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

EMSE 6543 Managing the Protection of Information Assets and Systems

Spring Semester, 2013

Instructor: Julie J. C. H. Ryan, D.Sc. email: jjchryan@gwu.edu

Note: This syllabus is subject to modification during the semester. Should such modifications be made, students will be notified in writing with as much advance notification as possible.

Course Description

This course presents an overview of the various methodologies that may be used in implementing and managing effective information protection in contemporary highly networked enterprises. The focus of this course is to build upon EMSE 6540, which is a prerequisite to this class. This is a systems engineering class, not a computer science class. As such, a systems engineering approach to the analysis and execution of the projects is expected.

This class will explore both technology and management issues related to the protection of information assets. 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.

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.

Course Objectives

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

1. Identify and critically assess issues and concepts related to the protection of information and information systems.
2. Describe the relationship between protective mechanisms and business processes.
3. Describe the time aspects of protection in terms of the phasing of response options.
4. Distinguish between the elements of personnel security, physical security, and cyber-security.
5. Describe synergistic effects and relationships of those elements.
6. Analyze and evaluate proposed or extant information protection practices and procedures in order to assess potential advantages and disadvantages that might flow from implementing them.
7. Describe the elements of the Common Criteria, and critically assess the utility of them.
8. Develop a protection profile in accordance with the Common Criteria.

Required Reading Materials:

Students should read the material required as soon as possible. The scope of this course is very broad, and a large amount of reading is required. Recommended background reading is valuable for overall understanding, may provide a technical depth beyond the requirements of the class, may provide valuable material for student research topics, and may be useful in responding to comprehensive essay questions.

Books:

- Fennelly, Lawrence J. ed. "Effective Physical Security" (4th edition) Stoneham Mass: Butterworth-Heinemann, 2012. ISBN: 9780124158924
- Paar, Christof and Jan Pelzl. Understanding Cryptography: A Textbook for Students and Practitioners

Other Material:

- Infosec News listserv. Subscribe at http://www.infosecnews.org
- Relevant NIST Computer Security Publications, http://csrc.nist.gov/publications/PubsTC.html
- Common Criteria (download from http://www.commoncriteriaportal.org/cc/)
- Orange, Yellow and Red Books (US DoD Standards)
  (Download from http://www.radium.ncsc.mil/tpep/library/rainbow/)
- Ware, Willis. "Security Controls for Computer Systems (U): Report of the Defense Science Board Task Force on Computer Security" Rand Report R609-1, The RAND Corporation, Santa Monica, CA (Feb 1970)
  Download from http://csrc.nist.gov/publications/history/index.html
- Bell, David E. and Leonard La Padula, "Secure Computer System: Unified Exposition and Multics Interpretation." ESD-TR-75-306, ESD/AFSC, Hanscom AFB, Bedford, Mass. 01731 (1975) [DTIC AD-A023588]
  Download from http://csrc.nist.gov/publications/history/index.html
- System Security Study Committee, National Research Council. "Computers at Risk: Safe Computing in the Information Age." 1990
  (Download from http://www.nap.edu/catalog/1581.html -- please look for the "read it for free online" button above the picture of the book cover)
- Fred B. Schneider, Ed. Committee on Information Systems Trustworthiness, National Research Council. "Trust in Cyberspace." 1999.
  (download from http://www.nap.edu/catalog/6161.html -- please look for the "read it for free online" button above the picture of the book cover)

Policy on Submissions

Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. After that, one half of a point (0.5 point) will be taken off for every hour it is late. For example, if the time stamp on a paper is 12:15, one half of a point will be deducted from the score. If the paper is time stamped 6 pm the following day, meaning that it is 18 hours late, nine points will be deducted from the score.

Each member of the group responsible for the paper will receive the same grade.

Please note that life emergencies happen. Do NOT wait until the last moment to start on your paper. If you do that and something comes up to impede your progress, it will hamper your ability to turn in your paper on time.

Papers MUST be submitted electronically via email.

