ECE 8484: Cybersecurity Threats and Defense

Class Meetings

Sections 8484-001, 8484-DL1: Wednesday, 6:10-8:50PM, CEER 307

Instructor

Name: Dr. James Solderitsch

Office location: Tolentine Hall Rm 404

Office phone number: (610) 519-4975; Cell phone number: (484) 612-5500

Email: james.j.solderitsch@villanova.edu

Office Hours

Wednesday, 11am-12pm, Thursday, 4PM to 5PM; other times by appointment (Zoom Teleconferencing Enabled)

Course Summary

Course Description

This course provides an overview of security challenges and strategies of countermeasure in the information systems environment. Topics include definition of terms, concepts, elements, and goals incorporating industry standards and practices with a focus on confidentiality, availability, and integrity aspects of information systems.

Major Instructional Areas

1. Information systems security (ISS) fundamentals
2. ISS within the seven domains of a typical information technology (IT) infrastructure
3. Risks, threats, and vulnerabilities found in a typical IT infrastructure
4. Security countermeasures for combating risks, threats, and vulnerabilities commonly found in an IT infrastructure
5. Compliance laws and standards that affect businesses today

Course Objectives

1. Explain information systems security and its effect on people and businesses.
2. Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.
3. Explain the role of access controls in an IT infrastructure.
4. Explain the role of IT operations, administration, and security policies.
5. Explain the importance of security audits, testing, and monitoring in an IT infrastructure.

6. Describe the principles of risk management, common response techniques, and issues related to recovery of IT systems.
7. Explain how businesses apply cryptography in maintaining information security.
8. Describe networking principles and security mechanisms.
9. Apply information security standards and U.S. compliance laws to real-world applications in both the private and public sector.
10. Describe information systems security educational opportunities and professional certifications.

Additional topics to be covered include

- malware and cyber threat characteristics including advanced persistent threats (APTs)
- computer network defense
- penetration testing/ethical hacking
- commercial software packages aimed at achieving increasing levels of Cyber Security covering the areas of Data Protection and Privacy, Security Information and Event Management (SIEM), Governance, Risk and Compliance (GRC) and others
- principles of building trusted computer systems and secure applications
- security in mobile systems and social media systems
- security in web applications and systems
- security in the cloud
- identity and access management including biometrics
- next generation security concepts

There will be some programming concepts covered in the course as we look at threats and defenses, but I will not require a programming project or assignments. So, reading awareness of Java/C and even some familiarity with operating system concepts would be nice, but I will not make programming details or construction part of student submissions.

Grading Policy

Your final grade will be determined based on a percentage score out of 350 points where the points will be based on the following course activities:

Virtual Labs

- All labs required (15) – must have lab access token: acquire ASAP
- Contributions will be graded based on submitted materials as required per lab
- 10 points per lab (total points: 150)

Quizzes – 5 over the semester – use as Final Exam preparation

- 10 points per quiz (total: 50 points)
- Short answer/multiple choice or one long answer
- Questions from text material and topics covered in class or selected readings

Final Exam

- Conducted through Blackboard
    - Comprehensive over semester
    - Short answer and objective questions
- 80 points

Other

- Class Participation on Yellowdig site: 70 points

Total points for course: 350

The scale used to assign letter grades is:

Letter Grade	Numerical Grade	Letter Grade	Numerical Grade
A	94 to 100	C+	77 to 79
A-	90 to 93	C	73 to 76
B+	87 to 89	C-	70 to 72
B	83 to 86	F	Less than 70
B-	80 to 82		

Attendance

The following paragraph on attendance, along with the list of excused absences, comes from the College of Engineering and is a required element of the syllabus.

Where possible, students should inform their instructors if they plan to be late or absent from class. In all cases, students should be prepared to provide documentation to petition for *excused* absences to the appropriate Associate Dean. Absence from class does not release the student from work assigned. Students who miss an in-class obligation (exam, presentation, etc.) due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement.

The University's list of excused absences for all students includes the following:

- participation in NCAA athletic competitions
- participation in special academic events (e.g., conferences, field trips, project competitions)
- participation in official university business (e.g., student representatives attending meetings related to university governance)
- attendance at significant events involving the immediate family (e.g., funerals, weddings)
- religious holidays - see the University's policy on Religious Holidays
- college-approved participation in placement activities (e.g., job interviews, graduate school interviews, attending job fairs)
- documented serious illness or disability (see below how to document)

This course is available as both an in-class section (001) offered in CEER 307 and as a distance learning section (DL1). DL1 students are encouraged, if their schedule permits, to attend in person at the regularly scheduled class time. 001 students may elect to attend the class remotely just like the DL1 students. However, it is highly recommended that students keep up with the class on a weekly basis. If circumstances, such as a work assignment or illness, cause a student to miss the weekly class, it is expected that an email is sent to the instructor documenting the nature and length of the class disconnect. Assignments will have due dates and normally a student is expected to complete all assignments on or before the posted due date. Please review the Deadlines section later in this syllabus.

Students are expected to (virtually) attend every class. Slides used in class and saved on Blackboard may have some of the material covered, but not all or even most. Students may contribute insightful information during class that you can learn from. **You are responsible for everything covered in class, regardless of whether the material is addressed in the readings or handouts or on Blackboard.**

Course Materials

There is a text book for this course:

Fundamentals of Information Systems Security, Third Edition by David Kim and Michael Solomon, Jones and Bartlett Learning; **ISBN:** 9781284116458. The e-book is also available from: https://www.vitalsource.com/products/fundamentals-of-information-systems-security-david-kim-v9781284128567.

