VeSPA: Vehicular Security and Privacy-preserving Architecture

Nikolaos Alexiou, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, and Panagiotis Papadimitratos

Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden

{alexiou, lagana, gisdakis, khodaei, papadim}@kth.se

ABSTRACT

Standardization and harmonization efforts have reached a consensus towards using a special-purpose Vehicular Public-Key Infrastructure (VPKI) in upcoming Vehicular Communication (VC) systems. However, there are still several technical challenges with no conclusive answers; one such an important yet open challenge is the acquisition of short-term credentials, *pseudonym*: how should each vehicle interact with the VPKI, e.g., how frequently and for how long? Should each vehicle itself determine the pseudonym lifetime? Answering these questions is far from trivial. Each choice can affect both the user privacy and the system performance and possibly, as a result, its security. In this paper, we make a novel systematic effort to address this multifaceted question. We craft three generally applicable policies and experimentally evaluate the VPKI system performance, leveraging two large-scale mobility datasets. We consider the most promising, in terms of efficiency, pseudonym acquisition policies; we find that within this class of policies, the most promising policy in terms of privacy protection can be supported with moderate overhead. Moreover, in all cases, this work is the first to provide tangible evidence that the state-of-the-art VPKI can serve sizable areas or domain with modest computing resources.

Keywords

Vehicular Communications, Security, Privacy, Access Control, Identity and Credential Management, Vehicular PKI

1. INTRODUCTION

Vehicular Communicationss (VCs) comprise vehicles and Road Side Infrastructure (RSI) acting both as end-hosts and routers, interacting in ad-hoc manner using wireless communication technologies, such as 802.11 and cellular networks. Safe driving is the milestone application for VC. Vehicles broadcast beacon messages in frequent time intervals to report on their location, velocity and other safety-critical information. Besides safety, proprietary applications like location-based services, tolling systems and leisure applications, are expected to be developed for VC. Therefore, a mixture of service providers and mobile devices will interact with the VC, essentially being part of it, and will therefore form the security and privacy challenges for vehicular networks.

Message alternation and fabrication, as well as Denial of Service (DoS) pose important security challenges for VC [13]. Availability of the infrastructure through wireless communications is an additional network requirement for Vehicle-to-X communications that should operate under low response times. Additionally, *Key Distribution* and *Authentication* are important aspects for VC that impose the existence of a Certification Authority (CA) and eventually, secure hardware modules in the vehicles to manage the cryptographic keys [15]. On the flip side of the coin, authentication should be addressed with respect to vehicle *Location Privacy* and *Anonymity*, by protecting the vehicle from adversaries or trusted but curious infrastructure.

The current standards [7] and automotive industry directions [4], as well as research projects [15], address security and privacy challenges by suggesting an instantiation of a Public Key Infrastructure (PKI), known as Vehicular Public Key Infrastructure (VPKI). Digital certificates signed by a trusted authority, allow the propagation of trust in the VPKI hierarchy and also, enable anonymous mutual authentication between vehicles and the infrastructure. Short lived digital certificates, the pseudonyms, are adopted as the prevalent means to prevent the potential breach of vehicle privacy. However, anonymous authentication *per se* cannot address the need for authorization and accountability posed by the large palette of future proprietary vehicular applications, and the current proposals should be enhanced towards this direction.

In this work, we present the first implementation of a VPKI, in order to secure VC using a privacy-preserving architecture according to the standards. We present a *kerberized* version of a VPKI using cryptographic tickets to enable Authentication, Authorization and Accountability (AAA) to the provided services. Our scheme offers credential management, while preserving the privacy against the VPKI itself. Finally, we present an efficiency evaluation of our implementation and demonstrate its applicability.

The remainder of this paper is organized as follows: in Sec. 2 we present the related work, while in Sec. 3 we define the problem statement. In Sec. 4 we outline our architecture and protocols, while in Sec. 5 we demonstrate latency and efficiency results. We conclude the paper with a discussion and our future directions in Sec. 6.

2. RELATED WORK

Three anonymization schemas based on pseudonymous certificates and group signatures presented in [2]. A draft version of standards for secure VC employing the pseudonym paradigm appeared in the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE) [7]. Other standardization and harmonization efforts by the Car-to-Car Communication Consortium (C2C-CC) [4] and European Telecommunications Standards Institute (ETSI) [5] also converged towards the usage of pseudonymous certificates for privacy-preserving vehicular applications. The European Project SeVeCom [9] defines the architecture for secure VC. In addition, it addresses aspects such as key management and distribution, vehicle certification, and credential management.

