CSE597: Security of Emerging Technologies

Spring'21

Instructor: Syed Rafiul Hussain
Email: hussain1@psu.edu
Office Hours: T-TH 12:00pm-1:00pm
Zoom (Link on CANVAS)

Time: T-TH 10:35am-11:50am
Location: Zoom (Link on CANVAS)
Teaching Mode: Remote Synchronous

Course Webpage: https://syed-rafiul-hussain.github.io/index.php/teaching/cse597-s21/

Course Overview

In this course, we primarily study the latest research and development in analyzing the security and privacy of emerging technologies. Different security analysis techniques, including formal verification, model checking, fuzzing, dynamic and static analysis have been shown to be effective for verifying the security of the design and deployment of systems. Applying these techniques for large and complex systems, however, pose additional challenges. Advances in formal verification, programming languages, and software testing over the last several years have addressed many of these challenges and enabled wide-scale adoption of these techniques for analyzing the security and privacy properties of large and industry-scale complex systems. This course aims to lay the foundations of two key aspects: (1) current security and privacy postures of these emerging technologies, including 5G cellular systems, Internet-of-Things, and cyber-physical systems (2) how to leverage different security analysis techniques, such as formal verification, model checking, cryptographic protocol verification, and program analysis to evaluate the security and privacy guarantees provided by these systems' design and real deployments. Students satisfactorily completing the course will be able to formulate a security model for such systems, apply formal analysis techniques to assess them, and design and evaluate both clean-slate security solutions and countermeasures for them.

Topics will include vulnerabilities in network and systems, basic security principles, foundations of formal verification, static analysis, dynamic program analysis, bug finding techniques in a design, software/hardware implementations, security policy analysis, specialized analyses for specific types of security problems. We will review a combination of classic papers (to set the desired goals) and recent papers (to explore emerging techniques). The intent is not solely to explore techniques, but to build approaches in which the security of systems and networks (in particular their risks) can be precisely articulated.

A detailed list of a lecture by lecture contents, and project due dates (subject to change as semester evolves) is available on the course schedule.

Please note that the specifics of this Course Syllabus are subject to change. Even if you print this syllabus, please check the course website often. Students are expected to log in to Canvas daily, to check for course updates, announcements, emails, discussions, etc.

Reading Materials

Most of the course readings will come from research papers in the field. The list of papers including instructor- and student-proposed papers will be provided on https://syed-rafiul-hussain.github.io/index.php/teaching/cse597-s21/papers.html.

The papers for specific lectures will be posted on https://syed-rafiul-hussain.github.io/index.php/teaching/cse597-s21/schedule.html.

Grading

There are no exams or quizzes in this course! The course will be graded based on research project, paper presentation, paper reviews, and class participation in the following proportions:

50%	Research Project (including final presentation and paper write-up)
25%	Paper presentation
15%	Paper reviews
10%	Class Participation

Research Project: The main deliverable from this course will be a course project, preferrably a paper prepared for submission to a top security conference. The paper's topic must be network and system security related and the student must be a lead author. Details of the projects can be found at https://syed-rafiul-hussain.github.io/index.php/teaching/cse597-s21/projects.html.

Presentations: You will present your project and four (this number will vary depending on the class size) research papers during this class. You may use the author's slides if you prefer.

In each class, we will form two teams: a leading team and an opposition team. The leading team (includes the pre-assigned presenters of the day) will be responsible for leading the discussion and defending the paper whereas the opposition team will identify the limitations (e.g., when a proposed attack may not work or when a proposed defense is not robust enough). All students must read the assigned research papers before the class. They are also expected to actively participate in discussions during lectures and presentations, e.g., by asking questions. This is important since participation will also be assessed for grading.

More details about the presentations are posted on https://syed-rafiul-hussain.github.io/index.php/teaching/cse597-s21/presentations.html.

Paper Reviews: Understanding research papers is a key task in computer science research. Each week students will write a review (maximum 2 page) for one of the four papers assigned to that week. The review must be turned in through the online submission portal prior to the Tuesday's lecture of that week. You may follow the following review template.

Class Participation: Class participation focuses on the readings assigned for the class lecture. During the lecture, we will discuss the readings, and students are required to participate in discussions during each lecture. It is strongly suggested that students do the reading prior to this class. Ultimately, the students' ability to exhibit comprehension of readings is essential to a good grade.

Lateness Policy All milestones are assessed a 15% per-day late penalty, up to a maximum of 4 days. Unless the problem is apocalyptic, don't give me excuses. Students with legitimate reasons who contact the professor before the deadline may apply for an extension.

