Background and Problem

- We are moving towards an era of smart and autonomous vehicles. Which will be highly network centric and will remove the human out of the vehicle control loop.
- This is compounded by the fact that over the last decade, the attack sophistication has increased while the attack complexity has decreased. Thus allowing novice attackers to execute highly sophisticated attacks.
- Thus these vehicles move towards autonomous and self driving nature, it will be increasingly important to ensure that they are secure against cyber attacks.

Objectives

- Design a framework that will enable securing the autonomous car environment against cyber - attacks.
- Identify threats for the different subsystems and develop threat models.
- Develop micro Intrusion Detection Systems (mIDS) for each of the sub-systems to target the threat model.
- Integrate the designed systems with the Qualcomm S820amv2 Automotive development platform

Approach

- The mIDS designed to secure the different sub systems of the smart car, use anomaly based behavior analysis approach (ABA) to find the abnormal behavior of the system.
- The normal behavior of the system is used to train machine learning models to identify the normal behavior of the system. Thus allowing us to identify the abnormal behavior.

Current Work

- We have developed the framework to secure the autinfotainment system.
- We have developed threat models for different sub systems like Wi-Fi, Bluetooth, Camera, LTE, Lidar etc.
- We have developed mIDS’ for the Wi-Fi and Bluetooth environments, and are working on development of the mIDS for the camera system.
- We are deploying the IDS’ on the S820am v2 ADP which being an android based system requires building applications around the NDK based IDS.