The effectiveness of pseudonyms in preserving anonymity and location privacy for VC is studied in [17, 1]. Attackers with overwhelming monitoring capabilities can compromise privacy, but pseudonymous schemas undoubtedly offer improved resilience against adversaries. The impact of security on safety beaconing has been studied in [8, 12]. Although the current proposals for security and privacy rely on the implementation of a VPKI, this is the first work to provide efficiency results and considers a AAA solution.

Ticket-based authentication mechanisms, such as Kerberos [10], centralize the identity management and accountability but do not offer anonymous service access. In [14] a resolution approach using cryptographic tokens issued by a trusted authority is presented. However, the pseudonym acquisition protocol presented can compromise vehicle privacy (discussed later in Sec. 4.3). In this work, we present a method of preserving the unlinkability of two consecutive requests and thus improving privacy.

De-anonymization of the vehicles in case of user misbehavior is a requirement for safety applications in VC [15, 4]. Therefore, PKI paradigms such as [18, 6] cannot be employed since they do not provide revocation or anonymity, respectively. Moreover, revocation schemas as presented in [3, 16] are not directly applicable in the VC setting, since they do not offer identity resolution capabilities.

3. PROBLEM STATEMENT

Each vehicle is equipped with a tamper-resistant crypto-module able to perform advanced cryptographic operations, such as to digitally sign and encrypt messages. All packets transmitted by the vehicles should be authenticated. Packet authentication is not a guarantee of correctness, but the hardware security module greatly improves security as it reduces the chances of cryptographic keys being stolen. Each vehicle frequently broadcasts safety messages.

We consider adversaries that deviate from the expected operation of the VC protocols and can harm the security of the system and the privacy of its users in various ways. Launching impersonation attacks, the attacker claims to possess a legitimate identity and can fabricate messages or replay old packets. Attackers can deliberately change the content of packets to achieve erroneous or malicious behaviour. Such packet forgery attacks can result in serious implications for VC especially when targeting safety beacons. Moreover, adversaries might try to gain access to VC services, and eventually obtain valid credentials, for example pseudonyms. Non-repudiation is an important security property for VC, especially for accountability purposes. Jamming in VC is a *low effort* attack that can be launched over small or wider geographical areas, but is out of the scope for this paper. Adversaries targeting vehicle privacy and anonymity by linking successive pseudonyms, can leverage on the information included in safety-beacons, in order to reconstruct real vehicles' whereabouts. For this, academia, industry, and standardization bodies have converged on the use of pseudonymous credentials for privacy protection. Moreover, privacy needs to be considered even in the presence of untrusted (i.e. honest-but-curious) infrastructure and misbehaving users. In the later case, the anonymity provided by the pseudonymous identifiers needs to be revoked.

All of the above underline the importance of secure and privacy-preserving credential management for safety applications in VC. Nevertheless, given the near-deployment status of VC, a whole ecosystem of non-safety services and applications is on the way. To facilitate their adoption by users, a VPKI must offer them security (i.e. AAA services) and protect the privacy of travellers/users against inference attacks and profiling. All these define the need for a scalable, modular and resilient VPKI implementation whose services support, but can be extended beyond, the domain of safety-applications. This becomes critical given the absence of an implementation and evaluation of such an infrastructure. These points comprise the motivation and the scope of our work. We design, implement and evaluate a standard-compliant VPKI, able to accommodate the security and privacy requirements for safety applications and to offer secure and privacy-preserving credential management to any other vehicular application.

4. THE VPKI ARCHITECTURE

In this section we present our architecture and the relevant protocols. We focus on the security and privacy aspects of our approach, and define a privacy-preserving pseudonym acquisition protocol which can be easily extended to support other vehicular services.

4.1 Security & Privacy Discussion

Packets signed under the private key of the vehicle, residing inside the hardware security module, are then transmitted along with the corresponding certificate. The VPKI architecture should support key management and certificate distribution, thus ensuring (i) VC message integrity, (ii) message & vehicle authentication in both Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V), and (iii) non-repudiation of origin security properties. Vehicles can establish secure channels (e.g., using TLS tunnels), thus achieving confidentiality against external eavesdroppers. Authorization and accountability is accomplished using *tickets*; that is reusable proofs of access rights to a given service. Tickets are signed by a trusted authority to avoid forgery and integrity attacks as presented in Sec. 4.3. We now discuss the usefulness of two types of certificates:

Pseudonyms. In order to preserve location privacy and anonymity in VC, each vehicle possesses a set of short-lived pseudonyms, obtained by a trusted pseudonym provider. Each pseudonym has a lifetime ranging from seconds to hours, defined by the pseudonyms provider. A vehicle can decide to change the active pseudonym in order to prevent the tracking of its location. Safety beacons are digitally signed under the current pseudonym identity. By increasing the frequency of pseudonym changes, the chances for an adversary to launch a successful attack against privacy are reduced.

