

Titre : ML/AI for cybersecurity of Software Defined Vehicles

Supervisors :

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

Summary:

New vehicle architectures are of the Software Defined Vehicle type. There are fewer ECUs and less inter-ECU communication. We have more powerful ECUs equipped with VM (Virtual Machine), HPC (High performance computing), and Linux based OS. Detection based on observation of messages exchanged between ECUs may have to replace observation of Linux process behavior.

The internship will begin with a study of attacks carried out by ethical hackers to determine the relevance of the type of data to be processed.

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.

New vehicle architectures are of the SDV (Software Defined Vehicle) type. There are fewer ECUs and less inter-ECU communication. We have more powerful ECUs equipped with VM (Virtual Machine), HPC (High performance computing), and Linux based OS.

Detection based on observation of messages exchanged between ECUs may have to replace observation of Linux process behavior. The internship will begin with a study of attacks carried out by ethical hackers to determine the relevance of the type of data to be processed.

The large amount of information will be processed by ML/AI. In the SDV model, AI may no longer process raw data (inter-computer messaging), but rather detections (memory violations, system calls, IO monitoring). This detection data will be available on condition that Linux process monitoring probes have been developed and prototyped beforehand.

ML/AI processing will have to meet two objectives:

- Firstly, to provide a constant, controlled stream to Offboard, in order to supply the AI in the cloud with the data it needs to monitor the vehicle.
- Secondly, to provide detection with zero false positives, with the aim of triggering a reaction from the autonomous vehicle. The triggering of the reaction could be conditioned by formal rules.

The definition of the embedded system will have to take into account the following constraints