Executive Summary

An advanced automotive environment may consist of one or more vehicles with the ability to connect to the Internet. If more than one of these vehicles is present, there is the possibility to create a car-to-car network. Due to the fact that vehicle networks are still in the prototype phase, the focus of this paper will be on the individual vehicle. However, car-to-car networks will be considered in the future research section.

Throughout this paper, an analysis of emerging automotive technology, as well the accompanying risks will be presented. The main points of entry into the vehicle (the telematics system, OBD-II, door locks, key fob, MP3 malware, and unauthorized apps) will be discussed as well as what can be done to defend against attack at each location.

The paper will also evaluate quality of service concerns, user interface issues, as well as driver distraction. The mechanics of vehicular encryption techniques will be analyzed and evaluated. Additionally, the basics of data confidentiality, availability, and integrity will be discussed.

Following, will be an assessment of the future direction of in-car communications along with emerging vulnerabilities. The paper will close with suggestions to automotive manufacturers as well as practical advice for the secure operation of their vehicle.