is central to the learning and teaching process. Students are expected to conduct themselves in a manner that will contribute to the maintenance of academic integrity by making all reasonable efforts to prevent the occurrence of academic dishonesty. Academic dishonesty includes, but is not limited to, obtaining or giving aid on an examination, having unauthorized prior knowledge of an examination, doing work for another student, and plagiarism of all types. Appendix A to this syllabus provides examples of plagiarism. Ignorance is no excuse.

Disabled Students:

Please be aware that faculty members are not empowered to make decisions regarding the treatment of students with disabilities of any sort. Any student who has a disability or is in need of special consideration must inform the instructor of this need within the first week of class (or immediately if the disability appears after the first week of class) so that appropriate arrangements can be made in accordance with University Policies and Regulations. This includes students with reading or learning disabilities who may require extra time on tests. In all cases, the student must communicate with the Disability Services Center and have registered the disability with the University. See http://gwired.gwu.edu/dss/ for more information.

Class Plan

The following is the course plan. It is subject to change as the semester progresses.

#	Date	Topic	Book Reading	NIST Reading	Project Part Due
1	Oct 6	Introduction of course; administrative material; intro to course content	None		
2	Oct 7	Threats and Vulnerabilities; Architecting security and understanding trust	Conklin Chap 1, 2, 10, 15	SP 800-100 SP 200	
3	Oct 20	Physical security: more important than you might think! Personnel security: the key to trustworthy enterprise operations	Conklin Chap 3, 4, 8; McCumber Chap 1 through 5	SP 800-116 SP 800-114 SP 800-30	Part 1
4	Oct 21	Policy: the framework for enterprise security	Conklin Chap 22	IR 7316	
5	Nov 3	Cryptography: a critically important tool; Firewalls, AV, and backups, oh my!	Conklin Chap 5, 6, 9	FIPS 196 SP 800-41 SP 800-53 SP 800-83	Part 2
6	Nov 4	Detecting Problems	Conklin Chap 13, 19	SP 800-94 SP 800-92	
7	Nov 17	Business Continuity: Reacting to and correcting problems	McCumber Chap 6 through 10	SP 800-84 SP 800-34	Part 3
8	Nov 18	Digital forensics; Cyber Law: When to Call Your Lawyer	Conklin Chap 23, 24	SP 800-88 SP 800-86	
9	Dec 1	Security and Social Media: an emerging challenge; Security as an enterprise enabler	McCumber Chap 11, 12, and appendices		Part 4
10	Dec 2	Final Exam			

Appendix A Academic Integrity

> "We, the Students, Faculty, Librarians and Administration of The George Washington University, believing academic honesty to be central to the mission of the University, commit ourselves to its high standards and to the promotion of academic integrity. Commitment to academic honesty upholds the mutual respect and moral integrity that our community values and nurtures. To this end, we have established The George Washington University Code of Academic Integrity."
>
> *preamble to the GWU Code of Academic Integrity*

The number one problem that students run into with regards to academic integrity is plagiarism. It is not okay to copy, use, or otherwise exploit other people's ideas, words, or creations without giving them credit in the proper form. Sometimes this means you must use quotation marks, while other times a simple source citation will do the trick. Changing a few words in a paraphrase is not enough to turn source material into "your own words" – in fact, that's a really bad idea to even try. Changing the phrasing order of sentences is not okay and using the thesaurus to find ways to change "happy" to "glad" is also a very bad idea.

It is expected that students know how to correctly quote and cite material, and also how to write well. This is a doctoral level course and students will be held to the high standards associated with this level of education. For those students who need assistance, the GWU Writing Center is available. See http://www.gwu.edu/~gwriter/.

From the Bulletin, University Regulations:

> Use of Correct English—A report regarding any student whose written or spoken English in any course is unsatisfactory may be sent by the instructor to the dean of the school, who may assign supplementary work, without academic credit, varying with the needs of the student. If the work prescribed is equivalent to a course, the regular tuition fee is charged. The granting of a degree may be delayed for failure to make up any such deficiency in English to the satisfaction of the dean.
>
> http://www2.gwu.edu/~bulletin/grad/unrg.html

There is no such thing as "boilerplate" or "standard language" in academia. Students are expected to write their reports themselves, using their own language and their own formulation. If it is necessary to use material from other sources, it is expected (and mandatory) that the standards of academic style and integrity will be followed. This includes glossaries and appendices.