Long-term Certificates. A pseudonym acquisition protocol is necessary to obtain new sets of pseudonyms when the old ones are close to expire or have been already used. However for accountability and authorization purposes, the vehicle needs to be authenticated using its long-term identifier and then obtain anonymous authorization credentials, in the form of tickets. For this reason, each vehicle should be able to prove its real identity using a *long-term identity*.

4.2 Architecture Proposal

Our scheme comprises the following three trusted CAs, according to the terminology used in [15] and compatible with the definitions in [5]:

- **Long-Term Certification Authority (LTCA)**: The LTCA is the issuer of the vehicle's long-term certificates and tickets.
- **Pseudonym Certification Authority (PCA)**: The PCA is the provider of the vehicle's pseudonyms.
- **Resolution Authority (RA)**: The RA *de-anonymizes* pseudonymous certificates in case of misbehavior detection.

The long-term certificate is a digital signature of the LTCA over a set of vehicle-specific identifying data, a validity period $[t_s, t_e]$, and the vehicle's long-term public key K_v:

$$LT_v = Sig_{\mathrm{LTCA}}(K_v, \mathrm{data}_v, [t_s, t_e])$$

We assume that each vehicle v has a long-term certificate LT_v and the corresponding private key k_v pre-installed in its hardware security module, as proposed in [11]. The vehicle also obtains and stores a set of pseudonyms of the following form:

$$P_v^i = Sig_{\mathrm{PCA}}(K_v^i, [t_s, t_e])$$

Pseudonyms also have a specified validity period $[t_s, t_e]$ and contain a public key K_v^i for verification.

4.3 Pseudonym Request Protocol

We now describe the protocol for the vehicles to obtain pseudonyms from the PCA. All communications are performed over a secure TLS tunnel, which guarantees confidentiality against external adversaries, and prevents tickets hijacking. For vehicle-to-PCA communications one-way authentication of the server to the vehicle is used, in order to preserve the anonymity of the vehicle. In a nutshell, the protocol starts with the vehicle being authenticated by the LTCA using its long-term credentials to obtain a *ticket*. The ticket, *tkt*, does not contain any data attributable to the vehicle and it is of the form:

$$tkt = Sig_{\mathrm{LTCA}}([t_s, t_e], \{S_1\}, \ldots, \{S_n\}),$$

where $[t_s, t_e]$ is the ticket validity period and S_i is a generic service identifier. By ensuring that t_e does not exceed the subscription expiration time for any of the S_i included in *tkt*, the LTCA can guarantee that service subscription periods are not violated.

$$V \longrightarrow LTCA : Sig_{k_v}(t_1, \mathrm{Request}) \parallel LT_v \tag{1a}$$
$$LTCA \longrightarrow V : tkt \tag{1b}$$

Initially, the vehicle issues a ticket request to the LTCA in order to obtain access to the PCA. The LTCA checks the validity of the request, generates *tkt* and sends it back to the vehicle. The vehicle then generates a set of private/public key pairs (k_v^i, K_v^i) inside its hardware security module and sends the public keys K_v^i, along with *tkt*, to the PCA.

$$V \longrightarrow PCA : t_3, tkt, \{K_v^1, \ldots, K_v^n\} \tag{2a}$$
$$PCA \longrightarrow V : t_4, \{P_v^1, \ldots, P_v^n\} \tag{2b}$$

The PCA assesses the validity of the ticket and signs the received public keys K_v^i using its private key. The pseudonyms P_v^i are then sent back to the vehicle. The same ticket can be re-used for multiple pseudonym requests, or different service providers during its validity period.

