Boston University Metropolitan College

MET CS 695 Enterprise Cybersecurity

Instructor Name: Shengzhi Zhang
Email: shengzhi@bu.edu

LfA classroom: CAS-229
Office hours: Thursday 10am – 11am and 10pm- 11pm (EDT) or by appointment

Course Description

This course introduces fundamental concepts, principles of cybersecurity and their use in the development of security mechanisms and policies. Topics include basic risk assessment and management; basic legal and ethics issues, various cyber attacks, defense methods and tools; security principles, models and components; different crypto protocols, techniques and tools, including symmetric and asymmetric encryption algorithms, hashing, public key infrastructure, and how they can be used; security threats and defense to hardware, operating systems, networks and applications in modern computing environments. Hands-on labs using current tools are provided and required.

Prerequisites

MET CS 535 or MET CS 625, or with in advance permission of the instructor.

TextBook

Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, 5th Edition, Prentice hall

Learning Outcomes

At the end of the semester, students are expected to

1. Explain the fundamental concepts of the cyber security discipline.
2. Describe basic risk assessment and management.
3. Describe basic elements of a cryptographic system, and how crypto can be used.
4. Identify strengths and weaknesses, modes, implementation issues and applications of different crypto protocols, techniques and tools including symmetric and asymmetric algorithms, encryption and hashing, PKI, etc.
5. Identify potential cyber attacks, as well as cyber defense tools, methods and components to repel attacks.
6. Describe appropriate measures to be taken should a system compromise occur.

7. Properly use the vocabulary associated with cyber security
8. Explain principles of cybersecurity and how they should be applied in the development of security mechanisms and policies
9. Describe the security implications of various components in a computer system such as, hardware, OS, applications, network, and the user.
10. Describe the security implications of the emerging technologies such as mobile and IoT.

Assessments

- 3 Discussion topics
- 5 Labs
- 4 Written Assignments
- 6 Quizzes
- Final Exam

Courseware
https://learn.bu.edu/

Fall 2020 COVID-19 Policies

Classrooms on campus have new capacities that follow guidelines issued by state and local health and government authorities related to COVID-19 and physical distancing. Before the beginning of the class, and throughout the semester, I will be asking if students want to attend the classroom in-person or not. Our classroom is with the LfA capacity of 16, which is enough to hold all students.

Compliance: All students returning to campus will be required, through a digital agreement, to commit to a set of Health Commitments and Expectations including face coverings, symptom attestation, testing, contact tracing, quarantine, and isolation. The agreement makes clear that compliance is a condition of being a member of our on-campus community.

You have a critical role to play in minimizing transmission of COVID-19 within the University community, so the University is requiring that you make your own health and safety commitments. Additionally, if you will be attending this class in person, you will be asked to show your Healthway badge on your mobile device to the instructor in the classroom prior to starting class, and wear your face mask over your mouth and nose at all times. If you do not comply with these rules you will be asked to leave the classroom. If you refuse to leave the class, the instructor will inform the class that they will not proceed with instruction until you

leave the room. If you still refuse to leave the room, the instructor will dismiss the class and will contact the academic Dean's office for follow up.

Boston University is committed to offering the best learning environment for you, but to succeed, we need your help. We all must be responsible and respectful. If you do not want to follow these guidelines, you must participate in class remotely, so that you do not put your classmates or others at undue risk. We are counting on all members of our community to be courteous and collegial, whether they are with classmates and colleagues on campus, in the classroom, or engaging with us remotely, as we work together this fall semester.

Class Policies

1. **Attendance & Absences**: Attendance, either in classroom or online, is expected at all class meetings. Students with legitimate reasons who contact the professor before class begins can ask for a leave, but watching the recorded classes is required to catch up.

2. **Assignment Late Policy:** Each assignment, including lab, quiz, discussion, etc., has a deadline. All assignments are assessed a 33% per-day late penalty, up to a maximum of 3 days. No assignments will be accepted four days after the deadline. Students with legitimate reasons who contact the professor before the deadline may apply for extension. There are milestone deadlines for the final project, which is firm. A deadline miss means zero for the grade of that phase. It is the students' responsibility to keep secure backups of all assignments and project milestones.

3. **Academic Conduct Code:** Cheating and plagiarism will not be tolerated in any Metropolitan College course. They will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code: http://www.bu.edu/met/for-students/met-policies-procedures-resources/academic-conduct-code/**.**
   NOTE: [This should not be understood as a discouragement for discussing the material or your particular approach to a problem with other students in the class. On the contrary – you should share your thoughts, questions and solutions. Naturally, if you choose to work in a group, you will be expected to come up with more than one and highly original solutions rather than the same mistakes.]

