The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems

Mohammad Khodaei and Panos Papadimitratos
Networked Systems Security Group
KTH Royal Institute of Technology
Stockholm, Sweden
{*khodaei, papadim*}@kth.se

***Abstract* - Vehicular Communication (VC) systems will greatly enhance intelligent transportation systems. But their security and the protection of their users' privacy are a prerequisite for deployment. Efforts in industry and academia brought forth a multitude of diverse proposals. These have now converged to a common view, notably on the design of a security infrastructure, a Vehicular Public Key Infrastructure (VPKI) that shall enable secure conditionally anonymous VC. Standardization efforts and industry readiness to adopt this approach hint to its maturity. However, there are several open questions remaining, and it is paramount to have conclusive answers before deployment. In this article, we distill and critically survey the state of the art for identity and credential management in VC systems, and we sketch a roadmap for addressing a set of critical remaining security and privacy challenges.**

I. Introduction

VC systems can greatly enhance transportation safety and efficiency. Using VC, vehicles can directly communicate [Vehicle-to-Vehicle (V2V)] across one or multiple hops, or they can exchange information with Roadside Units (RSUs) [Vehicle-to-Infrastructure (V2I)]. The Cooperative Awareness Message (CAM) and Decentralized Environmental Notification Message (DENM) can disseminate valuable information [1] on potentially dangerous vehicle movement (e.g., collision avoidance), environmental hazards, traffic conditions, and other location-relevant information or even assist regulating traffic [2].

While the benefit is clear, such a large-scale deployment enabling high-stake applications cannot materialize unless VC systems are secure and do not expose users' privacy. For example, only legitimate VC on-board equipment should be part of the system, and any modification or forgery of V2V or V2I messages should be detected. The frequent beaconing of safety CAMs should not leak the whereabouts of drivers (or passengers) to anyone that deploys a set of commodity radios. These concerns are well understood [3], and the results of several significant projects and initiatives led to a set of common tools and approaches.

V2V and/or V2I (V2X) communication is protected with the help of public key cryptography where a set of certification authorities (CAs) provide credentials to legitimate vehicles. The credentials are then anonymized, and they are short-lived, which enhances privacy and maintains non-repudiation. The system maintains a mapping of these short-term identities to a long-term identity of the vehicle. These ideas can be found in the first VC security architecture [4], elaborated by the SeVeCom project as well as in subsequent projects [e.g., CAMP [5] and Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) (http://www.preserve-project.eu/)] and technical standardization documents, notably the IEEE 1609.2 WG (IEEE P1609.2/D12, *Draft Standard for Wireless Access in Vehicular Environments*, January 2012), European Telecommunications Standards Institute (ETSI) (ETSI TR-102-731, *Intelligent Transport Systems (ITS) Security; Security Services and Architecture* and ETSI TR-102-941, *Intelligent Transport Systems (ITS) Security; Trust and Privacy Management*), and harmonization documents [Car2Car Communication Consortium (C2C-CC) (http://www.car-2-car.org/) [6]]. More important, there is a willingness to proceed fast, in the near future, with rolling out the first instances of VC protected accordingly.

This can be seen positively, as a vote of confidence, to these available solutions, and there are already Field Operational Testing (FOT) efforts, seeking to bring them closer to deployment. Furthermore, such security and privacy protection is essentially a baseline. It addresses significant yet specific VC problems, but it leaves a range of possible optimizations of secure VC protocols, as well as the protection of the in-car network and software and information the whole system relies on (e.g., reliable time and location, and, thus, secure global positioning). The question this raises is: *do we indeed have a cornerstone to build upon secure and privacy-protecting VC systems?* More precisely, *do we have all the answers needed to deploy an identity and credential management infrastructure for VC*?

