Privacy of V2X Communications

Masoud Naderpour
University of Helsinki Helsinki
Finland
masoud.naderpour@helsinki.fi

***Abstract*—We present an accountable de-anonymization in V2X communications which is compliant with current solutions for providing anonymity in vehicular networks. Our approach complements the pseudonymity schemes based on short-term digital certificates, e.g. security credential management system (SCMS) in the U.S. [2], and improves the overall privacy of drivers.**

I. Introduction

Today, we are closer than ever to the deployment of intelligent and autonomous vehicles. For instance, the U.S. Department of Transportation is considering passing a law mandating all light vehicles to be equipped with onboard units for vehicle-to-vehicle communication. The enabler wireless technology for vehicular networks, namely dedicated short-range communication (DSRC) is mature and ready for commercial usage. In the meantime, the development of LTE-V and 5G networks are rapidly progressing and consolidated specifications are being emerged in standardization development organizations for use of cellular networks for intelligent transportation systems.

Privacy is a critical factor for success and public acceptance of such connected vehicle environment. Vehicles broadcast frequently basic safety as well as cooperative awareness messages to nearby peers that embed personally identifiable information towards drivers. The challenge is to remove any personal information that could distinguish a vehicle while other vehicles could still be able to authenticate the messages received from the vehicle. Moreover, no one should be able to link messages to each other and track the vehicles based on broadcasted messages.

The two leading families of standards for DSRC-based vehicular networks, namely the European ETSI ITS G5 and the U.S. IEEE WAVE, propose the deployment of a specifically-designed Public Key Infrastructure (PKI) for vehicular networks. In its basic form, vehicles possess a long-term certifi-cate as the base identity and use it to request for a batch of short-term certificates, known as pseudonyms, from a certifi-cate authority in the PKI. Messages broadcasted by the on-board unit are signed using the pseudonyms and authenticated by other vehicles before processing and acting on them.

From the legal perspective, however, the vehicular communication could not be fully anonymous. It is desirable to have the capability to resolve the real identity behind a pseudonym in certain circumstances, e.g. when the onboard unit is compromised or sends faulty messages. On the other hand, any usage of identity resolution feature by law enforcement agencies should be noticed eventually by the vehicle owner. Legislation for this requirement already exists, e.g. in Switzerland [1]. In this research work, we introduce an audition system based on a publicly readable blockchain that keep the parties involved in a de-anonymization operation accountable. More specifically, law enforcement agencies are enforced to obtain a court consent before proceeding with the task. In addition, all the logs from the de-anonymization operations are recorded in a public blockchain. The vehicle owners are then able to check whether they have been subject of any de-anonymization in the past. Our technical design prevents an individual to check the information of other users in the blockchain.

References

[1] James Titcomb and Agence France-Presse. *Switzerland will notify citizens when they have been spied on under new surveillance laws*, 2016 (accessed May 15, 2017). http://www.telegraph.co.uk/technology/2016/09/26/switzerland-will-notify-citizens-when-they-have-been-spied-on-un/.

[2] William Whyte, Andre Weimerskirch, Virendra Kumar, and Thorsten Hehn. A security credential management system for V2V communications. In *2013 IEEE Vehicular Networking Conference*. IEEE, dec 2013.

ISSN 2305-7254