Boston University Metropolitan College

MET CS 697 Special Topics: IoT Security

Instructor Name:	Shengzhi Zhang
Email:	shengzhi@bu.edu
LfA classroom:	CGS-423
Office hours:	Tuesday 9am – 10am and 9pm- 10pm (EDT) or by appointment

Course Description

This course overviews the emerging topics in IoT security. We discuss three major components in IoT architecture, endpoint IoT devices, mobile applications, and cloud platforms, with emphasis on the threats against them as well as countermeasures defeating the threats. For each of the three areas, we focus on the security design at the system level and platform level. The course aims to provide foundations for students to understand the vulnerabilities and defense mechanisms in those three areas. Hands on lab exercises about mobile app security analysis and firmware analysis are included.

Prerequisites

MET CS 695/595 or Instructor's consent. The students are expected to have background on security fundamentals and operating system. This course is not a programming-intensive course. However, hands-on labs will be assigned. Students can choose programing-intensive projects.

TextBook

We don't require textbook. The slides and reading documents will be posted on Blackboard.

Reference books:
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. Understand the fundamentals of system security and the tradeoff of security design
2. Know the general IoT architecture, security issues in different scenarios, and commonly-used protocols in IoT

3. Know the mobile platform architecture, understand the security issues and the security solutions used in mobile platform
4. Tell the potential threats in cloud and the challenges of building trust in cloud
5. Use tools to perform mobile app security analysis and IoT device firmware analysis
6. Present clearly the project in both the oral and written form.

Assessments

- Final project
- 2 Labs
- 5 reading assignments and discussions
- 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 12, 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.
   Reading assignments and discussions (20%)
   Labs (20%)
   Final project (25%)
   Class participation (10%)
   Final exam (25%)

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)

Module 1 Introduction

Topics:

1. Motivation to study cybersecurity, real world examples of cyberattacks.
2. Basic concepts: CIA, vulnerability, threat, risk, attack, compromise, control
3. Bug: buffer overflow, TOCTTOU, covert channel, confused deputy
4. IoT architecture: mobile apps, cloud platform and endpoint devices

Module 2 Mobile app security

Topics:

1. Permission model
2. Access control
3. Mobile platform security model
4. Advanced threats (e.g., privilege escalation, collusion attack, malicious ad library, etc.) and defense (e.g., static/dynamic analysis, isolation, etc.)

Module 3 Cloud platform security

Topics:

1. Virtualization security
2. Co-hosting threats and side channel attacks
3. Verifiable computation and Intel SGX solution

Module 4 IoT device security

Topics:

1. Firmware analysis
2. Protocols (REST, MQTT, OAuth)

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, 2		
2	09/21	Module 1, Topic 3, 4	Discussion 1	
3	09/28	Module 2, Topic 1		Discussion 1
4	10/05	Module 2, Topic 2	Discussion 2	
5	10/13	Module 2, Topic 3	Lab 1	Discussion 2
6	10/19	Module 2, Topic 4	Final project	
7	10/26	Module 3, Topic 1	Discussion 3	
8	11/02	Module 3, Topic 2, 3		Discussion 3
9	11/09	Module 4, Topic 1	Discussion 4	
10	11/16	Module 4, Topic 1	Lab 2	Discussion 4
11	11/23	Module 4, Topic 2	Discussion 5	
12	11/30	Final project presentation		Discussion 5

13	12/07	Final Review		Lab 2, final project