Unlinkability of requests. We avoid signing pseudonym requests under the long-term or the current-pseudonym identities of the vehicle. In both cases the PCA can breach vehicle privacy. In the first case, linking the issued pseudonyms to the long-term identifier is trivial; in the latter case, the PCA is able to link the new set of issued pseudonyms with the one used for the request. Therefore the PCA can link sets of pseudonyms and thus, compromise privacy. On the other hand, using a new *ticket-per-request* can effectively protect vehicle privacy against the PCA, since no linking is possible between the ticket, the long-term certificate, or any of the pseudonyms. Moreover, the vehicle can issue a request per pseudonym, thus restricting the ability of PCA to link pseudonyms within a request. The proof of the unlinkability is straightforward and omitted here due to space limitations.

4.4 Pseudonym & Token Revocation

Pseudonyms and long-term certificates should be revoked in a number of different scenarios: for example when a vehicle is involved in an accident or misbehaves. Similarly, a ticket can be revoked to deny access to the service e.g., in case the ticket should not be reused. In order to keep the network *up-to-date* in terms of the status of revoked certificates and tickets, Certificate Revocation Lists (CRLs) are used. Revocation lists are publicly available, so that every entity in the VC network has access to them. CRLs are digitally signed with the private key of the authority that issues them. The PCA signs the revocation lists containing the revoked pseudonyms and the LTCA the CRLs containing the long-term certificates. The dissemination of the CRLs is orthogonal to this work. Equivalently, Ticket Revocation List (TRL) can be used for ticket revocation, published by the LTCA in case of ticket revocation. We omit further discussions on ticket and certificate revocation in this work because of the limited space.

4.5 Resolution Protocol

Due to the safety critical nature of VC, the revocation of anonymous credentials is not sufficient *per se* and complete vehicle de-anonymization is required. The resolution protocol is executed with the RA acting as a coordinator between the PCA and the LTCA. The PCA reveals to the RA the link between the pseudonyms and the anonymous ticket. Then, the LTCA reveals the link between the the ticket the vehicle's real identity. Therefore, the RA can combine both pieces of information and perform the resolution.

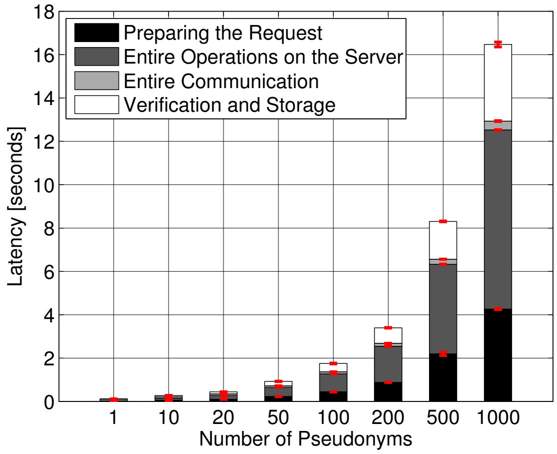

Figure 1: Latency to obtain pseudonyms in seconds (per vehicle).

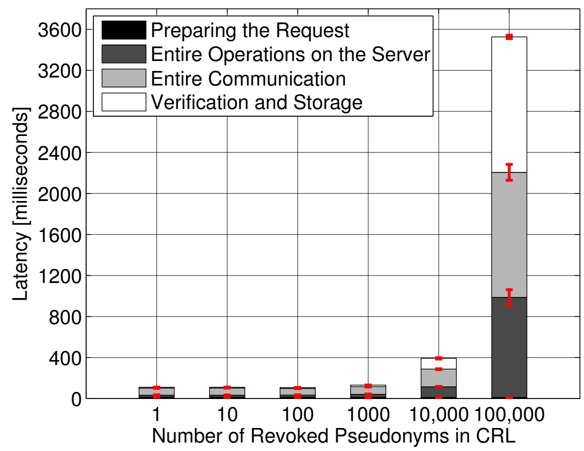

Figure 2: Latency to obtain CRLs (per vehicle).

The RA generates a digitally signed *resolution request* to the PCA. The request includes the pseudonym P_v^i (or the set of pseudonyms) that have to be resolved. The PCA retrieves all the pseudonyms that were issued as a result of the same vehicle pseudonym acquisition request from its database, along with the corresponding ticket tkt.

$$RA \longrightarrow PCA : Sig_{\mathrm{RA}}(P_v^i, t_1) \quad (3a)$$

$$PCA \longrightarrow RA : Sig_{\mathrm{PCA}}(tkt, t_2) \quad (3b)$$

Having received the ticket tkt the RA forwards it to the LTCA, which can in turn reveal the corresponding long-term identity of the vehicle. Mappings between issued tickets and the corresponding long-term identifiers exist in the database of the LTCA.

$$RA \longrightarrow LTCA : Sig_{\mathrm{RA}}(tkt, t_3) \quad (3c)$$

$$LTCA \longrightarrow RA : Sig_{\mathrm{LTCA}}(LT_v, t_4) \quad (3d)$$

With the completion of the protocol, the long term identity LT_v is resolved and the vehicle's pseudonyms have been revoked. Revocation is performed according to the previous section, which will eventually evict the vehicle from the VC network. The LTCA should also invalidate the received tickets by including them in the TRL, to prevent adversaries from distributing tickets among each-other.