4. **Grading Criteria:** The grade that a student receives in this class will be based on the class participation, quizzes, labs, discussion the project and the final exam. The grade is breakdown as below. All percentages are approximate and the instructor reserves the right to make necessary changes.
   Written assignments (20%)
   Quizzes (18%)

Lab exercises (20%)
Discussion and class participation (12%)
Proctored final exam (30%)

Letter grade/numerical grade conversion is shown below:

A (94-100)	A- (90-93)	B+ (85-89)	B (80-84)	B- (79-77)
C+ (74-76)	C (70-73)	C- (65-70)	D (60-65)	F (0 – 59)

Course Outline

(This is a tentative schedule. It is subject to change based on the class progress and students' feedback) This course is organized into six modules of about 2 lectures each.

Module 1 Introduction to Cybersecurity

Topics:

1. Basic concepts and terminology in cybersecurity
    a. Motivation to study cybersecurity, real world examples of cyberattacks.
    b. Branches of cybersecurity
    c. Basic concepts: CIA, vulnerability, threat, risk, attack, compromise, control
2. Legal issues and ethics,
3. Risk analysis and security management

Reading: Chapter 1, Chapter 10 and Chapter 11.

Module 2 Attacks and defense

Topics:

1. Malware: virus, worms, trojan horse, rootkit, zombie, bot, botnet, ransomware,
2. Bug: buffer overflow, integer overflow, TOCTTOU, covert channel
3. Security model: threat model, trust model, trusted computing base
4. Security principles and countermeasures

Reading: Chapter 3.

Module 3 Introduction to Crypto

Topics:

1. The role and property of crypto

2. Terminology: Alice, Bob, Eve, encrypt, decrypt, cryptography, cryptanalysis
3. Classical encryption: Caesar Cipher, ROTx, substitution cipher
4. Symmetric encryption: DES, AES
5. Key negotiation: DH
6. Asymmetric encryption: RSA
7. Hash: MD, MAC, HMAC
8. Blockchain and bitcoin

Reading: Chapter 2.3.

Module 4 Authentication and authorization

Topics:

1. Something you know, you are, and you have: password, biometrics, token.
2. Digital signature and Kerberos
3. Digital certificate and PKI
4. Access policy, access control matrix, access control list, capability, RBAC

Reading: Chapter 2.1 and Chapter 2.2.

Module 5 Network security and web security

Topics:

1. Threats to network: data interception, replay attack, port scanning, DoS, DDoS, MITM
2. Network defense: IPsec, VPN, Firewalls
3. Browser attacks, email attacks, misleading/malicious web content

Reading: Chapter 6 and Chapter 4.

Module 6 Cyber System Security

Topics:

1. Hardware security: meltdown, spectre, TEE.
2. Operating system security: reference monitor, layered design, security kernel, DAC, MAC.
3. Mobile security and IoT security

Reading: Chapter 5.

Boston University Metropolitan College

Course Schedule

Lectures, Readings, and Assignments subject to change, and will be announced in class as applicable within a reasonable time frame.

Class	Date	Topics	Assignment Release	Assignment Due
1	09/14	Module 1, Topic 1	Assignment 1, Lab 1	
2	09/21	Module 1, Topic 2, 3	Quiz 1 and Discussion 1	Lab 1
3	09/28	Module 2, Topic 1, 2	Lab 2	Quiz 1, Discussion 1
4	10/05	Module 2, Topic 3, 4	Assignment 2, Quiz 2	Assignment 1
5	10/13	Module 3, Topic 1, 2, 3, 4	Lab 3	Lab 2, Quiz 2
6	10/19	Module 3, Topic 5, 6, 7, 8	Quiz 3	
7	10/26	Module 4, Topic 1, 2,	Assignment 3, Discussion 2, Lab 4	Assignment 2, Lab 3, Quiz 3
8	11/02	Module 4, Topic 3, 4	Quiz 4	Discussion 2
9	11/09	Module 5, Topic 1, 2	Lab 5	Lab 4, Quiz 4
10	11/16	Module 5, Topic 3	Discussion 3, Quiz 5, Assignment 4	Assignment 3
11	11/23	Module 6, Topic 1, 2		Lab 5, Quiz 5. Discussion 3
12	11/30	Module 6, Topic 3	Quiz 6	
13	12/07	Final Review		Quiz 6, Assignment 4