Ad Hoc Networks 11 (2013) 2693–2709

Contents lists available at SciVerse ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Privacy-preserving and accountable on-the-road prosecution of invalid vehicular mandatory authorizations

A.I. González-Tablas *, A. Alcaide, J.M. de Fuentes, J. Montero

COSEC – UC3M Computer Security Lab: http://www.seg.inf.uc3m.es/, Computer Science and Engineering Department, University Carlos III of Madrid, Avda. de la Universidad, 30, 28911 Leganés, Madrid, Spain

ARTICLE INFO

Article history:
Received 15 October 2012
Received in revised form 19 April 2013
Accepted 20 May 2013
Available online 30 May 2013

Keywords:
Traffic law enforcement
Privacy
Accountability
Vehicular mandatory authorization
Anonymous credential
Privacy attribute-based credential

ABSTRACT

Nowadays, improving road safety is one of the major challenges in developed countries and, to this regard, attaining more effectiveness in the enforcement of road safety policies has become a key target. In particular, enforcing the requirements related to the technical and administrative mandatory documentation of on-the-road motor vehicles is one of the critical issues. The use of modern technologies in the context of Intelligent Transportation Systems (ITS) could enable the design of a more convenient, frequent and effective enforcement system compared to the traditional human patrol controls. In this article we propose a novel system for the on-the-fly verification of mandatory technical and administrative documentation of motor vehicles. Vehicles not complying with the required regulations will be identified and sanctioned whereas those vehicles, observant of the mandatory regulations, will maintain anonymity and non-traceability of their whereabouts. The proposed system is based on the use of anonymous credentials which will be loaded onto the vehicle to automatically and on-the-fly prove holdership of required credentials without requiring the vehicle to stop beside the road. We also implement a prototype of the credential system and analyze the feasibility of our solution in terms of computational cost and time to perform such telematic controls.

1. Introduction

Nowadays, improving road safety is one of the major challenges in developed countries. Effectiveness of road safety policies enforcement is related to the intensity of controls and compliance with safety requirements. Regulating technical and administrative requirements on vehicles (such as registration certificates or mandatory periodic technical inspections) is part of current strategies to achieve a better road safety. Current regulations usually require a vehicle or its keeper to hold five different documents in order to assert its compliance with mandatory requirements: certificate of conformity (or technical characteristics certificate), registration certificate, valid and up-to-date technical inspection report, proofs of up-to-date motor vehicle local tax and compulsory third party insurance payment. However current situation is far away from its solution (e.g., in Spain 400.000 cars were reported of being driven without having passed the mandatory technical inspection in 2009 [1]).

The use of information and communication technologies in vehicular environments has led to a new family of advanced services that have been referred to as Intelligent Transportation Systems (ITS). In this type of systems it is assumed that vehicles count with sensing, processing, and communicating capabilities. Under this assumption, it is possible to build a more convenient, frequent and effective telematic road enforcement system while reducing the number of human patrols deployed to control road stretches. The system will be more convenient because ITS can make possible the telematic on-the-road verification of the documents – that is, without the car needing to stop

* Corresponding author. Tel.: +34 91 624 5957; fax: +34 91 624 9429.
E-mail addresses: aigonzal@inf.uc3m.es (A.I. González-Tablas), aalcaide@inf.uc3m.es (A. Alcaide), jfuentes@inf.uc3m.es (J.M. de Fuentes).

1570-8705/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.adhoc.2013.05.008

and presenting the documents to a traffic agent, provided that a set of equivalent electronic documents are issued. With an ITS-based road enforcement system, the frequency of document inspection can be set as a dynamically configurable parameter, and its possibilities will be mainly limited by the size and availability of the deployed road side infrastructure. The system will be more effective in two ways. Firstly, well-designed electronic credentials will be more difficult to forge than current paper-based ones. Secondly, if such credentials verification is unsatisfactory, a fine could be immediately issued by the Traffic Authority and notified to the offender [2].

Electronic License Plates (ELP) or Electronic Chasis Number (ECN) have already been suggested as long-term electronic identities for vehicles and it is assumed that vehicles will hold a public key certificate linked to that identity [3]. This credential could be understood as an electronic registration certificate.

