Résumé d'anglais

Arnaud Vinsard
CEA-Grenoble

Sujet de stage :
Outils de découverte protocolaire basée sur les algorithmes génétiques

My intership takes place at CEA in a laboratory in the city of Grenoble. The main goal is to implement a tool to discover unknown communication protocol using algorithm genetic. The second goal is to study if the genetic algorithm is the best way to evaluate ECU's security. ECU are the Electronic Control Unit which control several electronic component in car. Indeed, it is possible to hack a car to remove the immobilizer, locking doors or to change the behavior of each electronic component. There is what will be trying to reproduce.

The biggest part of my intership is the implement of the genetic algorithm in the code of existing software : Peach Fuzzer. For this, we implemented many plugin like publisher, monitor and mutator. This software use fuzzing method. Fuzzing is an approach to software testing whereby the system being tested (ECU) is bombarded with test cases generated by a another program (Peach fuzzer). The program is then monitored, in the hope of finding errors that arise as a result of processing this input.

My intership was oriented more research than industrial. It's biggest different than I have worked before. It's possible to conclue that this method is not to adapt our system being tested.
For the moment (because I haven't finish my intership), we have discovered all the command of the ECU, but we have tested only one communication protocol. To obtain best result, we should test other systems and other communication protocol.

I have been satisfied to do my intership at CEA because I have worked in a laboratory about security with a dozen employees. It likes a small company with the advantage of big one.

Fuzzing, security, algorithm genetic.