Security issues in vehicular systems: threats, emerging solutions and standards

Hendrik Schweppe (hendrik.schweppe@eurecom.fr)*
Yves Roudier (yves.roudier@eurecom.fr) *

Abstract: This extended abstract aims at giving a comprehensive overview of the state of the art of information and network security in vehicular systems today and of future development.

Current research topics, which in particular focus on enabling e-safety services are covered. In the near future, safety services and applications will be deployed in vehicles as well as at roadside infrastructure, as for example envisaged by the Car-to-Car Communication Consortium or ETSI.

Such applications motivate new attacks. Without security, false alerts can be created and attackers may exploit safety applications for their benefit, thus endangering the safety of drivers. Examples of successful attacks are shown to illustrate the need for security.

In order to provide a trusted base for inter-vehicle communication, a secure on-board communication for vehicles is crucial. In the EU project EVITA a trusted in-vehicle environment is developed based on a trusted platform and means of secure communication. Furthermore, the research landscape is discussed, in particular relating to industrial research projects, such as field operational tests, as well an overview about the current state of standardization. An outlook on future research and industrial activities concludes the extended abstract.

Keywords: automotive, security, embedded systems, V2X, VANET, trusted platforms

1 Introduction

Vehicles have traditionally been a mechanical domain. In recent decades, this changed drastically. Starting with electronic engine management in the 70s, vehicles have evolved to a multi-connected computerized platform. At the same time, safety systems - not only mechanical but also electronic systems (electronic stability, anti-lock brakes) have been introduced with great success. Vehicle-to-vehicle systems will take a first step towards autonomous driving, despite the fact it is not yet realistic (although recent DARPA challenges show the feasibility [MBB$^+$08, TMD$^+$06]). As a first step, vehicles will dispose of information provided by road side units (RSUs) and will be aware of each other, thus being able to warn the driver of upcoming dangers early and adequately.

Attacks The current in-vehicle network architecture, which is used to exchange data between control units (ECU, Electronic Control Unit), has grown historically. There has not yet been the need to secure buses, as they were not connected from the user domain or the outside of the vehicle. However, attacks on vehicle bus systems show the

* EURECOM, 2229 route des crêtes, BP 193 , 06560 Sophia-Antipolis cedex
Tel. : +33 4 93 00 81 00 - Fax : +33 4 93 00 82 00

severe impact an attack may have [KCR+10]. Similar experiments have been conducted earlier by [HKD08]. The roadside infrastructure already in place today, namely the TMC system [TMC] for traffic management and tolling systems, has been target to successful attack experiments. In 2007, Barisani and Bianco showed how TMC over RDS may be manipulated with limited effort [BB07]. In 2008, Nate Lawson demonstrated weaknesses of the California FasTrak tolling system [Law08]. Both attacks were based on reverse engineering and revealed that no cryptographic security was present in the systems.

2 Vehicle Security

After the first cooperative vehicle-to-vehicle communication systems were successfully tested [FFH+04], the need for certain security has become evident, as attacks on safety functions may possibly be fatal. The SeVeCOM project took up this need and conducted several experiments. It turned out that certificates, that are needed for communication partners to authenticate remote vehicles, caused the main overhead. Thus, the choice of cryptography fell to ECC, which features a small key size but offers the same security level as RSA using longer keys[LBH+06]. There has been some research on the optimization of radio channel usage, e.g., by intelligently omitting certificate data if possible[Pap09].

