Cryptographic protocols for Low Emission Zones access control

Carles Anglés Tafalla [*]

Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili
Tarragona, Spain
carles.angles@urv.cat

1 Introduction

Reducing environment pollution and achieving greater sustainability into urban mobility are two of the major challenges that big cities confront in the 21st century. Promoting a rational use of vehicles, such as vehicle sharing incentives or electric vehicles use, are just some of the current strategies. On this basis, many cities have started establishing the so-called Low Emission Zones (*LEZ*), which are zones where a number of restrictions and penalties are applied to their users. These measures are aimed at reducing the traffic of combustion engine vehicles and encouraging the use of less polluting and low emission ones, preferably electric vehicles.

Although these strategies have proven to be effective in large cities, on a practical level, their implementation is neither simple nor economical. One of the main technological challenges regarding the *LEZ* scheme is to design a secure and reliable system which automatically controls the access of vehicles to these areas. Privacy also arises important challenges to the field and reveals that alternative user detection systems should be proposed instead of the use of video cameras that record all the vehicles plates that access the *LEZs*.

Our general objective is to provide secure protocols that automatically control the vehicle accesses to *LEZ*, but preserving the privacy of the drivers as long as they behave honestly.

2 Related Work

In recent years, several *LEZ* access control approaches, known as Electronic Road Pricing systems (*ERP*), on the basis of privacy by design have been proposed [1, 2, 3, 4, 5, 6, 7, 8]. All these systems require the use of an On-Board Unit (*OBU*) fitted with a *GPS* and a wireless communication system. The price of the fare is calculated according to the route the vehicle has

[*] PhD advisors: Jordi Castellà Roca and Alexandre Viejo

traveled. On the one hand, in [1] and [2], the information related to the external server is sent by the *OBU* to the external server, owned by the Service Provider (*SP*), which is in charge of setting the prices in each billing period. On the other hand, in [3, 4, 5, 6] it is the *OBU* which calculates the fees and sends them to the *SP* server in each billing period. In that way, the revealed information relating to the location of the vehicle is minimal. These systems use cryptographic evidences along with physical random-located checkpoints to demonstrate that the *OBU* has been honest when calculating the amounts corresponding to the traveled routes. The work in [7] presents a user privacy preserving protocol based on a time approach which, unlike the aforementioned works, offers a non-probabilistic fraud control. A further improvement of this protocol has been published in [8]. This proposal enhances the pricing system to dynamically adapt fares to the traffic changing conditions aiming at a better traffic distribution. Even when these protocols tackle the most important drawbacks of the systems proposed to date, due to their particularities, specific *OBU*s and full access to some of its functionalities are required for their feasibility. Nevertheless, *OBU*s integration in nowadays vehicles is not widespread and, as proprietary devices, most of their capabilities can be restricted to third parties.

3 Model of the system

Our general objective consists of encouraging the smartphone integration to the *LEZ* access control systems. The current anonymous approaches to control access to *LEZs* rely on the vehicles' On Board Units (*OBUs*), nevertheless, their integration in nowadays vehicles is not widespread. The adoption of the drivers' smartphone for this purpose may ease the rollout and acceptance of these zones. In any case, privacy is a mandatory issue and should be preserved as long as the drivers do not try to commit fraud. Only when a user accesses the *LEZ* without the proper authorization she should be identified and her anonymity revoked.

The scheme we propose in [9] presents a lightweight ERP solution that controls the access to a *LEZ* in a secure and reliable way, while providing privacy to honest users. In contrast to other systems, our approach uses the drivers' smartphone to validate their access instead of relying on an *OBU*. Those users who access the *LEZ* without proper authorization are automatically identified for their subsequent sanction. Accordingly, all anti-fraud measures do not affect the privacy of honest drivers.

The lifecycle of our system is divided into eight phases: i) Registration; ii) Installation; iii) Vehicle Registration; iv) Access; v) Exit; vi) Payment; vii) Fraud Control and; viii) Privacy Configuration.

