SEROSA: SERvice Oriented Security Architecture for Vehicular Communications

Stylianos Gisdakis, Marcello Laganà, Thanassis Giannetsos, Panos Papadimitratos
KTH Royal Institute of Technology
Stockholm, Sweden
{*gisdakis*, *lagana*, *athgia*, *papadim*}@kth.se

***Abstract*—Modern vehicles are no longer mere mechanical devices; they comprise dozens of digital computing platforms, coordinated by an in-vehicle network, and have the potential to significantly enhance the digital life of individuals on the road. While this transformation has driven major advancements in road safety and transportation efficiency, significant work remains to be done to support the security and privacy requirements of the envisioned ecosystem of commercial services and applications (i.e., Internet access, video streaming, etc.). In the era when "service is everything and everything is a service", Vehicular Communication (VC) systems cannot escape from this ongoing trend towards multi-service environments accessible from anywhere. To meet the diverse requirements of vehicle operators and Service Providers (SPs), we present SEROSA, a service-oriented security and privacy-preserving architecture for VC. By synthesizing existing VC standards and Web Services (WS), our architecture provides comprehensive identity and service management while ensuring interoperability with existing SPs. We fully implement our system and extensively assess its efficiency, practicality, and dependability. Overall, SEROSA significantly extends the state of the art and serves as a catalyst for the integration of vehicles into the vast domain of Internet-based services.**

Keywords*—*Vehicular Communications, Security, Privacy, Access Control, Identity Management, Web-Services

I. Introduction

For many years, researchers, car manufacturers, and politicians have aspired to a new technology that shall make travelling by car safer, faster and "greener". Vehicular Communications (VC) play a central role in this effort, bringing forth a number of benefits spanning from *road safety* and *traffic efficiency* to *driving convenience* [1, 2]. Thus far, the main benefit of VC has been safety systems that address the ever-growing safety concerns for citizens' well-being. Immediate impacts include alleviating the traffic congestion and improving operations management in support of navigation and safety applications, such as collision avoidance and environmental/hazard warnings among others [3].

Nonetheless, as vehicles become more automated, integrating more consumer devices [4] and featuring powerful embedded platforms and antennas, a new trajectory of commercial applications and services will emerge. Indeed, in the era when "*service is everything and everything is a service*", there is a growing demand for accessing the Internet and personalized services (tailored to the specific interests of individuals) from vehicles. This transformation is driven by the concept of leveraging "car as a platform" capable of running a gamut of services and performing numerous transactions for their users. The envisioned ecosystem of applications will range from simple infotainment services [5] and content distribution [6] to Internet access and the development of an "Application Store" for automotive applications [7, 8]. Such multi-service environments are expected to provide clear customer benefits and motivate commercial operators to invest in large-scale deployments of VC systems.

Security and *Privacy* are paramount in vehicular networking environments, especially in the context of safety applications where critical decisions are based on information collected by vehicles. Intensive efforts in academia, industry, and standardization bodies have converged to the use of Vehicular Public Key Infrastructures (VPKIs) [5, 9] for credential and identity management. However, the anticipated transplantation of commercial services into the VC domain calls for comprehensive solutions that can bring closer the worlds of VC networks and Internet-based services, giving birth to a *service-oriented* vehicular ecosystem.

If we are to fruitfully benefit from this evolution, security and user privacy remain key pillars. Addressing the diverse requirements of vehicle operators and Service Providers (SPs) for identity management and fine-grained access control across multiple domains, is the challenge ahead. *How can we synthesize VC standards with solutions currently deployed for Internet-based services? How to create an efficient and globally recognized credential and identity management architecture to enable vehicles to access any service they are entitled to from anywhere?*

The answers to these questions are not straightforward; they pose a series of new technical and research challenges. Existing architectures and standards are tightly coupled with the rigid security and privacy requirements of current VC applications. Thus, they cannot, per-se, facilitate the fusion of Internet-based services into the vehicular domain. An alternative approach would be to directly incorporate currently deployed Internet-based security technologies (i.e., SAML [10], OAuth [11], OpenID [12]). However, this is not desired due to the intricacies and the inherent operational constraints (e.g., strong privacy and liability attribution) of vehicular networking environments. Furthermore, since existing Internet business models already entail a plethora of commercial SPs, it would be best if stakeholders from the vehicular domain tried to lure them in providing VC-tailored services instead of looking for new ones. This calls for a synthesis of VC-specific standards with widely accepted Internet technologies such as Web Services (WS).

We address these challenges with *SEROSA*, a service-oriented security and privacy-preserving architecture for VC

978-1-4799-2687-9/13/$31.00 ©2013 IEEE

systems. *SEROSA* provides authentication, authorization, accountability and user privacy along with a comprehensive set of services for identity management in multi-service automotive ecosystems. Service discovery and registration support the provision of various personalized services and motivate SPs to enter the vehicular market. Furthermore, the establishment of trust relations (*federations*) among different system entities facilitates access control across multiple domains. User privacy still remains at the core of *SEROSA* which encompasses existing vehicular communication standards and enhances the underlying VPKI by leveraging long-term credential and identity managing entities (expected to be deployed in VC systems). We propose novel and efficient authentication protocols, based on the use of WS, to support a multiplicity of diverse services so as to engage the participation of more vehicle operators.

Overall, *SEROSA* extends VC security and privacy state of the art by offering: *(i)* diverse service discovery and registration across multiple domains, *(ii)* fine-grained authorization, access control and accountability, *(iii)* user privacy enhancement and service unlinkability, *(iv)* flexible, interoperable, dependable and scalable multi-domain identity management, and *(v)* a full-blown implementation of all system components and protocols, according to the WS paradigm, along with an evaluation of their efficiency, practicality and dependability through extensive and realistic simulations.

The remainder of this paper is organized as follows: The current status of vehicular communication systems is discussed in Section II. Section III defines the adversarial model assumed throughout this work. Sections IV and V comprise the core of this work; they give an insight to *SEROSA* and the services it offers, an overview of its architecture along with a detailed presentation of all implemented components and protocols. In Section VI, we present a qualitative security and privacy analysis of our scheme. Section VII assesses the proposed architecture in terms of efficiency, practicality and dependability and in Section VIII we conclude.