Communication Policy

Announcements will be made through CANVAS/Piazza and the online class discussion will occur via Piazza. Questions related to class materials, projects, assignments, and exams will occur in Piazza. The instructor or the TA will try their best to respond to questions in Piazza within 24 hours. Unless there is a strong reason, the questions should be made public to everyone so that other students can chime in and the discussion can benefit all students. For sensitive subjects (e.g., grading), email the TA and CC the instructor.

Academic Integrity Policy

Please be aware of the EECS Department's Academic Integrity Policy at ttp://www.eecs.psu.edu/students/resources/EECS-CSE-Academic-Integrity.aspx.

Students are required to follow the university guidelines on academic conduct at all times. Students failing to meet these standards will automatically receive a 'F' grade for the course. The instructor carefully monitors for instances of offenses such as plagiarism and illegal collaboration, so it is very important that students use their best possible judgement in meeting this policy. The instructor will not entertain any discussion on the discovery of an offense, and will assign the 'F' grade and refer the student to the appropriate University bodies for possible further action.

Note that students are explicitly forbidden to copy anything off the Internet (e.g., source code, text) for the purposes of completing an assignment or the final project. Also, students are forbidden from discussing or collaborating on any assignment except were explicitly allowed in writing by the instructor.

Webcam Policy

This course may require you to have a webcam for class sessions and assessments. Classes and assessments may be conducted using Zoom or other technology which may use your computer's webcam or other technologies to communicate, monitor, and/or record classes, class activities, and assessments. Assessments may also be conducted using proctoring software, which may listen to you, monitor your computer screen, view you and your surroundings, and record (including visual and audio recordings) all activity during the proctoring process. Please contact your instructor if you are unable to comply or have any questions or concerns.

Class Recording

Video and audio recordings of class lectures will be part of the classroom activity. The video and audio recording is used for educational use/purposes and only may be made available to all students presently enrolled in the class. For purposes where the recordings will be used in future class session/lectures, any

type of identifying information will be adequately removed. (See https://virusinfo.psu.edu/faq/topic/classes-and-academics-for-faculty-and-instructors).

Copyright Statement

All course materials students receive or to which students have online access are protected by copyright laws. For courses in which they have previously been or are currently enrolled, students may use course materials and make copies for their own use as needed, but unauthorized distribution and/or uploading of materials without the instructor's express permission is strictly prohibited. Policy AD 40 (Recording of Classroom Activities and Note Taking Services) addresses this issue. Students who engage in the unauthorized distribution of copyrighted materials may be held in violation of the University's Code of Conduct, and/or liable under Federal and State laws.

Ethics Statement

This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.

When in doubt, please contact the course professor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor Hussain.

Disability Accommodation Statement

Penn State welcomes students with disabilities into the University's educational programs. Every Penn State campus has an office for students with disabilities. Student Disability Resources (SDR) website provides contact information for every Penn State campus (http://equity.psu.edu/sdr/disability-coordinator). For further information, please visit Student Disability Resources website (http://equity.psu.edu/sdr/).

Counseling and Psychological Services Statement

Many students at Penn State face personal challenges or have psychological needs that may interfere with their academic progress, social development, or emotional wellbeing. The university offers a variety of confidential services to help you through difficult times, including individual and group counseling, crisis intervention, consultations, online chats, and mental health screenings. These services are provided by staff who welcome all students and embrace a philosophy respectful of clients' cultural and religious backgrounds, and sensitive to differences in race, ability, gender identity and sexual orientation.

- Counseling and Psychological Services at University Park (CAPS) (http://studentaffairs.psu.edu/counseling): 814-863-0395
- Penn State Crisis Line (24 hours/7 days/week): 877-229-6400
- Crisis Text Line (24 hours/7 days/week): Text LIONS to 741741

Educational Equity/Report Bias Statements

Penn State takes great pride to foster a diverse and inclusive environment for students, faculty, and staff. Acts of intolerance, discrimination, or harassment due to age, ancestry, color, disability, gender, gender identity, national origin, race, religious belief, sexual orientation, or veteran status are not tolerated and can be reported through Educational Equity via the Report Bias webpage (http://equity.psu.edu/reportbias/).

Wellness Days

Tuesday, 2/9 and Thursday, 3/11 have been designated as Wellness Days. No class meeting will happen, either in person or remotely, for those two days, and no assignments will be due on those days. Students are encouraged to use these days to focus on their physical and mental health. Please see wellnessdays.psu.edu for university sponsored events focusing on wellness that may be of interest to you. See Canvas and the course syllabus for any work that may be due before the next class meeting.