CS6570: Secure Systems Engineering

Course Instructor : Chester Rebeiro, Assistant Professor, IIT Madras

Classes will be held from 1/Feb/2021 in Slot D.

– Monday : 11:00 - 11:50 AM

– Tuesday : 10:00 - 10:50 AM

– Wednesday : 9:00 - 9:50 AM

– Thursday: 1:00 - 1:50 PM (will be used for Lab and Tutorials)

Teaching Assistants

- Keerthi K (RISE Lab)
- Prithwish Basu Roy (RISE Lab)
- Vikash Kumar (RISE Lab)
- Ayalur Vedpuriswar Lakshmy (RISE Lab)
- Nipam Basumatary

Course Objectives

This is a 12 credit elective course that can be taken by 6-th, 7-th, 8-th semester BTech students, Dual Degree students, and MTech students. The objective of the course is to introduce students to secure systems. The course would cover the design and implementation of secure systems.

There will be three parts in the course (1) security threats and exploits in programs (2) mitigation techniques (3) detection techniques.

Learning Outcomes

- The students will be able to identify and exploit vulnerabilities in software and hardware platforms.
- Students will be able to evaluate systems for certain form of vulnerabilities.
- Students would be able to partially design software and hardware for security.

Course prerequisite(s)

None

Classroom Mode

Regular lectures 2 times a week. Assignments / tutorials will be conducted roughly once a fortnight. The course requires tutorials to be of a longer duration.

TextBooks

Research papers will be followed. These will be shared with the students during the lectures.

Course Requirements

Tutorials / Assignments

- There would be around 7 tutorials and assignments. The assignments will be given in the tutorial hour and students are expected to submit by midnight of the same day.
- Attendance will be taken and followed and requirements is as per the institute rules.

Planned Syllabus

The following is the syllabus (not necessarily in this order).

- Vulnerabilities and Exploits : buffer overflows, return-to-libc, ROPs, double frees, format string vulnerabilities, covert channels
- Mitigations : W^X, ASLR, Canaries, hardware and compiler mitigations
- Capability and sandboxing systems : SGX, Trustzone
- Embedded Security : Security in Automobiles as a case study
- Hardware Security: side-channel attacks, physically unclonable functions, hardware trojans.

Tentative Grading Policy

Mid Semester : 20 marks
Endsem : 20 marks
Assignment : 40 marks
Course Project : 20 marks

Exam Dates

- Mid Semester Exam: March 23rd, 2021
- End Semester Exam: as per schedule

Academic Honesty

Academic honesty is expected from each student participating in the course. NO sharing (willing, unwilling, knowing, unknowing) of assignment code between students, submission of downloaded code (from the Internet, Campus LAN, or anywhere else) is allowed.

Academic violations will be handled by IITM Senate Discipline and Welfare (DISCO) Committee. Typically, the first violation instance will result in ZERO marks for the corresponding component of the Course Grade and a drop of one- penalty in overall course grade. The second instance of code copying will result in a 'U' Course Grade and/or other penalties. The DISCO Committee can also impose additional penalties.

Please protect your Moodle account password. Do not share it with ANYONE. Do not share your academic disk drive space on the Campus LAN.