The Dilemma of Data Security, Privacy, Control and Liability in V2X

André Weimerskirch[1], Kai Schramm[1], Lars Wolleschensky[1], and Thomas Wollinger[2]

[1] escrypt Inc., 315 E Eisenhower Parkway, Suite 008, Ann Arbor, MI 48108, USA
email: {aweimerskirch, kschramm, lwolleschensky}@escrypt.com
phone: +1-734-418-2797

[2] escrypt GmbH, Lise-Meitner-Allee 4, 44801 Bochum, Germany
email: twollinger@escrypt.com
phone: +49 (0)234 43870 209

ABSTRACT

It is foreseen that vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication systems will be deployed in the next decade. Data security is an enabler for V2V and V2I communication, because the authenticity, integrity and confidentiality of exchanged network traffic must be guaranteed, especially since these messages will certainly be used for safety applications. Furthermore, privacy of the participants must be ensured. While there are mechanisms available to provide protection against mechanical or electronic failures, data security provides protection against malicious attacks motivated by ill will. Malicious parties might attack the communication channel or try to manipulate the integrity of data stored or processed in vehicles. Data security enables trustable safety applications and thus results in fruitful business model revenue. Unfortunately, designing and implementing data security in V2X is not a trivial task but needs to be considered from various perspectives. In this article, we will present the main problems and show approaches to overcome these.

INTRODUCTION

It is predicted that dedicated short range communication (DSRC) will be introduced to the automotive mass market at the end of the next decade. It will enable a variety of innovative applications based on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. While a main motivation for such applications are the improvement of traffic safety and the reduction of fatalities due to accidents, there are also plans for commercial exploitation such as providing digital content on demand, location-based advertisement and high speed tolling. There are many technical aspects to overcome before deployment of such a technology, in particular related to reliability and safe failure handling, is possible. These mechanisms are widely researched and currently tested. An area that is less understood is data security and privacy for V2X communication. Data security provides protection against malicious attackers that are motivated by ill will; the attacker's motivation might range from curiosity and vandalism to distinct financially motivated reasons. Clearly, data security is a requirement for any vehicular communications network and an enabler for trustable safety applications and new exciting business models. Privacy is a requirement that is less well understood. The opinions range between two extremes: one extreme argument is that privacy is not required at all since it limits performance and convenience, avoids full control of the communication network, and is unnecessary since each vehicle driver carries a mobile phone that can be used for tracking the vehicle anyways. The other extreme is that privacy is

absolutely necessary and that no party, even not government authorities, should be able to record any data about the vehicle or its driver.

Data security and privacy in V2X applications encompass a technological and engineering level as well as an organizational and governance level. There are several standards and projects dealing with data security and privacy in vehicular communication networks worldwide, including the IEEE 1609.2 standard draft [7], the American VSC-A and IntelliDrive (formerly known as VII) initiatives [8], European C2CC initiative [5] as well as the European Network on Wheels (NoW) [12] and SEVECOM (secure vehicular communications) projects [14]. These projects mainly deal with technical aspects and, except for the IEEE draft 1609.2, security is not the main focus.

In the remaining article, we will give an overview of security and privacy approaches for vehicular communication networks and describe problems that need to be resolved before deployment.

COMMUNICATION SECURITY

The two main challenges in communication networks are to prevent sniffing and manipulation of exchanged data. While sniffing is a passive attack, alteration of exchanged data requires an attacker to actively manipulate the communication messages. Data security provides mechanisms to protect communication networks against sniffing and manipulation of exchanged data, namely by providing encryption and data authentication. Further services provided by data security include data origin authentication (which makes sure that the data originates from a valid and trusted source) as well as non-repudiation (which makes it impossible for a sender to deny having sent given data). The mechanisms to provide such services are well understood. Cryptography provides so called symmetric and asymmetric mechanisms to efficiently encrypt data and to digitally sign data. While in symmetric data encryption, the sender and receiver usually share the same cryptographic key, in digital signature applications the sender uses his/her private key to digitally sign data whereas receivers use the sender's public key to verify the signature. So-called digital certificates, which are issued by a trusted certificate authority (e.g., the national department of transportation), enable parties to securely communicate without having met and exchanged data before. There is also a mechanism that allows two parties to agree on a shared symmetric cryptographic key without having met before and without the necessity to send this key over an unsecure communication channel such as a DSRC communication link (so-called hybrid data encryption).

