CSE 708 Fall 2021: Security and Privacy in IoT

General Information

Class Schedule

- Fri 10:25am - 12:30pm, Aug 30 - Dec 10, 2021
- Davis Hall 113A

Instructor

- Marina Blanton
- Email: mblanton at buffalo.edu
- Office: 333 Davis Hall
- Office hours: TBD

Course Objectives

The objectives of this course consist of developing an in-depth understanding of the current security and privacy landscape as related to constrained connected devices and Internet of Things (IoT). The focus of the course is on learning about and discussing security and privacy violations and defense mechanisms as well as new security solutions developed for the specific properties and operating environments of IoT. The course project additionally includes a research component to demonstrate the ability to evaluate a solution, build a non-trivial security mechanism, or perform a rigorous literature review.

Course Description

This course is reading-based and provides an in-depth treatment of security and privacy weaknesses, defense mechanisms, and solutions in IoT viewed broadly.

Assignments in this course will consist of research paper reading and presentations, reviews of presented papers, a course project, and one finals assignment. The course project can take the form of implementing an existing technique, using or extending an existing tool relevant to the scope of the cource, designing a new technique or application (must properly demonstrate security-related properties), or perform a literature review. Each project can be done individually or in teams of two (non-survey projects only).

All students are expected to participate in class discussions and perform all assignments regardless of the number of credit hours they are registered for.

Grading

Grading for this course will tentatively consist of 40% for presentations, 30% for the course project, 10% for the reviews, 10% for the final assignment, and 10% for class participation. The overall performance of 70% or higher is required for getting the S grade.

Assignment Policies

- Any assignment (a paper review, project report, etc.) must be **typed** (diagrams can be hand-drawn).
- Final assignments must be done individually.
- Any external source that aided assignment preparation must be clearly referenced.
- Each review must be turned in within one week of the paper's presentation in class.

Academic Integrity

Computer science, as a profession, requires us to seek truth not only in scientific discoveries, but also in dealing with the public, as the public depends on our expertise and honesty to construct their computing infrastructure. Thus, competence and trust are essential to being a scholar and a computing professional in particular.

Your instructor will treat you as a professional, and you should plan on conducting yourself in an appropriate way. No

behavior that compromises academic honesty (such as use of someone else's work or code, using prohibited materials during tests, or making your work available to others) will be tolerated in this course. If you need assistance with anything, do not hesitate to contact the instructor.

It is expected that your work represents your own understanding of the problem. If work of others is used, it must be properly cited. Use of properly cited material is acceptable, but no referencing is treated as claiming the work as your own.

Academic dishonesty will not be tolerated in this course. It is the CSE policy that each case of academic integrity violation is recorded. The standing policy of the department is that all students involved in an academic integrity violation will receive an F grade for the course, unless the instructor recommends a lesser penalty for the first instance of academic integrity violation for the student in question.

Information about the CSE policies can be found here; UB academic integrity policies are available here; and UB graduate school guidelines can be found here.