In-Vehicle Security Although it is mentioned in many preceding projects that in-vehicle security systems must eventually establish the necessary trust for cooperative applications [Kun08, EB06, GFL+07], none of these projects has investigated possible solutions and the implications of a secure in-vehicle platform. The EU project EVITA aims at exactly this: provide security and trust already inside the vehicle. Already at sensor-level it is necessary to add security measures, because in-car data will possibly activate vehicle-to-vehicle applications.Thus internal messages, such as “airbag deployed” or “emergency brake”, can cause warning messages to be broadcasted outside the vehicle. We have adapted attacker models and combined these with attack probabilities and possible impact of successful attacks. Using this model, we have been able to identify security requirements for individual components of the car [RWW+09]. We use an approach to secure in-vehicle communication by providing a trusted platform: a small, integrated hardware security module. This does not only enable platform integrity but is used to securely store cryptographic material and to perform accelerated cryptographic operations. The security architecture provides the building block for all further communication and interaction [AEKH+10]. Furthermore, communication protocols used in the vehicle are customized to hold a security payload. Depending on the security requirements of an application, strong or weak cryptography is used to enable authenticity, integrity and confidentiality. As the vehicle is intrinsically an embedded domain and very sensitive to additional cost, additional overhead caused by security payload must be kept to a minimum.

Field Trials There exist so-called Field Operational Tests (FOTs) to evaluate the feasibility and performance of vehicular communication. In FOTs, a number of vehicles is equipped with on-board systems and is operated in a specific area with RSUs. In all current FOTs, foremost the German project simTD, cryptographic security is applied. In simTD, a public key infrastructure for long-term identity as well as short-term identities, which provide pseudonymity, are established and operated [BSM+09].

3 Outlook

In the scope of EVITA, it is envisioned to associate in-vehicle security systems together with external communication and corresponding safety applications, as well as provide a base for future projects concerned with in-vehicle security. The EU project OVERSEE focuses on secure vehicle runtime environments [GHR$^+$09] and the German project SEIS is going to implement the Internet Protocol (IP) into automotive on-board network architectures [GHM$^+$10].

The outcome of FOTs will largely influence standardization and industrial feasibility. The European Commission has issued a mandate, covering vehicular communication and applications, to the standardization bodies ETSI and CEN [Com09b]. In the United States, VII[1] projects have already resulted in the IEEE WAVE standards [Dep09], which is used in a modified form for european FOTs and is therefore likely to be acknowledged by standardization. Apart from vehicle-to-vehicle systems, the emergency eCall system [Com09a] is going to be mandatory for new vehicles. We are going to see more and more integration of communication hard- and software into vehicles in the coming years, which demands for increased security awareness.

References

[AEKH$^+$10] Ludovic Apvrille, Rachid El Khayari, Olaf Henniger, Yves Roudier, Hendrik Schweppe, Herve Seudié, Benjamin Weyl, and Marko Wolf. Secure automotive on-board electronics network architecture. In *FISITA'10, World Automotive Congress, 30 May-4 June, 2010, Budapest, Hungary*, 2010.

[BB07] Andrea Barisani and Daniele Bianco. Hijacking RDS-TMC traffic information signals. *The Phrack Magazine*, 64(5), May 2007.

[BSM$^+$09] Norbert Bißmeyer, Hagen Stübing, Manuel Mattheß, Jan Peter Stotz, Julian Schütte, Matthias Gerlach, and Florian Friederici. simTD Security Architecture: Deployment of a Security and Privacy Architecture in Field Operational Tests. *7th ESCAR Embedded Security in Cars Conference, Düsseldorf*, November 2009.

[Com09a] The European Commission. eCall – saving lives through in-vehicle communication technology. online, factsheet 49, August 2009.

[Com09b] The European Commission. M/453 EN standardisation mandate addressed to CEN, CENELEC and ETSI in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the european community, October 2009.

[Dep09] US Department of Transportation. Family of standards for wireless access in vehicular environments (WAVE). online: http://www.standards.its.dot.gov/fact_sheet.asp?f=80, September 2009.

[EB06] Thomas Eymann and Michael Busse. Deliverable D1.2-12 Security and Firewall concepts for gateways. Technical report, EASIS-Project, 2006.

[1] Vehicle Infrastructure Integration

[FFH$^+$04] Andreas Festag, Holger Füßler, Hannes Hartenstein, Amardeo Sarma, and Ralf Schmitz. Fleetnet: Bringing car-to-car communication into the real world. In *Proceedings of 11th World Congress on ITS, Nagoya, Japan*, 2004.