The strategy implemented in most projects so far and defined in IEEE 1609.2 is straight-forward: For message authentication, each message is digitally signed and a certificate is attached. The receiver is then able to immediately verify the message even, if he/she has never had contact with the sender before. The receiver first verifies the certificate, extracts the sender's public key and then verifies the digital signature. For example, such an approach is used for safety V2V applications where each vehicle mainly broadcasts regular heartbeat messages. If confidentiality is required as well, e.g. for commercial applications or financial transactions, data needs to be encrypted and a hybrid data encryption scheme can be used. While the described digital signature mechanism is not based on transactions but on individual messages, the encryption scheme requires the exchange of certificates first. These mechanisms are mainly taken from the "traditional" PC world, which traditionally provides powerful computational resources. There are very different requirements in vehicular communication networks though. From the business perspective, keeping costs low is the main requirement. Through the safety application lens, small time delays and minimized

over-the-air bandwidth overhead are crucial. Although it is widely agreed in the IEEE 1609.2 draft to use a very efficient cryptographic system, namely elliptic curve cryptography (ECC), the demand for computational resources and the corresponding over-the-air overhead is still rather high. Currently, the computational costs of ECC for V2X applications can only be fulfilled using dedicated cryptographic hardware which in turn increases cost.

VSC-A proposed an alternative approach based on highly efficient cryptographic methods at the cost of a slightly increased delay [2], [3]. These approaches are based on TESLA [10], [13] and TADS [1], which combine efficient symmetric cryptography with asymmetric cryptography. TESLA is far more efficient than ECDSA in terms of CPU load at the cost of a slightly increased latency (the time it takes for a message to be transferred from the sender's application layer to the receiver's application layer). Table 1 summarizes and compares the performance of IEEE 1609.2 ECDSA, TESLA and TADS [4]. Another approach is to filter incoming messages and to only verify messages that have an adjustable level of impact and that represent a threat to the driver's safety. This approach was presented in [3] and described more detailed in [8]. Both TESLA and TADS save computational resources and allow the integration of the data security module in a computing platform that is already available in a vehicle, such as the DSRC radio on-board-unit (OBU).

	IEEE 1609.2 ECDSA	**TESLA**		**TADS**	
Authentication generation	6.5 ms* (ECC-224) / 10 ms (ECC-256)	1.5 ms		8 ms* (ECC-224) / 11.5 ms (ECC-256)	
Authentication verification	26 ms* (ECC-224) / 39 ms (ECC-256)	1.5 ms		1.5 ms (TESLA) / 40.5 ms (ECDSA-256)	
CPU Load for 2 OBEs at 10 messages per second: Signing / Signing + Verifying	13% / 67%	3% / 3.8%		14.3% / 21.7%	
Latency: Min. / Max.	61 ms / 90 ms	*piggy-back*	*separate*	*piggy-back*	*separate*
		91 ms / 123 ms	26 ms / 28 ms	116 ms / 145ms	40 ms* / 42 ms*
OTA packet size (send certificate with each 3rd message and using ECC-256)	115 bytes	102 bytes	167 bytes	141 bytes	210 bytes

*** estimated value**

Table 1: Authentication Protocols @ 400 MHz

Data security in vehicular networks comes with a variety of requirements that are very different to the requirements of data security in traditional PC networks. Intensive work is currently performed in this area and it can be expected that reliable and efficient solutions will be available soon. Nonetheless, further work will be required to implement secure applications. For instance, low-cost applications based on DSRC, such as high-speed tolling,

and privacy protection mechanisms are currently researched. Such applications were already implemented and successfully presented as part of the VII Proof of Concept program [11]. However, today's IEEE 1609.2 standard requires ECDSA that demands for computationally powerful devices which in turn are relatively costly for the targeted application. Therefore designing security protocols that run on cost efficient computing platforms is a major objective of research.