II. Vehicular Communication Background

Intelligent Transport Systems enhance transportation safety and efficiency [2], based on the communication between vehicles, Roadside Units (RSUs) and back-end infrastructure. Communication modules operate either in an ad-hoc manner (i.e., IEEE Wireless Access in Vehicular Environments (WAVE) [9] 802.11p) or over the existing cellular infrastructure (i.e., over 3G/LTE networks). VC systems need strong and practical security and user privacy mechanisms to meet the rigid requirements of vehicular networking environments [13, 14]. Standardization bodies and working groups such as the IEEE 1609 working group, the Car2Car Communication Consortium (C2C-CC) [15] and the European Telecommunications Standards Institute (ETSI) [5], have been releasing VC-related specifications for multi-channel wireless operations, message formats, as well as security and privacy-preserving architectures.

At the same time, the strong research interest in feasible, versatile, collaborative and secure VC systems, has spurred a number of European projects. The E-safety Vehicle Intrusion protected Applications (EVITA) [16] project developed a prototype for securing in-car networks, while the Secure Vehicle Communication (SeVeCom) [17] and Privacy Enabled Capability in Co-operative Systems and Safety Applications (PRECIOSA) [18] projects addressed the complex security and privacy challenges over the wireless channel. The Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) [19] project is working towards the design, implementation, and evaluation of a complete secure and privacy-preserving subsystem that employs a Hardware Security Module (HSM). DRIVE C2X [20], instead, aims at a comprehensive assessment of cooperative driving systems through Field Operational Testss (FOTs), while OVERSEE [21] is developing a platform capable of providing a generic, standardized communication and application development framework for vehicle operators.

The aforementioned research efforts have converged to the use of pseudonym-based schemes as the main privacy preserving mechanism for VC [13]. Following the IEEE and ETSI standards specifications, each vehicle has a unique, long-term identifier L_{id}, a public key LK and the corresponding private key Lk. The LK is bound to L_{id} by means of certificates. Each vehicle is also provided with a set of anonymous credentials, the pseudonyms Ps_i, which correspond to ephemeral asymmetric key-pairs (PK_i, Pk_i). In contrast to L_{id}, pseudonyms contain no information that can identify the vehicle. To enhance the trustworthiness of the system, HSMs securely store Lk and Pk_i keys and generate digital signatures. The effectiveness and efficiency, in terms of communication overhead, of such pseudonym-based architectures have been studied in [22, 23].

VC standards define how Certification Authorities (CAs) offer credential management services by issuing, certifying and revoking L_{id} and Ps_i. Long Term CAs (LTCAs) are responsible for the management of L_{id}, of both vehicles and RSUs, whereas pseudonym management is performed by Pseudonym CAs (PCAs). Actual VC deployments are expected to include multiple (of the aforementioned) authorities, spanning different administrative and geographical domains, organized into a VPKI. In this line of research, the authors in [24] considered solely pseudonym provision and resolution. VeSPA [25], and its extension [26], paved the way for *multi-service*, multi-domain architectures in VC systems. Nevertheless, they rely on custom authentication protocols and, thus, are not compatible with existing Internet SPs. Besides being more efficient than VeSPA (see Section VII-B), our scheme also considers advanced aspects such as service registration and discovery.

A Vehicle-to-Infrastructure (V2I) authentication scheme based on vehicle movement prediction is proposed in [6]. The authors in [27] defined an Authentication, Authorization and Accounting (AAA) system leveraging e-currency to improve authentication delay, security and privacy while providing billing and access control properties. Although these works propose a (limited) security and privacy service-oriented architecture for VC, in contrast to SEROSA, they do not comply with the current vehicular standards and do not consider diverse multi-domain services offered by existing SPs.

III. Adversarial Model

The inherently open VC systems are vulnerable to abuse by both *outsider* and *insider* adversaries [14]. The latter ones setup as registered and authorized participants and exhibit faulty behavior. The former are unauthorized entities that seek to compromise the VC system and disrupt its operation. Outsiders have no credentials or trust relationships with other system

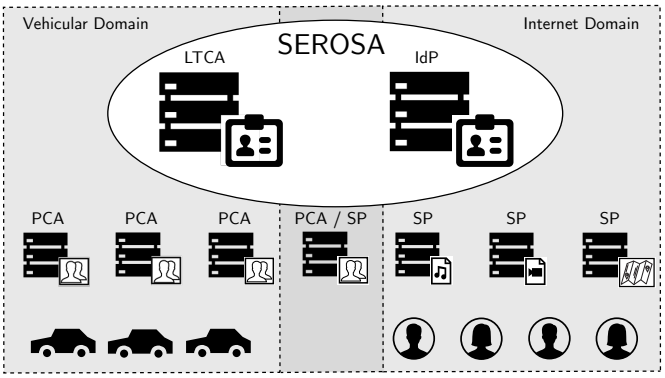

Figure 1: Merging VC with Internet-based services

entities and this limits their disruptive capabilities. Irrespectively of their type, both aim at disrupting the system operation by launching a plethora of attacks. Especially internal adversaries might pose as multiple vehicles (acting as a Sybil entity). We do not dwell on communication network attacks and outages such as jamming, DoS and DDoS as they are orthogonal to this investigation.

In the context of service provision, we consider adversarial behavior of users who might either try to access services that are not entitled to (i.e., *free-riders*) or repudiate having received them. Nevertheless, we do not limit adversaries solely to users. We additionally address the case of misbehaving VC authorities and entities. More specifically, we consider the following cases:

- *Honest-but-curious entities*: SPs and VC authorities, that do not deviate from the expected protocol behavior, might try to violate the privacy of users by de-anonymizing or profiling them.
- *Fraudulent SPs*: Malicious SPs that might fraudulently accuse users for having received a service in order to benefit from them.

