

Privacy and Identity Management for Vehicular Communication Systems: a Position Paper

| | | | |
|--|--|--|---|
| P. Papadimitratos IC-LCA, EPFL Switzerland panos.papadimitratos@epfl.ch | A. Kung TRIALOG France antonio.kung@trialog.com | J-P. Hubaux IC-LCA, EPFL Switzerland jean-pierre.hubaux@epfl.ch | F. Kargl Ulm University Germany frank.kargl@uni-ulm.de |
|--|--|--|---|

Abstract—The emerging technology of vehicular communications (VC) raises a number of technical problems that need to be addressed. Among those, security and privacy concerns are paramount for the wide adoption of VC. In this position paper, we are concerned with privacy and identity management in the context of these systems. We identify VC-specific issues and challenges, considering the salient features of these systems. In particular, we view them in the context of other broader privacy protection efforts, as well as in the light of on-going work for VC standardization, and other mobile wireless communication technologies.¹

I. INTRODUCTION

A number of initiatives that seek to create safer and more efficient driving conditions have recently drawn strong support. The key enabling technology towards this goal are *Vehicular communications* (VC). *Vehicular ad hoc networks* (VANET) are envisioned to support a variety of applications for *safety, traffic efficiency and driver assistance*, and *infotainment*. For example, warnings on environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency braking), traffic and road conditions (e.g., congestion or construction sites), and tourist information downloads will be provided by such systems. The European Commission is sponsoring a large number of eSafety projects such as Prevent (preventive safety) [1], Safespot (cooperation for road safety) [2], CVIS (cooperation for traffic efficiency) [3], and Coopers (seamless services along the travel chain) [4].

A number of concerted research efforts in the industry and the academia are currently investigating a pleiad of technical issues. The realization of VC systems, however, is strongly dependent on their security and privacy protection features. Without security integrated into vehicular communication protocols, these systems can make anti-social and criminal behavior easier, in ways that will actually jeopardize the benefits from their deployment.

Beyond VC, the protection of privacy, which is the focus on this paper, that is, the management of personal data dissemination, has been increasingly important with the proliferation of Internet and mobile communication applications. The outcome of this growing awareness has been a number of recent and on-going research projects focusing on privacy protection:

PAMPAS [5], Modinis-IDM [6], PORTIA [7], FIDIS [8], and of course PRIME [9]. At the same time, coordination and liaison efforts have been underway in the context of SecurIST [10] and eSafety [11].

The emerging vehicular communication systems are not merely a subset or an extension of the cyber-space, but rather raise a number of specific issues and unique challenges with their salient features. As such, we believe that addressing privacy and identity management in VC warrants not only novel approaches but it can also have a strong impact in the overall architecture, beyond security, of those systems.

In the rest of this position paper, we first outline the characteristics of vehicular networks and the on-going development and standardization efforts. We then discuss what can constitute identities in the VC context. We consider the challenges that lie ahead, in the form of requirements and objectives, and identify points of similarity or difference with current privacy-enhancing identity management approaches. Finally, we briefly survey the scope and suitability of standardized mobile wireless communication technologies with respect to the problem at hand.

II. VEHICULAR NETWORKS

The entities that are part of a vehicular communications system are private and public vehicles, road-side infrastructure, and authorities, with the latter considered primarily as network entities. An authority will be responsible for the identity and credential management for all vehicles registered in its region (e.g., national territory, state, canton, metropolitan area), similarly to what is currently the case. Public vehicles (e.g. police cars) may have specific roles and be considered as mobile infrastructure.

VANET will enable both vehicle-to-vehicle and vehicle-to-roadside communications. Vehicular networking protocols will require nodes, that is, vehicles or road-side infrastructure units, to communicate directly when in range, or in general across multiple wireless links (hops). Nodes will act both as end points and routers, since vehicle-to-vehicle communication can often be the only way to realize safety and driving assistance applications, while the deployment of an omnipresent infrastructure can be impractical and too costly. In fact, vehicular networks are emerging as the first commercial instantiation of the *mobile ad hoc networking* (MANET) technology.

