AUTHENTICATION AND PRIVACY IN VEHICULAR NETWORKS: STATE-OF-THE-ART AND OUTLOOK

André Weimerskirch, Kai Schramm, and Lars Wolleschensky

escrypt Inc. – Embedded Security

315 E Eisenhower Parkway, Suite 008

Ann Arbor, MI 48108, USA

+1-734-418-2797, {aweimerskirch, kschramm, lwolleschensky}@escrypt.com

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 to guarantee authenticity, integrity and confidentiality of exchanged messages. Furthermore, privacy of the participants must be ensured. While there are mechanisms available to provide protection against operational failures, data security provides protection against malicious attacks motivated by ill will. Data security enables trustable safety applications and thus results in fruitful business model revenue. Unfortunately, designing and implementing data security as well as privacy in V2X is not a trivial task but needs to be considered carefully. In this article we describe the work previously done in this area, and the work that needs to be done in the future. In particular it is described what needs to be done to standardize the solutions of vehicular data security for interoperability among the various manufacturers and parties involved.

Keywords: communication security, authentication, privacy, IEEE 1609.2

INTRODUCTION

It is predicted that dedicated short range communication (DSRC) will be introduced to the automotive mass market by 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 is the improvement of traffic safety and the reduction of fatalities due to accidents, there are also plans for commercial exploitation by providing digital content on demand and high speed tolling. However, there are many technical aspects to overcome before the mass deployment of this technology is possible, in particular related to reliability and safe failure handling. 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 communication network and an enabler for trustable safety applications and new exciting business models.

Besides communication security, privacy is a strong requirement for V2X deployment. Although there are no clear requirements defined and tested yet, it is clear that a lack of privacy will endanger deployment of V2X systems. Privacy as well as communication security are neither trivial to solve and implement nor are they purely technical issues. In the

following, we will describe the state-of-the-art, describe open research and organization problems, and especially consider interoperability by means of a standard such as IEEE 1609.2.

STATE-OF-THE-ART

There are two major projects in the USA working on vehicular networks: VSC-A and VII. While VII focuses on V2I, VSC-A focuses on V2V communication. Both projects incorporate data security but approach it in different manners. VII applies so called digital signatures based on Elliptic Curve Cryptography (ECC), namely ECDSA (Elliptic Curve Digital Signature Algorithm). Such digital signatures can be used in a uni-cast manner (one sender – one receiver) or in a broadcast manner (one sender – many receivers). ECDSA adds 64 bytes of over-the-air (OTA) overhead to each message but also requires the broadcasting of so-called certificates of at least 120 bytes. These certificates can be attached to each message, or they can be attached to messages only once in a while (say, every 500 ms). Usually, heartbeat messages are digitally signed and broadcast at a rate of around 10 Hz. ECC is also used to implement data encryption. Data encryption is always performed in a uni-cast manner and requires two entities, usually a vehicle's on-board unit (OBU) and a road-side unit (RSU), to establish a session. The OTA overhead due to encryption mainly requires the exchange of two certificates. In the past VII used dedicated hardware based on an FPGA to implement the computational expensive cryptographic ECC routines. The FPGA is able to verify 150 signatures per second. However, using a more powerful FPGA it would be possible to verify 1,000 signatures per second. VII implemented these mechanisms according to the IEEE 1609.2 standard draft (1) and the results of the implementation were fed back to the standard.