The aforementioned attacks can be launched by single SPs or collaboratively, by multiple *colluding* SPs. We assume that Identity Providers (IdPs) are trusted. Nevertheless, in Sec. VI we discuss mechanisms that can weaken this assumption.

IV. Motivation and Design Choices

A gamut of diverse applications and services are expected to find their way to the vehicular ecosystem. Existing Internet-based service providers with multiple security policies and service agreements will be soon offering their services to VC users. Moreover, users seeking personalized services will wish to subscribe to many of them. As vehicle mobility cannot be geographically constrained, it is likely that such services will span over multiple administrative domains.

We argue that, in their current form, VC security architectures cannot address this complex and dynamic setting. On the other hand, a direct application of existing security solutions from the Internet domain is not desired as they cannot meet VC security and privacy requirements [13, 14]. What we are after is a comprehensive security and privacy-preserving identity management that is a *synthesis* of the current VC and Internet-based standards (Figure 1). Towards this, we present SEROSA, *a service-oriented security and privacy-preserving architecture for VC* that focuses on the following:

- *Privacy Preserving Identity Management and Authentication*: A service-oriented VC architecture should provide the necessary means that allow the creation, authentication and management of the identities of system entities (i.e., vehicles, authorities and SPs) across multiple domains. However, such an identity management scheme should not come at the expense of user privacy.
- *Authorization, Access Control and Liability*: Each vehicle should be able to access any service it is entitled to within any administrative domain in a privacy-preserving, efficient, and accountable manner. Furthermore, it is critical that VC identity management systems enforce fine-grained security policies to accommodate the requirements of different SPs. Vehicles and system entities should be kept accountable of their actions that could result in system disruption. Therefore, proper mechanisms to attribute liability in cases of misbehavior are essential. Nevertheless, we have to note that although misbehavior detection is an important part of vehicular security, it is orthogonal to this investigation.
- *Service Unlinkability*: Service requests should not be linked and traced back to the long-term identity of the requesting users and vehicles.
- *Federated Trust*: A service-oriented VC architecture should transparently establish strong trust relations (federations) among different entities of the system. Vehicles should be able to receive services from various SPs, which in turn rely on multiple IdPs for authentication and access control. This defines the need for a scalable Web of Trust (WoT) among the involved stake-holders.
- *Service Discovery*: To support the provision of various personalized services and motivate SPs to enter the vehicular market, a service-oriented VC architecture should offer the necessary means for advertisement and discovery of all offered services within an administrative domain.

All of the aforementioned functionalities should be provided in a *standard-compliant* and *platform-neutral* manner to ensure interoperability and scalability.

V. System Entities and Design

SEROSA synthesizes Web Services and VC credential management entities, as defined by the current standards. More specifically, the LTCA (see Sec. II and Figure 1) becomes an IdP that offers security services (i.e., Authentication, Authorization and Access Control) for any SP. Accordingly, PCAs are SPs that provide standard-compliant pseudonyms to the requesting vehicles. Vehicles register to the system and receive certified long-term credentials. Consequently, they query for the services offered within a domain and receive identifiers of the ones they are entitled to acquire. Finally, in case it is mandated by legal authorities, vehicles are evicted from the system (e.g., as a consequence of misbehavior) and prevented from further participation. In what follows, we present the services and protocols offered by SEROSA. We consider pseudonym provision as a use-case of a service for the rest 1of this paper.

A. Federated Trust

Trust relationships among the SEROSA entities are established by means of Security Assertion Markup Language (SAML). In order to establish trust between the Identity Provider and each involved SP, a WS-Metadata exchange

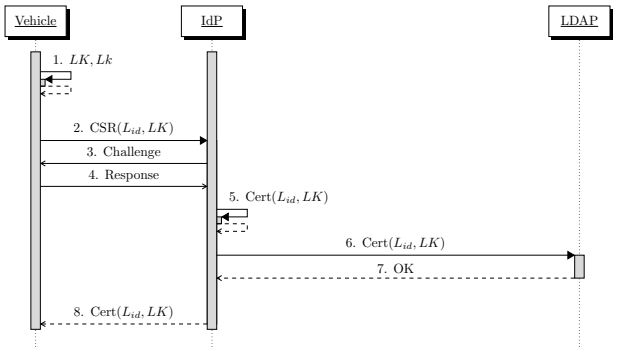

Figure 2: Vehicle Registration

takes place [28]. Metadata are Extensible Markup Language (XML)-based entity descriptors that contain various pieces of information, such as authentication requirements, Uniform Resource Identifiers (URIs), protocol bindings and digital certificates. More specifically, metadata published by an IdP contain the *X.509* certificates that have to be used by the various SPs in order to verify the signatures generated by the IdP. Similarly, SPs publish metadata that contain their corresponding digital identifiers and certificates. After the establishment of a trust relation, SPs can receive identity management services from the IdP.

These mechanisms are used to build large and complex trust models among multiple IdPs and SPs, thus, enabling the establishment of a globally recognized identity management and access control system that spans over multiple VC domains.

B. Vehicle Registration

The first step in a vehicle identity life-cycle is its registration to an authority (i.e., IdP) and the subsequent generation of its long-term credentials (Figure 2). The HSM of a vehicle generates a key-pair: a public key LK and a private key Lk (Step 1). Then, it issues a Certificate Signing Request (CSR) that contains its long-term identity and LK (Step 2). The IdP then initiates a *proof-of-possession* protocol for verifying the ownership of the corresponding private key Lk (Steps 3 and 4). Upon successful completion, the IdP issues a certificate, $Cert_{(L_{\text{id}},LK)}$, and delivers it to the requesting vehicle (Steps 6, 7 and 8). All required information about registered vehicles is stored in a Lightweight Directory Access Protocol (LDAP) [29] server. In case the registration process is executed over the network, communications between the vehicle and the IdP are secured over a Transport Layer Security (TLS) tunnel (the certificate of the IdP is assumed to be pre-installed on the vehicle's HSM). By the end of this protocol, the vehicle is a legitimate entity of the VC system and ready to register to any provided services.

