Secure and Privacy Preserving Vehicular Communication Systems: Identity and Credential Management Infrastructure

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group, KTH Royal Institute of Technology, Stockholm, Sweden
{*khodaei, papadim*}@kth.se

Abstract

The concept of smart cities is shaping future urban infrastructure and influences transportation systems. Smart vehicles, as the principal building block of Intelligent Transport Systems (ITSs), are on the way and car-makers are mandated to equip vehicles with new communication technologies. Meanwhile, Field Operational Testing (FOT) for self-driving cars is on-going. These set the ground for the emergence of innovative applications to improve road safety, transportation efficiency, environmental hazards and driving experience.

In Vehicular Communication (VC) systems, vehicles are to be provided with special-purpose sensors and equipments to monitor their operation and surrounding. Vehicles are to be fitted with On-Board Units (OBUs) to facilitate Dedicated Short Range Communication (DSRC), over ITS-G5 (i.e., IEEE 802.11p [1, 2]) or leveraging the cellular infrastructure with other OBUs or Roadside Units (RSUs). They broadcast their movement behaviors to nearby vehicles, e.g., beaconing their position as well as lane changing and emergency braking notifications, or communicate with the back-end infrastructure. Vehicles periodically disseminate messages about their actions and whereabouts containing location, velocity, and acceleration. As a result, neighboring vehicles will be informed about possible unexpected incidents or objects beyond their sight. Typical use cases of such safety-related applications are *''intersection collision warning''* and *''motorcycle approaching indication''*. VC systems are not limited to safety-related applications; it also entails Location Based Services (LBSs) [1, 3] and Vehicular Social Networks (VSNs) [4] which provide efficiency and infotainment in the VC systems. All these facilitate the emergence of next generation of connected vehicles, the so-called *Internet of Vehicles (IoV)*.

Deploying such a large-scale VC system cannot materialize unless the VC systems are secure and do not expose their users' privacy. On the one hand, user privacy is highly at risk: according to standards, vehicles should disseminate spatio-temporal information frequently, e.g., location and velocity. By periodically beaconing information across the open wireless network, user private information is exposed potentially to everyone. Due to openness of the wireless communication, an observer can eavesdrop the vehicular communication to infer users' sensitive information, thus profiling users based on different attributes, e.g., trace their commutes and identify home/work locations. The experience from mobile applications and LBSs hints that this is a realistic threat to user privacy, aggravated, of course, by the recent stream of disclosures on mass surveillance. Thus, vehicles should participate in the VC system and communicate with each other (ideally) anonymously. To further enhance their privacy, vehicles should communicate anonymously with the security infrastructure entities and service providers.

By the same token, the security of the VC system is paramount: an attacker could contaminate large portion of the system with false information, or meaningfully forge a message or impersonate an identity to mislead other vehicles [5]. The importance of secure communication in the VC systems is due to the physical damages and injuries to the human safety: a fatal crash could threaten human safety as vehicles could be compromised or their sensors become faulty. Anonymity may be abused by ''malicious'' (compromised or malfunctioning) vehicles to corrupt system operations to disseminating bogus information across the network. Thus, vehicles should be held accountable for their operations and actions, and the system should detect and evict misbehaving vehicles [5]; otherwise, the reliability and robustness of the entire system might be compromised, eventually, perhaps, jeopardizing human safety. But, accountability and strong privacy preservation, at the same time, appear at a first glance contradictory; the question this raises is: *how to design a secure VC system that ensures accountable vehicle identification while protecting user privacy.*

Last but not least, in the light of the VC large-scale environment, the efficiency, scalability and robustness of any scheme that we design are paramount. We need to extensively evaluate its viability in terms of performance and cost for a large-scale deployment as VC becomes ubiquitous. We further need to enable interoperability of vehicles from different Original Equipment Manufacturers (OEMs) while facilitating their operation in a multi-domain VC system.

Several years of academic and industrial research efforts have converged to a common understanding on fundamental security building blocks for the upcoming VC systems. There is a growing consensus towards deploying a special-purpose identity and credential management infrastructure, i.e., a Vehicular Public-Key Infrastructure (VPKI), with standardization efforts towards that direction. In spite of the progress made by standardization bodies (IEEE 1609.2 [2] and ETSI [1]) and harmonization efforts (Car2Car Communication Consortium (C2C-CC) [6]), significant questions remain unanswered towards deploying a VPKI. The precise understanding of the VPKI, a central building block of secure and privacy-preserving VC systems, is still lacking. This presentation contributes to the closing of this gap. We point out the remaining challenges to be addressed [7] in order to build a central building block of secure and privacy-preserving VC systems. We present SECMACE [8], as the most promising VPKI system, which is compatible with the IEEE 1609.2 and ETSI standards specifications, taking security, privacy, and efficiency into account. More precisely, our scheme facilitates multi-domain operations in VC systems, enhances user privacy and offers increased user privacy protection in the presence of *honest-but-curious* VPKI entities. We further extensively evaluate the performance, i.e., scalability, efficiency, and robustness, of the full-blown implementation of our VPKI for a large-scale VC deployment. We provide tangible evidence that it is possible to support a large area of vehicles by investing in modest computing resources for the VPKI entities. Our results confirm the efficiency, scalability and robustness of our VPKI [8, 9, 10]. We further have a fully operational vehicular testbed as part of the FOT phase of PRESERVE project [11] configured with 20 VC Security Subsystem (VSS) boxes. They could be configured to communicate with our VPKI or with each other.

REFERENCES

[1] European Telecommunications Standards Institute, ''Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions,'' ETSI Tech. TR-102-638, Jun. 2009.

[2] ''IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages,'' *IEEE Std 1609.2-2016 (Revision of IEEE Std 1609.2-2013)*, Mar. 2016.

[3] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, ''Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation,'' *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95, Nov. 2009.

[4] H. Jin, M. Khodaei, and P. Papadimitratos, ''Security and Privacy in Vehicular Social Networks,'' in *Vehicular Social Networks*. Taylor & Francis Group, 2016.

[5] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, ''Securing Vehicular Communications-Assumptions, Requirements, and Principles,'' in *ESCAR*, Berlin, Germany, pp. 5–14, Nov. 2006.

[6] Car-to-Car Communication Consortium (C2C-CC). [Online]. Available: http://www.car-2-car.org/

[7] M. Khodaei and P. Papadimitratos, ''The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems,'' *IEEE VT Magazine*, vol. 10, no. 4, pp. 63–69, Dec. 2015.

[8] M. Khodaei, H. Jin, and P. Papadimitratos, ''SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems,'' *Submitted to the IEEE Transactions on Intelligent Transportation Systems*.

[9] M. Khodaei and P. Papadimitratos, ''Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems,'' in *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, Paderborn, Germany, pp. 7–12, July 2016.

[10] M. Khodaei, H. Jin, and P. Papadimitratos, ''Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure,'' in *IEEE VNC*, Paderborn, Germany, Dec. 2014.

[11] ''Preparing Secure Vehicle-to-X Communication Systems - PRESERVE.'' [Online]. Available: http://www.preserve-project.eu/