CS 4550 / 7550, Cyber Defense

Instructor: Dr. Prasad Calyam (calyamp@missouri.edu)

Lectures: Two 75-minute lecture sessions and one 2-hour lab/homework every week

Course Description: Cyber attacks are occurring at unprecedented levels on both legacy and state-of-the-art systems that are vital to our society for media, finance, manufacturing, healthcare and energy. Given that attacks are occurring in unexpected ways at different scales, the problem of cyber defense has become a critical area that uses synergies between various cyber tools, techniques and technologies. The course topics will familiarize students with intrusion detection systems; application and network attacks; security architectures; design principles; compliance standards; risk assessment and management; policy management; authentication and access control; and moving target defense. The course also will provide hands-on skills to apply cyber defense at the application and network levels. Course students will conduct experiments on the “Mizzou Cyber Range” relating to attack detection, resource adaptation as well as human/behavioral aspects. Finally, students will collaboratively survey research literature, real-world case studies and latest trends in data science, artificial intelligence, and human-centered design that are shaping next-generation cyber defense services in enterprise systems and critical infrastructures.

Prerequisite: CS 3330 or Instructor Consent


Course Topics: This course will explore the cyber security principles that will provide understanding of sophisticated cyber attacks and their defense with the related analytics, architectures, design and standards of enterprise systems and critical infrastructures (e.g., media, finance, manufacturing, healthcare and energy). Topics include:

- **Module-1) Application and Network Analysis**
  - Network and application layers – security concepts
  - Packet sniffing and spoofing
  - Intrusion detection systems
  - Legal and ethical issues

- **Module-2) Application and Network Attacks**
  - Attacks on the TCP protocol
  - Denial-of-Service attack
  - Cross-side scripting attack
  - SQL injection attack
  - Miscellaneous: Ransomware, Cryptojacking, Heartbleed bug and attack

- **Module-3) Cybersecurity Analytics**
  - Security architectures
  - Moving target defense, Defense by pretense
  - Anomaly detection
  - Threat intelligence collection
  - Penetration testing
  - Risk assessment and management

- **Module-4) Security Controls**
  - Security policies
Homeworks, Labs and Team Presentations:

There will be 4 Homeworks (1 per Module), 6 Labs (3 SEED Labs + 3 Mizzou Cyber Range Labs) and 4 Team Presentations (Problem Formulation and Area Survey; Mid-term Progress; Solution and Testbed Ideas; Final Progress) assigned during the course. Each Graduate Student will have extra work involving: one additional SEED Lab (a list of extra lab exercises will be provided) and one Final Demo Presentation.

Homework assignments will be assigned to deepen understanding of concepts in each Module. Students will perform homeworks individually. The solutions to all homework assignments will be discussed in class.

Lab exercises will be assigned to develop students’ skills and understanding for working on cyber defense tools and technologies. There will be 3 lab sessions that will focus on the “Mizzou Cyber Range” hands-on laboratory exercises and 3 other lab sessions that will focus on textbook laboratory exercises i.e., SEED Labs (Graduate students will be assigned 4 SEED Labs). Step-by-step instructions will be provided for each lab to access and use the content, and a set of questions will need to be answered as part of the lab reports, which will demonstrate good understanding of the concepts being explored in the lab steps. Students will perform labs individually.

To develop students’ programming and performance evaluation skills and to reinforce the understanding of major concepts discussed in the course, Graduate/Undergraduate Student team projects will be assigned that will require use of either Python, C/C++ or Java, as well as cloud-platform specific tools and applications. Undergraduate Student participation is optional for the project assignment. However, Undergraduate Student participation in a project will change the grading points weightage of Lab Sessions, Midterm Exam and Final Exam that count towards the final grade. Each project team will be required to submit a written report with evaluation, demo video and an oral presentation in class.