C. Service Provision

1) Service Registration: The vehicle needs to subscribe to the corresponding SP in order to be able to receive a service. We assume that a trust-relation is already established between the desired service provider and the IdP with which the vehicle has been registered. To achieve service registration and acquisition, we leverage SAML assertions that represent security claims produced by the IdP for the SP. SAML assertions carry the following types of security claims:

- **Authentication Statements:** Assert a SP that the vehicle (mentioned in the assertion) was authenticated according to an agreed authentication protocol.
- **Authorization Statements:** Assert that the vehicle was deemed eligible for acquiring a service.
- **Attribute Statements:** Contain information regarding the vehicle attributes, such as its type (i.e., public or private vehicles) and its clearance.

To register to a service, the following protocol is executed:

$$V \rightarrow SP : request\,\{ses_{\text{id}}, IdP\} \quad (1)$$

$$SP \rightarrow V \rightarrow IdP : reg\_req\,\{ses_{\text{id}}, serv_{\text{id}}, SP_{\text{id}}, t\}_{SP_{sig}} \quad (2)$$

$$IdP \rightarrow SP : reg\_res\,\{ses_{\text{id}}, serv_{\text{id}}, SP_{\text{id}}, t\}_{IdP_{sig}} \quad (3)$$

$$SP \rightarrow V : success\,\{ses_{\text{id}}, OK\} \quad (4)$$

Initially, the vehicle (V) contacts the desired SP and issues a service registration request. To protect user privacy, the vehicle does not reveal its L_{id}. A *session identifier* (ses_{id}) is used for identifying and managing the session during further execution of the protocol. This request also contains the id of the IdP to which the vehicle has registered (1). Once the SP generates the corresponding registration request, it is relayed by the vehicle to the IdP. Overall, the request contains the ses_{id}, the identifier of the requested service ($serv_{\text{id}}$), the identifier of the SP (SP_{id}) and a time-stamp t (for preventing replay attacks). To ensure authenticity, the request is signed by the issuing SP (2). Furthermore, to guarantee confidentiality and execution (of the request) only by the designated IdP, it can be optionally encrypted with the key specified during the metadata-exchange between the SP and the IdP (Sec. V-A). Additional pieces of information such as billing can be included in the request. Upon reception, the IdP authenticates the vehicle on the basis of its *long-term identity*. If successful, it issues a registration response as a proof that the vehicle has been registered for the service (3). Finally, the SP sends an acknowledgment back to the vehicle (4).

2) Service Discovery: A vehicle in a foreign administrative domain wishing to discover offered services can issue a Simple Object Access Protocol (SOAP) request to a Web Services Discovery Language (WSDL) enabled server and receive their description [28]. For instance, if the vehicle wishes to discover PCA services, then it can query the server for them. If trust relationships were established between the discovered PCA and the IdP (responsible for the domain from which the vehicle originates), the vehicle can receive the required pseudonyms. The details of service acquisition from foreign administrative domains is described later in this section.

3) Service Acquisition: Figure 3 illustrates the steps executed during the authentication protocol[1]. Initially, the vehicle requests the desired service (in an anonymous way) without disclosing its L_{id} to the SP (Step 1). Thereupon, the service provider issues an *authentication request* designated for the IdP. According to the specifications of SAML [28], the request is relayed by the vehicle (Steps 2 and 3). Consequently, the vehicle engages in an interactive authentication protocol with the IdP, based on TLS and their digital certificates. The vehicle reveals its long-term identity, L_{id}, and the IdP examines if it is entitled

[1]Due to space limitations we omit the specifications of SAML and instead refer the reader to [28].

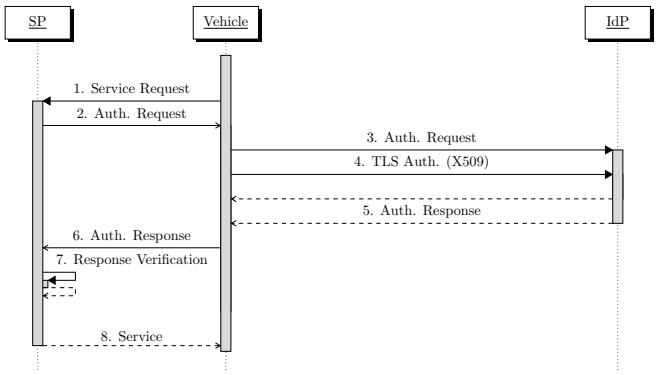

Figure 3: Service Acquisition

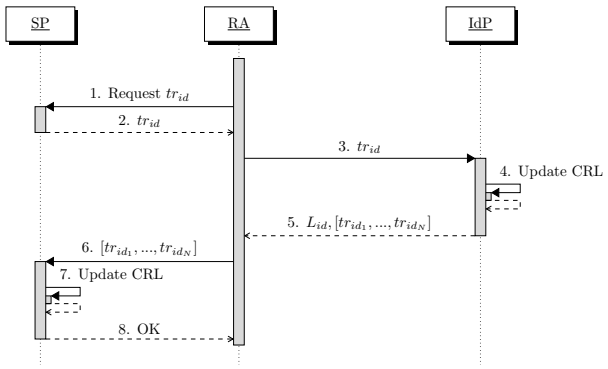

Figure 4: Pseudonym resolution and revocation

to receive the requested service (Step 4). Upon successful authentication, the IdP issues an *authentication response* that contains a SAML assertion. This assertion does not reveal the vehicle's L_{id} but instead contains a *transient identifier* tr_{id} (a random identifier generated by the IdP). Such identifiers obfuscate the long-term identity of the requesting vehicle, thus, preventing SPs from linking service requests to it. They are valid only for a single authentication request and change for each subsequent attempt. Upon reception, the SP validates the authentication response and examines the eligibility of the vehicle with respect to the service. Accordingly, it grants or denies access (Steps 7 and 8). The complete protocol runs over Hypertext Transfer Protocol (HTTP). To authenticate both the IdP and the SP, we leverage one-way TLS authentication that additionally ensures the confidentiality and integrity of communications.