The text covers the basics of Information System Security. In addition, we will be reviewing on average 3-4 Cybersecurity papers/web locations a week. These resources will be posted on Blackboard and/or Yellowdig.

The Virtual Labs are from the InfoSec Security Information Security Fundamentals Lab Sequence. Information on acquiring a token to access these labs will be provided in class.

Academic Integrity

The College of Engineering is committed to creating an environment of academic integrity and ethical decision-making that we hope is reflected in the actions of our students and graduates. As Villanova students, integrity is central to the University mission. As engineers, our code of conduct requires us to place honor and integrity at the forefront of everything we do. As engineering students, it is expected that you will begin to adopt these values and instill them into your work habits. Students violating the academic integrity policy will receive a zero on that assignment or exam and the violation will be reported to the Associate Dean for Academic Affairs.

The University's academic integrity policy can be found here: https://www1.villanova.edu/villanova/provost/resources/student/policies/integrity.html.

The College of Engineering has adopted the following exam guidelines:

- Students must arrive before the start of the exam. Under exceptional circumstances a student may need to arrive late, but he/she can enter the exam no later than 5 minutes after the start of the exam.
- All cell phones must be turned off and stored away until the student exits the exam room.
- The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an exam.
- Each student must write and sign the following statement, "*I have neither given nor received any unauthorized assistance in the completion of this exam.*"

The statement given above about exam protocol is meant for in-class exams that will not be part of this course.

Don't be evil

The knowledge you gain in class is for educational purposes only. You may gain powers in this class that you are duty and honor bound not to misuse. You will promise not to scope out, attack, subvert or disrupt Villanova ECE, Villanova, corporate, county, US state or federal computer systems. US State and Federal law does not take these things lightly - prison and $10,000s of fines. Foreign students will probably lose their visa and be deported. Be careful with what you do and where and how you do it.

Students with Disabilities

It is the policy of Villanova to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability please contact me after class or during office hours to make arrangements.

If you have a non-physical disability you need to register with the Learning Support Office by contacting 610-519-5176 or at learning.support.services@villanova.edu as soon as possible. Registration is needed to receive accommodations.

The Office of Disability Services collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The ODS provides Villanova University students with physical disabilities the necessary support to successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact and register with Gregory Hannah, advisor to students with disabilities @ 610-519-3209 or visit the office on the second floor of the Connelly Center.

Schedule

The following calendar of the course is tentative. For the majority of the semester, each week's class be based on a text book chapter with one or more additional items added in as time permits. In some classes, hands-on technology demos will be covered. The class on April 8 may be canceled if there are no snow days to make up for.

DATES AND TOPICS ARE SUBJECT TO CHANGE

January 15:	Intro to Cybersecurity, Chapter 1 of text; Overview of Lab infrastructure; Lab 1
January 22:	Chapters 2, 3 of text, Cybersecurity Current Events; Lab 2
January 29:	Chapter 4, The Dark Web; Lab 3, Quiz 1
February 5:	Chapter 5, WannaCry, notPetya; Lab 4
February 12:	Chapter 6, Smart SOC; Lab 5, Quiz 2
February 19:	Chapter 9, Threat Intelligence; Lab 6 (InfoSec 15: Encryption)
February 26:	Chapter 7, Application Security; Lab 7; Lab 8 posted for Fall Break
March 11:	Chapter 8, COTS Security Tools; Lab 9, Quiz 3
March 18:	Chapter 10, Next Generation Tools; Lab 10
March 25:	Chapter 11, Cloud Security; Lab 11, Quiz 4
April 1:	Chapter 12, ICS Security; Lab 12, Lab 13 posted early
April 8:	Chapter 15, IoT Security; Lab 14, Quiz 4
April 15:	Chapters 13 and 14, Mobile Security; Lab 15 (InfoSec 6: Data Backups)
April 22:	Privacy including GDPR, Big Data Analytics and/for Security
April 29	Catch-Up; Semester Review; Final Exam posted.

Assignments

Assignments and Labs for this course will be distributed throughout the course and typically be due within 1 to 2 weeks from the class at which they are assigned. Detailed preparation and submission instructions will be provided when the assignment is made available.

Virtual Labs

A link to enroll in the InfoSec Security Labs offering will be provided in the first class. There are 15 labs in all and to some degree later labs build on the skills acquired in the earlier labs. Lab reports may be required for some labs that will include screen shots captured while you are taking the lab along with answers to questions about what you learn/discover while executing the lab instructions.

Quizzes

Material for quizzes (5 in all) will be drawn from the text book's topics as well as additional material brought to your attention throughout the semester. Recent emerging events and approaches related to cybersecurity are often made available through recorded webinars. At least one quiz will ask for your reaction and opinion after watching one of these webinars.

Final Exam

While the exam will not include a large number of questions, it will be comprehensive.

Deadlines

Submissions of exam and assignment response are done via Blackboard by midnight of the posted due or completion date. Late submission of any lab or assignment may be subject to a deduction of 2 percentage points from the grade for the late lab or assignment per business day per offense. For example, for a lab worth 10 points, 0.2 points could be deducted per day. This penalty will be deducted from the lab/assignment grade as determined by the other course requirements.

Prerequisites

None. The backgrounds of students participating in the class are expected to be quite different from one another. The lab exercises may require you to have hands-on information technology exposure that may be challenging while for others the labs border on the trivial. This course is one of the two required courses for both the MS and Certificate Program in Cybersecurity and is meant to prepare the student for later courses in the program even when ECE 8484 is not listed as an explicit pre-requisite.