CS 442/642: Cybersecurity in the Internet of Things
Syllabus

Course Information

- Class room: McCormack M01-0213
- Class time: MoWeFr 12:00PM - 12:50PM
- Class websites: Check Blackboard at `https://umb.umassonline.net/`

Instructor: Dr. Xiaohui Liang

- Email: Xiaohui.Liang@umb.edu
- Office location: McCormack Hall, 3rd floor, 201-24
- Office hour: Monday & Wednesday 2:00 PM - 3:00 PM or by appointment
- Office phone number: 617-287-6791

(Optional) Suggested Textbook and Reading Materials

- Rethinking the Internet of Things: A Scalable Approach to Connecting Everything, by Francis daCosta, ISBN: 978-1-4302-5740-0, 2013
- Architecting the Internet of Things, by Dieter Uckelmann, Mark Harrison and Florian Michahelles, ISBN: 978-3-642-19157-2, 2011
- Internet of Things: Privacy & Security in a Connected World, Federal Trade Comission, 2015
- Security and the IoT ecosystem, KPMG International, 2015
- Securing the Internet of Things: Explore Security and Privacy in an Interconnected World, Hewlett Packard Enterprise, 2015

Course Description

"Internet of Things" (IoT) is an emerging technology that is changing our world with its innovative products such as "smart home", "consumer wearable", and "autonomous vehicle". This course aims to introduce the concept of IoT and its impact on our daily lives, to understand the architecture and components of IoT, and to address the challenges and solutions of deploying IoT in reality. Students will learn how to make design trade-offs between communication and computation costs and between hardware and software. In addition, cybersecurity is a critical design issue of the IoT system. From this course, students will become aware of the cybersecurity issues raised by IoT and gain the knowledge of the related security techniques. Students will also gain hands-on experiences on building IoT devices and implementing security techniques through team projects.

Topics Covered

- Sensors and actuators in IoT
- Communication and networking in IoT
- Real-time data collection in IoT
- Data analytics in IoT
- IoT applications and requirements
- Security threats and techniques in IoT
- Data trustworthiness and privacy in IoT
- Balancing utility and other design goals in IoT
- Programming IoT applications using Arduino or Raspberry Pi

Course Goals and Learning Objectives

Students successfully completing this course will:

- Understand the impact of IoT technologies
- Be able to draw the big picture of IoT ecosystem
- Be able to identify the architecture of IoT systems
- Be able to describe the essential components of IoT
- Have the knowledge of the emerging technologies of IoT
- Be able to examine the security and privacy challenges of IoT
- Be able to find appropriate security/privacy solutions for IoT
- Have hands-on experience on IoT and security projects.

Pre-requisite

CS310

Course Work

- Attendance: 5%
- Three assignments + one final project: 45% = 10% *3 + 15%
- Midterm exam: 20%
- Final exam for undergraduate students: 30%
- (Final exam (20%) and final paper (10%) for graduate students.)

Grading Scale

- 90+ = A; 87-89 = A-; 84-86 = B+; 80-83= B; 77-79 = B-; 74-76 = C+;
- 70-73 = C; 67-69= C-; 64-66 = D+; 60-63 = D; <60 = F

Grading Policies

- For assignment and project, no late submissions are accepted unless you have made prior arrangements with me.
- There will be no makeup exam for midterm and final exams.

Accommodations
This class seeks ways to become a working and evolving model of inclusion and universal design for all participants. Individuals with disabilities of any kind (including learning disabilities, ADHD, depression, health conditions), who require instructional, curricular, or test accommodations are responsible for make such needs known to the instructor as early as possible. Every effort will be made to accommodate students in a timely and confidential manner. Individuals who request accommodations must be registered with the Ross Center for Disability Services, which authorizes accommodations for students with disabilities. If applicable, students may obtain adaptation recommendations from the Ross Center for Disability Services, M-1-401, (617-287-7430), `www.rosscenter.umb.edu`. The student must present these recommendations and discuss them with each professor within a reasonable period, preferably by the end of Drop/Add period.