5. RESULTS

In this section we present the performance of the proposed VPKI architecture. CAs were implemented using OpenCA, on separate servers equipped with an Intel Xeon Dual-Core 3.4 GHz processor and 8 Gbytes of RAM. All V2I and Infrastructure to Infrastructure links are secured with TLS, while the study of the communication channels are out of the scope of this paper. ECC-256 keys are used for both infrastructure and vehicle certificates. Our implementation is compatible with the IEEE 1609.2 draft proposal [7]. The ticket size is 498 bytes and the pseudonym size is 2.1 KBytes.

Vehicle: Pseudonym Request. In Fig. 1, we present latency results for acquiring a set of pseudonyms from the PCA. The vehicle needs $73,4$ ms to obtain a new ticket from the LTCA (eq. 1). To acquire one pseudonym the vehicle needs 120 ms and $3,400$ ms for 200 pseudonyms (eq. 2). For requests of $1,000$ pseudonyms, which should be sufficient for a relatively long period or time (e.g., for a day if the pseudonym lifetime is around 1 minute), we observe that the total latency is $16,460$ ms. 50% of the total latency concerns PCA side operations, and 26% is devoted on the preparation of the query, for examples the creation of private/public keys and digital signatures over the public keys.

The preparation of the request can take place off-line, which can eventually reduce the total time by $4,260$ ms (darkest bar in Fig. 1). Excluding the verification and storage time that occurs at the vehicle, the total processing time (communication plus operation on the server) to obtain $1,000$ pseudonyms is reduced to $8,670$ ms. Results suggest that our approach is efficient. Additionally, taking into consideration the fact that the vehicles will be equipped with hardware accelerators [15], we can conclude that the time required for a vehicle to obtain a pseudonym will be significantly reduced.

Pseudonyms Req.	**1**	**100**	**1.000**	**5.000**	**20.000**
Signature Ver.	$0,004$	$0,361$	$3,3618$	$18,09$	$72,33$
Pseudonyms Gen.	$0,004$	$0,349$	$3,34$	$17,72$	$70,9$
Total Time	$0,02$	$0,817$	$8,826$	$41,672$	$167,3$

Table 1: Latency to issue pseudonyms in seconds by the PCA

PCA: Pseudonym Issuance. Table 1 shows the time needed by the PCA to process pseudonym requests from vehicles. The processing time includes the verification of the received request (including ticket verification), pseudonym generation time and other relevant PCA operations (e.g., storage and handling of the received public keys). For a total of $5,000$ pseudonym requests issued by multiple vehicles, $41,672$ ms are needed. For $20,000$ pseudonyms the server needs $167,300$ ms. It is straightforward that the pseudonym's lifetime is a determinant factor for the PCA's workload.

CRL Distribution. Fig. 2 shows the time needed by a vehicle to obtain the CRLs of revoked pseudonyms. The preparation of the request by a vehicle takes 11 msecs. The

Server Operations time corresponds to the generation of the CRL (including signing it) at the PCA. We observe that latency increases with the number of entries in the CRL. For large chunks of information (e.g., $100,000$ entries in the CRL) the communication time is an important fraction of the total time; $1,218$ ms for $100,000$ entries in the CRL. For the latter case, the verification of the PCA's signature and the storage of the obtained CRL, can take up to $1,324$ ms.

