ENPM665: Cloud Security - Spring 2024

Day: Wednesday
Time: 4:00 pm – 6:40 pm
7:00 pm – 9:40 pm
Location: JMP

Instructor: Everett Daviage
edaviage+ENPM665@umd.edu

TA: Sharanya Sisodia
ssisodia+enpm665@umd.edu

When contacting the instructor please include "ENPM665" in the Subject line.

ELMS Link: https://umd.instructure.com/courses/

Course Description

Cloud computing infrastructure has become a mainstay of the IT industry, opening the possibility for on-demand, highly elastic, and infinite computing power with scalability and supporting the delivery of mission-critical secure enterprise applications and services. This course provides the ground-up coverage on the high-level concepts of cloud landscape, architectural principles, techniques, design patterns, and real-world best practices applied to Cloud service providers and consumers and delivering secure Cloud-based services. The course will describe the Cloud security architecture and explore the guiding security design principles, design patterns, industry standards, applied technologies, and addressing regulatory compliance requirements critical to designing, implementing, delivering, and managing secure cloud-based services. The course delves deep into the secure cloud architectural aspects with regards to identifying and mitigating risks, protection, and isolation of physical & logical infrastructures including compute, network and storage, comprehensive data protection at all OSI layers, end-to-end identity management & access control, monitoring and auditing processes and meeting compliance with industry and regulatory mandates. The course will leverage cloud computing security guidelines set forth by ISO, NIST, ENISA, and Cloud Security Alliance (CSA). Students will learn and develop an understanding of the following:

- Fundamentals of cloud computing architectures based on current standards, protocols, and best practices intended for delivering Cloud-based enterprise IT services and business applications.
- Identify the known threats, risks, vulnerabilities, and privacy issues associated with Cloud-based IT services.
- Understand the concepts and guiding principles for designing and implementing appropriate safeguards and countermeasures for Cloud-based IT services
- Approaches to designing cloud services that meet essential Cloud infrastructure characteristics including on-demand computing, shared resources, elasticity, and measuring usage.
- Design security architectures that assure secure isolation of physical and logical infrastructures including compute, network, and storage, comprehensive data

protection at all layers, end-to-end identity and access management, monitoring and auditing processes, and compliance with industry and regulatory mandates.

- Understand the industry security standards, regulatory mandates, audit policies, and compliance requirements for Cloud-based infrastructures.

During the course, there will be a midterm group project and a final group project. Students will also perform hands-on exercises and assignments both during class and outside of class to reinforce the lecture material. While we will primarily focus on Infrastructure-as-a-Service we will also discuss Platform-as-a-Service and Software-as-a-Service, specifically around security considerations for those services.

Learning Outcomes

After successfully completing this course you will be able to:

- Understand the similarities and differences between securing cloud-based workloads vs traditional IT.
- Develop and implement a secure migration path for a workload into the cloud.
- Understand the challenges of securing data in the cloud and the best practices to protect data in the cloud.
- Perform incident response in the cloud.

Office Hours – via Zoom link in ELMS

- Online: Monday 3-5 pm; Thursday 3-5 pm and by appointment.
- Zoom link: https://umd.zoom.us/my/edaviage
- In person: by appointment.

Required Technology:

This is a hands-on class. Students will need a computer and will need to create accounts with Amazon Web Services, Microsoft Azure, and Google Cloud Platform. The hands-on exercises will involve work that should be either no charge, within the free tiers of Amazon Web Services, Microsoft Azure, and Google Cloud Platform, or covered by the free credits these cloud vendors give new accounts. **Students should plan to set aside $50 to cover any incidental costs of running exercises in these cloud environments.**

Grading

The grade breakdown is as follows:

>>>> Insert Grading Chart Here: <<<<<

Late Assignment Policy: Assignments are expected to be submitted on time. Late assignments will have 10% of the points deducted every day the assignment is late. Assignments submitted over one week late will not be accepted or graded. If there are extenuating circumstances for you to submit work late please contact the instructor as soon as possible along with proof of your extenuating circumstance (preferably before the assignment is due.)