Thirty (30) points will automatically be deducted from any submission infected with any manner of nasty stuff. For example, if a paper comes in to me with an extract from a webpage that includes a web bug, the grading for that paper will maximize at 70 points.

All papers must include the following statement:

"This paper or presentation is my own work. Any assistance I received in its preparation is acknowledged within the paper or presentation, in accordance with academic practice. If I used data, ideas, words, diagrams, pictures, or other information from any source, I have cited the sources fully and completely in footnotes and bibliography entries. This includes sources which I have quoted or paraphrased. Furthermore, I certify that this paper or presentation was prepared by me specifically for this class and has not been submitted, in whole or in part, to any other class in this University or elsewhere, or used for any purpose other than satisfying the requirements of this class, except that I am allowed to submit the paper or presentation to a professional publication, peer reviewed journal, or professional conference. In adding my name following the word 'Signature', I intend that this certification will have the same authority and authenticity as a document executed with my hand-written signature.
Signature _____"

Policy on Group Projects:

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 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.

Each member of the group must sign group projects. Membership in the group must be clearly specified on the title page of the deliverable.

Grading Policy:

The overall course grade will be established as follows:

Project 1:	15%
Project 2:	15%
Project 3:	15%
3 Exams:	30% (10% each)
Final Exam:	25%

Exams will be closed books, closed notes.

Other Items of Importance

Incompletes

Don't ask for an incomplete for convenience. The University has very specific policy on when a grade of incomplete may be awarded. See the Bulletin for more information on grading policies.

Writing and Speaking Standards:

Written communication is an important element of the total communication process. This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations. The University recognizes and expects exemplary writing to be the norm for course work. To this end, all papers, individual and group, must demonstrate graduate level writing and comply with and conform to standard academic format as specified in A Manual For Writers of Term Papers, Theses, and Dissertations by Kate L. Turabian, Sixth Edition. Points will be subtracted for format errors. Points will also be subtracted for spelling and grammatical errors. Use of Standard English ensures that your points will be both understood and correctly interpreted by all readers, a skill that will be vital to your success after graduation.

Effective managers, leaders, and teachers are also effective communicators. It is no understatement to say that effective speaking and writing skills are as important to career success as technical mastery of a subject. Speaking and writing effectively are a critical part of this course. Correct and graduate level Standard English must be used.

Academic integrity:

The George Washington University Code of Academic Integrity
http://www.gwu.edu/~ntegrity/

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.

Plagiarism is the intentional or unintentional presentation of another person's idea or product as one's own. Plagiarism includes, but is not limited to, the following: copying verbatim all or part of another's written work; using phrases, charts, figures, illustrations, or mathematical or scientific solutions without citing the source; paraphrasing ideas, conclusions, or research without citing the source; and using all or part of a literary plot, poem, film, musical score, or

other artistic product without attributing the work to its creator. Students can avoid unintentional plagiarism by following carefully accepted scholarly practices. Notes taken for papers and research projects should accurately record sources of material to be cited, quoted, paraphrased, or summarized, and papers should acknowledge these sources.

There is no such thing as “boilerplate” in academia.

If you don’t understand what plagiarism is and how to avoid it, consult the University’s academic integrity policy.

This is a graduate program. Students are assumed to have learned how to prepare academic papers in their earlier studies, including how to reference works used in preparation of their papers and presentations.

The penalties for plagiarism include a zero or a grade of "F" on the work in question, a grade of "F" in the course, suspension with a file letter, suspension with a transcript notation, or expulsion.

Students are not permitted to submit an assignment or paper that already has been submitted for another course at GWU or any other institution, even if it is entirely their own work. This includes cutting and pasting portions of previous papers or other written assignments.

The penalties will be the same as those listed above for plagiarism. Please check your work carefully. Turabian contains complete guidance on how to correctly reference all forms of material.

IMPORTANT: There is no such thing as “boilerplate” or “standard language” in academia. Students are expected to write their reports themselves. 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 material from the Common Criteria used for project 3.