[GFL$^+$07] Matthias Gerlach, Andreas Festag, Tim Leinmüller, Gabriele Goldacker, and Charles Harsch. Security architecture for vehicular communication. In *Fourth International Workshop on Intelligent Transportation (WIT2007)*, 2007.

[GHM$^+$10] Michael Glass, Daniel Herrscher, Herbert Meier, Martin Plastowski, and Peter Schoo. SEIS - security in embedded ip-based systems. ATZ elektronik worldwide 1/2010, p. 36, 01 2010.

[GHR$^+$09] André Groll, Jan Holle, Christoph Ruland, Marko Wolf, Thomas Wollinger, and Frank Zweers. OVERSEE a secure and open communication and runtime platform for innovative automotive applications. *7th ESCAR Embedded Security in Cars Conference, Düsseldorf*, November 2009.

[HKD08] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security threats to automotive can networks — practical examples and selected short-term countermeasures. In *SAFECOMP '08: Proceedings of the 27th international conference on Computer Safety, Reliability, and Security*, pages 235–248, Berlin, Heidelberg, 2008. Springer-Verlag.

[KCR$^+$10] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Experimental security analysis of a modern automobile. In *31st IEEE Symposium on Security and Privacy*, volume 31, 2010.

[Kun08] Antonio Kung (Ed.). Security architecture and mechanisms for V2V / V2I. Technical Report Deliverable D2.1, Sevecom Project, 2008.

[Law08] Nate Lawson. Highway to hell: Hacking toll systems. *Blackhat USA*, 2008.

[LBH$^+$06] Tim Leinmüller, Levente Buttyan, Jean-Pierre Hubaux, Frank Kargl, Rainer Kroh, Panos Papadimitratos, Maxim Raya, and Elmar Schoch. SEVECOM - secure vehicle communication. In *Proceedings of IST Mobile Summit 2006*, 2006.

[MBB$^+$08] Michael Montemerlo, Jan Becker, Suhrid Bhat, Hendrik Dahlkamp, Dmitri Dolgov, Scott Ettinger, Dirk Haehnel, Tim Hilden, Gabe Hoffmann, Burkhard Huhnke, Doug Johnston, Stefan Klumpp, Dirk Langer, Anthony Levandowski, Jesse Levinson, Julien Marcil, David Orenstein, Johannes Paefgen, Isaac Penny, Anna Petrovskaya, Mike Pflueger, Ganymed Stanek, David Stavens, Antone Vogt, and Sebastian Thrun. Junior: The stanford entry in the urban challenge. *Journal of Field Robotics*, 25(9):569–597, 2008.

[Pap09] Panos Papadimitratos. Secure vehicular communication systems: Towards deployment. *CAST Workshop on Mobile Security for Intelligent Cars*, 2009.

[RWW+09] Alastair Ruddle, David Ward, Benjamin Weyl, Sabir Idrees, Yves Roudier, Michael Friedewald, Timo Leimbach, Andreas Fuchs, Sigrid Gürgens, Olaf Henniger, Roland Rieke, Matthias Ritscher, Henrik Broberg, Ludovic Apvrille, Renaud Pacalet, and Gabriel Pedroza. Security requirements for automotive on-board networks based on dark-side scenarios. Technical Report Deliverable D2.3, EVITA Project, 2009.

[TMC] TMC Forum. http://www.tmcforum.com/.

[TMD+06] Sebastian Thrun, Mike Montemerlo, Hendrik Dahlkamp, David Stavens, Andrei Aron, othersCelia Oakley, Mark Palatucci, Vaughan Pratt, Pascal Stang, Sven Strohb, Cedric Dupont, Lars erik Jendrossek, Christian Koelen, Charles Markey, Carlo Rummel, Joe Van Niekerk, Eric Jensen, Gary Bradski, Bob Davies, Scott Ettinger, Adrian Kaehler, Ara Nefian, and Pamela Mahoney. Stanley: The robot that won the darpa grand challenge: Research articles. *J. Robot. Syst.*, 23(9):661–692, 2006.