Grading:

<table>
<thead>
<tr>
<th>ASSIGNMENTS</th>
<th>CS 4550 – Project</th>
<th>CS 4550 – No Project</th>
<th>CS 7550 – Project</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homeworks</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>Lab Sessions</td>
<td>20%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Midterm Exam</td>
<td>15%</td>
<td>20%</td>
<td>15%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
<td>25%</td>
<td>20%</td>
</tr>
<tr>
<td>Project</td>
<td>20%</td>
<td>10%</td>
<td>20%</td>
</tr>
<tr>
<td>Class Attendance</td>
<td>5%</td>
<td>5%</td>
<td>5%</td>
</tr>
</tbody>
</table>
Grading Scale:

Passing grades (A/B/C) ≥ 65%; +/- grades (A+, A-, B+, B-, C+, C-)

- CS 4001 (Undergraduate):
  - A+ (97-100), A (93-96), A- (89-92)
  - B+ (85-88), B (81-84), B- (77-80)
  - C+ (73-76), C (69-72), C- (65-68)
  - D+ (60-64), D (55-59)
  - F (< 55)

- CS 7001 (Graduate):
  - A+ (97-100), A (93-96), A- (89-92)
  - B+ (85-88), B (81-84), B- (77-80)
  - C+ (73-76), C (69-72), C- (65-68)
  - F (< 65)

Academic Dishonesty: Academic integrity is fundamental to the activities and principles of a university. All members of the academic community must be confident that each person’s work has been responsibly and honorably acquired, developed, and presented. Any effort to gain an advantage not given to all students is dishonest whether or not the effort is successful. The academic community regards breaches of the academic integrity rules as extremely serious matters. Sanctions for such a breach may include academic sanctions from the instructor, including failing the course for any violation, to disciplinary sanctions ranging from probation to expulsion. When in doubt about plagiarism, paraphrasing, quoting, collaboration, or any other form of cheating, consult the course instructor. Any student found to have cheated during an exam will be given a 0 grade for that exam and the evidence will be sent to the Provost’s Office. Students submitting the same or similar solutions to homework or programming assignments will be given a 0 for the assignment and the evidence will be sent to the Provost's Office for determination of possible disciplinary action. Unless an assignment is specifically structured as a group project, duplicate homework written in collaboration with others is not acceptable. Although it is permissible to discuss the homework with others, these discussions should be of a general nature. All work at a detailed level must be done on your own. Students submitting the same or similar solutions to the homework will be considered as having cheated. No statements or actions made by anyone can alter this policy.

ADA statement: If you need accommodations because of a disability, if you have emergency medical information to share with me, or if you need special arrangements in case the building must be evacuated, please inform me immediately. Please see me privately after class, or at my office. To request academic accommodations (for example, a notetaker), students must also register with the Office of Disability Services, (http://disabilityservices.missouri.edu), S5 Memorial Union, 882-4696. It is the campus office responsible for reviewing documentation provided by students requesting academic accommodations, and for accommodations planning in cooperation with students and instructors, as needed and consistent with course requirements. For other MU resources for students with disabilities, click on “Disability Resources” on the MU homepage.

Intellectual Pluralism: The University community welcomes intellectual diversity and respects student rights. Students who have questions or concerns regarding the atmosphere in this class (including respect for diverse opinions) may contact the Departmental Chair or Divisional Director; the Director of the Office of Students Rights and Responsibilities (http://osrr.missouri.edu/) or the MU Equity Office (equity@missouri.edu; http://equity.missouri.edu/). All students will have the opportunity to submit an anonymous evaluation of the instructor(s) at the end of the course.
**Course Policy on Recording:** It is vitally important that our classroom environment promote the respectful exchange of ideas. This entails being sensitive to the views and beliefs expressed during discussions whether in class or online. Please speak with me before recording any class activity. It is a violation of University of Missouri policy to distribute such recordings without my authorization and the permission of others who are recorded.

**Decreasing the Risk of COVID-19 in Classrooms and Labs:** This course may be sometimes recorded for the sole purpose of sharing the recording with students who can’t attend class. The instructor will take care not to disclose personally identifiable information from the student education records during the recorded lesson. Compliance with these guidelines is required for all; anyone who fails to comply will be subject to the accountability process, as stated in the University’s Collected Rules and Regulations, Chapter 200 Student Code of Conduct.

If an instructor has concerns about how a student is following COVID-19 policies and protocols, he/she can report those concerns to the Office of the Dean of Students through the Form here: https://cm.maxient.com/reportingform.php?UnivofMissouriSystem&layout_id=38

*By taking the above measures, we are supporting your health and that of the whole Mizzou community. Thank you in advance for joining me and your peers in adhering to these safety measures.*