To address this question, we critically survey the literature, distilling the latest understanding in academia and industry. A set of open questions remains, and they need to be addressed before deployment. For example, user privacy is not thoroughly protected against infrastructure entities (servers) that are honest but curious, or VPKI entities do not enforce policies or are not equipped to preclude special types of misbehavior (disruption or privacy breach related). These issues are primarily technical ones, calling for necessary research. However, they also relate

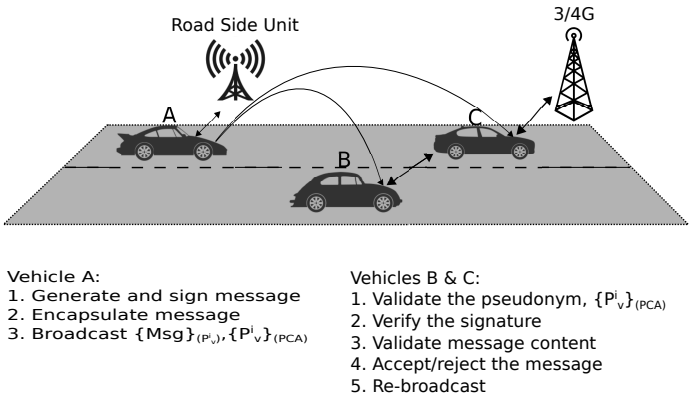

Fig. 1. Secure and privacy-protecting V2X communication.

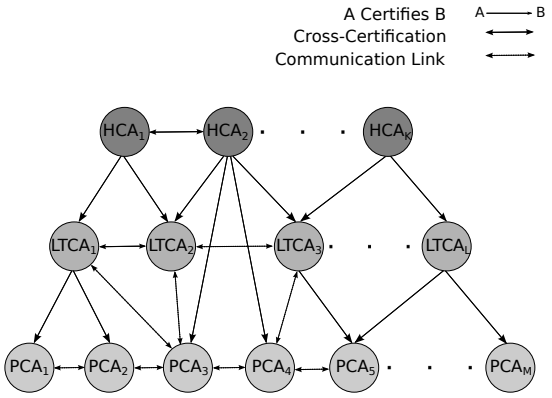

Fig. 2. Hierarchical organization of the VC security infrastructure.

to nontechnical considerations, which affect the systems that will eventually be deployed. In this article, we focus on the technical considerations and briefly discuss how they relate to other factors and the potential deployment scenarios.

In the rest of this paper, we first provide a brief overview of security and privacy-protecting VC systems, focusing mostly on the security infrastructure entities (Sec. II). Then, we discuss a number of important VPKI components and operation requirements (Sec. III), critically comparing how the related literature approaches and addresses (or not) these problems. For example, we are concerned with the overall robustness of the secure VC, the protection of user privacy, and the practicality of alternative proposals. We find that there are not only distinct approaches but in some cases conflicting views. More important, we realize that there are a number of technical considerations and questions that still have no conclusive answers. We outline those focusing on the deployment of an identity and credential management infrastructure (Sec. IV).

II. Shaping the VC Security Infrastructure

Each vehicle is equipped with a set of short-term certificates, termed *pseudonyms*, each with a corresponding short-term private key to sign outgoing messages. Fig. 1 illustrates this: Vehicle A digitally signs outgoing messages (time- and geo-stamped) with the private key, k_v^i, corresponding to the pseudonym P_v^i ($\{P_v^i\}_{(PCA)}$ represents the pseudonym signed by the pseudonym issuer) and is attached to messages to facilitate verification on the receiver side. Receiving vehicles B and C verify the pseudonym $\{P_v^i\}_{(PCA)}$ and validate the signature (assuming they trust the pseudonym issuer discussed below). This process ensures the authenticity and integrity of the message and enables further validation based on its content. At the same time, transmissions by vehicle A do not reveal its identity (as the short-term certificates are anonymised), and messages signed under different pseudonyms (with different private keys) are, in principle, unlinkable. Vehicles switch from one pseudonym to another (not previously used) to achieve unlinkability.

Security Infrastructure Entities: A VPKI comprises a set of authorities with distinct roles: the Root Certification Authority (RCA), the Long Term Certification Authority (LTCA), the Pseudonym Certification Authority (PCA), and the Resolution Authority (RA). Different proposals may refer to these entities with various names, e.g., CAMP [5] refers to the LTCA as the Enrollment Certification Authority (ECA). The RCAs are the highest-level authorities certifying LTCAs, PCAs, and RAs. An LTCA is responsible for registering vehicles and issuing Long Term Certificates (LTCs). A PCA issues sets of pseudonyms for the registered vehicles. An RA can initiate a process to resolve a pseudonym, i.e., identify the long-term identity of the vehicle that used (in a nonrepudiable manner) its short-term keys and credentials.