Use-Case: Regarding pseudonym acquisition, the PCA serves as a service provider that issues pseudonyms to vehicles according to the 1609.2 specification [9]. Similar to the registration phase, the public (PK_i) and private (Pk_i) keys are generated inside the HSM. Once a vehicle is authenticated (following the above described protocol), it can request pseudonyms from the PCA. A certified pseudonym Ps_i is a digital signature, produced by the PCA, for the public key PK_i.

An advantage of our scheme is that there is no need to initiate the authentication process whenever the vehicle wishes to request a service. SEROSA supports Single-Sign-On (SSO) capabilities because SAML assertions can be re-used transparently for requesting services from multiple SPs within federated domains. SSO can accelerate service reception, by skipping authentication, in case no cellular network-based connectivity is available; thus, V2I communications are only feasible when the car is within the proximity of RSUs. Nonetheless, receiving services with SSO might harm the privacy of vehicle operators. A detailed discussion on SSO and its impact on user privacy is included in Sec. VI.

SEROSA allows registered vehicles (within one administrative domain) to be authenticated at foreign domains through SAML assertions. To enable this, we make use of *delegated authentication*. More specifically, when a vehicle (registered with domain D_A) accesses a SP in a foreign domain (D_B), it is redirected for authentication to the IdP_B of D_B. Since IdP_B has no information regarding the vehicle, it redirects the request to the IdP_A of D_A. Consequently, the authentication protocol is executed and a SAML assertion is generated by IdP_A and endorsed by IdP_B. This assertion is presented to the SP that delivers the service.

D. Pseudonym Resolution and Revocation

For liability attribution, our architecture provides mechanisms to trace a pseudonym, Ps_i, back to the vehicle's long-term identifier, L_{id}. In this context, authorities might additionally request the eviction of misbehaving vehicles from the system. To achieve pseudonym resolution, our scheme assumes that a Resolution Authority (RA), e.g., a law enforcement agency, initiates the process. An illustration of the protocol is presented in Figure 4.

The RA requests from the PCA the identifier tr_{id} of the SAML assertion for which Ps_i was issued (Step 1). The PCA responds with the corresponding tr_{id} (Step 2). The RA then provides the IdP with the tr_{id} that generated Ps_i (Step 3). The IdP updates the Certificate Revocation List (CRL) to include the $Cert_{(L_{\text{id}},LK)}$ of the vehicle with the corresponding transient identifier (Step 4). From this point on, the misbehaving vehicle can no longer be authenticated and, thus, receive new pseudonyms. Additionally, the IdP provides the RA with the L_{id} (of the vehicle) and the list of all the tr_{id_j} for which it has issued assertions (Step 5). This list is dispatched to the PCA which in turn updates its CRL to include all the Ps_i issued under these transient identifiers.

Steps $1, 2, 3$ and 5 of the protocol suffice in case simple pseudonym resolution, and not complete eviction from the system, is requested.

VI. Security and Privacy Analysis

In this section, we qualitatively analyze the security and privacy properties of SEROSA with respect to the requirements presented in Sec. IV. The *integrity* and *confidentiality* of all Vehicle-to-Infrastructure communications are protected by secure and authenticated (i.e., TLS) channels; thus, the system is immune to a wide range of attacks, e.g., session hi-jacking, eavesdropping, etc. The IdP is responsible for strict identification and authentication of all vehicles while authorities are authenticated through the use of digital certificates.

As discussed above, SAML offers great versatility when it comes to *Access Control and Policy Enforcement*. Identity and service providers can exchange authorization information through SAML assertions: they serve as the Policy Decision Points and Policy Enforcement Points respectively. Additionally, Role Based Access Control is feasible on the basis of SAML attribute statements, which can associate vehicles to specific

roles (i.e., public or private). In case of more complex security policies, over multiple domains, SEROSA supports eXtensible Access Control Markup Language [30]. Furthermore, the revocation protocol described in Sec. V-D can be used to revoke the anonymity of vehicles when they have been deemed misbehaving (*liability attribution*). All the above provide a globally recognized identity management and access control system that can span over multiple VC domains.

Compounding the issue of *Sybil attacks*, SEROSA mitigates their effects by means of HSMs similar to the one currently developed by PRESERVE [19]. More specifically, these trusted platforms serve as secure storage for all produced cryptographic keys. L_{id} and pseudonyms, Ps_i, are bound to such keys that never leave the HSM. If the pseudonyms of a vehicle have *non-overlapping* lifetimes (i.e., no two pseudonyms are valid during the same time interval) sybil attacks do not pose a threat.

Our architecture also ensures privacy in the case of "honest-but-curious" and colluding infrastructure. Curious SPs may attempt to passively violate a vehicle's privacy profile. However, linking of subsequent service requests (originating from the same vehicles) is infeasible because a different transient-identifier is used for each SAML assertion. Nevertheless, if SPs collude with an IdP, assertions issued by the misbehaving IdP can be tracked and resolved to the L_{id} of the vehicle. To address even this scenario, anonymous authentication methods, e.g., group signatures [31], or cryptographic vehicular tokens [24] could be used. At the same time, unauthorized users that have not subscribed to a service (see Sec. V-C), cannot fraudulently access it as the involved IdP will not issue a SAML assertion (during authentication). This renders SEROSA secure against *free-riders* (under the condition that the IdP does not misbehave). Moreover, SAML tokens serve as proof of service receptions; thus, malicious users cannot repudiate having received a service.

Re-using previously acquired assertions in a SSO manner may result in the linking of subsequent service requests and, thus, might harm the privacy of vehicle operators. This trade-off needs to be addressed by *policies* that (based on the mobility status of the vehicle) will define if and how SSO will be used.

VII. Performance Evaluation

In this section, we evaluate various aspects of our system's efficiency and reliability. Three properties are of interest: *vehicle authentication*, *pseudonym acquisition* and *revocation*. In an attempt to avoid confining our results, we have also considered the *network latency* induced by vehicular mobility which usually implies volatile network connectivity. In all cases, our goal is to provide strong evidence on efficient service provision in a vehicular networking environment.

