The Villanova University
Master of Science in Cybersecurity
Department of Electrical and Computer Engineering
ECE 8492
Secure Software Development
August 23 - December 19, Fall 2017

Instructor:
Dr. Charles Pak
Email: charles.pak@villanova.edu; charlespak@verizon.net
Email is the best way to contact me. Here is my cell number if needed: (443)610-7986

General Course Information:
This is a graduate level class. Students are expected to apply time management skills to their work, home, and academic life. Any due dates for materials for this class are designed to spread the workload over the semester. Material, such as reading assignments, with no due date given should be done as soon as possible by the student so the workload does not become overwhelming prior to the end of course.

Course Description
Secure software development addresses the real software issues from the inception of the software lifecycle. Software security is a new security concept that had been ignored for many years when developing software. Software security deals with the vulnerabilities in software design from the requirement analysis phase of the software design life cycle (SDLC). We find most of the software vulnerabilities while using the software in operation. However, many of these software vulnerabilities are induced from the life cycle of software from the development to maintenance phases. This course explores the real software security issues to minimize the impacts to an organization.

Course Objectives
Upon completion of this course, the student will be able to:

- assess software security requirements to prevent data loss;
- design software to meet software security requirements;
- develop strategies to mitigate security vulnerabilities;
- develop guidelines for operational security;
- conduct software security reviews and audits; and
- develop a software security monitoring policy.

Required Reading Materials:
Books:

- Van Wyk, K. R., Graff, M. G., Peters, D. S., & Burley, D. L. (2014). *Enterprise software security: A confluence of disciplines*. ISBN-13: 978-0321604118

Course Structure
Secure Software Design and Development is a three-credit online course consisting of seven modules. Modules include an overview, topics, learning objectives, study materials, and activities. Module titles are listed below.

Module 1: Software Vulnerabilities
Module 2: Designing Secure Software
Module 3: Testing Software Vulnerability in SDLC
Module 4: Mitigating Software Vulnerabilities in SDLC
Module 5: Operating Software Security
Module 6: Maintaining Software Securely
Module 7: Review of Software Security

Methods of Learning

The method of instruction will combine the following elements:

Discussion Participation
Secure Software Design Phase in SDLC Research Paper
Secure Coding Phase in SDLC Research Paper
Secure Software Testing in SDLC Research Paper
Lab1 - Virus and Worm VIPRE Antivirus Internet Security
Lab2 – Denial of Service Using Wireshark
Lab3 – Nessus Scanner
Final Course Project

Secure Software Design Phase in SDLC Research Paper
Your paper should include a novel or practical approach of secure software design phase of the SDLC. Your paper should describe the current secure software design methodologies in cyberspace and recommend the best approach to securely design software.

Secure Coding Phase in SDLC Research Paper
Your paper should include a novel or practical approach of secure software coding phase of the SDLC. Your paper should describe the current secure coding methodologies in cyberspace and recommend the best approach to securely code software.

Secure Software Testing in SDLC Research Paper
Your paper should include a novel or practical approach of secure software testing phase of the SDLC. Your paper should describe available secure software testing methodologies and recommend the best approach to securely test software.

Policy on Paper Submission
Papers are due on the date they are due. Up until midnight of that night, no penalty will accrue. 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 online.

Final Course Project - Secure Software Design and Development

OVERVIEW

In recent years, we have seen cyberattacks on national critical infrastructure, corporate networks, and government organizations. The Stuxnet worm was one of the Cyberterrorism exploitations that raised many controversial issues in politics, academia, and industry. Russia has exercised its cyber capabilities against its neighbors by attacking power grids with cyberattacks. An Indian city lost power for several days due to a cyberattack. India believes it was an act of cyberterrorism.

Considering these prevalent cyber vulnerabilities, we must ensure our software is secure enough to operate critical infrastructure systems such as power grids, water system, transportation, communication, and others. The Department of Homeland Security (DHS) is chartered with protecting these national critical infrastructure systems. Our supervisory control and data acquisition systems (SCADA) that manage the national critical infrastructure are interconnected to Cyberspace for management, configuration, and monitoring. Any failure in one of these systems can present a debilitating consequence to national security, economy, health, and others.

The student will research and write a 10-15 page, APA formatted, paper on software security to include the prominent security issues, especially the issues in software deployed in national critical infrastructure systems. The paper will include recommendations to mitigate these security issues in the SDLC process.