Trust Associations: Fig. 2 illustrates a generalized hierarchical organization of the VC security infrastructure, with multiple LTCA and PCA entities shown (as those are primarily involved in interactions with the vehicles).

VC systems will be deployed widely, thus one can envision that higher-level CAs (HCAs) could be established to facilitate a trust establishment across distinct parts of the hierarchy. Without loss of generality, let the corresponding numbers of HCAs, LTCAs and PCAs, be denoted by K, L and M, so that $K \leq L \leq M$. It is also possible to have direct cross-certification between CAs. There may be direct communication needed among CAs, e.g., for lookup operations while issuing credentials.

VPKI Structure: In VC systems, a domain was first described [3] as a set of mobile nodes registered with an authority, with communication independent of administrative or geographical boundaries. Alternatively, a domain could be defined as a (fine- or coarse-grained) geographic region, each with the corresponding CAs. The former definition is more general and it is assumed here. A set of vehicles registered with only one LTCA can obtain credentials from several PCAs, subject to compatible policies, as long as the two CAs have a trust association. In a multidomain environment, we must determine how to identify available PCAs and inter-CA trust associations when roaming in a foreign region or interacting with vehicles and roadside infrastructure from a foreign domain;

TABLE I
CRYPTOGRAPHIC PRIMITIVES CONSIDERED FOR VC SYSTEMS.

VC Standards and Harmonization \ Cryptographic Primitives	Asymmetric Key	Symmetric Key	Hash Functions
IEEE 1609.2	ECC: ECDSA (P-224 or P-256 curves) or ECIES (P-256 curve)	AES-CCM	SHA-256
ETSI	ECC: ECDSA (only P-256 curve) or ECIES (P-256 curve)	AES-CCM	SHA-256
C2C-CC	LTC (ECDSA-256) and Pseudonyms (ECDSA-224)	—	SHA-256

a lightweight directory access protocol service can facilitate this [7].

Cryptographic Primitives: Table I shows cryptographic primitives considered in standardization documents (IEEE P1609.2/D12, *Draft Standard for Wireless Access in Vehicular Environments*, January 2012, ETSI TR-102-731, *Intelligent Transport Systems Security; Security Services and Architecture*, and ETSI TR-102-941, *Intelligent Transport Systems Security; Trust and Privacy Management*), and harmonization efforts. The motivation for Elliptic Curve Digital Signature Algorithm (ECDSA) is that it produces shorter signatures than the ones by the Rivest-Shamir-Adleman (RSA) cryptosystem. IEEE 1609.2 considers a Discrete Logarithm and Elliptic Curve Integrated Encryption Scheme (DL/ECIES) to protect communication during the pseudonym acquisition phase, as do other proposals. Symmetric cryptography, i.e. an Advanced Encryption Standard in Counter Mode with a Cipher Block Chaining Message Authentication Code (AES-CCM), is proposed for other wireless networking standards IEEE 802.11 or Zigbee/IEEE 802.15.4 (IEEE P1609.2/D12 document).

III. VC SECURITY INFRASTRUCTURE DEVELOPMENT

In most of the literature [5, 8, 9, 10, 11, 12], including standardization documents (IEEE P1609.2/D12, ETSI TR-102-731, and ETSI TR-102-941), the VPKI entities are assumed fully trustworthy. This is a reasonable assumption; however, recent experience from mobile computing applications and Location-Based Services (LBSs) shows that applications and services aggressively collect user information. While they may remain trustworthy, not deviating from their protocol specifications and offering reliable services to their users, service providers can be tempted to infer sensitive user information and profile users (e.g., attempting to monetize this by offering customized services), based solely on the prescribed functionality.

This type of deviation relates to the *honest-but-curious* adversarial model. In the VC context, we consider VPKI servers (e.g., LTCAs and PCAs) to be honest, complying with security policies and correctly executing protocols, but also curious, seeking to infer user-sensitive information. This can be especially tempting, because a transcript of V2X communication (e.g., as it could be collected by a mesh network of VC-compatible radios) could be converted into a rich set of user trajectories and profiles if processed with the information that the VPKI entities possess.