¹This work is sponsored in part by the European Commission (IST-027795, framework 6 priority 2.4.12, eSafety)

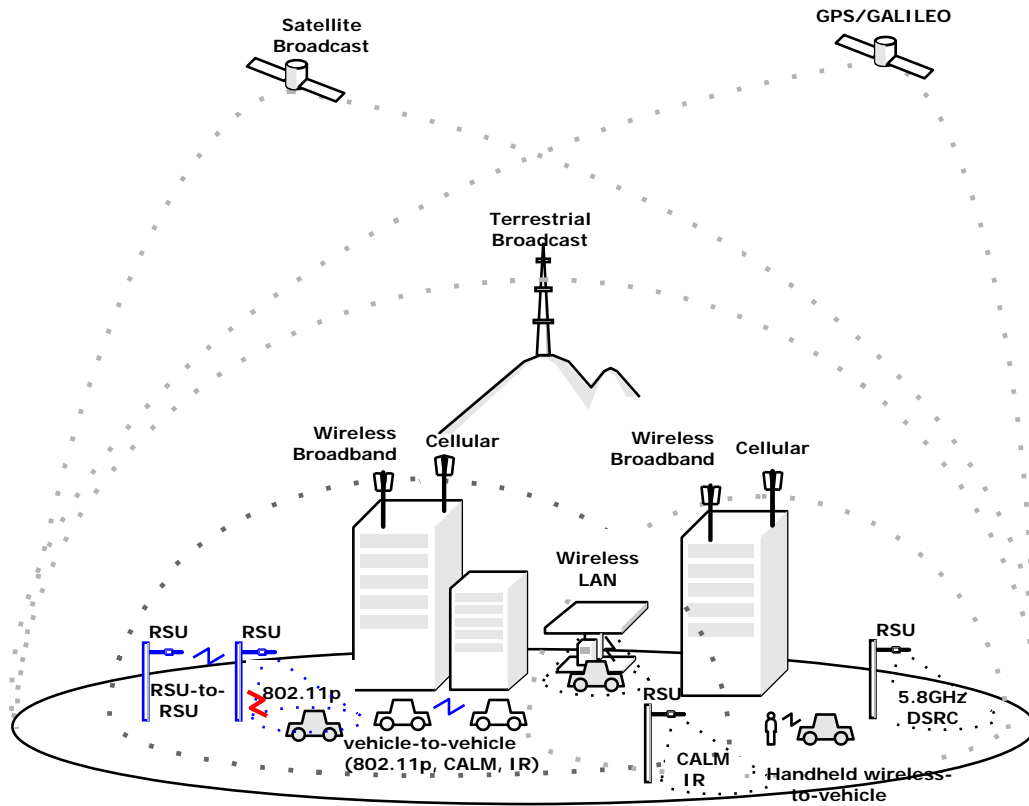


Fig. 1. Vehicular Communications System - An Architectural view

VANET may ultimately rely on several communication channels, including for example cellular telephony or broadband wireless (e.g., WiMax [23]) transceivers. Nevertheless, the emerging defacto standard is the DSRC (Dedicated Short Range Communications) [12]. DSRC is based on IEEE 802.11 technology and proceeds towards standardization under the name of IEEE 802.11p. Roadside infrastructure may consist of short-range (up to 1 km) DSRC base stations placed on intersections, highways, and other critical spots of the transportation infrastructure. Or it may leverage on licensed-frequency technologies (e.g., cellular), with the Continuous Air interface for Long and Medium distance (CALM) platform combining WLAN and GPRS technologies [3] for example.

There is a number of completed and ongoing projects on VC all over the world, such as the Berkeley PATH [13] and the Fleetnet [14] projects in the USA and Germany respectively, beyond those within eSafety [11]. However, VC security is not considered in those projects either. This is why new projects strive now to investigate security issues.