GUIDELINES

- You should follow accepted research approaches and citation format (APA).
- Your paper should be well developed and convey your understanding of the research and the concepts learned.
- Your paper should be organized, coherent, and unified.
- Your paper should be free of spelling and grammatical errors.
- Be sure to document all contentions and "facts" mentioned in an academically acceptable manner. (See writing resources below).

Project Milestones

Week 2: Topic Approval

- The student will submit a 1-2 page executive summary describing the project topic, the expected outcomes, and the relevance of software security.

Week 4: Literature Survey

- The student will research for literature, other than the textbook, relevant to their project topic and will submit a list of at least five references, in APA format, of the literature they intend to use.

Week 8: Paper Outline

- The student will submit an outline of his or her final paper. The outline should include, at a minimum:
  - ✓ Title and References pages;
  - ✓ a brief summary of the articles used;
  - ✓ a statement of the key problem(s) with SDLC phases;
  - ✓ a discussion of the importance of testing SDLC phases;
  - ✓ an explanation of software related cyber vulnerabilities;
  - ✓ recommendations on how to mitigate cyber vulnerabilities;
  - ✓ the real software security issues;
  - ✓ recommendations for secure software development and deployment; and
  - ✓ conclusions.

Week 10: Draft Paper

- The student will submit a 10-15 page draft of the final paper, based on the outline submitted in week 8.
  - ✓ The professor will critique the draft, and provide feedback that may be used to enhance the final-version.

Week 12: Final Paper

- The student will submit a final paper, that contains the same elements required of the draft paper, including modifications, as needed, and, perhaps, based on the professor's feedback for the draft version.

WRITING AND RESEARCH RESOURCES

The following links provide online writing and research aids to help you with your paper assignments.

- OWL (Online Writing Lab) at Purdue University
- Writer's Handbook, the Writing Center at the University of Wisconsin–Madison
- APA Guidelines

The student will write an APA formatted software security project paper to include the prominent security issues in SDLC. Additionally, the paper must address the cybersecurity issues in software deployed in national critical infrastructure systems. The paper should be in 10-15 pages.

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 that 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 _____"

Reading Assignments:
The scope of this course is very broad, and a large amount of reading is required. However, the relative importance of materials, as specified in the course outline, varies. Specifically assigned materials must be read in detail. Materials to which students are directed or for which copies are provided but which are not specifically assigned are recommended for added understanding of required material, but are optional in the sense that students will not be held explicitly responsible for anything that appears only in these materials. They are appropriate either for students who have difficulty with the subject matter based on the required readings or for those who want a deeper understanding of the material. 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.

Since much of what is happening in information security is happening now, current events will play a role in class discussions. As professionals, it is crucial for you to keep up with events as they unfold. There is no substitute for regular reading of business and technology news in a major newspaper, for following current journal articles, visiting key web sites, and for noting the direction of industry organizations such as the IEEE, IETF, and the ACM. You should constantly consider how what you read in such sources fits into the subject you are studying. Current articles, including Web articles, may be assigned as supplementary reading as the course progresses.

Students are encouraged to use as many and varied sources as possible in exploring the questions presented during the course, and to share those sources with their classmates. References to sources should be explicit in exchanges among the students and instructor, and will be considered in determining the extent to which each student participated for purposes of awarding grades.

Grading Policy:
The overall course grade will be established as follows:

Grading Criteria	Percentage
Discussion Participation	20
Research Paper 1 - Secure Software Design Phase in SDLC	10
Research Paper 2 -Secure Coding Phase in SDLC	10
Research Paper 3 -Secure Software Testing in SDLC	10
Lab1 - Nessus Scanner	10
Lab2 – Denial of Service Using Wireshark	10
Lab3 – Virus and Worm VIPRE Antivirus Internet Security	10

Final Course Project Paper	20
Total	**100**

http://www1.villanova.edu/villanova/enroll/registrar/policies.html#question_faq_5

Letter Grade	Approximate percentage grade range	Grade Points
A	95–100	4.00
A−	90 < 95	3.67
B+	85 < 90	3.33
B	80 < 85	3.00
B−	75 < 80	2.67
C+	70 < 75	2.33
C	65 < 70	2.00
F	< 65	0.00

Other Items of Importance
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, Seventh 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*:**
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.

Citing Sources: Your research paper must be properly cited and referenced in APA format. You should use reliable scholarly publication rather a web site. The primary purpose is for you to become familiar with sources of security

information in the school library or on the Internet. Students must submit the assignment (with its source clearly indicated) to the Digital Drop Box by midnight on the due date. For assignments that require finding a news article, the article should be no more than 3 months old. Students must also be prepared to share the assignment with the class either in the classroom or via the discussion topics when requested.

