Villanova University
Master of Science in Cybersecurity
Department of Electrical and Computer Engineering

ECE 8484 - Cybersecurity Threats and Defense

Spring 2021: **ECE 8484 - DL1 - Cybersecurity Threats and Defense CRN 33987**
Day: Wednesday from 6:10 pm to 8:50 pm via Zoom
Location: Distant Learning
Office Hours: by email appointment via Zoom

Prerequisite Course: none

ECE 8484 – Cybersecurity one of two core courses

Gerard J. "Gerry" Mayer
Adjunct Professor - Electrical and Computer Engineering
Villanova University
gerard.j.mayer@villanova.edu 609-828-7621
linkedin: Gerry Mayer (photo in the F-16)
linkedin VU ECE group manager - “Villanova Electrical and Computer Engineering”
- 500+ members, please join this linkedin group

General Course Information

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)
- 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
• 10 points per lab (total points: 150)

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

- 20 points per quiz (total: 100 points)
- Short answer/multiple choice
- Conducted through Blackboard
- Questions from text material and topics covered in class

Final Exam

- Conducted through Blackboard
- Comprehensive over semester
- Short answer and objective questions
- Open book exam
  • 100 points

Total points for course: 350

Course Materials

Textbook There is a required text book for this course:
Fundamentals of Information Systems Security, Third Edition by David Kim and Michael Solomon, Jones and Bartlett Learning; ISBN: 9781284116458.

This is an excellent text that matches this course and is available in new, used and ebook format from Amazon, Ebay, Google Play, and others

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.

Virtual Lab:

The Virtual Labs are from the InfoSec Lab Sequence

Our course is Information Security Fundamentals. OVESIAOLVZ

Information on acquiring a token to access these labs

Create an account > https://lab.infoseclearning.com/user/register

Open a Chrome browser and go to lab.infoseclearning.com

https://lab.infoseclearning.com/labs

https://www.youtube.com/watch?v=k7jGRU3FXPg&feature=emb_title

Spring 2021 ECE 8484 Class Schedule - 6:10 to 8:50 pm

27 Jan	Class 1 – Intro to Cybersecurity, Text Chapter 1; Lab Overview; Lab 1
03 Feb	Class 2 – Text Chapter 2, 3; Cybersecurity Current Events; Lab 2
10 Feb	Class 3 – Text Chapter 4, The Dark Web; Lab 3, Quiz 1
17 Feb	Class 4 – Text Chapter 5, WannaCry, notPetya; Lab 4
24 Feb	Class 5 – Text Chapter 6, Smart SOC; Lab 5, Quiz 2
03 Mar	Class 6 – Text Chapter 9, Threat Intelligence; Lab 6: Encryption
10 Mar	Class 7 – Text Chapter 7, Application Security; Lab 7; Lab 8
17 Mar	Class 8 – Text Chapter 8, COTS Security Tools; Lab 9, Quiz 3
24 Mar	Class 9 – Text Chapter 10, Next Generation Tools; Lab 10
31 Mar	Class 10 – Text Chapter 11, Cloud Security; Lab 11, Quiz 4
07 Apr	Class 11 – Text Chapter 12, ICS Security; Lab 12, Lab 13
14 Apr	Class 12 – Text Chapter 15, IoT Security; Lab 14, Quiz 4
21 Apr	Class 13 – Text Chapters 13 and 14, Mobile Security; Lab 15 Backups
28 Apr	Class 14 – Text Privacy including GDPR, Big Data Analytics

03 - 11 May – Final Exam

Distant Learning via Zoom

Go to Blackboard > Spr21_ECE_8484_DL1

Go to left pane > VU Zoom

Wed, Jan 27 (Recurring) 6:10 PM
Cybersecurity Threats and Defense - ECE 8484 – Lecture > Start

Office Hours via Zoom

Go to Blackboard > Spr21_ECE_8484_DL1

Go to left pane > VU Zoom

Recurring
Cybersecurity Threats and Defense - ECE 8484 - Office Hours > Start

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 before the first class. There are 15 labs in all and to some degree later labs build on the skills acquired in the earlier labs. Ignore the “capture the flag” additional Lab reports.

Quizzes

Material for quizzes (5 in all) will be drawn from the text book’s. Recent emerging events and approaches related to cybersecurity are often made available

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

No prerequisite courses required. 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 Villanova 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.

- Final exam — submitted to Blackboard before COB 11 May 2021

The sum of all activities will receive a numerical grade of 0–100. You will receive a score of 0 for any work not submitted. Your final grade in the course will be a letter grade. Letter grade equivalents for numerical grades are as follows:

A standard grade scale will be used: A: 95-100; A-: 90-94; B+: 87-89; B: 83-86; B-: 80-82; C+: 77-79; C: 73-76; C-: 70-72; F: < 70

Lectures and Attendance

You should try to view every Class : virtually (distance learning). Class slides may have most of the material covered, but not all. Students may contribute insightful information or questions via Zoom during Class that you can learn from. You are responsible for everything covered in Class , the course text or on Blackboard.

Academic Honesty

You are allowed to discuss high level issues with your fellow students, look up more on topics on the Internet, and so on. However, submitted work must be your own solution, your own words, nothing copied without attribution.

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 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.

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

Learning Support

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 http://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.