A. Evaluation Environment Setup

In all our experiments, we considered a testbed comprising various Virtual Machines (VMs), each one dedicated to a different authority (IdP, PCA, and RA), together with remote clients that request to access some of the provided services. We employ the OpenSSL library for cryptographic operations; Elliptic Curve Digital Signature Algorithm (ECDSA), RSA signature schemes, and TLS connection establishment. To abide with the current standards and directives, we require that the ECDSA keys are computed over curves of 256-bit primes. Furthermore, to emulate network delay, we use a queuing discipline that increases randomly the data link delay following a normal distribution with $\mu = 10\,ms$ and $\sigma^2 = 2.5$. A summary of the whole system hardware and software configuration can be found in Table I.

	IdP	PCA	RA
Virtual Machines	1	3	1
Dual-core CPU 2.0 GHz	8x	1x	1x
System Memory	4 Gb	2 Gb	1 Gb
Web Service Software	SimpleSAMLphp	Shibboleth 2	✗
Apache Web Server	✓	✓	✓
Apache Load Balancer	✗	✓	✗
MySQL Database Server	✓	✓	✗
OpenLDAP Server	✓	✗	✗
OpenSSL	✓	✓	✓

Table I: The host setup for the system deployment.

B. Pseudonym Request

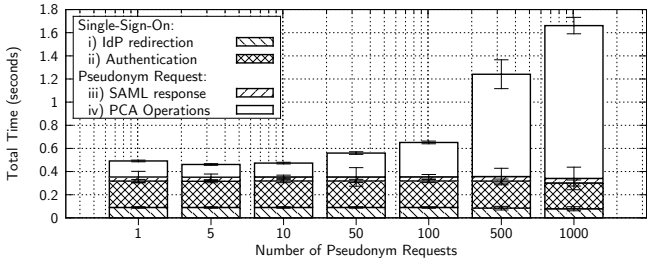

Figure 5: t_i for a single request containing an exponentially increasing number of pseudonyms, averaged over 1 000 runs.

A critical aspect for any VPKI is its *scalability*; while the L_{id} has (by definition) low variation frequency (e.g., from months to years), pseudonyms need to be frequently updated within time intervals from minutes to days, depending on the system policies. Consequently, a PCA should be able to handle not only as many requests per second as possible, but also support high-level concurrency, typical for dense vehicular mobility scenarios. For this reason, we replicated the functionalities of a PCA with 2 web-servers behind a proxy/load-balancer. We evaluated the time required for a single pseudonym request and studied the impact of multiple concurrent requests through a real-case scenario.

As described in Sec. V-C, to obtain the pseudonyms a vehicle needs to: (1) contact the PCA and receive the SAML authentication request, (2) authenticate itself to the IdP, (3) provide the assertion back to the PCA and, finally, (4) send the pseudonym signing requests in order to receive the new pseudonyms. We assume that the pseudonym signing requests are prepared in an off-line manner (by the vehicle) before protocol instantiation. We also consider the time for each authentication step t_1, t_2, t_3, and t_4 while $t_{\text{TOT}} = t_1+t_2+t_3+t_4$ denotes the total pseudonym acquisition time.

1) Single Vehicle: Each step of the service acquisition protocol (t_i) has been sampled 1 000 times for varying numbers of requested pseudonyms (from 1 to 1 000 assuming an exponential increase). The results are depicted in Figure 5. As expected, the first 3 steps do not depend on the size of the request, while step (4) shows the correlation with the number of requested pseudonyms. A significant increase in terms of latency is observed only for requests containing more than 10 pseudonyms. Indeed, before reaching this point, the network operation time compensates the time required for signatures,

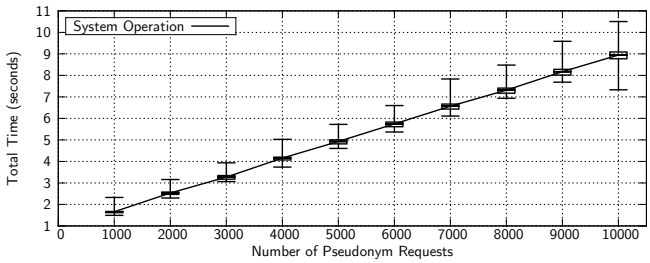

Figure 6: t_{TOT} with respect the number of pseudonyms in a single request. Samples from 1 000 observations.

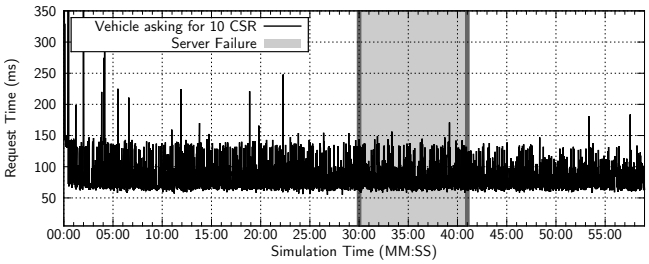

Figure 7: 5 000 emulated vehicles operating for 1 hour and asking for 10 pseudonyms every 10 minutes.

meaning that the processing time is negligible with respect to the network latency.

Moreover, $t_1 + t_2$ is the time required for a vehicle to receive a valid SAML assertion. The assertion can be reused in subsequent requests (Sec. V-C), avoiding an overhead of approximately $300\,ms$.

In case vehicle mobility adds time constraints (due to RSU coverage), and pseudonyms are not *refilled* while the vehicle is parked, the latency for requesting even 1 000 pseudonyms ($t_{\text{TOT}} \simeq 1.62\,s$), can be easily accommodated.

Figure 6 depicts measured t_{TOT} sampled over 1 000 observations assuming a linear increase of the size of the request, from 1 000 to 10 000 pseudonyms per request. We do not limit the request size because a vehicle could (theoretically) refill a rather large number of pseudonyms, i.e., before a long trip. Therefore, the system should be able to handle any request size without any significant performance degradation. As the figure shows, the latency grows linearly with the number of pseudonyms contained in a single request up to approximately $9\,s$ for 10 000 certificate generations (without any hardware acceleration).

