












Creative Inquiry:
Automotive Security and
Privacy (Spring 2023)
CPSC 1990/3990

Instructor Info —

-  Mert D. Pesé
-  Office Hours: None
-  215 McAdams Hall
-  <http://www.mpese.com>
-  mpese@clemson.edu

Course Info —

-  Prereq: None
-  Wed
-  4-6p
-  112A McAdams Hall

Course Description

Modern vehicles are getting increasingly connected. Together with more automotive electronics and wireless interfaces, the number of possible attack surfaces increases, raising security concerns. Attacks on cars can have multiple implications, ranging from financial incentives or damage to the compromise of human safety. In-vehicle infotainment (IVI) platforms are a major component of each passenger car. Besides car manufacturer (OEM) apps and services, the next generation of IVI platforms are expected to offer integration of third-party apps. To accommodate this trend, Google has been pushing towards standardization among proprietary IVI operating systems with their Android Automotive platform. Android Automotive will have access to the in-vehicle network (IVN), allowing read/write access from/to the IVN. This increased connectivity opens new business opportunities for both the car manufacturer as well as third-party businesses, but also introduces a new attack surface on the vehicle. Therefore, Android Automotive must have a secure system architecture to prevent any potential attacks that might compromise the security and privacy of the vehicle and the driver. In particular, malicious third-party entities could remotely compromise a vehicle's functionalities and impact the vehicle safety, causing financial and operational damage to the vehicle, as well as compromise the driver's privacy and safety. This CI project is designed to introduce students to the field of Android Automotive from a security and privacy perspective, and teach students to conduct cutting-edge research on this novel research topic. Furthermore, this course will also prepare students to understand automotive security and privacy in general, as well as open new career opportunities in automotive and security companies and academic research. The CI team will identify new vulnerabilities, learn how to write technical reports and responsible disclosures, as well as write peer-reviewed academic papers. Participation in a security workshop or conference is particularly encouraged.

(Tentative) Grading Scheme

50%	<u>CI Project</u> : Please refer to "detailed description" for the scope of this semester's focus.
40%	<u>CI Forum Poster</u> : Annual Focus on Creative Inquiry (FoCI) event
10%	<u>Meeting Attendance</u> : Weekly meetings to learn new material, discuss progress and next steps.

Required Materials

There is no official textbook for the class. Teaching material such as slides, video tutorials, research papers, etc. will be provided.

Learning Objectives

- Demonstrate critical thinking by analyzing automotive systems to determine and solve real-world automotive security and privacy problems
- Learn to summarize their findings by writing a technical report and/or responsible disclosure.

Detailed Description

This Creative Inquiry (CI) class consists of three semesters. In the inaugural semester, students will work on analyzing network traffic from Android Automotive production builds (currently Volvo, Polestar and GM). Aforementioned production builds can be emulated on the students' computer and no vehicle access is required at this stage. Students will learn how to set up the emulators, as well as the basics of the Android platform. They will learn how to interact with the Android emulator using the Android Debug Bridge (adb). Students will understand the basics of network security, including cryptography, in a hands-on way using a real system. Network tools such as Wireshark and proxies will be covered and deployed within the project. Network traffic data from OEM, Google and third-party apps and services will be collected and later analyzed to identify the privacy impact of aforementioned apps on the driver. Students will learn how to dissect and interpret large amounts of data using Python libraries such as pandas. Finally, students will assist in writing an academic paper and contributing experimental results.

Grading Policies

Letter grades are assigned according to the standard 10-point scale:

A	90-100
B	80-89
C	70-79
D	60-69
F	0-59

The final score will be rounded up, e.g., if you receive a 89.5, it will be rounded up to 90 and you will still receive an A. There will be no extra credit opportunities throughout the semester. Curving is at the discretion of the professor.

Absences

You are expected to attend every meeting unless classes have been officially canceled by the University. Attendance will be recorded at every meeting and it is used in grade calculation (see Grading Policy). Students who miss class meetings (without an official excuse, e.g. doctor's note etc.) will be dropped from the course.

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.

See the Undergraduate Academic Integrity Policy website for additional information and the current catalogue for the policy. For graduate students, see the current Graduate School Handbook for all policies and procedures.

Accessibility

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 let the instructor 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 have accommodations are strongly encouraged to request, obtain and send these to their instructors through the AIM portal 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 at the Student Accessibility website. Other information is at the university's Accessibility Portal.

The Clemson University Title IX Statement Regarding Non-Discrimination

The Clemson University 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 Title IX policy is located on the Campus Life website. Ms. Alesia Smith is the Clemson University Title IX

Clemson University aspires to create a diverse community that welcomes people of different races, cultures, ages, genders, sexual orientation, religions, socioeconomic levels, political perspectives, abilities, opinions, values and experiences.

Emergency Preparation

Emergency procedures have been posted in all buildings and on all elevators. Students should be reminded to review these procedures for their own safety. All students and employees should be familiar with guidelines from the Clemson University Police Department. Visit [here](#) for information about safety.

Clemson University is committed to providing a safe campus environment for students, faculty, staff, and visitors. As members of the community, we encourage you to take the following actions to be better prepared in case of an emergency:

1. Ensure you are signed up for emergency alerts
2. Download the Rave Guardian app to your phone
3. Learn what you can do to prepare yourself in the event of an active threat

Changes to Syllabus

Lecture topics and assignments are subject to change. The course syllabus is a general plan for the course; deviations to the class may be necessary and will be announced to class by the instructor.

Ethics and Law

To defend a system, you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy in this course is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what the law prohibits. The EFF provides helpful advice on vulnerability reporting and other legal matters.