The US Vehicle Safety Communication Consortium

(VSCC) promotes and produces the DSRC standards for VC, part of which is the IEEE P1609.2/D2 draft standard [?]. It proposes using asymmetric cryptography to sign safety messages, while keys and IP and MAC addresses change over time, as measures to achieve some degree of unlinkability. Node certificates are envisioned to have short lifetimes and are periodically requested by vehicles through roadside base stations.

VC security is considered to a certain extent the European Global System for Telematics (GST) [17] and the German Network on Wheels (NoW) [16] projects. This is also true for the Car2Car Communication Consortium (C2C-CC) and in particular its security workgroup [18]. Security and privacy are among the primary objectives of the recently started SEcure VEHICULAR COMMUNICATIONS (SEVECOM) European project [19].

III. IDENTITIES IN VC SYSTEMS

The identity of the entities that make part of a vehicular communication (VC) system, as discussed in the previous

section, is data that uniquely characterize them. In general, an identity can be context-specific. Independently of VC, vehicles and transportation systems have been in place for many years, and so have administrative processes, including management of the identities of the involved entities. In this section, we first briefly describe what has been the status quo before the advent of VC systems. Then, we pose the question and consider what can and will constitute an identity in the context of VC.

Vehicles have a predominant role in VC, while a tight coupling between vehicles and users, especially drivers, will usually exist. In general, the driver-vehicle relation is many-to-many, as a driver can operate many vehicles, and similarly, many users may be entitled to operate a particular vehicle. Even though the two types of entities are clearly distinct, as it will become clear later, they may be bound to each other.

Currently, the identities of vehicles and (their) users are managed by a variety of organizations. The identity of the users is in general established by states (e.g., identity cards, passports), and in the context of transportation by specific organizations, such as the Department of Motor Vehicles (DMV), which grant drivers licenses and attest to the ability of users to operate a vehicle.

The DMV is responsible for the identification of vehicles as well. On the one hand, the registration process, which is repeated periodically, has basically a two-fold output. First, a license plate that uniquely identifies the vehicle, determining the issuing authority, perhaps a division within the area covered by or corresponding to the authority, and an identifying string. Second, a binding between the plate, the vehicle, and the owner of the vehicle.

Nonetheless, identification is not done by the authority (e.g., DMV) alone, but can involve manufacturers. The vehicle itself is, on the other hand, identified by a presumed unique and assigned by the manufacturer vehicle identification number (VIN), as well as technical details such as manufacturer, date of production, model and color.

All these 'brick-and-mortar' attributes are expected to be part of digital identities, which are to be defined in VC systems. Nonetheless, an electronic-world identity of a vehicle can be significantly broader, or multiple identities may exist and used alternately as needed. The reason is that a large variety of applications will emerge, mixing not only attributes as those mentioned above, but also including new ones that convey access control privileges to on-line data and services. The variety of applications will be commensurate with the multiplicity of identities that will be used by vehicles and users.

At the same time, the VC systems will necessitate, beyond the application context, a within-the-network identification of nodes. This will transcend the entire networking protocol stack: network addresses at the data link and network layers (e.g., NIC and IP address respectively), end node identifiers (e.g., TCP port), and user-friendly names. All these identifiers, seemingly independent according to the layering concept, as well as other context specific data, such as geographical coordinates, can be critical in terms of privacy.

IV. CHALLENGES AND OPEN ISSUES

Digital identities and their attributes should be designed and managed within VC systems. These tasks will be undertaken by multiple organizations or authorities, which will be responsible for generating and granting credentials for the VC system entities.

Personal or sensitive data warrant special protection or limited disclosure. Yet, as vehicular networks are systems in the making, decisions by involved parties are necessary to specify both precise requirements and processes for privacy protection. Especially because privacy is a rather broad notion.