Academic Integrity Policy: Your success in meeting your academic goals is of the utmost importance to the university. Therefore, it is important that you are aware of a policy the university has designed to nurture academic honesty. We wish to provide a sound learning environment for you as you carry out your responsibilities in the classroom here at Towson University. Please refer to the Student Academic Integrity Policy in the Student Handbook.

Papers, presentations, labs, discussion postings, exams, assignments, etc. submitted to the instructor must be original and may not have been submitted for a grade in any other course. Drafts are considered submissions. Submitted work that is not in compliance with the Academic Integrity Policy will be returned to the student. The student will have one opportunity to resubmit the work. If the work is still not in compliance, it will receive a grade of zero. The Department Chair will be notified of any non-compliance issues.

Computer and Electronic Communication Resources Policy: Access to computer and electronic communication resources, such as the Internet, electronic mail, computer labs and networks, is a privilege provided at the discretion of the university to:

- Support teaching and learning.
- Serve the information and communication needs of the university community.
- Deliver instructional content.
- Disseminate information about the college.
- Conduct official college business.

Acceptable uses of computer and electronic communication resources are those that support the purpose above. Computer, Internet and network usage at the university is governed by university policy as well as federal, state and local laws. Individuals who inappropriately or illegally use computing and network services and resources may suffer all applicable college and legal penalties for such misuse.

Research Paper Grading Rubric

Criteria					
	Poor	**Fair**	**Good**	**Excellent**	**Percent**
Organization	Sequence of information is difficult to follow. (0 – 7)	Reader has difficulty following work because student jumps around. (8 – 14)	Student presents information in logical sequence which reader can follow. (15 – 22)	Information in logical, interesting sequence which reader can follow. (23 – 30)	30%
Content Knowledge	Student does not have grasp of information; student cannot answer questions about subject. (0 – 12)	Student is uncomfortable with content and is able to demonstrate basic concepts. (13 – 24)	Student is at ease with content, but fails to elaborate. (25 – 37)	Student demonstrates full knowledge (more than required). (38 – 50)	50%
Grammar and Spelling	Work has significant spelling	Presentation has several and/or	Presentation has a couple	Presentation has no misspellings or	10%

	errors and/or grammatical errors. (0 – 2)	grammatical errors. (3 – 4)	misspellings and/or grammatical errors. (5 – 7)	grammatical errors. (8 – 10)	
APA Formatting	Work has significant formatting errors (i.e. references page, title page, spacing, citations). (0 – 2)	Work has several formatting errors (i.e. references page, title page, spacing, citations). (3 – 4)	Work has a few formatting errors (i.e. references page, title page, spacing, citations). (5 – 7)	Work has no formatting errors (i.e. references page, title page, spacing, citations). (8 – 10)	10%

Student Code Conduct: Students are expected to be courteous and to respect each other and the instructor in online discussions/interaction at all time.

Discussion Rubric

Criteria	Non-compliant	Minimal	Compliant	Advanced
One initial major response (minimum 125 words) to first discussion question	Did not complete this portion of the assignment or most of the discussion points were inappropriate or were not identified. (1)	The discussion points were identified and described but with fair accuracy and some of the discussion points were inappropriate or were not identified. (3)	The discussion points were identified and described with good accuracy and appropriate information was identified and discussed. (6)	The discussion points were identified and described with high accuracy and all appropriate information was identified and discussed clearly. (10)
Writing – grammar, sentence structure, paragraph structure, spelling, punctuation (APA required).	5 or more different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Major issues) (1)	3-4 different errors in sentence structure, paragraph structure, or APA usage. References are expected. (Many issues) (3)	1-2 different errors in sentence structure, paragraph structure, spelling, punctuation, or APA usage. References are expected. (Minor issues) (6)	No errors in sentence structure, paragraph structure, spelling, punctuation or APA usage. References are expected. (Minor issues) (10)
Responding to other students.	Did not respond to other students or responses were trite with no substance. (1)	Responded to other students but responses were trite with no substance. (3)	Responded to one other student, response was substantive. (6)	Responded to two or more other students, responses were substantive. (10)
Frequency of responses.	Did not post in the threaded discussion. (1)	Posted one message only 1 day of the week. (3)	Posted more than 1 message but only one day of the week. (6)	Posted on two or more different days of the week. (10)

Course Schedule – Each module spans two weeks

Module Objectives, Discussion Topics, Assignments Schedule

SECURE SOFTWARE DEVELOPMENT: (8/23-12/19), Fall 2017

Module 1 – Software Vulnerabilities; Week 1-2 (8/23-9/5)

Class Orientation

- Introductions
- Course overview and introduction, review of syllabus and readings, assignments
- Instruction Components and Learning Styles
- Paper – Format, Expectations, Some Pointers
- Research Paper Assignments
- Lab Assignments

In this module, the student will analyze the prevalent software vulnerabilities in the cyberspace and explore the future trends in software attacks.