Student Conduct
Students are required to adhere to the University Policy on Academic Standards and Cheating, to the University Statement on Plagiarism and the Documentation of Written Work, and to the Code of Student Conduct as delineated in the catalog of Undergraduate Programs, pp. 44-45, and 48-52. The Code is available online at: `https://www.umb.edu/life_on_campus/policies/community/code`.

Additional information
My emails to the class will be sent from the Blackboard system so make sure that your email address is set up correctly with Blackboard. You should visit the Blackboard website regularly for other information including latest announcements about the class. Make sure you check your UMB e-mail address (usually firstname.lastname001@umb.edu) regularly and/or redirect it to another e-mail address you use more frequently. No excuses regarding infrequent use of this e-mail address will be accepted.

This is a face-to-face course conducted as lectures, presentations and labs. The material will be posted on Blackboard before class time. Students are expected to read class materials before coming to class. Other notes and materials are accessible from Blackboard during class.

Schedule

- Week 1:
  - Course overview
  - IoT definition, advantages, and impact (Introduction of IoT devices and discussion on the difference among IoT devices, computers, and embedded devices. How will IoT possibly change our lives?)
- Week 2:
  - IoT architecture, component and technology (Device, networking, cloud computing, and big data analysis)
  - IoT challenges (computation and communication constraints, power constraints, maintenance cost, reliability, data trustworthiness, security, and privacy); Quiz 1 on general knowledge of IoT
- Week 3:
  - Sensors and actuators in IoT (accelerometer, photoresistor, buttons, motor, LED, vibrator, analog signal vs. digital signal)
  - Lab 1: setup sensors on Arduino or Raspberry Pi and obtain sensor readings
- Week 4:
  - Networking in IoT (real-time communication and bandwidth efficiency)
  - Lab 2: setup wireless communication between IoT devices and Cloud servers
- Week 5:
  - Data analytics in IoT (simple data analyzing methods and machine learning algorithms)
  - Lab 3: analyze sensor data at computer servers and trigger an actuator's event
- Week 6:
  - Case study: discussion on specific IoT applications and their design considerations
  - Team project brainstorming
- Week 7:
  - Midterm review
  - Midterm exam
- Week 8:
  - Cybersecurity overview in IoT
  - Case study: discussion on security threats on specific IoT applications; Quiz 2 on general cybersecurity concepts in IoT
- Week 9:
  - Security threats in IoT (unauthorized access, side-channel attacks, safety risks)
  - Lab 4: implement encryption on IoT devices

- Week 10:
  - Data privacy in IoT (What and when IoT data are privacy-sensitive? Who cares?)
  - Introduction to privacy enhancing techniques including keyword search and differential privacy
- Week 11:
  - User authentication in IoT (What is user authentication? How to balance usability and security?)
  - Introduction to authentication techniques including password, biometric, proximity-based, and behavior-based techniques
- Week 12:
  - Data trustworthiness problem in IoT and some mechanisms to enhance data trustworthiness (Should we trust the IoT data? How much value the IoT data has?)
  - Quiz 3 on the introduced security techniques
- Week 13:
  - Project demonstration and evaluation
  - Course review

Sample Team Projects

1. "IoT weather station": Students will build a small IoT device that integrates with temperature sensor, light sensor and rain sensor. The device creates a website where a user is able to read temperature, light, and rain data. This project enables students to implement a small IoT system and learn how to write programs on embedded devices. Some security-related mechanisms will be implemented.
   - Hardware: NodeMcu Lua WIFI Internet Things development board based ESP8266 CP2102 Arduino
   - Sensors: Temperature sensor, light sensor and rain sensor
   - `http://www.instructables.com/id/Esay-IoT-Weather-Station-With-Multiple-Sensors/`.
2. "Home IoT system": Students will learn how to implement a voice-based home IoT system to control home appliance. In this project, students will get familiar with the latest Home IoT technology from Google, called Google Home. Google Home is a voice-activated speaker powered by the Google Assistant. Students will also learn how to do programming on Rasperry Pi device and how to connect Google Home with Rasperry Pi to implement home IoT applications. Some privacy-related mechanisms will be implemented.
   - Hardware: A Google Home and a Raspberry Pi
   - `https://www.instructables.com/id/Google-Home-Raspberry-Pi-Power-Strip/`.