UPCOMING TRENDS IN THE AUTOMOTIVE IT AND ASSOCIATED SECURITY CHALLENGES

André Groll, Jan Holle, Christoph Ruland
University of Siegen, Germany
{andre.groll, jan.holle, christoph.ruland}@uni-siegen.de

Abstract. The following article wants to give an overview of the essential upcoming trends in the automotive IT, often summarized as ITS (Intelligent Transport Systems). Since most of the upcoming trends are not be deployed until know, a use case driven approach will be used to illustrate the benefits and requirements of this kind of novel applications. The main focus of this work is the description of challenges regarding future vehicles in terms of IT security due to their strong impact on road safety which is often condensed to the slogan "Safety by Security". Hence, the security challenges will be evaluated and – where possible – a rough outlook towards possible countermeasures will be given. The conclusion summarizes the work and provides recommendations and information on further research work and some references to already started research projects which will lead to suitable countermeasures on the security challenges.

Keywords: ITS, Automotive Security, V2V, V2I, Automotive IT

I. Introduction

Modern vehicles are an integral part of the daily life in industrial nations, e.g., in 2005 more than 170 million cars were registered in the European Union [5]. Besides the use of cars for individual transport of citizen, commercial road vehicles are an inherent part of flexible logistic chains and an additional load to the road networks. With respect to the amount of vehicles and the vehicle miles travelled per year there are two main goals for the use of vehicles and the operation of the road networks: For one thing the number of fatalities and injuries on the road has to be reduced in order to provide safety, for another thing the use of vehicles should be as efficient as possible with regard to the emission of CO2, consumption of fossil fuels and the use of road infrastructure. The development and deployment of ITS (Intelligent Transportation Systems) and innovative automotive applications will help to achieve these goals while also enhancing the convenience for drivers and passengers in road transport.

Obviously ITS and innovative automotive applications are only feasible if they are implemented in a reliable manner since they have strong impact on the vehicle safety. Unfortunately, the

aspect of IT security is often neglected within the development process of such kinds of applications, which leads to weak and unsecure and hence safety jeopardizing systems.

In this paper we briefly outline some upcoming trends for ITS and innovative automotive applications and their inherent security challenges that could impede the successful deployment respectively causing hazards in road transport if deployment is taking place before solving the security issues.

II. Upcoming Trends in the Automotive IT

The biggest anticipated innovation in the automotive IT in the next decade will be probably the availability of DSRC (Digital Short Range Communication) capabilities for vehicles. This new technology that uses the 5.9GHz band (at least in Europe) [9] will offer the opportunity to build ad hoc connections between vehicles, termed V2V (Vehicle to Vehicle) communication, as well as between vehicles and the infrastructure, named V2I (Vehicle to Infrastructure) communication. **Figure 1** shows an overview of the proposed communication architecture according to the Basic Set of Applications (BAS) for ITS specified by the European Telecommunications Standards Institute (ETSI).

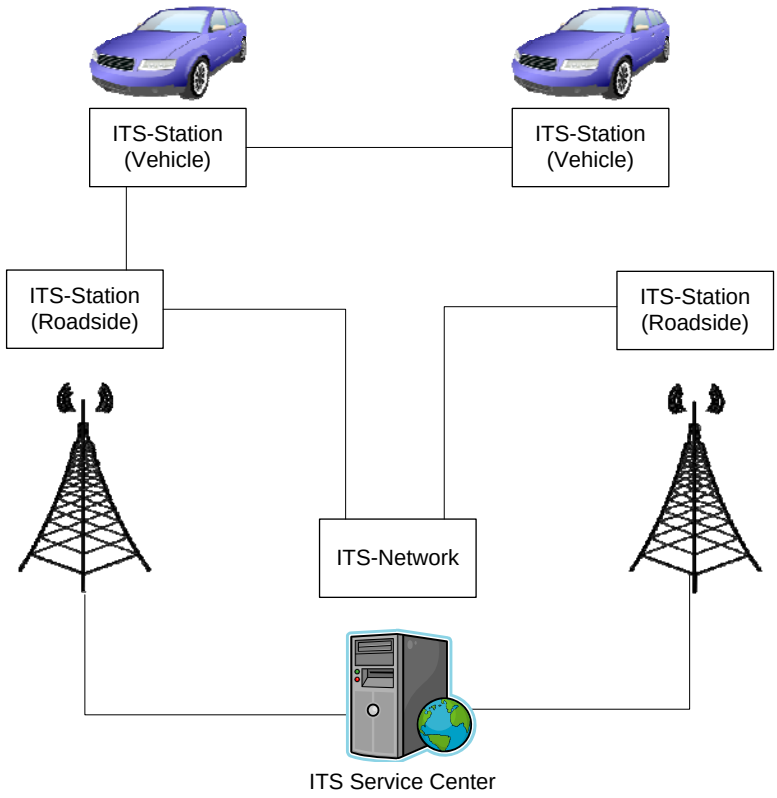

Figure 1 Simplified view of the ITS environment (according to [6])

