Topics for Formal Methods for Software Development (CSE 914)  
Spring 2019

Instructor: Dr. B. Cheng, 1129 Engineering Bldg., chengb at cse dot msu dot edu

Class Time: T, Th: 12:40-2:00, 2320 Engineering Bldg;
Finals schedule: May 1, 2019; 10 am -12 pm. (to be used for project presentations)

Class web page: TBD

Required Text:
• Papers from the Literature

Grading:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Written Assignments</td>
<td>40%</td>
</tr>
<tr>
<td>Presentations and Questions</td>
<td>25%</td>
</tr>
<tr>
<td>Term Project</td>
<td>25%</td>
</tr>
<tr>
<td>In-class participation</td>
<td>10%</td>
</tr>
</tbody>
</table>

Course Scope:
Given the increasing trend towards onboard autonomous features and increasing communication between vehicles (V2V), between vehicles and infrastructure (V2I), the potential for cybersecurity threats also increases. Furthermore, the unique communication infrastructure for automotive onboard communication via the Controller Area Network (CAN) bus makes onboard control highly vulnerable to cybersecurity threats, thereby posing safety risks. The type and impact of cybersecurity threats differ in terms of the level of detailed knowledge of proprietary information and/or physical access to the device. In contrast, a denial of service attack (e.g., flooding any one of communication media used by one or more automotive subsystems) may only require limited proprietary information and no physical contact with the vehicle, while still making it possible to disrupt operation of one or more automotive subsystems to one or more vehicles. These nuances and others will be considered as the class explores the topic of software-based approaches to automotive cybersecurity.

The readings for the seminar course will explore how model-based techniques, automated analysis techniques, with particular focus on those techniques that make use of machine learning, evolutionary computation, and formal, mathematical-based techniques to address cybersecurity for automotive systems. We will also study techniques that address environmental uncertainty such as that faced by current and future automotive systems) to address the prevention, detection, and mitigation of cybersecurity threats for both new and existing automotive designs as they relate to functionality and safety requirements. Given the demand for assurance, reliability, and safety, the
cybersecurity and safety research literature will target the ADAS (advanced driver assistance systems) and connected and automated driving systems.

In particular, we are interested in techniques from disciplines outside of software engineering, such as evolutionary computation, robotics control, and machine learning to address uncertainty, assurance, and adaptation.

Course objectives:
The class will cover literature that describes research in the area of cybersecurity for automotive systems, with a particular focus on techniques that address explicitly uncertainty and safety. In addition to reading and presenting the research papers, the class will engage students in discussions regarding the current state of the art, research challenges, and promising future directions to address the challenges. Students will have opportunities to develop and/or improve their technical writing and research skills.

Format of Course:
- Lectures by instructor
- Writing assignments
- Presentations by students
- Student-led discussions regarding research challenges
- Term project