Prof. Dr. Dominik Schoop

Challenges in Automotive Security

A modern road vehicle is a complex distributed system, in which many Electronic Control Units (ECUs) are interconnected by dedicated bus systems. Furthermore, this distributed system is interconnected, often over wireless networks, to other external distributed systems to provide efficient diagnosis, comfort functions for the vehicle owner or co-operative safety functions in the context of vehicle-to-X communication (V2X). A modern road vehicle, therefore, exposes several communication interfaces to the outside world, which could be the target of attackers who want to influence the behaviour of vehicles and could cause accidents in the worst case. Consequently, the security of vehicles has direct impact on their safety. While in current road vehicles, the driver controls the vehicle and, therefore, can react to unexpected events and the dynamics of the vehicle, autonomous road vehicles rely heavily on their sensory input, which might be the target of attacks. Autonomous vehicles have to handle every situation safely, even in the case they are fed manipulated sensory input.

The talk presents the security challenges that arise from the exposure of communication interfaces and sensors of modern (autonomous) vehicles and discusses possible solutions.