Finally, our system outperforms the scheme presented in [25]: without considering the request preparation and verification of the received Ps_i (since both can be performed asynchronously), VeSPA requires approximatively $5\,s$ more compared to SEROSA for requests of 1 000 Ps_i.

2) Realistic Mobility: To evaluate the efficiency and scalability of SEROSA in a dense urban environment, we used data from a real life scenario. We extracted 5 000 vehicle traces around the city of Cologne (Germany) from the "TAPAS Cologne" project [32]. To emulate vehicles, we assigned a thread to each one of the traces and assumed a pseudonym request policy of 10 pseudonyms every 10 minutes (i.e., pseudonym lifetime of 1 minute [33]).

Figure 7 depicts the observed latency for a simulation interval of 1 hour: the system response time is around $100\,ms$ (on average). During the 1 hour TAPAS scenario simulation, we also introduced a temporary outage of the PCA by disconnecting completely one of the two Web-servers behind the load-balancer. As shown in the shaded area, the pseudonym request latency does not increase and the PCA recovers transparently from such a disruption.

C. Resolution and Revocation

In this section, we conduct additional simulations to further examine the behavior of SEROSA in the case of pseudonym resolution and revocation. These protocols can be summarized as follows (see Sec. V-D): (1) the RA inquires the PCA for the tr_{id} used by the vehicle to request pseudonym Ps_i, (2) the RA asks IdP to revoke the L_{id} associated with this tr_{id} and to provide all the other issued tr_{id_i}, (3) finally, the RA requests from the PCA to revoke all the pseudonyms associated with all the tr_{id_i}.

Here the focus is on the time spent by the PCA (t_{PCA}), the IdP (t_{IdP}), and the RA (t_{RA}) for a single pseudonym resolution (and its revocation) with respect to the number of already revoked pseudonyms.

To maximize the entropy of the pseudonym set, we require that pseudonyms are assigned to different L_{id} with equal probability. We assume that each vehicle (L_{id}) uses 10 different (tr_{id}) to request 10 pseudonyms. Therefore, the overall ratio is ($1\,L_{\text{id}} : 10\,tr_{\text{id}} : 100\,Ps_i$).

Figure 8 shows the latency for each system component, for a single pseudonym revocation. Results are averaged over 100 runs, with the set of revoked pseudonyms (in the database) increasing from 10 000 to 100 000 items linearly. As it can be seen, the performance of the revocation protocol is not affected (at all) by the number of already revoked pseudonyms. Moreover, as expected, it holds that $t_{\text{PCA}} > t_{\text{IdP}} > t_{\text{RA}}$, due to the fact that the RA needs only to dispatch the commands to the IdP and the PCA.

Additionally, the time to resolve the sought pseudonym, i.e., requesting the tr_{id} from the PCA and the L_{id} from IdP, is about $320\,ms$. In [34] the authors evaluated the pseudonym resolution performance of their system (under similar conditions) and demonstrated a latency of $550\,ms$, which increases with the size of revoked pseudonyms database.

On the other hand, both the IdP and the PCA must update and sign their Certificate Revocation Lists for each revoked certificate. However, their list lengths differ one order of magnitude ($1\,L_{\text{id}}$ corresponds to $100\,Ps_i$). If such a delay is considered critical, an Online Certificate Status Protocol could be employed to reduce the resultant communication overhead.

VIII. Conclusions and Future Work

We presented SEROSA, a secure and privacy-preserving service-oriented architecture for VC. SEROSA provides a comprehensive set of identity management and access control services while guaranteeing the security and privacy requirements of VC. Leveraging widely accepted Internet standards, such as Web Services, SEROSA transparently caters to the needs of vehicular users and service providers, independently of the domain they belong to. Through extensive experimental

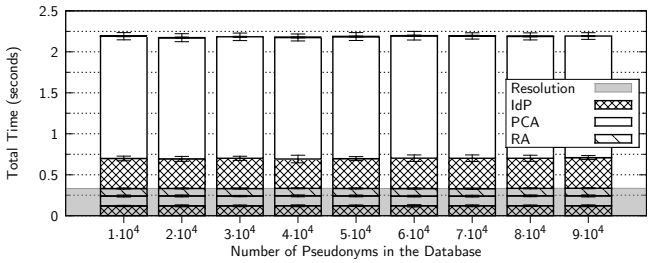

Figure 8: Time spent on each system component for a single pseudonym revocation. The gray area denotes the time spent for the resolution of the revoked pseudonym.

evaluations we demonstrate its dependability and efficiency compared to state of the art VPKIs.

Helped by SEROSA, the merging of vehicular networks and web technologies can yield numerous advantages for VCs. Furthermore, the extendability of WS leaves space for anonymous and unlinkable authentication schemes that can ensure privacy even in the presence of trusted-but-curious infrastructure and, thus, reduce the knowledge gathered by the IdP.

REFERENCES

[1] L. Chunli and T. L. Fang. "The Application Mode in Urban Transportation Management Based on Internet of Things". In: *proceedings of the 2nd International Conference on Electric Technology and Civil Engineering (ICETCE)*. Three Gorges, China, May 2012.

[2] P. Papadimitratos, A. L. Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. "Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation". In: *IEEE Communications Magazine* 47.11 (Nov. 2009), pp. 84–95.

[3] M. Gerla and L. Kleinrock. "Vehicular Networks and the Future of the Mobile Internet". In: *Computer Networks* 55.2 (Feb. 2011), pp. 457–469.

[4] P. Papadimitratos. ""On the road" - Reflections on the Security of Vehicular Communication Systems". In: *Proceedings of the IEEE International Conference on Vehicular Electronics and Safety (ICVES*. Columbus, OH, USA, 2008, pp. 359–363.

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

[6] H. Zhu, R. Lu, X. Shen, and X. Lin. "Security in service-oriented vehicular networks". In: *IEEE Wireless Communications* 16.4 (Aug. 2009), pp. 16–22.