HARDWARE INTEGRITY

The previous section described mechanisms to protect the communication among vehicles. However, a malicious party might mount a physical attack in order to extract cryptographic key data or to manipulate the vehicle's sensors, which feed for instance a digital tachograph. If a malicious party is able to extract cryptographic keys, then the attacker is able to authenticate or encrypt/decrypt any message using the extracted keys. For instance, an attacker might load the keys to a laptop that is connected to a DSRC radio. The attacker is then able to generate any message on the laptop, compute a valid authentication over the message, and broadcast it via DSRC radio. The attacker can also manipulate the vehicle's sensors in order to generate false sensor inputs which is then properly authenticated by the OBU and broadcast. For instance, an attacker might manipulate the sensor inputs in such a manner that he/she can trigger an emergency brake by pushing a button.

These attacks can be counteracted by introducing a secure vehicle on-board architecture and a secure in-vehicle communication network. This architecture is based on a few secure hardware controllers that provide security functions and that are tamper resistant. Software components based on secure hardware controllers can then provide security services to the V2X applications. The interested reader finds more details in [16]. The EVITA (E-safety vehicle intrusion protected applications) project performs extensive research in this area to secure in-vehicle networks and systems [6].

PRIVACY

The main concern regarding privacy is vehicle tracking and information that can be gained out of it (e.g., the vehicle was parked in a red light district, or the vehicle was transmitting heartbeat messages indicating a velocity of 100 mph). The underlying privacy problem is that vehicles can be identified due to the certificates they are broadcasting. Certificates include a cryptographic public key, which is unique and which can be used for identification purposes.

The VII Privacy Policies Framework [15] defines high-level policies that address privacy issues in the context of V2I. There are policies defined for all participants such as vehicle users, authorities, public-sector transportation and commerce entities and private-sector entities. It is currently unclear how to map the framework to a technical solution though. In many cases it might be necessary to rely on an organization to implement processes that preserve privacy since no technical solutions are available. In the following we describe technical solutions to achieve privacy. Each vehicle might come with a set of pre-installed certificates and use each certificate for a regular period, say every hour. An attacker that receives a heartbeat message in the morning when the vehicle passes his/her observation zone and another message in the evening when the same vehicle passes again will then not be able to link these two messages to the same vehicle. Therefore, changing certificates is commonly agreed to be a proper approach that can be easily implemented. Further technical approaches are discussed in the V2X community, but until now there has been no consensus on a more sophisticated approach. One proposal is to equip multiple vehicles with the same certificate

such that a broadcast message cannot be linked to an individual vehicle without further evidence (such as a picture of the license plate), but only to a set of potential vehicles. However, when using several certificates for each vehicle the organizing authority (e.g. the DOT) loses control over the communication network. A main requirement is the possibility to evict misbehaving vehicles from the communication network. For instance, if a vehicle sensor is broken or tampered with and delivers wrong information to the DSRC radio, the broadcast heartbeat messages are flawed. Vehicles receiving these messages might be able to recognize the flaw and report it to a central authority by forwarding the received messages. The authority then revokes the misbehaving vehicle based on the passed messages. If the authority is not able to uniquely identify the misbehaving vehicle, because of privacy mechanisms, it is impossible to evict a vehicle from the network based on a small amount of received messages and thus attackers would gain an advantage. This example makes clear that there is an intrinsic tension between privacy and revocation control; the more privacy a communication network offers, the less the network can be controlled, and vice versa. We believe that privacy needs to be based on a trustworthy central authority such as the national department of transportation so that the same authority is able to control the network, but it is trusted to use its power regarding privacy with care – technically supported by mechanisms to share power. Certainly it is crucial that privacy is preserved against any entity besides the authority.