Pseudonyms Resolved	**1**	**10**	**50**	**100**	**200**
Pseudonyms Prov. (PCA)	73	135	304	516	922
Identity Prov. (LTCA)	9	10	15	20	57
Resolution Auth. (PRA)	265	348	604	916	1598

Table 2: Resolution latencies in milliseconds; PCA, LTCA & PRA

Certificate Resolution. Certificate resolution (eq. 3) times are presented in Table 2. Calculation times include server side operations (e.g., fetching the requested certificate from the database), sign and publish the certification list. The LTCA has the lowest overhead, since the number of tickets is less than the number of pseudonyms that need to be retrieved from the databases of the LTCA and PCA respectively. The resolution of 200 pseudonyms takes less than $1,000$ ms for the the PCA, and we believe that our resolution protocol does not introduce a significant overhead for the VPKI. The RA has the highest workload during the resolution process ranging from 265 ms (for 1 pseudonym) to $1,598$ ms (for 200 pseudonyms).

6. CONCLUSION

In this paper, we presented the implementation of a distributed VPKI architecture in order to provide security and privacy protection in VC. We proposed the use of tickets to guarantee unlinkability between consecutive vehicle requests for pseudonyms, when a new ticket is used for each request. To the best of our knowledge, this is the first work that provides AAA capabilities for a VPKI according to the current standards and the privacy requirements. Part of our future work includes the integration of relevant privacy-preserving methods and anonymous authentication techniques in our protocols. We believe that our scheme is efficient, applicable and thus, it can pave the road towards secure and privacy-preserving VC.

7. REFERENCES

[1] L. Buttyán, T. Holczer, and I. Vajda. On the Effectiveness of Changing Pseudonyms to Provide Location Privacy in VANETs. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pages 129–141, July 2007.

[2] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy. Efficient and Robust Pseudonymous Authentication in VANET. In *Proceedings of the ACM International Workshop on Vehicular Ad hoc Networks (VANET)*, pages 19–28, Sep. 2007.

[3] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to Win the Clonewars: Efficient Periodic n-Times Anonymous Authentication. In *ACM CCS*, pages 201–210, Oct. 2006.

[4] Car-to-Car Communication Consortium (C2C-CC), Jan. 2013.

[5] ETSI TR 102 638. Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions, June 2009.

[6] J. Gu, S. Park, O. Song, J. Lee, J. Nah, and S. Sohn. Mobile PKI: A PKI-Based Authentication Framework for the Next Generation Mobile Communications. In *Australasian Conference on Information Security and Privacy*, pages 180–191, July 2003.

[7] IEEE 1609.2. Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, Jan. 2012.

[8] F. Kargl, E. Schoch, B. Wiedersheim, and T. Leinmüller. Secure and Efficient Beaconing for Vehicular Networks. In *Proceedings of the 5th ACM International Workshop on Vehicular Ad Hoc Networks*, pages 82–83, Sep. 2008.USA.

[9] A. Kung. Security Architecture and Mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1, Feb. 2008.

[10] B. Neuman and T. Ts'o. Kerberos: An Authentication Service for Computer Networks. *IEEE Communications Magazine*, 32(9):33–38, Sep. 1994.

[11] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure Vehicular Communication Systems: Design and Architecture. *IEEE Communications Magazine*, 46(11):100–109, Nov. 2008.

[12] P. Papadimitratos, G. Calandriello, J.-P. Hubaux, and A. Lioy. Impact of Vehicular Communications Security on Transportation Safety. In *IEEE INFOCOM Workshops*, pages 1–6, Apr. 2008.Phoenix, AZ.

[13] B. Parno and A. Perrig. Challenges in Securing Vehicular Networks. In *Proceedings of Workshop on Hot Topics in Networks (HotNets-IV)*, Nov. 2005.

[14] F. Schaub, F. Kargl, Z. Ma, and M. Weber. V-tokens for Conditional Pseudonymity in VANETs. In *IEEE WCNC*, NJ, USA, Apr. 2010.

[15] J. P. Stotz, N. Bißmeyer, F. Kargl, S. Dietzel, P. Papadimitratos, and C. Schleiffer. Security Requirements of Vehicle Security Architecture, PRESERVE - Deliverable 1.1, June 2011.

[16] P. P. Tsang, M. H. Au, A. Kapadia, and S. W. Smith. BLAC: Revoking Repeatedly Misbehaving Anonymous Users Without Relying on TTPs. *ACM Transactions on Information and System Security (TISSEC)*, 13(4):39, Dec.

[17] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos. Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change is not Enough. In *IEEE International Conference on Wireless On-demand Network Systems and Services*, pages 176–183, Feb. 2010.Slovenia.

[18] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon. AC-PKI: Anonymous and Certificateless Public-Key Infrastructure for Mobile Ad Hoc Networks. In *IEEE International Conference on Communications (ICC)*, volume 5, pages 3515–3519, May 2005.