Religious Observances: The student must inform the instructor of any intended absences for religious observances in advance. Notice should be provided as soon as possible but no later than the end of the schedule adjustment period.

Grade Breakdown:

A+ = 100 – 99	**B+** = 89.99 – 89	**C+** = 79.99 – 79	**D+** = 69.99 – 69	**F** = 59.99 – 0
A = 98.99 – 90.01	**B** = 88.99 – 80.01	**C** = 78.99 – 70.01	**D** = 68.99 – 60.01	
A- = 90	**B-** = 80	**C-** = 70	**D-** = 60	

Extra Credit: Extra credit is not offered for this class. Do the work and you'll be fine.
Curve: There will be no curve for the class. Do the work and you'll be fine.
Rounding: There will be no rounding up/down of grades. Do the work and you'll be fine.

- **All assignments must be submitted via ELMS. Assignments submitted outside of ELMS will not be accepted or graded.**
- **Assignments are not completed until they are submitted in ELMS.**
- **The only timestamp that matters is the one in ELMS.**
- **Check that you have submitted the correct assignment after you have uploaded it.**

Grade Disputes: All grading concerns must be sent to the instructor via e-mail within 2 weeks of the grade being posted. If the instructor elects to review your assignment it will be for an exhaustive re-grade and your score for the assignment may go up or down depending on what the re-grade determines.

Questions/Troubleshooting Matrix

Support Item	Support Contact
Class administrative issues	1. Review the syllabus 2. Review the week 1 slides 3. Contact the professor
Grading concerns	Contact the professor
Technical questions	1. Google 2. Contact the TA 3. Contact the Professor
ELMS/Canvas issues	IT Support- https://itsupport.umd.edu/
Issues with lecture video capture/playback	DETS - dets-support@umd.edu

Code of Academic Integrity

The University of Maryland, College Park has a nationally recognized Code of Academic Integrity, administered by the Student Honor Council. This Code sets standards for academic integrity at Maryland for all undergraduate and graduate students. As a student, you are responsible for upholding these standards for this course. It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information on the Code of Academic Integrity of the Student Honor Council, please visit http://shc.umd.edu/SHC/HonorPledgeInformation.aspx

OPTIONAL Textbooks

This class covers a great deal of information about Cloud security technologies, so no single textbook can cover it all. Class notes will be provided for all topics covered.

- Vehent, Julien, **Securing DevOps**, Manning Publications, 2018. ISBN: 978-1617294136
- Malisow, Ben, **CCSP (ISC)2 Certified Cloud Security Professional Official Study Guide, 2nd edition** Sybex, 2019. ISBN: 978-1119603375

Course Schedule

Week 1	**Introduction & Administrivia** **Homework #1 issued** Optional reading: CCSP book chapters 1, 5 , 6
Week 2	**Securing the Cloud – IaaS, PaaS, SaaS**
Week 3	**Designing and Redesigning Secure Applications for the Cloud** **Homework #1 due** Optional reading: CCSP book chapter 7
Week 4	**Identity and Access Management for the Cloud** **Homework #2 issued** Optional reading: CCSP book chapter 7
Week 5	**Protecting Data in the Cloud** **Midterm Project issued** Optional reading: CCSP book chapters 3, 4
Week 6	**Compliance in the Cloud** **Homework #2 due** Optional reading: CCSP book chapters 10, 11
Week 7	**Deep Drive: Amazon Web Services** **Homework #3 issued**
Week 8	**NO CLASS: WORK ON YOUR MIDTERM**

Midterm Project Due TBD	
Week 9	**Deep Dive: Microsoft Azure**
Week 10	**Deep Drive: Google Cloud Platform** **Homework #3 due, Homework #4 issued**
Week 11	**Incident Response and Forensics in the Cloud**
Week 12	**Vulnerability Scanning and Penetration Testing in the Cloud** **Homework #4 due; Homework #5 and Final Project issued**
Week 13	**THANKSGIVING BREAK - NO CLASS** You should get started on your final project (if you haven’t already)
Week 14	**Deep Dive: Securing SaaS Applications** **Homework #5 due**
Week 15	**Course wrap up**