This concern, aggravated by a potential spread of the responsibility to run credential and identity providers, is discussed first in this section. In spite of the common understanding that VPKI servers should have well-defined distinct roles, safeguarding users from honest-but-curious servers is not trivial and, in most cases, not achieved. At the same time, current VPKI designs do not fully prevent abuse of anonymity (or, to be precise, pseudonymity) by malicious (dishonest) clients, i.e., vehicles or RSUs. This can be seen as a by-product of the role separation. The second part of this section surveys how to improve VPKIs to render VC more trustworthy.

A. Privacy Considerations

Before issuing pseudonyms, the PCA either communicates with an LTCA to have the requester (vehicle) VPKI server authenticated or authenticates the vehicle itself. Several VPKI schemes [5, 8, 9, 12] follow the former approach, i.e., the C2C-CC design proposal where the PCA directly communicates with the vehicle's LTCA. Another set of VPKI schemes [7, 11, 13] proposes an indirect involvement of the LTCA, which issues a token to the vehicle that can be presented and verified by the PCA before issuing the pseudonyms.

For both approaches, the motivation is to maintain *distinct roles*, i.e., to separate the long-term identification of the vehicles from their short-term identities (their pseudonyms). A PCA should ideally be assured that it serves a legitimate vehicle, without accessing the long-term identity and credentials of the vehicle. On the other hand, the LTCA should not know which pseudonyms the vehicle obtained (and for which period). If either of the two happened, then a single VPKI entity would breach user privacy: the actions (signed messages) of the vehicle, matched to its pseudonyms, would be linked to each other and the vehicle long-term identity. For the same reason, the overall vehicle-PCA-LTCA communication should not be accessible by any other observer.

In all available proposals, the PCA can trivially link the pseudonyms issued as a response to one vehicle request, with the exception of a proxy-based scheme that shuffles requests from multiple vehicles and forwards them to the PCA [5]. However, this unlinkability would hold only if the proxy was fully trusted. Assuming this is so while the PCA is deemed honest but curious can be hard to motivate.

It is more important to prevent a PCA from linking sets of pseudonyms issued for the same vehicle as responses to two or more distinct requests (i.e., pseudonym acquisition protocols). This can be achieved by most proposals as they explicitly

preclude, for example, the use of long-term credentials or the use of an available pseudonym for vehicle authentication.

However, the involvement of the LTCA in authenticating the client reveals information. In most proposals, the LTCA learns which vehicle requests service from which PCA, and, thus, the actual pseudonym acquisition time. This information, along with some default policy data, could make it easy to guess which set of pseudonyms (thus, which set of signed messages) correspond to which vehicle (long-term identity). The problem has been identified only in a recent token-based scheme [7]. It hides from the LTCA the timing information as well as the PCA from which the vehicle seeks to obtain its next set of pseudonyms.

The ramifications of pseudonym lifetime and the use of time information to link pseudonyms are discussed further in the ''challenges'' section. Moreover, decoupling the LTCA and the PCA knowledge for the sake of privacy raises security and resilience considerations. This is discussed further when we consider revocation (which necessitates maintaining a mapping of short- and long-term identities, unless the scheme is fully anonymized [9]).

B. Resilience considerations

In a multidomain VC system with a multiplicity of PCAs, a compromised vehicle could obtain multiple (sets of) simultaneously valid pseudonyms simply by submitting multiple requests to distinct PCAs. This presumes a minimal protection to reject spurious requests from the same vehicle and to issue a set of nonoverlapping pseudonyms as a response to each request. With multiple short-term private/public key pairs and the corresponding certificates (pseudonyms), the attacking vehicle could appear as multiple vehicles. It could, for example, inject multiple erroneous hazard notifications and mislead the system (while, perhaps, a single report would not suffice to raise an alarm).

This ''Sybil-based'' misbehavior, the acquisition of multiple simultaneously valid credentials, is not considered in the C2C-CC and CAMP [5] designs. A number of other proposals [8, 9, 12, 13] do not manage to prevent this without any provision to tie the pseudonym acquisition period to a request. It is not straightforward to have the LTCA enforce a policy without revealing information, unless a specific design is put in place to keep information and still allow a policy to be enforced. For example, [7] does not reveal information to the LTCA since the vehicles hide their actual requested interval to obtain pseudonyms with universally fixed lifetimes determined by the LTCA. Thus, vehicles can obtain pseudonyms within the requested time interval without revealing the actual pseudonym acquisition period.