Every student is encouraged to visit these websites for interesting information regarding this issue (links verified August 26, 2006):

1. A true story about plagiarism gone awry
   http://www.aweekofkindness.com/blog/archives/the_laura_k_krishna_saga/000023.html
2. Another story about plagiarism in science
   http://www.geocities.com/physics_plagiarism/
3. Different types of plagiarism, including through paraphrasing
   http://www.english.udel.edu/wc/handouts/plagiarism.html
4. Goucher College's "Plagiarism-by-Paraphrase Risk Quiz"
   http://faculty.goucher.edu/writingprogram/sgarrett/
5. Copyright law, frequently asked questions, and other good stuff
   http://www.copyright.gov/
6. The Islam Online.net Fatwa on Plagiarism
   http://www.islamonline.net/servlet/Satellite?pagename=IslamOnline-English-Ask_Scholar/FatwaE/FatwaE&cid=1119503549102
7. The George Washington University Code of Academic Integrity
   http://www.gwu.edu/~ntegrity/

Guidance on Plagiarism

Every semester, someone turns in plagiarized material as part of an assignment. When confronted, the shocked looks and consternation are usually accompanied by some version of one or more of the following explanations:

"I didn't think the same rules applied to the research method paper."

"I thought using a sentence was okay."

"I noted the source, even if I didn't use quotation marks. I thought that was enough."

"It's not plagiarized, it's paraphrased – see, I changed some of the words."

None of these explanations excuses the student from the reality that plagiarism has occurred. Here are some examples of what is not okay. In this table, the student submission is in the first column while the original text is in the second column. The text that is identical is underlined.

EVERY ONE OF THESE IS CONSIDERED PLAGIARISM.

Student Work	Original Text
Another effective technology is Gasification. It is commonly called 'partial combustion'. This process devolatilizes solid or liquid hydrocarbons, and converts them into a low or medium BTU gas. (Klein 2002)	Gasification is a process that devolatilizes solid or liquid hydrocarbons, and converts them into a low or medium BTU gas. Klein, Alexander. "Gasification: An Alternative Process for Energy Recovery and Disposal of Municipal Solid Wastes" M.S. Thesis, Columbia University May 2002
This process works more effectively with the types of MSW consisting of sewage sludge, plastics, wood, tires, or agricultural wastes. It generates a fuel gas that can be integrated with combined cycle turbines, reciprocating engines and, potentially, and then it converts fuel energy to electricity.	Finally, gasification generates a fuel gas that can be integrated with combined cycle turbines, reciprocating engines and, potentially, with fuel cells that convert fuel energy to electricity more than twice as efficiently as conventional steam boilers. Klein, 2002 (noted above)
Looking at industrial practice during the past decade nothing appears to have had such a great impact on organizational innovation as the growing market of application software packages such as enterprise resource planning (ERP) systems. The aim of the application of information technology (IT) is the profound improvement of the economic efficiency and effectiveness of all business processes (Scherer, 2000). ERP systems such as SAP, Oracle Business Suites, PeopleSoft, Baan and J.D. Edwards were originally designed to increase organization internal efficiency by streamlining the day-to-day business process.	Looking at industrial practice during the past decade nothing appears to have had such a great impact on organizational innovation as the growing market of application software packages such as SAP, BAAN, Peoplesoft or J.D. Edwards. This growth is hardly imaginable but through its connection to the concept of reengineering. The aim of the application of information technology (IT) is the profound improvement of the economic efficiency and effectiveness of all business processes. Scherer, Eric "The knowledge network: knowledge generation during implementation of application software packages", Logistics Information Management Vol 13,Iss 4, 2000
Nikolenko and Kleiner (1996) argue that in a functional hierarchy of a vertically built company, individual jobs and information flow are geared towards control. The crossfunctional teams of the horizontal company do not require the same level of formal managerial control because their work is aligned with customers' needs, and "controlled" by a judgment of the final result.	In a functional hierarchy of a vertically built company, individual jobs and information flow are geared towards control. The cross-functional teams of the horizontal company do not require the same level of formal managerial control because their work is aligned with customers' needs, and "controlled" by a judgement of the final result. If the teams are arranged to complete their projects in parallel (from start to finish), thus minimizing subdivision of the processes, the hierarchy becomes flattened. Nikolenko, Alexander and Brian H. Kleiner, "Global trends in organizational design", Work Study Vol 45,Iss 7, 1996

EVEN IF YOU INCLUDE THE CORRECT SOURCE, YOU MAY NOT USE EXACT WORDS UNLESS YOU USE QUOTATION MARKS OR INDENTS!