VSC-A considers safety applications based on V2V communication. Therefore, mainly broadcast authentication is considered. VSC-A argues that using dedicated hardware solely for cryptographic purposes will increase the costs of the target platform and will be a burden for a widespread market penetration. Therefore efficient broadcast authentication mechanisms are investigated to replace ECDSA. TESLA (6) and TADS (1) are extremely computationally efficient by combining ECDSA digital signatures with so-called symmetric cryptography. These algorithms run on a standard embedded device that can already be found in vehicles, such as the DSRC radio which is foreseen to contain a CPU with a processing power of up to 800 MHz at deployment time. It is estimated at this point that an 800 MHz CPU is capable to verify around 1600 messages per second (1)(3). Therefore, a 400 MHz CPU that utilizes 75% for other applications is still able to verify around 200 messages per second. The average latency of message transfers due to security overhead is estimated to be around 120 ms, and the OTA overhead is 18 bytes per message. The increased efficiency comes at the cost of increased latency. Another approach is to verify only messages that actually have an impact to the safety of the considered vehicle. This verify-on-demand approach results in an extreme reduction of the required number of signature verifications (5). While it is estimated that a vehicle will receive up to 1,000 messages per second, only a small fraction of messages actually have an impact. It is estimated that the number of messages that needs to be verified is in the range of around 10 per second such that a 400 MHz CPU using TESLA or TADS only needs to utilize around 2% of its computational resources for security. The ECDSA, TESLA and TADS performance is summarized in Table 1.

	ECDSA (FPGA)	TESLA / TADS (@400 MHz)
Signature verification throughput	150 per second	800 per second
Latency (signature generation + verification)	≈10 ms	≈110 ms
OTA overhead	64 bytes	18 bytes

Table 1: Authentication protocols

The VII project considers privacy in detail and designs a model for privacy (6). It is suggested to generate a pool of certificates and deploy each vehicle with a small subset of the pool such that

1. Vehicles are equipped with several certificates such that they can change certificates once in a while to preserve location privacy
2. Multiple vehicles share the same certificate such that a single transmission cannot be linked to a specific vehicle.

However, we believe that the model is not resilient to massive compromise of vehicles' certificates; if only a small fraction of vehicles is compromised the system is almost unable to recover. Unfortunately, there is no common agreement so far on privacy requirements which makes it almost impossible to define a satisfactory technical solution.

OPEN ISSUES AND OUTLOOK

We believe that the authentication and encryption protocols in V2X communication networks will be defined in the near future. Advanced results will have to be incorporated in the IEEE 1609.2 standard such that interoperability of vehicles is ensured. Several organizational aspects need to be considered as well, in particular the management and organization of the certificate authority that issues certificates to vehicles. While it requires intensive work to define jurisdiction and responsibilities, it should be rather straightforward to define the organization by following today's organization of license plate authorities. It was discussed above that the requirements for V2V and V2I differ with regard to communication security. An approach that is currently discussed is to define a suite of security protocols fitted to specific applications, say one security protocol for V2V, another for V2I, and a third protocol for secure high-speed tolling.

The situation is very different for privacy. On one hand, privacy is not a strong technical requirement to make the system work. It is rather an emotional hurdle, and a lack of assured privacy mechanisms is likely to make a deployment impossible. Therefore, it is first of all important to bring together all involved parties: jurisdiction, law makers, car manufacturers, the department of transportation, and vehicle manufacturers. Only if these parties can agree on a set of requirements, it will be possible to finally define a technical solution that will not hinder deployment. Since privacy is such a crucial but also emotional aspect, we believe that it should be incorporated in a standard such as IEEE 1609, possibly as a further chapter of the standard.

Recently, a discussion emerged which minimum infrastructure is required in order to support security since there might be no wide-spread RSU network available. Potential ideas are to use the existing cell phone network or to use the vehicle owners' WLAN access points installed at their home. The infrastructure requirements evolving of certificate management, detection of misbehaving vehicles and privacy need to be considered carefully. Only then it is possible to deploy V2V safety applications without a wide-spread RSU network infrastructure in place.

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

(5) 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.

(6) Ken Laberteaux and Yih-Chun Hu, "Strong VANET Security on a Budget", escar 2006, Berlin.

(7) Telcordia Technologies, Inc., US Patent Application, Giovanni Di Crescenzo Stanley Pietrowicz Eric Van Den Berg Robert G. White Tao Zhang, Vehicle Segment Certificate Management Using Shared Certificate Schemes, September 2008.