Note that these issues emerge exactly because of the generalization of the system setup and the strengthening of the adversarial model, compared to earlier works, which nonetheless propose alternatives such as the reliance on a Hardware Security Module (HSM) (ensuring that all signatures are generated under a single valid pseudonym at any time) [14].

C. Revocation

In case of misbehavior, the wrongdoer can be evicted (i.e., prevented from further participating in the system). This is standardized in the Internet, and it is considered for long-term VC credentials, the LTC of vehicles, and the security infrastructure entities. Nonetheless, what is distinctive here is the multiplicity of short-term credentials used by the vehicles and the need to revoke those as well. Interestingly, the standardization documents (IEEE P1609.2/D12, ETSI TR-102-731, and ETSI TR-102-941) and harmonization (C2C-CC) efforts are inconclusive on that front.

The distinction of VPKI roles offers an interesting option: the vehicle can be shunned off by the LTCA, which does corroborate its legitimacy to the PCA [14], thus preventing the vehicle from obtaining any additional pseudonyms. This alone, of course, does not prevent a compromised vehicle from misbehaving while using any pseudonyms it has (and the corresponding private keys) until they expire. The revocation of pseudonyms is necessary to close down this vulnerability window. Consider, for example, the practice outlined in the C2C-CC documentation, which recommends preloading the vehicle with approximately 1,500 pseudonyms to be used for one year. An active malicious disruption from an ''insider'' for a significant fraction of a year could be disastrous.

One can reduce this vulnerability by requiring that vehicles interact with the VPKI regularly, e.g., once per day or a few times per day, or at least as frequently as the dissemination of revocation information by the PCAs. Still, within this period, the high-stakes nature of VC, possibly risking the well-being of individuals and property, can necessitate a reaction, i.e., revocation of pseudonyms.

The pseudonym revocation can be done by ''traditional'' methods adjusted to the requirements of VC. The distribution of Certificate Revocation Lists (CRLs) has been assumed by several proposals [5, 7, 11, 13]. It was investigated [15, 16], along with localized distributed protocols to protect against wrongdoers until they are revoked [17]. It was also integrated in recently implemented systems along with a brief comparison with the online certificate status protocol [7]. The challenge of timely dissemination of credential validity information that does not interfere with vehicle operation remains.

IV. Challenges

Based on and beyond the technical discussion in the previous sections, here we discuss a number of significant challenges for the identity and credential management of fundamental importance toward deploying a secure VC system. We extend this discussion by considering a non-technical operational uncertainty at this point.

Pseudonym Lifetime Policy: The more frequent the changes, the more effective the privacy protection (the higher the unlinkability); ideally, each pseudonym should be used for a single message authentication. However, this could be excessively costly, e.g., if one considers the high-rate safety beaconing (e.g., three to ten beacons per second) and the

resultant large numbers of pseudonyms to be provided to each vehicle. Equally important, safety applications necessitate partial linkability, over a period, to facilitate their task. For example, inferring a collision hazard based on logically unlinkable CAMs would be hard (e.g., needing strictly use of location information) and error prone. Thus, a ‘‘compromise’’ was considered early on with partial linkability (over the lifetime of the pseudonym) [3], while several proposals investigated when/how to change pseudonyms for effective protection. Some current considerations suggest, antidiametrically, using one or a few pseudonyms per day. This divergence of views comes along with the fact that standards and harmonization efforts have not established any guideline for the pseudonym lifetime or other policies. This is clearly a necessity, independently of the flexibility the user would like to enjoy.

A significant consideration that is not pertinent to the privacy-effectiveness tradeoff relates to security. As discussed earlier, without the necessary design, attacking vehicles could amplify the effect of their misbehavior when they obtain multiple simultaneously valid credentials. One approach to prevent this, mentioned previously, is to issue pseudonyms with nonoverlapping lifetimes. This tends to become de facto or implicitly common. However, when combined with flexible access to the PCA, as the user needs to, this can undermine unlinkability and timing information can reduce uncertainty and make sets of pseudonyms obtained by the same user linkable (more likely to be). This was recently discovered and a countermeasure was outlined based on enforcing a specific pseudonym lifetime policy [7]. Again, this emphasizes the need to standardize policies with clear objectives.