One approach, generally applied beyond the VC context, is the use of pseudonyms. These identifiers do not carry information about the identity of the system entities, in a way that any two or more pseudonyms cannot be correlated with the same identity and thus entity. An equally general approach is to equip the system with fine-grained control of the entities on the sought level of privacy. Furthermore, to ensure the minimum amount of identity information is disclosed for a specific context and transaction.

At the same time, access control and accountability are indispensable security attributes for VC systems [20]. This means that the above-discussed objective of anonymity, that is, concealing one's identity and avoiding linkability (with respect to a set of observers) of one's actions to its own identity, is not straightforward to achieve. In fact, the two aspects are seemingly contradicting.

Consequently, it appears that full and unconditional anonymity will not be acceptable. This is implied by the current status quo, with strong identification processes for vehicles and users in place. The notion of anonymous credentials with revocable anonymity has already been considered beyond VC; see for example [21] and references within. More specific requirements, such as anonymity revocation ('de-anonymization') globally or locally, are also relevant to VC, as it is almost certain that multiple administrative authorities will co-exist.

The system should enable different entities to obtain multiple credentials, perhaps from different organizations, to support the wide range of envisioned VANET functionality. Yet, the system should prevent users from sharing their credentials, either by passing them among themselves or 'presenting' them so that a third party is misled that the credentials belong to the same entity.

So far, we discussed in this section 'similarities,' in terms of requirements and characteristics, with existing or under-development, beyond the VC context, techniques for privacy protection. However, what can be more interesting are the 'differences' due to considerations that are specific, if not unique, to VC systems. At first, clearly, VC systems will not be merely another wireless technology to access the Internet (even though this will be supported as well), but a much more complex system that enables applications specific to the VC mission.

VC systems are not necessarily user-centric. Rather, non-human entities, vehicles, and most important, vehicles owned

or operated by private parties, will be multiply identifiable and play a central role. One could view the vehicle as the user, yet what remains as a difference is the the level of automation that the VC systems will require.

The significance of the vehicle role is mostly due to established administrative processes we discussed in Sec. III. Furthermore, not only the vehicle itself but the operational condition of any of its individual subsystems (sensory or mechanical) may be of interest and necessary to be identifiable.

This clues clearly on the importance of robustness, yet, in our context, clues also on the importance of liability and accountability, and, more subtly, on the role of the VANET communication pattern: *frequent, if not continuous, vehicle to vehicle communication.*

Communication in VANET will often, if not mostly, be *not* of transactional nature. Nodes will transmit data that are not addressed to a particular node, or in other words, communication will not be unicast, with two-party protocols. Instead, messages will be mostly 'floating' across the network, i.e., broad- multi- or any- casted, with destinations defined in terms of context- or node- specific attributes (e.g., location, or node characteristics).²

Such VC-specific communication, nonetheless, is at a relatively high rate; some representative widely accepted value: at least one message generated per node every 200 or 300 milliseconds. Depending on the density of the network, and the area across which each such message propagates, a multiple number of messages will need to be validated at each node. What is important is the network overhead due to the cryptographic mechanisms, especially if anonymity is supported. Moreover, the processing overhead can be a significant issue.

To illustrate this, we consider for the sake of an example, the Idemix system [22]: the showing of a credential with all optimizations mentioned by the authors (not implemented at the time of [22]), for the system running at a Pentium III, needs a running time of 2.5 seconds. This is roughly a period of time during which at least 12 messages should be transmitted. Of course, further application-specific optimizations may be possible, or somewhat more powerful on-board platforms may be used. Yet, this back of the envelope calculation points out the importance of processing overhead.

Finally, regarding communication, VC mandates that a significant fraction of the total traffic, namely safety messages, is frequent and periodic. However, it is not at the discretion of the user/owner of the device to stop or enable it. Furthermore, in contrast with approaches for ubiquitous computing, the user will not elect but will by default engage in context-rich (including, for example, the sender's/receivers' coordinates) communication.