Therefore, a first solution would consider the issuance of electronic credentials, such as attribute certificates, linked to that long-term identity, that attest each of the remaining mandatory requirements. Nodes of the road side infrastructure could require passing by vehicles to send these credentials and prove their holdership. However, creating such a system raises critical privacy concerns, as it may enable the Traffic Authority or other nearby entities to easily track vehicles and their drivers and know all attributes encoded in the credentials.

In ITS scenarios, the use of a set of pseudonyms has been devised as an alternative mechanism to authenticate vehicles. A public key certificate will be issued for each pseudonym, with a relatively short-term validity period, such as a week, and used only during a short period of time, such as a minute [4]. The certification authority issuing the certificates also serves as an identity escrow agent to satisfy the principle of accountability for malicious vehicle behaviors.

Therefore, a second solution would consider the issuance of attribute certificates linked to each of the pseudonym-based certificates a vehicle holds. Alternatively, instead of issuing attribute certificates for all the pseudonym-based certificates hold by a vehicle, only a specific subset or a separate set of certificates may be considered. However, the most convenient option under this approach would be to issue the pseudonym-based certificates with attribute extensions representing the satisfaction of the mandatory requirements. However, besides the privacy issues arising in pseudonym-based credential systems [5], the main problem of this type of solution is the credential life-cycle management (certificate issuance, revocation, refilling, etc.) of such a huge number of certificates. In the addressed scenario, this problem will be worse as the satisfaction of each mandatory requirement grants an authorization for a different validity period, starting at different times. In the more convenient pseudonym-based setting (certificates with attribute extensions), vehicles will only obtain valid credentials for the period in which all requirements are satisfied. Once the validity period of one requirement expires, vehicles will be forced to retrieve a new set of certificates. Moreover, if the verification of a set of credentials fails because the vehicle does not have valid credentials, it would not be possible to distinguish which requirement is not being fulfilled at the time of detection. Finally, public key and attribute certificates do not operate on the premises of minimal disclosure of information, i.e., when a certificate is shown, all attributes in the certificate are revealed at the same time.

By contrast, an anonymous attribute-based credential system (ABC-system) allows users authentication while guaranteeing partial information disclosure and unlinkability. Attribute-based anonymous credentials are certificates that provide the subject with a digital identity composed by a set of attributes. Users of anonymous credentials are able to prove, to a verifying entity, holdership of the credential, knowledge of all attribute values or that such values satisfy a given property (such as belonging to a range or satisfying a function). Moreover, users can choose to disclose a set of attributes while keeping others hidden (*partial disclosure of information*). Moreover, verifiers cannot link a request with a specific user or with other past requests (*unlinkability*). Finally, anonymous credential systems may allow for credential *revocation* and anonymity revocation (*de-anonymity*) ensuring accountability of misuses and misbehaviors.

Indeed, the privacy by design feature of anonymous credentials make them very attractive and highly suitable for the representation of authorizations required by regulations over motor vehicles. In this work we explore the feasibility of such an approach by proposing a privacy-preserving and accountable telematic on-the-road verification system of motor vehicle authorizations, being these authorizations represented by anonymous attribute-based credentials. To the best of our knowledge, this is the first proposal in the literature addressing this topic.

The main two technologies being currently developed for the implementation of anonymous credentials correspond to U-Prove [6–8] and Idemix [9–11] systems provided by Microsoft and IBM, respectively. Although, both systems present many core-concept similarities, they also differ on many other aspects, namely the mathematical foundations and the functionality features which have actually been implemented. Although our proposal is not based on any of these systems we briefly comment on their main characteristics. As for U-Prove, its current implementation offers the following features: (1) It allows proof of possession of the credential without disclosing the actual credential. (2) It preserves issuance-show unlinkability, this is, the authority issuing the credential cannot link the credential issued with the credential being shown to the verifying entity. (3) It allows partial information disclosure, meaning that when showing the credential, the user can disclose only some of the attributes in the credential, proving to the verifying party that those attributes were certified by the issuer without disclosing the other attributes. By contrast, it does not offer multi-show unlinkability (different uses or shows of the same credential can be linked together) and the user (credential holder) cannot prove that two of its undisclosed attributes hold the same value when being encoded into the same or into two different credentials. Due to the latter two non-implemented features we have not adopted the U-Prove technology.