In order for such solutions to properly work, it is necessary to have a discussion about legal aspects, governance, and organizational matters with all involved parties including police authorities, national departments of transportation, and the automotive manufacturers. It is impossible to fulfill the conflicting demands of all stakeholders; while the vehicle manufacturers are sensible to the vehicle owners' demands for a high level of privacy, police authorities on the other hand might demand access to the available data. We believe a careful privacy consideration and user education being crucial for future successful deployment of vehicular communication networks. It was shown in the past that privacy concerns by end users have often had a deep impact with regard to deployment of new technologies and even stopped it. One should never forget that privacy needs to be considered in a global context where requirements in different countries are very different, but such technology is sold everywhere. Therefore it is desirable to provide a privacy framework and platform that allows implementing local privacy policies.

CONCLUSIONS

Vehicular communication networks provide exciting new possibilities. Data security in such networks is currently researched and implemented, and it is expected that reliable solutions will be available in the next few years. Privacy on the other hand is heavily researched but still not well understood by the involved stakeholders; furthermore there is a lack of communication between stakeholders and the research community. Intensive work is therefore necessary to design and implement reliable privacy solutions that will be accepted by all stakeholders, both on the technical and organizational level.

REFERENCES

[1] Bhargav Bellur, Anitha Varghese, TESLA Authentication and Digital Signatures for V2X Messages, www.ip.com, IP.com number: IPCOM000175320D, IP.com Electronic Publication: October 9, 2008.

[2] CAMP, VSC-2, Security in VSC-A, presented at IEEE 1609 standard group meeting in Berkeley, CA, USA, by André Weimerskirch, August 2008.

[3] CAMP, VSC-2, Security in VSC-A, presented at IEEE 1609 standard group meeting in Albany, NY, USA, by André Weimerskirch, October 2008.

[4] CAMP, VSC-2, Security in VSC-A, presented at IEEE 1609 standard group meeting in San Diego, CA, USA, by André Weimerskirch, February 2009.

[5] Car-2-Car Communication Consortium, www.car-to-car.org

[6] EVITA (E-safety vehicle intrusion protected applications), http://evita-project.org.

[7] IEEE Trial-use Standard 1609.2TM-2006, WAVE - Security Services for Applications and Management Messages, 2006.

[8] IntelliDrive, http://www.intellidriveusa.org.

[9] Hariharan Krishnan, "Verify-on-Demand" – A Practical and Scalable Approach for Broadcast Authentication in Vehicle Safety Communication, www.ip.com, IP.com number: IPCOM000175512D, IP.com Electronic Publication: October 10, 2008.

[10] Ken Laberteaux and Yih-Chun Hu, "Strong VANET Security on a Budget", escar 2006, Berlin.

[11] MARK IV, "MARK IV successfully demonstrates toll and parking applications using 5.9GHz DSRC", available at http://www.ivhs.com/pdf/5.9GHzDSRC.pdf.

[12] Network on Wheels (NOW), www.network-on-wheels.de

[13] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Xiaodong Song, „Efficient Authentication and Signing of Multicast Streams over Lossy Channels", IEEE Symposium on Security and Privacy, 2000.

[14] SeVeCom, Secure Vehicle Communication – Project Presentation, February 2006, http://www.sevecom.org/Deliverables/Sevecom_Deliverable_D6.1_v1.0.pdf

[15] Vehicle Infrastructure Integration Privacy Policies Framework, Version 1.0.2, February 16, 2007.

[16] Marko Wolf, "Vehicular security hardware", Embedded Security in Cars (escar) Conference, Hamburg, Germany, 2008.