The new communication capabilities will lead to a wide range of new ITS applications helping to improve both safety and efficiency in road transport. Some exemplary foreseen use cases (e.g., described in the Basic set of ITS applications [6]) will be:

Road hazard and traffic warnings (V2V) will be achieved by the transmission of cooperative awareness messages publishing among others the current position and direction of a vehicle and decentralized environmental notification messages that will be transmitted on specified events, e.g., an accident. This messages help to extend the awareness range of drivers beyond the line of sight (e.g., providing information on a traffic jam beyond the next hill) and hence will be able to improve road safety.

Emergency vehicle preemption (V2V) will be an application to inform drivers about an approaching emergency vehicle being on duty to request a reaction, e.g., stopping at the roadside or stopping in front of a green traffic light if an emergency vehicle crossing an intersection. This application will have a strong impact on road safety and especially the safe and fast arrival of emergency services.

Dynamic Traffic management (V2I) is one of the most promising ITS technologies to improve the efficiency of road transport. The idea is to reroute and control the traffic flow based on precise information of the traffic situation. This information will be derived from the awareness messages received by RSUs (Road Side Units) and analyzed within a traffic management center). Dynamic traffic management will be beneficial not only in terms of efficiency but also in terms of reducing of CO2 emissions and fuel consumption.

Cooperative road condition monitoring (V2I) will be an application which will reuse already known information concerning the road surface condition to improve road safety for all traffic participants. Modern vehicles are equipped with a great amount of high-class sensors for road surface and weather condition (e.g., rain-sensing wipers). Collecting and analyzing this information in a traffic management center will lead to a precise picture of the current road surface condition situation and hence can be used to trigger suitable measures (e.g., setting speed limits by using dynamic traffic signs).

Independent from the upcoming ITS applications, which will be mainly driven by the widespread availability of V2V communication there is at least one other trend in the automotive industry, which will influence the progress in the next decade: The demand for an open platform for automotive applications. The idea of an open platform for vehicles is to offer a platform for vehicle independent plug & play applications (e.g., multimedia applications using the vehicle internal equipment). Furthermore an open platform can lead to a reduction of the amount of ECUs (Electronic Control Units) necessary to execute upcoming innovative automotive applications by the

shared use of only one powerful ECU (leads to a reduction of costs and weight and hence to more vehicle efficiency). This trend will also involve the secure integration of nomadic devices (e.g., mobile phones or multimedia players) into vehicle systems.

III. Security Challenges

The new trends and the development towards an "open car" as described in section II requires the consideration of automotive security, which is getting more and more important, because modern vehicles need and have access to several internal and external networks to provide their functionality and enable the mentioned new applications. In future vehicles with some nomadic devices and a broad range of third party applications, it is very important to secure these systems and the new services against random failures and malicious attacks. In particular, functionality with direct impact on the behavior of the vehicle – and therefore on road safety – need to be secured by IT security services in order to prevent bad consequences from these (malicious) faults (just consider a manipulation of the Electronic Stability Program). But even attacks that may origin from the vehicle components because of malicious code or faulty ECUs should be prevented in order to protect other entities.

Common security approaches known from the world of desktop computers can not be ported to the automotive domain directly, because of strong limitations regarding computational power of single ECUs (Electronic Control Units) and the necessity to process information in real-time. Additionally, there are different communication forms ranging from broadcast for onboard networks to ad-hoc networks for V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communication. To meet these challenges with respect to an open platform and the listed requirements, the following security objectives and challenges should be considered in modern automotive IT architectures:

In the following we describe the most important challenges in the area of automotive security. As a result of a security analysis, the most problems arise because of missing authentication and confidentiality in the automotive communication. For example, faked information regarding the road condition or a wrong signal preemption of emergency vehicles may have direct impact on road safety. Therefore, the enhancement of existing protocols with the security services authentication, confidentiality together with secure key and policy management are one of the main issues that have to be solved in the next years. To protect cryptographic credentials it seems to be mandatory to build solutions on basis of a tamper-proofed hardware.

