Towards Designing Secure In-Vehicle Network Architectures Using Community Detection Algorithms

Nasser Nowdehi (nasser.nowdehi@volvocars.com)

Efforts in securing the in-vehicle network have resulted in a number of proposed security mechanisms in recent years. However, so far little attention has been given to the actual architecture of the in-vehicle network. An approach within in-vehicle network design is to divide the network into domains, where each domain consists of a set of Electronic Control Units (ECUs) that handles some united functionality, e.g., body control, powertrain, and telematics. The identification of good domains can facilitate the implementation of security measures. However, as far as we are aware of, there are no existing tools that do this domain partitioning in an automated and optimal way and the current approach is based on "best engineering practice".

In our research [1], we study real traffic from a modern car and we try to divide the in-vehicle network into domains using automated partitioning algorithms. The aim is to show that community detection algorithms can be used to identify in-vehicle domains based on different selection criteria such as message types, payload sizes, or Automotive Safety Integrity Levels (ASILs). Also, we analyse the improvements gained by our approach with respect to communication, safety and security when compared to EVITA architecture that is a well-known in-vehicle reference architecture (The results are not yet published). We believe that our approach has great potential to help engineers in deriving secure in-vehicle network architectures during the design of a vehicle.

This research has been done by me and Pierre Kleberger and under supervision of Tomas Olovsson.

References

[1] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7013311