CprE 562x – Secure Software Engineering

Department of Electrical and Computer Engineering
Spring 2020

Catalog Listing: (3-0) 3 credits. Fundamentals and techniques to design and implement software systems. Assessment of security vulnerabilities in software systems, exploitation of software vulnerabilities, and methods to secure vulnerable software. Secure coding practices, data analytics for security, microservices and cloud services security. Reverse engineering and security assessment of cyber-physical systems.

Prerequisite: CprE 308 or ComS 352

Outcomes: Students will be able to:
- Assess the security in vulnerable software systems
- Exploit software vulnerabilities
- Apply methods to secure vulnerable software
- Apply best practices in secure software development
- Build effective cryptographic-based functionalities and assess their vulnerabilities
- Assess security implications for emerging software technologies

Course goals: The goal of the course is to provide students, as future software developers, with the knowledge and first-hand experience they need to develop secure software. The students will get familiar with exploiting software vulnerabilities, experiment with the techniques to design secure software and to ensure the security of developed software. In addition, they will learn to use of empirical research methods to study software security challenges.

Textbook: There is no textbook. A set of papers and chapters will be distributed.

Topics: Topics covered include the following:

1. Secure software-development life-cycle
2. Risk analysis
3. Security architecture
4. Implementing security features
5. Secure coding
6. Reverse engineering
7. Security assessment
8. Data analytics for security

Lecture: To be specified.
Instructor: Lotfi ben Othmane
Durham Hall #315
Office hours: To be specified. in Durham #315

Teaching Assistant: To be specified.

Grading: 20% Labs on software attacks
5% Report about security news
20% Assignments
20% Project
20% Research activity
15% Final exam

Mode of delivery: There will be three lecture sessions a week of 50 min each.

Assessment: The description of the assessment activities follows.

Take home labs: The students will work on four labs for three weeks each. They will get a virtual machine with pre-installed software that they can setup on their computers. They will be tasked to exploit the vulnerabilities in the pre-installed software.

Report about security news: Each pair of students will select a new announced vulnerability and present it to their colleagues

Assignments: The students will work individually on two assignments; each includes a set of practice exercises related to the course topics.

Project: The students will work in pairs on an integrative project that they choose from a set of proposed projects. Example of project topics will be assessment of the security of a given open source software and development of a set of security features for a given software.

Research activity: The students will work in pairs on a literature review for a specific software security challenge. They will write a report about their work and present the results in-class.

Final exam: The exam will evaluate the students’ knowledge.

Dishonesty: The class will follow Iowa State University’s policy on academic dishonesty. Anyone suspected of academic dishonesty will be reported to the Dean of Students Office. www.dso.iastate.edu/ja/academic/misconduct.html

Disability Accommodation: Iowa State University is committed to assuring that all educational activities are free from discrimination and harassment based on disability status. All students requesting accommodations are required to meet with staff in Student
Disability Resources (SDR) to establish eligibility. A Student Academic Accommodation Request (SAAR) form will be provided to eligible students. The provision of reasonable accommodations in this course will be arranged after timely delivery of the SAAR form to the instructor. Students are encouraged to deliver completed SAAR forms as early in the semester as possible. SDR, a unit in the Dean of Students Office, is located in room 1076, Student Services Building or online at [www.dso.iastate.edu/dr/](http://www.dso.iastate.edu/dr/). Contact SDR by e-mail at disabilityresources@iastate.edu or by phone at 515-294-7220 for additional information.

**Harassment and Discrimination:** Iowa State University strives to maintain our campus as a place of work and study for faculty, staff, and students that is free of all forms of prohibited discrimination and harassment based upon race, ethnicity, sex (including sexual assault), pregnancy, color, religion, national origin, physical or mental disability, age, marital status, sexual orientation, gender identity, genetic information, or status as a U.S. veteran. Any student who has concerns about such behavior should contact his/her instructor, Student Assistance at 515-294-1020 or email dso-sas@iastate.edu, or the Office of Equal Opportunity and Compliance at 515-294-7612.

**Religious Accommodation:** If an academic or work requirement conflicts with your religious practices and/or observances, you may request reasonable accommodations. Your request must be in writing, and your instructor or supervisor will review the request. You or your instructor may also seek assistance from the Dean of Students Office or the Office of Equal Opportunity and Compliance.

**Contact Information:** If you feel that any of your rights as a student have been violated, email academicissues@iastate.edu

Weekly topic coverage:

<table>
<thead>
<tr>
<th>Week</th>
<th>Activity</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>Lecture: Secure software-development life-cycle</td>
<td>Lab 1</td>
</tr>
<tr>
<td>Week 2</td>
<td>Lecture: Risk analysis</td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>Lecture: Risk analysis</td>
<td>Project</td>
</tr>
<tr>
<td>Week 4</td>
<td>Lecture security architecture</td>
<td>Lab 2</td>
</tr>
<tr>
<td>Week 5</td>
<td>Lecture: Implementing security features</td>
<td></td>
</tr>
<tr>
<td>Week 6</td>
<td>Lecture: Implementing security features</td>
<td>Assignment 1</td>
</tr>
<tr>
<td>Week 7</td>
<td>Lecture: Secure coding</td>
<td>Lab 3</td>
</tr>
<tr>
<td>Week 8</td>
<td>Lecture: Secure coding</td>
<td>Assignment 2</td>
</tr>
<tr>
<td>Week 9</td>
<td>Lecture: Reverse engineering</td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>Spring break</td>
<td>Lab 4</td>
</tr>
<tr>
<td>Week 11</td>
<td>Lecture: Security assessment</td>
<td></td>
</tr>
<tr>
<td>Week 12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week 13</td>
<td>Lecture: Security assessment</td>
<td></td>
</tr>
<tr>
<td>Week 14</td>
<td>Lecture: Data analytics for security</td>
<td></td>
</tr>
<tr>
<td>Week 15</td>
<td>Students presentations</td>
<td></td>
</tr>
<tr>
<td>Week 16</td>
<td></td>
<td>Final exam</td>
</tr>
</tbody>
</table>