Since the aim of most attacks would be the access to the onboard IT system of the car, where an attacker may be able to harm applications, send fake messages or eavesdrop sensitive informa-

tion (e.g., address book of the driver), as a first step it is important to provide a single point of access – maybe located at the central gateway – to the onboard system that can not be bypassed to enforce security policies. The control of any connection to the car also includes the onboard diagnostics (OBD) that can be used for physical attacks and nomadic devices which may be used to channel in malicious code into the vehicle. This can be done by implementing a firewall that filters all unauthorized access to the interfaces depending on user or manufacturer rules. Besides this prevention of common attack methods, car manufacturers started research work on intrusion detection systems that detect abnormal systems states and raise an alarm [4]. These central mechanisms are also able to supervise different ECUs and applications not to harm each other (especially when multiple applications are executed on a single hardware module).

Next to the protection of in-vehicle networks, we believe that security enhancement of V2V and V2I technologies and applications using these technologies are an important challenge in the following years. Besides the transmission of information concerning the road condition, etc., there are first efforts to use these interfaces for remote control of the car and remote flashing of ECUs [1,2]. Since the data sent from and to the car may have impact on its behavior and road safety, mechanisms to enable each participant to verify the authenticity and identity of messages and communication entities should be considered. This also includes that hazard warnings and other exchanged messages are correct and not out of date because of replay attacks.

Currently, the main focus should be on authentication services, but as a next step the confidentiality of communications becomes more and more important since modern vehicles may transmit the current location, navigation routes, address book information, etc. over internal as well as external networks and thus may be eavesdropped by attackers. In the medium term we see these privacy issues as a subject.

IV. Conclusion

In the present article we showed a selection of upcoming and IT related trends in the automotive domain. In addition to the new and useful functionalities as well as the gain of comfort for the driver it is important to recognize the possible security issues that come along with these new technologies. We described the most important security challenges in this field and directions for countermeasures. Fortunately, research institutes and car manufactures already started projects to meet these new challenges, e.g., in the EVITA project [7] for a secure onboard communication and the OVERSEE project [8] for a secure single point of access with secure interfaces to the outside world and runtime environments where different applications are isolated.

V. References

1. Spehr, Michael. BMW Connected Drive – Fahrer, Auto und Umgebung vernetzen. In: Frankfurter Allgemeine Zeitung vom 18.03.2008, page T4.
2. Viehmann, Sebastian. BMW ConnectedDrive – Big Bayer is watching you. http://www.sueddeutsche.de/automobil/artikel/ 734/168248/.
3. Grell, Detlef. Computer im Auto, Rad am Draht – Innovationslawine in der Autotechnik. In: c't 14/2003, S. 170.
4. Müter, M.; Groll, A.: Attack Detection for In-Vehicle Networks. In: Proceedings of the 25. VDI/VW conference on 'Automotive Security', Ingolstadt, 2009.
5. Eurostat website. http://epp.eurostat.ec.europa.eu
6. European Telecommunications Standards Institute (ETSI). Intelligent Transport Systems (ITS) Vehicular Communications Basic Set of Applications Definitions. TR 102 638
7. EVITA project website. http://www.evita-project.org
8. OVERSEE project website. http://www.oversee-project.com
9. European Telecommunications Standards Institute (ETSI). Intelligent Transport Systems (ITS); radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive. ETSI EN 302 571 (V1.1.1)
10. COMeSafety. European ITS communication architecture - overall framework proof of concept implementation (V.2.0).
11. M. Gerlach, H. Rechner, and T. Leinmüller. Security Framework for Vehicular Applications. In O. Altintas and W. Chen, editors, Proceedings of Third International Workshop on Vehicle-to-Vehicle Communications (V2VCOM), Istanbul, Turkey, June 2007.
12. Groll, A. Gefahren der In-Fahrzeug-Kommunikation moderner Automobile. In: Proceedings of the 11th German IT Security congress, SecuMedia Verlag.
13. Andre Weimerskirch, Christof Paar, and Marko Wolf. Secure In-Vehicle Communication. Chapter in "Embedded Security in Cars", Springer-Verlag, 2006.