Titre : Onboard AI for cybersecurity in connected cars

Supervisors :

Van-Tam Nguyen (van-tam.nguyen@telecom-paris.fr)

Summary:

This internship will focus on anomaly detection on CAN, especially on-board Ethernet networks, and on adapting the envelope model in line with updates to the car's software. What mechanism should be put in place to ensure that new applications or software updates are not taken as malware by the envelope model?

The adaptation or re-training of the model to adapt to changes in vehicle architecture when new vehicle phases or variations are released will also be studied. The strategy to be adopted with regard to adaptation or retraining when new attacks are discovered will also be investigated.

Description:

Vehicles are increasingly connected in a complex, multi-player and diversified connectivity ecosystem (cellular, Wifi, BT, V2X). They are equipped with increasingly advanced driver assistance systems (ADAS), which will eventually take the driver's hands off the wheel and his or her eyes off the road, giving the car autonomy in defined mission conditions (type of road, speed, etc.).

It will therefore become increasingly important to equip the car with attack detection and reaction capabilities to increase its resilience and keep the vehicle and its systems in an acceptable functional mode until the systems return to their nominal mode.

The vehicle's reaction must be proportionate to the type of attack, and in the case of certain attacks associated with assisted driving situations, the reaction must be close to real time. The aim is to ensure that the alert sent back by the car's sensors is a true positive and not a false positive, at the risk of applying an inappropriate remedy.

The research theme will therefore focus on using advanced ML to create a behavioral envelope model in nominal mode of the E/E architecture and software carried by the flows on the intra-vehicular network, and to consider that all behaviors outside this envelope will be indicative of attacks.

It will be important to define the boundary conditions of this model, with a possible zone of uncertainty that can be quantified in order to control the false positive rate.

The data needed to build the model can be captured in the vehicle during its proto running phases, and the model can be built with adequate off-board resources. On the other hand, when the model is in use (inference), it will have to be on-board the vehicle to enable detection and reaction in the shortest possible time.

The application of this internship will focus on anomaly detection on CAN and especially on-board Ethernet networks.

A second stage of the study will focus on adapting the envelope model in line with updates to the car's software (downloading of new applications, system upgrades, etc.). What mechanism should be put in place to ensure that new applications or software updates are not taken as malware by the envelope model?

The adaptation or re-training of the model to adapt to changes in vehicle architecture when new vehicle phases or variations are released will also be studied. The strategy to be adopted with regard to adaptation or retraining when new attacks are discovered will also be part of the scope.