School of Computing

CPSC 8580: Security in Emerging Computing and Networking Systems

Fall 2020 Syllabus

Instructor: Dr. Hongxin Hu
Office: McAdams Hall 205
E-mail: hongxih@clemson.edu
Office hours: MW 9:00 AM – 11:00 AM; By Appointment

Time and Location: MW 4:00 PM – 5:15 PM, Online & McAdams Hall 114 (Note that the class will be taught fully online if circumstances deem it appropriate)

Zoom Meeting: https://clemson.zoom.us/j/97609894249?pwd=WEY5T3d6QWhZSDlINQmFFSnVPSXizUT09

Class website: http://people.cs.clemson.edu/~hongxih/teaching/2020fall/cpcs8580/2020fall.htm

Course Description: A computing and networking system is considered emerging if it recently started getting deployed in the real-world, or is deemed promising for a wide-scale deployment in the near future. The security issues surrounding such emerging systems, however, may prevent end users from utilizing their full potential, or, even worse, may rule out the chances of their deployment in the future. Currently, these emerging systems range from deep learning systems and Internet of Things (IoT) to mobile systems. In this course, we will study security challenges in these emerging systems and discuss potential solutions.
Topics:

Basic security principles:
- Authentication
- Access Control
- Network Security
- Software Security
- Cryptography

Emerging system security:
- Deep learning system security and privacy
- Deep learning for security and privacy
- Internet of Things (IoT) platform security
- Mobile platform security

Text book (Optional):

Evaluation Procedures:

<table>
<thead>
<tr>
<th>Evaluation Procedures</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper Presentation (1)</td>
<td>5%</td>
</tr>
<tr>
<td>Survey Papers (3)</td>
<td>15%</td>
</tr>
<tr>
<td>Lab Assignments (5)</td>
<td>25%</td>
</tr>
<tr>
<td>Participation</td>
<td>5%</td>
</tr>
<tr>
<td>Final Project Proposal, Presentation and Report (1)</td>
<td>50%</td>
</tr>
</tbody>
</table>

Grading: Letter Grade

<table>
<thead>
<tr>
<th>Grade</th>
<th>Score Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>90 – 100</td>
</tr>
<tr>
<td>B</td>
<td>80 – 89</td>
</tr>
<tr>
<td>C</td>
<td>70 – 79</td>
</tr>
<tr>
<td>D</td>
<td>60 – 69</td>
</tr>
<tr>
<td>F</td>
<td>0 – 59</td>
</tr>
</tbody>
</table>

Lab Assignment

The projects will involve writing programs that demonstrate important security concepts. The purpose of the projects is to connect theory with practice by giving you practical experience in emerging system security. Each project will require a substantial time commitment. The most common reason for not doing well on projects is not starting them early enough. You will be given plenty of time to complete each project. However, if you wait until the last minute to start, you may not be able to finish. Start early and plan to have it finished a few days ahead of the due date.

Many unexpected problems typically arise during programming, particularly when debugging. You should plan for these things to happen. The school computer lab will be available for project work. We
will also make an environment available for you that can be used to work on projects on your own computer. Your lack of staring early is not an excuse for turning in your project late, including having your computer crash. There are a number of sources for help. This includes office hours, and discussion groups on the class website.

**Final Project**

The project in this course has two goals. The first goal is to help you learn more about doing research in general. The second goal is to give you the opportunity to study particular areas of Security in greater detail. Therefore, you are expected to perform a substantial research project; this involves selecting an open problem, reading the related work, designing, implementing, and evaluating a solution, and presenting your results.

For your project, you need to read research paper(s) to identify a real security problem, understand the solution proposed by existing research paper(s), and provide a concrete implementation and extensive evaluation for the proposed solution. There will be three deliverables for this project which will count toward your final project grade: a project proposal (30%), class presentations (30%), and a final report (40%). You are encouraged to schedule periodic project status meetings with the instructor.

1. **Project proposal**
   Your project proposal should be around 2 pages in length. The project proposal should clearly state the goals of your project and the research question you are investigating. Describe why you think the project you are proposing is interesting and important. Your research plan should include (1) related work that shows you have enough background in the area to know that you are not simply reproducing someone else's work, (2) hypotheses about the conclusions you expect to draw from the work, (3) experimental setup which describes what experiments you plan to conduct and how you plan to do your measurements, (4) a description of hardware and software you will need for your work so that we can make sure we have it available, and (5) a detailed schedule for your work including dates, milestones, and tasks that will be done by each group member.