Disabled Students:

Any student who has a disability and 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. 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.

Group Projects

Each group is assigned a general scenario to give context to the project execution. Each group is responsible for fleshing out the scenario to the extent required to complete the assignments. This context must be included in the solutions to each project. Groups should not mirror a template, use NIST guidelines, or follow any other standard form of developing policies and procedures. The point of this project is not to see how well you can follow directions but instead is on the creative thought process and critical analyses of needs and implementation details. Projects are graded on the basis of creative thought and engineering analysis with a view towards the solution space workability and applicability to the challenges of the environment postulated.

There are three projects. Each of these projects must reflect the virtual reality of the scenario.

Scenarios

The scenarios are as follow:

Group 1: The Superspy Detective and Investigative Company

The Superspy Detective and Investigative (SDI) Company is a firm that specializes in collecting and analyzing technical evidence for use in civil and criminal actions. Clients include suspicious spouses, employers, and other people interested in specialized information collection. SDI is licensed by the state as a detective agency. SDI has four employees/ owners at this time but is looking to grow both by hiring more people and by expanding their ability to collect digital evidence and investigate cyber crimes.

Group 2: The Ministry of Justice Cyber Crime Laboratory

The Ministry of Justice Cyber Crime Laboratory (MOJCCL) is a government run laboratory that examines digital evidence for criminal activity. The evidence is received from law enforcement agencies countrywide. The Laboratory has 40 technical specialists on staff, with a staff turnover rate of 5% per year, mostly due to retirement. The Laboratory has the facilities to examine hardware and software associated with personal computers, phones, personal digital devices, and digitally enhanced appliances. Due to the increase in cases involving digital forensics, the Laboratory is looking to double its processing capacity.

Group 3: The Peace in Our Time Legal Mediation Center

The Peace in Our Time Legal Mediation Center (PIOT LMC) is a law firm that specializes in bringing parties together who are about to become or currently are involved in litigation with the goal of finding a middle ground that will keep the matter out of court. Clients include divorcing couples, parties with contractual disagreements, and other aggrieved parties. Within the last few years, the PIOT LMC has increasingly had to deal with the issues of digital evidence in their mediation efforts and is looking to hire a full time staff to deal with these issues. They are currently considering an initial staff of four technicians.

Project 1: Physical Security

Each group will develop a set of physical security policies and procedures for their group scenario.

The group will prepare a formal document describing and explaining the physical security plan and polices, and will present their solution during class during Session 4. The report will be due that date. Groups will have 30 minutes maximum to present their solution. The grade for the project will include the presentation.

The written report on physical security must conform to Turabian format and include the following elements at a minimum:

- A graphical representation of the environment, including road systems, entry and exit controls, emergency access elements, lighting, and other germane elements.
- Discussion on each element of physical security and how it contributes to the physical security goals
- Identification of how each element of physical security contributes to slowing or impeding a violator, to include traps or other containment elements
- Identification of processes for detecting violations or security failures and reaction mechanisms

Project 2: Communication Security

Groups will develop a communication security solution for their group scenario. The communication security system must address the protection of information in all forms, from

digital to physical to oral. Clearly, cryptography will be an important part of this challenge and, just as clearly, cryptography is not sufficient to address the totality of the challenge.

The group will prepare a formal document describing and explaining the communication security solution, and will present their solution during class during Session 8. The written report will be due that date. Each group will have 30 minutes to present their solution.

The written report on communications security must conform to Turabian format and include the following elements at a minimum:

- Identification of types and amounts of information subject to the security controls
- A systems engineering decomposition of the problem
- A systems engineering analysis of the solutions, including measures of effectiveness and cost
- Description of protective measures and expected utility of each
- Description of how all the elements of the plan work together in a systemic solution
- Identification of processes for detecting violations or security failures and reaction mechanisms

Project 3: CC Protection Profile

Groups will develop a protection profile (PP) in accordance with Common Criteria guidance. Please see http://www.commoncriteria.org/ and view the listed evaluated protection profiles to get an idea of scope. The subject of the project will be specified by the instructor in consultation with the group members.