What is most important is that vehicle-to-vehicle communications will call for anonymity as well as security (e.g., authentication). Moreover, anonymity appears as a pre-requisite for the channel communication; in other words, achieving

²More 'traditional' types of communication are surely possible and expected; the actual fraction of the overall traffic can only be determined once a set of applications are at the (pre-)deployment phase.

anonymity during a transaction is not meaningful if network communication allows a vehicle to be tracked otherwise.

V. RELATED MOBILE AND WIRELESS NETWORKING TECHNOLOGIES

Considering identity management and privacy protection, it can be useful to look at standardized wireless communication technologies. At first, we take cellular networks and GSM as an example. There are two forms of IDs in GSM; the first one being the International Mobile Subscriber Identity (IMSI), which identifies the subscriber and is stored in the SIM card. The cellphone providers keep a database, the so called Home Location Register (HLR) where these IMSI is connected to the subscriber data. Second, there is the International Mobile Equipment Identity (IMEI), which uniquely identifies the GSM equipment. Similarly to the HLR a provider keeps a Equipment Identity Register (EIR) where the IMEIs of banned or monitored mobile phones are stored.

All the identity management within a network is completely managed by the provider, including authentication and revocation. In case of roaming between providers, they grant access to their HLR so authentication can take place. In cellular networks, the mobile nodes only attach and authenticate with the base stations of own or foreign providers (in case of roaming). Therefore authentication and especially generation and resolution of pseudonyms are straight-forward, the base station plus core network is considered to be trusted. This is not the case in VANETs, where cars communicate with each other or with infrastructure provided by multiple organizations who may not all be considered trusted.

In order to protect privacy, there is a form of pseudonyms, the so called Temporary Mobile Subscriber Identity (TMSI). It is assigned to a mobile device as soon as it connects to a Location Area and used thereafter instead of the IMSI. This should prevent tracking of devices. Of course if an attacker manages to eavesdrop on the initial handshake, it will be able to track the device by its TMSI later on. Mechanisms like the IMSI Catcher also show the vulnerabilities and concept failures of the system.

To probe further, we consider the Wireless LANs according to IEEE 802.11. There are no identities in the core WLAN standard itself, perhaps with the exception of the unique MAC addresses used. Instead there is the option of using a shared key for accessing the network.

The IEEE 802.1x/802.11i additional mechanisms, when used, provide a standard authentication mechanism with the access point, using the credentials for authentication. The credentials are typically managed in one or more radius servers that check the authentication credentials. However, these servers are not expected to be available online in VANET scenarios.

There is no real mechanism for privacy protection in WLANs, as MAC addresses are always sent in the clear. However, at least IEEE 802.1x/EAP-TLS secures the authentication dialogue, so the credentials cannot be eavesdropped.

Finally, a number of approaches have been proposed for generic MANET, which are neither standardized nor target necessarily specific applications. For example, the instantiation of certification authorities in a distributed manner, with network nodes acting as CA servers, has been proposed. However, literature on MANET has largely neglected the question of identity management. The development of VANET, with a more precise application context, not only allows to pose specific questions on identity management but also move towards providing answers. Furthermore, requirements on anonymity and privacy protection, which were largely not investigated in the context of MANET, can be set more precisely.

VI. CONCLUSION

The pursuit of security and privacy-enhancing identity management are two seemingly conflicting objectives. For example, system entities can be accountable if they can be linked to their actions (objects resulting from their actions), but entities maintain their anonymity if they cannot be linked to their actions. The solution lies in-between: pseudonymity and conditional anonymity, with designated entities capable of extracting information about a pseudonym, is one approach the can cover the space between the two extremes.

However, before one applies such an approach, or any other one, to the vehicular communications (VC) environment, a precise requirement specification as well as a large number of architectural and design choices must be made. Most important, the salient features of VC, along with other extraneous constraints and requirements, must be accounted for.