[7] S. Mollman. *From Cars to TVs, Apps are Spreading to the Real World*. Oct. 2009. URL: http://www.cnn.com/2009/TECH/10/08/apps.realworld/.

[8] A. Goodwin. *Ford Unveils Open-Source Sync Developer Platform*. Oct. 2009. URL: http://reviews.cnet.com/8301-13746_7-10385619-48.html.

[9] IEEE 1609 WG. *Family of Standards for Wireless Access in Vehicular Environments (WAVE)*. Sept. 2009.

[10] N. Ragouzis, J. Hughes, R. Philpott, and E. Maler. *Security Assertion Markup Language (SAML) V2.0 Technical Overview*. Mar. 2008.

[11] B. Leiba. "OAuth Web Authorization Protocol". In: *IEEE Internet Computing* 16.1 (Jan. 2012), pp. 74–77.

[12] D. Recordon and D. Reed. "OpenID 2.0: a platform for user-centric identity management". In: *proceedings of the 2nd ACM workshop on Digital identity management*. Alexandria, Virginia, USA, Oct. 2006.

[13] 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". In: *IEEE Communications Magazine* 46.11 (Nov. 2008), pp. 100–109.

[14] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. "Securing Vehicular Communications - Assumptions, Requirements, and Principles." In: *proceedings of the 4th Workshop on Embedded Security in Cars (ESCAR)*. Berlin, Germany, Nov. 2006.

[15] Car2Car Communication Consortium. URL: http://www.car-to-car.org/.

[16] B. Weyl, O. Henniger, A. Ruddle, H. Seudié, M. Wolf, and T. Wollinger. "Securing vehicular on-board IT systems: The EVITA Project". In: *proceedings of the 25th Joint VDI/VW Automotive Security Conference*. Ingolstadt, Germany, Oct. 2009. URL: http://www.evita-project.org/.

[17] P. Papadimitratos, L. Buttyan, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya. "Architecture for Secure and Private Vehicular Communications". In: *IEEE International Conference on ITS Telecommunications (ITST)*. Sophia Antipolis, France, 2007, pp. 1–6.

[18] PRECIOSA. *PRivacy Enabled Capability In Cooperative Systems and Safety Applications - D1*. Nov. 2009. URL: http://www.preciosa-project.org/.

[19] PRESERVE Project. *Security Requirements of Vehicle Security Architecture*. June 2011. URL: http://preserve-project.eu/.

[20] R. Stahlmann, A. Festag, A. Tomatis, I. Radusch, and F. Fischer. "Starting European field tests for CAR-2-X communication: The DRIVE C2X framework". In: *proceedings of the 18th ITS World Congress Exhibition*. Orlando, FL, USA, Oct. 2011.

[21] A. Groll, J. Holle, C. Ruland, M. Wolf, T. Wollinger, and F. Zweers. "OVERSEE: a Secure and Open Communication and Runtime Platform for Innovative Automotive Applications". In: *proceedings of the 7th Embedded Security in Cars (ESCAR) Conference*. Düsseldorf, Germany, Nov. 2008.

[22] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos. "Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change Is Not Enough". In: *proceedings of the International Conference on Wireless On-Demand Network Systems and Services (WONS)*. Kranjska Gora, Slovenia, Feb. 2010.

[23] M. Feiri, J. Petit, and F. Kargl. "Evaluation of congestion-based certificate omission in VANETs". In: *proceedings of the 4th IEEE Vehicular Networking Conference (VNC)*. Seoul, Republic of Korea, Nov. 2012.

[24] F. Schaub, F. Kargl, Z. Ma, and M. Weber. "V-Tokens for Conditional Pseudonymity in VANETs". In: *proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*. Jersey City, NJ, USA, Apr. 2010.

[25] N. Alexiou, M. Laganà, S. Gisdakis, M. Khodaei, and P. Papadimitratos. "VeSPA: Vehicular Security and Privacy-preserving Architecture". In: *ACM Workshop on Hot Topics on Wireless Network Security and Privacy (ACM HotWiSec)*. Budapest, Hungary, Apr. 2013.

[26] N. Alexiou, S. Gisdakis, M. Laganà, and P. Papadimitratos. "Towards a Secure and Privacy-preserving Multi-service Vehicular Architecture". In: *proocedings of the 4th International Workshop on Data Security and PrivAcy in wireless Networks (D-SPAN)*. Madrid, Spain, June 2013.

[27] L. Yeh and J. Huang. "PBS: A Portable Billing Scheme with Fine-Grained Access Control for Service-Oriented Vehicular Networks". In: *IEEE Transactions on Mobile Computing* (2013).

[28] S. Cantor, J. Kemp, R. Philpott, and E. Maler. *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. Tech. rep. Mar. 2005. URL: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf.

[29] J. Sermersheim. *Lightweight Directory Access Protocol (LDAP): The Protocol*. RFC 4511 (Proposed Standard). Internet Engineering Task Force, June 2006. URL: http://www.ietf.org/rfc/rfc4511.txt.

[30] T. Moses. *XACML 2.0 Core: eXtensible Access Control Markup Language (XACML) Version 2.0*. Feb. 2005.

[31] D. Boneh, X. Boyen, and H. Shacham. "Short group signatures". In: *proceedings of Advances in Cryptology (CRYPTO)*. Santa Barbara, CA, USA, Aug. 2004.

[32] S. Uppoor and M. Fiore. "Large-scale urban vehicular mobility for networking research". In: *proceedings of the 3rd IEEE Vehicular Networking Conference (VNC)*. Amsterdam, The Netherlands, Nov. 2011.

[33] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux. "Eviction of Misbehaving and Faulty Nodes in Vehicular Networks". In: *IEEE Journal on Selected Areas in Communications* 25.8 (Oct. 2007), pp. 1557 –1568.

[34] N. Bißmeyer, J. Petit, and K. M. Bayarou. "Copra: Conditional Pseudonym Resolution Algorithm in VANETs". In: *proceedings of the 10th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. Banff, Canada, Mar. 2013.