Appendix B Project Assignment

The project for this class is to develop an information security solution for a specific challenge, described below. There will be four incremental deliverables associated with this project. These four deliverables are as follows:

Part 1: Requirements analysis and decomposition. In this part of the project, groups will take the customer supplied material and expand upon that information to identify comprehensive system performance and security requirements. These requirements must include both explicit and derived requirements. Once the explicit and derived requirements are identified, implicit requirements must be expressed as well.

Part 2: Development of Technical Performance Measurements. In this part of the project, groups will take the results of Part 1 and define how performance and mission success will be measured.

Part 3: Functional analysis and diagramming. In this part of the project, groups must decompose and diagram the requirements using diagramming techniques.

Part 4 (Final): The final part of the project will be for students to combine all of the previous parts into an architecture that meets the requirements and performance goals. Please note: this is more than simply putting all the previous parts together. This final architecture must marry the pieces together into a coherent and synergistic whole. More work will be required to accomplish this than simply moving parts 1 through 3 into a single document.

Neatness counts! The grammar, spelling, and coherence of the finished document will count in the assessment of the effort.

Scenario for Design Challenge

The United Nations has brokered a treaty with many nations that reinforces and strengthens controls on production of material that may be associated with the development of nuclear weapons. Part of this treaty stipulates the enforcement of these controls in signatory countries through the use of technical means. This has been interpreted by the enforcement agency as allowing the use of covert data collection in suspect areas for confirmation of treaty compliance.

Your company has been selected by the United Nations enforcement agency to design a system to do a very specific element of this covert data collection: collection of sensed data resulting from the specific radioactive signature of treaty covered material.

The customer supplied requirements are that your system will be required to do the following actions:

1) while in place, detect radioactive particles of a specific nature (collect target specific data)

2) perform preprocessing on the collected data in order to contextualize meaning

3) transmit the collected data out of the target area in a covert manner (exfiltrate the data)

4) provide absolute assurance that the data collected is accurate and truthful, and can be used if necessary to punish violators of the treaty

5) completely process the data at a remote location

6) provide reports to identified users only

7) securely store the collected data for 20 years with 99.999% accuracy

8) while in place, it must not be detectable through either physical observation or technical observation (sensing technologies)

Because of the covert nature of the system, it must include elements of physical security as well as all other forms of security.

While doing your analysis, keep in mind that there are differing needs for confidentiality, integrity, and availability in each segment of the system, and in the different information states of communications, processing, and storage.

Examples from a solved challenge:

In order to assist you in completing the project successfully, examples from what a successful solution may include are provided here.

Part 1: Requirements decomposition

Example of a confidentiality requirement:

Explicit: "The system must not be detected while in operation."

Implicit: "The system must either be camouflaged or incorporated into some other system."

"The system must detect circumstances that indicate a probability of detection, such as movement or loss of access to the target environment."

Example of an integrity requirement:

Explicit: "The data collected must be of sufficient quality to support the storage accuracy goals."

Implicit: "There must be integrity checks that provide the ability to measure the integrity of the data at every part of the system."

"There must be multiple paths for data processing so that the processed values can be compared and adjudicated for integrity purposes."

Example of an availability requirement:

Explicit: "The processed data must only be made available to authorized users."

Implicit: "There must be a list of authorized users and that list must be used for access control."

"There must be an accountability function that correctly and completely shows specifically who accessed the reports from the system, when those reports were accessed, and from which location."

Part 2: Development of Technical Performance Measurements.

Examples:

The collection element must be undetectable by testers using every means at their disposal to detect the existence of the collection element (including physical examination and technical sensing).

During testing in real world environments, data exfiltration must be performed successfully without detection by test teams actively trying to detect the communication.

The data communication process must not reveal the location of the covert elements.

Part 3: Functional analysis and diagramming.

You may use any diagramming technique you wish. This example is of a functional decomposition diagram.