Module 1 Discussion Topics.

- Malicious software exploitation in the cyberspace
- Web Server Vulnerabilities
- Malicious software attacks in Cyber Terrorism
- Inherent software vulnerabilities

Module 1 Objectives

After successfully completing Module 1, students should be able to:

- evaluate malicious software in the cyberspace;
- assess mission critical software for vulnerabilities;
- critique embedded firmware vulnerabilities.

Introduction Forum

In the Introductions Forum, start a discussion topic titled "Introductions/[Your Name]." In your posting, please address any of the following topics or anything about yourself that you would like to share with the class so that we can get to know you better. Reply to at least two classmates' responses by the end of Module 1.

- Your reasons for taking this course
- Your interest in Secure Software Design and Development
- Your background in general
- Your experience with online learning
- Your expectations from this course

Note: The Introductions Forum is not graded but required

Discussion Forum 1

In Discussion Forum 1, post your response to the following discussion topic. Reply to **at least two** classmates' responses by the end of Module 1.

Software vulnerabilities in cyberspace can range from the simple outdated security patches on national critical infrastructure systems to poorly designed defense missile control systems. When these industrial control systems,

military weapon control systems, air control transportation systems are designed without security built into the software, their security vulnerabilities are paramount to the national security, economy, and human health.

- Do research on the latest prominent software vulnerabilities and share your literature review findings with the class.

Textbook Readings

- Van Wyk, et al. (2015) - Chapters 1.

Reading Assignment – Read Chapter 1

Written Assignment 1: Software Vulnerabilities

Software vulnerabilities can cause debilitating consequences in our national critical infrastructure, mission critical applications in a corporate network, and in health and transportation systems. It is paramount to mitigate these vulnerabilities in the initial stages of software design. Do your research on software vulnerabilities and write a 5-10 page, APA formatted, research paper on software vulnerabilities that have devastated our networks.

- Considering the impacts of software vulnerabilities, do a literature review to select at least five sources, other than the course's textbook, that discuss the current software vulnerabilities in cyberspace.
- After analyzing your findings on the impacts of cyber vulnerabilities, write a 5-10 page APA formatted paper [not including Title Page, References Lists, etc.], based on your research, in which you identify and analyze cyber vulnerabilities that have inflicted our society with grave consequences.
    - Your paper, should include:
        - a brief summary of the selected articles;
        - a clear description of cyber vulnerabilities you have identified from your research;
        - details on how these vulnerabilities had been exploited.
        - any implications or problems you have identified for the affected environment;
        - a summary section that provides any conclusions you have reached as a result of doing the research and writing the paper; and
        - a reference page.

Note: The research findings included in the written assignment paper, may reference, or be related to, the topic discussed in Discussion Forum 1.

Module 2—Designing Secure Software; Week 3-4: (9/6-9/19)

In this module, the student will examine security controls in the software requirements to ensure software will be designed with "security built-in." The student will analyze the software functions and security controls to provide well-balanced software.

Module Topics

Module 2 covers the following topics:

- Security requirements
- Security balance
- Code review
- Security mechanisms and controls

Assignment – Read Chapter 2, Review Paper Topics
After successfully completing Module 2, students should be able to:

Week 2: Project Topic Approval

- The student will submit a 1-2 page executive summary describing the project topic, the expected outcomes, and the relevance of software security.

Module 2 Objectives

- analyze security requirements in software;
- ensure security controls and mechanisms are applied;
- develop security safeguards in software design.

Textbook Readings

- Van Wyk, et al. (2015) - Chapters 2-3.

Discussion Forum 2

In Discussion Forum 2, post your response to the following discussion question. Reply to **at least two** classmates' responses by the end of Module 1.

> In this forum, the student will research the best secure software design methodologies to prevent vulnerabilities, and share his/her findings with the class. The student will post a literature review on a researched ACM or IEEE paper.

