Boston University Metropolitan College

Enterprise Cybersecurity

MET CS 695

Instructor Name: Shengzhi Zhang
Email: shengzhi@bu.edu
Office hours: Monday 2:30pm-4:30pm, 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.

Books

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

Courseware

https://learn.bu.edu/

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 milestones for Mini Project
- 5 Labs
- 3 Written Assignments
- 6 Quizzes
- Final Exam

BU Community COVID-19 Public Health Policies
All students returning to campus will be required to be vaccinated against COVID-19, and upload information about their status (including applications for a medical or religious exemption or an extension) to the Patient Connect portal. In addition to the vaccine requirement, students must follow all other safety protocols, including the face covering policy, and screening, contact tracing, and testing requirements.

Class Policies

1) **Attendance & Absences** – Attendance is expected at all class meetings. Students with legitimate reasons who contact the professor before class begins can ask for a leave, but studying the lecture slides and reading books are required to catch up. Missing three classes without asking for leave will fail the course.
2) **Assignment Completion & Late Work** – 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 an 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 student's responsibility to keep secure backups of all assignments and project milestones.
3) **Academic Conduct Code** – Please use the following wording, or an equivalent, in your syllabus: "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/metropolitan_college_people/student/resources/conduct/code.html.

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.]

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 (15%)
Quizzes (18%)
Lab exercises (25%)
Mini Project (12%)
Final exam (30%)

Letter grade/numerical grade conversion is shown below:

A (>= 93)	A- (90 <= and < 93)	B+ (85<= and < 90)
B (80 <= and < 85)	B- (77 <= and < 80)	C+ (74 <= and < 77)
C (70 <= and < 74)	C- (65 <= and < 70)	D (60 <= and < 65)
F (< 60)		

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.

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. Data authenticity and confidentiality

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. Virtualization and Cloud computing security
2. Mobile security and IoT security

Reading: Chapter 8, Chapter 13.1.

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	01/22	Module 1, Topic 1	Lab 1	
2	01/29	Module 1, Topic 2, 3 Project related	Quiz 1 and Project M1	Lab 1
3	02/05	Module 2, Topic 1, 2	Lab 2	Quiz 1
4	02/12	Module 2, Topic 3, 4 Module 3, Topic 1, 2, 3, 4	Quiz 2, Lab 3	Project M1
5	02/21	Module 3, Topic 5, 6, 7	Quiz 3	Quiz 2, Lab 2,

6	02/26	Module 3, Topic 8 Module 4, Topic 1	Lab 4	Lab 3, Quiz 3
7	03/04	Module 4, Topic 2, 3	Project M2	
8	03/18	Module 4, Topic 4	Quiz 4	Lab 4
9	03/25	Module 5, Topic 1, 2	Lab 5, Project M3	Quiz 4
10	04/01	Module 5, Topic 3	Quiz 5	Project M2
11	04/08	Module 6, Topic 1		Lab 5, Quiz 5
12	04/22	Module 6, Topic 2	Quiz 6	Project M3
13	04/29	Final Exam Review		Quiz 6