Before a user could start using the proposed access model, she should complete the Registration (i), Installation (ii) and Vehicle Registration phases (iii);

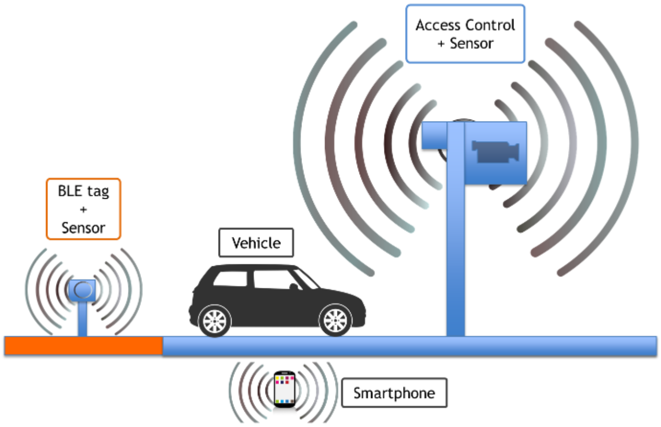

Fig. 1: Access infrastructure.

where she registers her personal data to the Competent Administration of the LEZ ($CALEZ$), installs the mobile application into her smartphone and registers the vehicles she will use to access the LEZ, respectively. Figure 1 shows a general scheme of the LEZ Access (iv) and Exit (v) phases. Both phases are presented together as they perform the same operations. When the vehicle approaches the LEZ access area, a Bluetooth Low Energy (BLE) tag awakens the application on the user's smartphone. This process is automatically done without the intervention of the user. For its part, the Input Sensor notifies to the Access Control (AC) entity that a vehicle has entered the LEZ access area. The mobile phone application establishes a secure communication with the AC entity through a cryptographic protocol and proves that it is a valid user. During the process, the user's anonymity is preserved through the use of a pseudonym. Then, the AC verifies whether the user's access permissions are correct or not. Moreover, the access and exit points are equipped with several sensors to obtain the vehicle's profile (height and length). If the user's credentials are valid, the access is registered and the user can privately access the LEZ. This access information will be used during the Payment phase (vi) to calculate the fee the user has to pay. Conversely, if the user does not have valid access permissions, the AC will take a photo of the vehicle license plate. With this photo the system will be able to identify the offending user. Additional anti-fraud measures are performed in Fraud Control phase (vii), where an independent entity looks for inconsistent patterns in the registered accesses and exits. Finally, to avoid that all the registered accesses of a user could be bind together though her pseudonym, a user can ask for a new one by running the protocol defined on the Privacy configuration phase (viii).

Acknowledgement. This work was partially supported by the DGT under the project SPARK & GO SPIP2015-01783 and the Spanish Government under AccessTur TIN2014-54945-R AEI/FEDER UE, SmartGlacis TIN2014-57364-C2-R and Red de excelencia Consolider ARES TIN2015-70054-REDC projects. Some of the authors are members of the UNESCO Chair in Data Privacy, yet the views expressed in this paper neither necessarily reflect the position of the UNESCO nor commit with that organization.

References

[1] R. A. Popa, H. Balakrishnan, A. J. Blumberg, Vpriv: Protecting privacy in location-based vehicular services, in: USENIX Security Symposium, USENIX 2009.

[2] X. Chen, G. Lenzini, S. Mauw, J. Pang, A group signature based electronic toll pricing system, in: ARES, IEEE Computer Society, 2012, pp. 85–93.

[3] J. Balasch, A. Rial, C. Troncoso, B. Preneel, I. Verbauwhede, C. Geuens, Pretp: Privacy-preserving electronic toll pricing, USENIX Security Symposium, 2010.

[4] S. Meiklejohn, K. Mowery, S. Checkoway, H. Shacham, The phantom tollbooth: Privacy-preserving electronic toll collection in the presence of driver collusion, in: USENIX Security Symposium, 2011, pp. 32–32.

[5] J. Day, Y. Huang, E. Knapp, I. Goldberg, Spectre: spot-checked private ecash tolling at roadside, in: WPES, ACM, 2011, pp. 61–68.

[6] F. D. Garcia, E. R. Verheul, B. Jacobs, Cell-based privacy-friendly roadpricing, Computers & Mathematics with Applications 65 (5) (2013) 774–785.

[7] R. Jardí-Cedó, M. Mut Puigserver, M. Payeras-Capellà, J. Castellà-Roca, A. Viejo, Time-based low emission zones preserving drivers' privacy, Future Generation Computer Systems, Available online 27 June 2016.

[8] R. Jardí-Cedó, J. Castellà-Roca, A. Viejo, Privacy-preserving electronic road pricing system for low emission zones with dynamic pricing, Security and Communication Networks, 2016, vol. 9, no 16, p. 3197-3218.

[9] J. Castellà-Roca, M. Mut Puigserver, M. Payeras-Capellà, A. Viejo, C. Anglès-Tafalla, Secure and Anonymous Vehicle Access Control System to Traffic-Restricted Urban Areas, 3rd International Workshop on Vehicular Networking and Intelligent Transportation Systems (VENITS 2017), August 2017.