Tutorial: Intrusion Detection and Prevention Systems for Automotive

Abstract:
Todays' vehicles are increasingly networked computer systems with a broad range of functionality. Ever since, the primary design goal of vehicles has been reliability and, thus, safety. With the advent of networked electronic control units, reliability only can be achieved with safety and security. Remote access to vehicles bears the risk of manipulations with catastrophic impact on the safety. As a consequence, it is imperative to apply modern cryptographic mechanisms to increase the vehicle's security. ‚Security by design' is a widely used design principle and ensures that security is applied in a meaningful manner from the early beginning of the design phase. However, unlike smart phones or computers, vehicles are intended to run for far more than just a few years. During the life cycle of vehicles, new weaknesses of, e.g., software stacks might become public and new forms of attacks might threaten the vehicular system once deployed on the road. As a consequence, risks have to be re-evaluated and corresponding security mechanisms have to be adopted in a regular manner after production. In such a scenario it is imperative to allow security to be changed and updated within the life cycle of a vehicle. In contrast to conventional computer systems, safety-critical environments cannot wait until patches are approved and deployed. Attacks have to be detected immediately and the risk of security breaches 'on the road' has to be reduced.
With a similar intention, Intrusion Detection and Prevention Systems (IDPS) have been introduced for conventional IT systems decades ago. Translating the concept of IDPS to vehicular systems is promising since it offers the possibility to monitor and safeguard vehicles w.r.t. unknown attacks. Gathering information about new potential threats and reducing the impact of new attacks on vehicles will be of major importance in the future.
In this tutorial, we will introduce to ID(P)S and basic concepts. Moreover we will discuss automotive security and the inherit challenges of IDPS within the automotive domain.