Revocation: As discussed previously, there is no consensus on the need and the method for revocation of pseudonyms. While several VPKI proposals address the need of pseudonym revocation [5, 7, 8, 11, 13, 16], standardization bodies and harmonization efforts propose revocation of only long-term credentials, but not the pseudonyms. Moreover, revocation could be necessary for other reasons (e.g., revoking an attribute of a whole class of vehicles [18]). Essentially, there is a tradeoff between vulnerability and cost, which also rises if one seeks to reduce risk by mandating more frequent vehicle-VPKI interactions. This needs to be explored, along with a clear determination of a policy on what events necessitate revocation.

Extending to Anonymous Authentication Primitives: Although classic public-key cryptography has been a pillar for securing VC systems, there have been proposals to leverage anonymous authentication in the context of VC. Calandriello et al. [19] use group signatures for vehicles to issue on-the-fly pseudonyms with two follow-up investigations in [20] and [21]; Studer et al. [10], Lin et al. [22], and Lu et al. [23] also propose the use of group signature protocols with the former using keys as long-term credentials; and Förster et al. [9] use zero-knowledge proofs [24] to the VPKI infrastructure. A convergence with the standardized approaches could yield significant benefits, and, thus, a recommendation for additional investigations.

TABLE II
LATENCY FOR ISSUING 100 PSEUDONYMS.

	D_{PCA} (ms)	CPU_{PCA} (GHz)
VeSPA [11]	817	3.4
SEROSA [13]	650	2.0
PUCA [9]	1,000	2.53
SR-VPKI [7]	260	2.0

Extensive Experimental Validation: In the light of the VC large-scale multidomain environment, the efficiency of the VPKI and, more broadly, its scalability are important. Thus far, this has received limited attention, with few schemes evaluating implementation performance. Table II shows the latency to issue 100 pseudonyms in different VPKI systems. The dual-core CPU clock is provided only as an indication of the processing power, but clearly a direct comparison is not straightforward with the available information, although the four experimental setups resemble or are at least close to each other. The motivation is to highlight the need for extensive experimental evaluation to ensure the viability (in terms of performance and cost) of the VPKI as the VC system scales up.

Operational Challenges: As discussed in the ‘‘Shaping the VC Security Infrastructure’’ section, a domain is not yet precisely defined across different standardization documents and efforts. The key questions are who will operate the identity and credential provision and how trust relationships will be established. Moreover, policies that determine how to select and certify these VPKI entities are necessary. At the same time, VC systems will also operate as an extension of the mobile Internet, offering other (e.g, infotainment) services to their users. This would raise the question of how to manage identities and credentials for those applications and how to enable a coexistence of the two ‘‘worlds.’’

In conclusion, it is necessary to pave the way for the deployment of secure and privacy-protecting VC systems with an identity and credential management infrastructure that builds upon the past multiyear efforts and developed understanding, and addresses a number of open questions to achieve enhanced protection (of the system and its users) and scalability as VC becomes ubiquitous.

V. ACKNOWLEDGEMENT

The research leading to these results received funding from the Preparing Secure Vehicle-to-X Communication Systems FP7 European project (http://www.preserve-project.eu).

Author Information

Mohammad Khodaei (khodaei@kth.se) earned his diploma in software engineering from Azad University of Najafabad in Isfahan, Iran, in 2006 and his M.S. degree in information and communication systems security from KTH, Stockholm,

Sweden, in 2012. He is currently pursuing his Ph.D. degree at the Networked Systems Security Group, KTH, under the supervision of Prof. Panos Papadimitratos. His research interests include identity and credential managements in vehicular ad hoc networks, the Internet of Things, and smart cities.

Panagiotis (Panos) Papadimitratos (papadim@kth.se) earned his Ph.D. degree from Cornell University, Ithaca, New York, in 2005. He then held positions at Virginia Tech, École Polytechnique Fédérale de Lausanne, and Politecnico of Torino. He is currently an associate professor at KTH, where he leads the Networked Systems Security Group. His research agenda includes a gamut of security and privacy problems, with emphasis on wireless networks.