In this paper, we presented a first discussion on privacy and identity management for VC and identified challenges and open issues. At the same time, we discussed currently standardized and other proposed related approaches, and presented on-going efforts in the industry and the academia. This is the space from which future solutions to safeguard privacy will emerge.

In place of conclusion, we note that privacy is not a matter to disregard: even a few events of compromising users' privacy can fuel an increase in user distrust, slow down deployment (to the extent this is not mandated by law), and perhaps impede adoption of vehicular communication systems.

Nevertheless, we believe that this is an excellent opportunity for VANETs to address security and privacy issues: their development is already taking place under different conditions that the development of older mobile communication technologies. Moreover, we are confident that SeVeCom, in conjunction with other on-going projects, can ensure that both objectives, security and privacy, will be achieved.

REFERENCES

- [1] "PReVENT: PReVENTive and Active Safety Applications," URL: <http://www.prevent-ip.org/>
- [2] "SAFESPOT: Cooperative vehicles and road infrastructure for road safety" URL: <http://www.safespot-eu.org/pages/page.php>
- [3] "CVIS: Cooperative Vehicle Infrastructure Systems," URL: http://www.ertico.com/en/activities/efficiency_environment/cvis.htm
- [4] "COOPERS: Cooperative Networks for Intelligent Road Safety"
- [5] "PAMPAS: Pioneering Advanced Mobile Privacy and Security," URL: <http://www.pampas.eu.org/index.html>
- [6] "MODINIS-IDM: Study on Identity Management on eGovernment," URL: <https://www.cosic.esat.kuleuven.be/modinis-idm/wiki/bin/view.cgi/Main/WebHome>, Volume 12, Issue
- [7] "PORTIA: Privacy, Obligations, and Rights in Technologies of Information Assessment," URL: <http://crypto.stanford.edu/portia/>
- [8] "FIDIS: Future of Identity in the Information Society," URL: <http://www.fidis.net/>
- [9] "PRIME: Privacy and Identity Management for Europe," URL: <http://www.prime-project.eu.org/>
- [10] "SecurIST: ICT Security and Dependability Taskforce" URL: <http://www.ist-securist.org/>
- [11] "eSafety," URL: http://europa.eu.int/information_society/activities/esafety/forum/index_en.htm
- [12] "DSRC: Designated Short Range Communications," URL: <http://grouper.ieee.org/groups/scc32/dsrc/index.html>
- [13] "PATH: California Partners for Advanced Transit and Highways," URL: <http://www.path.berkeley.edu/>
- [14] "FleetNet: Internet on the Road," URL: <http://www.et2.tu-harburg.de/fleetnet/english/vision.html>
- [15] "IEEE P1609.2/D2 - Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages," November, 2005
- [16] "NoW: Network on Wheels," URL: <http://www.network-on-wheels.de/>
- [17] "GST: A Global System for Telematics enabling on-line safety services," URL: <http://www.gstproject.org/>
- [18] "C2C CC: Car-to-Car Communication Consortium," URL: <http://www.car-to-car.org/>
- [19] "SEVECOM: Secure Vehicular Communications," URL: <http://www.sevecom.org>
- [20] M. Raya, P. Papadimitratos, and J-P. Hubaux, "Securing Vehicular Networks," *IEEE Wireless Communications*, Volume 13, Issue 5, October 2006 (to appear)
- [21] E. Bangerter, J. Camenisch, and A. Lysayankaya "A Cryptographic Framework for the Controlled Release of Certified Data," in proceedings of the *Twelfth International Workshop on Security Protocols*, Cambridge, England, April 2004
- [22] J. Camenisch and E. Van Herreweghen "Design and Implementation of the idemix Anonymous Credential System," in proceedings of the *ACM Conference on Computer and Communications Security (CCS)*, Washington, DC, November 2002
- [23] "The IEEE 802.16 Working Group on Broadband Wireless Access Standards," URL: <http://www.ieee802.org/16/>