Boston University Metropolitan College

Network Security

MET CS 690

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

Course Description

This course is designed to provide students with a comprehensive understanding of the fundamental concepts, principles, technologies, and best practices to secure both computer networks and clouds. Topics include an overview of network threats, SSL/TLS, Kerberos, PKI, IPsec, DNSsec, SSH, Firewall, IDS, VPD, electronic mail security, wireless network security, Blockchain, TOR, Cloud architecture, an overview of cloud threats, architecture protection and data protection in Cloud, IAM, security best practice, etc. Upon the completion of the course, students are expected to know the threats and vulnerabilities that networks and cloud systems face, along with the strategies and tools used to mitigate those risks. Hands-on labs based on existing tools are provided and required.

Prerequisites

CS535(CS) /CS625 (CIS) and CS695 or CY100

Books

- *Network Security: Private Communication in a Public World, ISBN: 978-0130460196*
- *Securing the Cloud: Cloud Computer Security Techniques and Tactics, ISBN: 978-1597495929*

Other Reference Books

- *Practical Cloud Security: A Guide for Secure Design and Deployment, ISBN: 978-1492037514*
- *Computer Security: A Hands-on Approach, ISBN: 978-1548367947*
- *Introduction to Network Security: Theory and Practice, ISBN: 978-1118939482*

Courseware

https://learn.bu.edu/

Learning Outcomes

At the end of the semester, students are expected to:

1. Describe various attacks/threats against computer networks.
2. Understand the design of network protocols like IPsec, TLS, SSH, PKI, Kerberos, Shibboleth, DNSSEC, and identify their pros and cons.
3. Know different types of network defense mechanisms, design, as well as their applications, including firewall, IDS, etc., and tell their pros and cons.
4. Apply real world tools like Wireshark to capture network packets and firewall to protect internal networks from the outside.
5. Explain the demand and principles to implement anonymous communication and tell the design of TOR network.
6. Describe the fundamental concepts like characteristics, architecture, different models in cloud computing, explain the threats/attacks in cloud computing environments and the root causes of them.
7. Understand the importance of data and architecture protection in cloud computing and detail/compare best security practices.
8. Configure security policies/procedures to safeguard cloud platforms.

Assessments

- 4 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. Zoom is only used for students registering E1 section. Students registering A1 section should always attend classes in person.
2) **Assignment Completion & Late Work** – Each assignment, including lab, quiz, discussion, etc., has a deadline. All assignments are assessed a 25% per day late penalty, up to a maximum of 4 days. No assignments will be accepted five 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%)
Discussion and participation (5%)
Lab exercises (32%)
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 and network security overview

Topics:

Course introduction, review of security fundamentals

Attacks on computer networks

Deliverables:

Lab 1: Seedlab exploration

Assignment 1

Quiz 1

Module 2: Wireless security and secure communication

Topics:

Wireless security

IPsec, TLS, Secure email, SSH

Deliverables:

Lab 2: ARP cache poisoning attack

Quiz 2

Module 3: Trusted Intermediaries

Topics:

PKI, Kerberos, shibboleth

DNSSEC

Deliverables:

Assignment 2:

Discussion 1

Quiz 3

Module 4: Network perimeter security and anonymous networks

Topics:

Firewall and IDS

Anonymous network

Deliverables:

Lab 3: Firewall exploration

Discussion 2

Quiz 4

Module 5: Cloud security (1)

Topics:

Cloud characteristics, architecture, models, threats/attacks, root causes of threats, details of co-hosting problem

Deliverables:

Lab 4: Cloud security

Quiz 5

Module 6: Cloud security (2)

Topics:

- Identify access management
- Protect cloud architecture and data, security best practices

Deliverables:

- Assignment 3
- Quiz 6

Wrap up