REFERENCES

[1] European Telecommunications Standards Institute, ''Intelligent transport systems (ITS); vehicular communications; basic set of applications; definitions,'' ETSI Tech. TR-102-638, June 2009.

[2] P. Papadimitratos, A. La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza, ''Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation,'' *IEEE Communications Magazine*, vol. 47, no. 11, pp. 84–95.

[3] P. Papadimitratos, V. Gligor, and J.-P. Hubaux, ''Securing vehicular communications-assumptions, requirements, and principles,'' in *ESCAR*, pp. 5–14.

[4] 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*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

[5] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, ''A security credential management system for V2V communications,'' in *IEEE VNC*, pp. 1–8.

[6] N. Bißmeyer, H. Stubing, E. Schoch, S. Gotz, J. P. Stotz, and B. Lonc, ''A generic public key infrastructure for securing car-to-x communication,'' in *ITS World Congress*, Orlando, Florida, USA, Oct. 2011, p. 12.

[7] M. Khodaei, H. Jin, and P. Papadimitratos, ''Towards deploying a scalable & robust vehicular identity and credential management infrastructure,'' in *IEEE VNC*, pp. 33–40.

[8] F. Schaub, F. Kargl, Z. Ma, and M. Weber, ''V-tokens for conditional pseudonymity in VANETs,'' in *IEEE WCNC*, NJ, USA, pp. 1–6.

[9] D. Förster, H. Löhr, and F. Kargl, ''PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET),'' in *IEEE VNC*, Paderborn, Germany, pp. 25–32.

[10] A. Studer, E. Shi, F. Bai, and A. Perrig, ''TACKing together efficient authentication, revocation, and privacy in VANETs,'' in *IEEE SECON*, pp. 1–9.

[11] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos, ''VeSPA: Vehicular security and privacy-preserving architecture,'' in *ACM HotWiSec*, Budapest, Hungary, pp. 19–24.

[12] N. Bißmeyer, J. Petit, and K. M. Bayarou, ''Copra: Conditional pseudonym resolution algorithm in VANETs,'' in *IEEE WONS*, pp. 9–16.

[13] S. Gisdakis, M. Laganà, T. Giannetsos, and P. Papadimitratos, ''SEROSA: Service oriented security architecture for vehicular communications,'' in *IEEE VNC*, Boston, MA, USA, pp. 111–118.

[14] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, ''Architecture for secure and private vehicular communications,'' in *IEEE ITST*, Sophia Antipolis, pp. 1–6.

[15] J. J. Haas, Y.-C. Hu, and K. P. Laberteaux, ''Design and analysis of a lightweight certificate revocation mechanism for VANET,'' in *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*, New York, NY, USA, pp. 89–98.

[16] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, ''Certificate revocation list distribution in vehicular communication systems,'' in *ACM VANET*, San Francisco, CA, pp. 86–87.

[17] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, ''Fast exclusion of errant devices from vehicular networks,'' in *IEEE SECON*, San Francisco, CA, pp. 135–143.

[18] P. Papadimitratos, ''"On the road" - Reflections on the Security of Vehicular Communication Systems,'' in *IEEE ICVES*, Columbus, OH, USA, pp. 359–363.

[19] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ''Efficient and robust pseudonymous authentication in VANET,'' New York, USA, pp. 19–28.

[20] P. Papadimitratos, G. Calandriello, A. Lioy, and J.-P. Hubaux, ''Impact of Vehicular Communication Security on Transportation Safety,'' in *Proceedings of the 28th IEEE INFOCOM Workshop on Mobile Networking for Vehicular Environments (MOVE)*, Phoenix, AZ, USA, pp. 1–6.

[21] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, ''On the performance of secure vehicular communication systems,'' *IEEE TDSC*, vol. 8, no. 6, pp. 898–912.

[22] X. Lin, X. Sun, P.-H. Ho, and X. Shen, ''GSIS: a secure and privacy-preserving protocol for vehicular communications,'' *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456.

[23] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ''ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications,'' in *IEEE INFOCOM*, Phoenix, AZ, USA, pp. 13–18.

[24] 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*, New York, NY, USA, Oct. 2006, pp. 201–210.