2. **Project presentations**
   Each group will give 3 presentations on their project in class. Proposal Presentation should be 5 minutes, with about 2 minutes for questions afterwards. Midterm Project Presentation should be 10 minutes, with about 2 minutes for questions afterwards. Final Project Presentation should be 10 minutes, with about 2 minutes for questions afterwards.

3. **Final report**
   Your final report should be roughly 6 pages in length, including graphs, diagrams, and citations. You should complete the writing early enough that you have time to reread your work and critique it with the same rigor that you applied in reviewing other papers for the course. There should be a complete description of experimental results with all support measurements and data. You should be honest and state shortcomings in your work. You should discuss future work and possible follow-on projects. In addition, there should be a description about contributions of each group member. Besides, each student will need to send TA an individual email for peer evaluations (each team member evaluates the contributions of his/her teammates) and self-evaluations (each team member documents and evaluates his/her own contributions to the team) after submitting your final report.

Please prepare your survey papers, proposal, final report using the IEEE article template: https://www.ieee.org/conferences/publishing/templates.html
**Submission**

All work will be submitted electronically. Homework and Projects are due at 11:59 PM on the due date described in the assignments. Late policy is as follows:

- 10% grade penalty for one day of lateness
- 50% grade penalty for two days of lateness
- A grade of zero for >2 days of lateness

**Academic Integrity**

As members of the Clemson University community, we have inherited Thomas Green Clemson’s vision of this institution as a “high seminary of learning.” Fundamental to this vision is a mutual commitment to truthfulness, honor, and responsibility, without which we cannot earn the trust and respect of others. Furthermore, we recognize that academic dishonesty detracts from the value of a Clemson degree. Therefore, we shall not tolerate lying, cheating, or stealing in any form. In instances where academic standards may have been compromised, Clemson University has a responsibility to respond appropriately to charges of violations of academic integrity.

**Accessibility Statement**

Clemson University values the diversity of our student body as a strength and a critical component of our dynamic community. Students with disabilities or temporary injuries/conditions may require accommodations due to barriers in the structure of facilities, course design, technology used for curricular purposes, or other campus resources. Students who experience a barrier to full access to this class should inform the professor know, and make an appointment to meet with a staff member in Student Accessibility Services as soon as possible. You can make an appointment by calling 864-656-6848, by emailing studentaccess@lists.clemson.edu, or by visiting Suite 239 in the Academic Success Center building. Appointments are strongly encouraged – drop-ins will be seen if at all possible, but there could be a significant wait due to scheduled appointments. Students who receive Academic Access Letters are strongly encouraged to request, obtain and present these to their professors as early in the semester as possible so that accommodations can be made in a timely manner. It is the student’s responsibility to follow this process each semester. You can access further information here: [http://www.clemson.edu/campus-life/campus-services/sds/](http://www.clemson.edu/campus-life/campus-services/sds/)

**Title IX Statement**

Clemson University is committed to a policy of equal opportunity for all persons and does not discriminate on the basis of race, color, religion, sex, sexual orientation, gender, pregnancy, national origin, age, disability, veteran’s status, genetic information or protected activity in employment, educational programs and activities, admissions and financial aid. This includes a prohibition against sexual harassment and sexual violence as mandated by Title IX of the Education Amendments of 1972. This policy is located at [http://www.clemson.edu/campuslife/campus-services/access/title-ix/](http://www.clemson.edu/campuslife/campus-services/access/title-ix/).

Ms. Alesia Smith is the Clemson University Title IX Coordinator, and the Executive Director of Equity Compliance. Her office is located at 110 Holtzendorff Hall, 864.656.3181 (voice) or 864.656.0899 (TDD).
**Academic Continuity Plan for this Class**

Clemson has developed an academic continuity plan for academic operations. Should University administration officially determine that the physical classroom facility is not available, class will be conducted in a virtual (online) format. The University issues official disruption notifications through email/ www/ test notification / social media. When notified, use one of the following links to navigate for Clemson Canvas, where you will find important information about how we will conduct class:

- Primary access link: www.clemson.edu/canvas
- Secondary access link, if needed: https://clemson.instructure.com/
- You can also use the Canvas Student App.