Building security in the design phase of the software development lifecycle (SDLC) is important to be successful in securing software. What is the right approach in securing SDLC phases so that we can identify software issues early and mitigate them while designing software. Explain what implications we may face if we don't identify and mitigate security issues in the SDLC phases.

Written Assignment 2

> *Secure Software Design Methodologies* – The student will write a 1-2 page, APA formatted, literature review paper on secure software design methodologies. The paper topic may be related to the discussion topic.

Write your research paper based on your findings on secure software design methodologies. You will recommend the best software security design methodology that can prevent security issues while designing the software in the SDLC phases rather than after the software deployment phase. Further, justify why your approach is better than others with realistic benefits.

Assignment - Lab1 - Nessus Scanner

You have access to the Lab 1- Nessus Scanner document in assignment folder. Please following the instruction to complete the lab and provide your findings and results in your lab activities. Your lab report should be prepared in APA. Please see the lab instruction documents.

Week 4: Project Literature Survey

- The student will research for literature, other than the textbook, relevant to their project topic and will submit a list of at least five references, in APA format, of the literature they intend to use.

Module 3—Testing Software Vulnerability in SDLC: Week 5-6: (9/20-10/3)

In this module, the student will analyze, test, and recognize software vulnerabilities using security testing tools.

Module Objectives

After successfully completing Module 3, students should be able to:

- assess software security vulnerabilities;
- test security vulnerabilities in software;
- utilize software vulnerability testing methodology.

Textbook Readings

- Van Wyk, et al. (2015) - Chapters 4-5.

Discussion Forum 3

In Discussion Forum 3, post your response to the following discussion question. Reply to **at least two** classmates' responses by the date indicated in the Course Calendar.

> In this forum, the student will research a proven software security testing methodology to discover software vulnerabilities, and share his/her findings with the class. The student will post a literature review on a researched ACM or IEEE paper.

Research for proven software security testing methodologies to discover software vulnerabilities. Select one that can be effective in an organization, and justify why your selected testing methodology is best for a specific organization.

Written Assignment 3

> *Secure Software Testing Methodologies* – The student will write a 1-2 page, APA formatted, literature review paper on a secure software testing methodology. The paper topic may be related to the discussion topic.

There are many software security testing methodologies as such as risk-based, agile, and other structured testing methodologies. In your research, synthesize your findings of best software security testing methodologies that can be adopted by organizations to defend the asymmetric cyber threats

Module 4—Mitigating Software Vulnerabilities in SDLC: Week 7-8; (10/4-10/17)

OVERVIEW

In this module, the student will mitigate software vulnerabilities using security tools. In this module, the student will mitigate software vulnerabilities using security tools.

Chapter 4 Code Review with a Tool: Week 5-6, 9/20-9/2/9

Module 4 covers the following topics:

- Software vulnerabilities
- Software security tools
- Software vulnerability mitigation

OBJECTIVES

After successfully completing Module 4, students should be able to:

- mitigate security vulnerabilities in SDLC phases;
- utilize security mitigation tools in removing vulnerabilities;
- leverage proven methodologies in mitigating vulnerabilities.

STUDY MATERIALS

Textbook Readings

- Van Wyk, et al. (2015) - Chapters 4-5.

Discussion Forum 4

In Discussion Forum 4, post your response to the following discussion question. Reply to **at least two** classmates' responses by the date indicated in the Course Calendar.

> In this forum, the student will research the best secure software mitigation methodologies using tools and share his/her findings with the class. The student will post a literature review on a researched ACM or IEEE paper.

Automation is key to our success in security to minimize manual processes and avoid errors. Research any automation we can apply in software security; especially, in the initial stages of the SDLC phases. Software errors and bugs discovered in the SDLC will save the program cost and engineers' effort in mitigation them after deployment. Provides evidence of benefits of using the automation or tools in your post.

Written Assignment 4

> *Secure Software Mitigation Methodologies* – The student will write a 1-2 page, APA formatted, research paper on secure software mitigation methodologies using tools. The paper topic may be related to the discussion topic.

From your research, write a security software mitigation methodology using a tool. Benefits from the automation can empower the security professionals in cost reduction and efficient automation in mitigating software vulnerabilities. Describe the best security mitigation methodology to automate the vulnerability removal process using a tool.

Assignment – Lab2 - Denial of Service Using Wireshark

You have access to the Lab 1- Nessus Scanner document in assignment folder. Please following the instruction to complete the lab and provide your findings and results in your lab activities. Your lab report should be prepared in APA.

