Abstract

The driving assistance softwares become more important and widespread nowadays. For example the lane assist systems, that prevents the lane changes without the persmission of the driver.

Since the developers make new software changes very frequently, the companies have to reach the on board computer in their cars to change something in the software when an update is required.

Because of the large amount of vehicles, and because of the frequent updates it would be a very big problem for users and the services to handle all these software updates. To avoid this problem the companies has to reach the vehicles through the internet. Although this solution has other weaknesses. The internet connection is not secure and the connection can be attacked. To encounter this problem the cars must have a software component which is responsible for the security of the connection. This software has to run security checks before installing the software updates.

A working solution is based on cryptography. Whenever someone try to reach the car through the internet it has to provide a certificate, which will be verified by the car's software. The car must have trusted certificates and the verification process will use these certificates to make sure that the software updates are safe. Since digital signatures are used to make certifications, the cryptography is very important in this field.