The group deliverable is a formal report and must conform to Turabian format with the actual Protection Profile as an appendix to the report. The report should include the following as a minimum:

- A complete description of the subject of the PP
- A concept of operations for the subject in the environment, including the security theory(ies) that inform the development of the PP
- Discussion on which controls were chosen and why, specifically how each contributes towards security goals
- Appendix incorporating the actual protection profile

Your PP should be at EAL-3. You may choose elements of EAL-4 to augment your PP if it seems useful or plausible.

The protection profile will be presented in class during Session 12. Each group will have 30 minutes to present their solution, including trade space.

DO NOT USE A PROTECTION PROFILE GENERATOR or any other automated tool. Make sure you follow strict academic integrity standards.

Some discussion regarding protection profiles:

> To understand this project, it is useful to parse the definitions.
>
> What is a Protection Profile? Simply stated, it is:
>
> "An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs."
>
> OK, so let's look at the critical words in that definition. First of all, a PP is implementation independent. That means that you're not designing a specific implementation of something -- you're addressing the more global definition of the something, which could be implemented in many different ways or venues. Secondly, it's a set

of security requirements. This means that the PP consists of a set of security requirements -- not one, not two, but many, which together in concert define a security profile. Third, the PP is for a category of TOEs that meet specific consumer needs. This means that the PP is specifically designed for a product that someone actually would want to use to do something.

But, what's a TOE???? Again the definition:

"An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation."

And, again with the parsing...

A TOE is first of all "an IT product or system" -- okay, so we're not talking about a building here! It's smaller than that. It's more defined than that. It's specific. It's a single product or system. But, the TOE must include "associated administrator documentation" -- okay, so that means that part of the TOE is paperwork. And more paperwork -- a TOE must also include "user guidance documentation ". And all of the above is "the subject of an evaluation." That means that the concept is tested to see if it actually meets the design goals.

Now, here's the tricky part. A PP is an implementation independent solution, right? So, you're not actually going to build a box and test it. So how do you evaluate it? Well, as it says on the CC website:

"PPs can be submitted for evaluation to one of the evaluation facilities. Through this process the contents of the PP is checked against the CC requuirements to ensure that it is technically correct, clear, and internally consistent."

I highly recommend you read the following website for a nice clear picture of what a PP is and how to go about defining one: http://www.commoncriteria.org/protection_profiles/pp.html

Examples of PPs include ATMs, DBMSs, OSs, etc. You can see all the currently evaluated PPs by going to the following website: http://www.commoncriteria.org/epl/index.html There are tabs at the top that take you to lists of the types of evaluated products. Please note, some of these products are actual products while others are PPs.

Do not use a PP generator or any template for developing a PP. The point of this project is for you to understand how the Common Criteria can assist you in defining security functionalities and additionally to help you understand the critical problem with buying a CC-evaluated product (the caveat emptor problem). You will just be short changing yourself if you try to take short cuts.

Do not print out the CC! It’s extremely large and fills 3 large binders when printed out.

Class Plan

#	Topic	Due
1 Jan 15	Introduction	
2 Jan 22	Physical Security 2	
3 Jan 29	Personnel Security	
4 Feb 5	Systems engineering security	
5 Feb 12	Exam 1: Physical Security	
6 Feb 19	Presentations Approaches for Evaluating Computer Security	Proj 1
7 Feb 26	The role of standards and compliance	
8 Mar 5	Legal issues	
Mar 12	Spring Break	
9 Mar 19	Exam 2: Cryptography	
10 Mar 26	Presentations Metrics	Proj 2
11 Apr 2	Architecting computer security	
12 Apr 9	Evaluating security	
13 Apr 16	Exam 3: Common Criteria and Computer Security	
14 Apr 23	Presentations Wrap up discussions	Proj 3
Final	Final exam	