Week 8: Project Paper Outline

The student will submit an outline of his or her final paper. The outline should include, at a minimum:

- ✓ Title and References pages;
- ✓ a brief summary of the articles used;
- ✓ a statement of the key problem(s) with SDLC phases;
- ✓ a discussion of the importance of testing SDLC phases;
- ✓ an explanation of software related cyber vulnerabilities;
- ✓ recommendations on how to mitigate cyber vulnerabilities;
- ✓ the real software security issues;
- ✓ recommendations for secure software development and deployment; and
- ✓ conclusions.

Module 5—Operating Software Security: Week 9-10 (10/18-10/31)

OVERVIEW

In this module, the student will operate software securely using security tools.

TOPICS

Module 5 covers the following topics:

- Security Thresholds
- Intrusion Detection
- Mission Critical Applications
- Incident Response

OBJECTIVES

After successfully completing Module 5, students should be able to:

- operate software securely;
- utilize software security tools;
- protect mission critical applications.

Discussion Forum 5

In Discussion Forum 5, post your response to the following discussion question. Reply to **at least two** classmates' responses by the date indicated in the Course Calendar.

> In this forum, the student will research for proven software security operations, the use of software security tools, and share his/her findings with the class. The student will post a literature review on a researched ACM or IEEE paper.

In operational security, we run and maintain the security operations center (SOC) in any organization, large or small in size. Research for a well-accepted, best software security operations using tools. These tools may come in bundled with other network appliances. Post your findings on software security operations using automations, used in SOC.

Textbook Readings

- Van Wyk, et al. (2015) - Chapter 7

Written Assignment 5

> *Secure Software Operation Methodologies* – The student will write a 1-2 page, APA formatted, research paper on secure software operation methodologies using tools. The paper topic may be related to the discussion topic.

Secure software operation methodologies must be integrated with the IT, SOC, and the management to be effective. Many of the recent cyberattacks involved some software vulnerabilities on endpoint computers, networks, or in user applications. Describe the best software vulnerability mitigation methodologies using automation with tools.

Week 10: Project Draft Paper

The student will submit a 10-15 page draft of the final paper, based on the outline submitted in week 8.

- The mentor will critique the draft, and provide feedback that may be used to enhance the final version.

Module 6—Maintaining Software Security: Weeks 11-12 (11/1-11/14)

OVERVIEW

In this module, the student will maintain software securely by auditing.

TOPICS

Module 6 covers the following topics:

- Maintain software securely
- Feedback security vulnerabilities into SDLC
- Security validation and audit

OBJECTIVES

After successfully completing Module 6, students should be able to:

- maintain software securely;
- audit software security;
- improve software security.

Textbook Readings

Van Wyk, et al. (2015) - Chapters 8-9

Discussion Forum 6

In Discussion Forum 6, post your response to the following discussion question. Reply to **at least two** classmates' responses by the date indicated in the Course Calendar.

> In this forum, the student will research the best secure software maintenance methodologies to prevent vulnerabilities, and share his/her findings with the class. The student will post a literature review on a researched ACM or IEEE paper.

Upon delivery of the software, its maintenance and operational cost more than any SDLC cost in other phases. One of the cost factor is that we are finding software vulnerabilities after we deploy the software and exercise all available functions and features in the software.

Written Assignment 6

> *Secure Software Maintenance Methodologies,* the student will write a 1-2 page, APA formatted, research paper on secure software maintenance methodologies. The paper topic may be related to the discussion topic.

Based on your research, what secure software maintenance methodologies do you find most effective and why? Write your paper with supporting evidence to justify which secure software maintenance methodologies would be best for an organization. Substantiate your findings with examples and data.

Assignment - Lab3 - Virus and Worm VIPRE Antivirus Internet Security

You have access to the Lab 3- Virus and Worm VIPRE Antivirus Internet Security document in assignment folder. Please following the instruction to complete the lab and provide your findings and results in your lab activities. Your lab report should be prepared in APA.

Week 12: Final Project Paper

The student will submit a final paper, that contains the same elements required of the draft paper, including modifications, as needed, and, perhaps, based on the mentor's feedback for the draft version.

Module 7—Review of Software Security: Weeks 13-14 (11/15-11/28)

Review for the Final exam, submit all assignment papers by 11/28
Submit all assignments

Final Week - Course Wrap-up (11/29-12/12)