An interoperability system for authentication and authorisation in VANETs

Valentina Casola*
Dipartimento di Inforomatica e Sistemistica,
Università degli studi di Napoli Fedrico II,
Napoli, Italy
E-mail: casolav@unina.it
*Corresponding author

Jesus Luna
Barcelona Digital Centre Technologic,
Barcelona, Spain
E-mail: jluna@bdigital.org

Antonino Mazzeo
Dipartimento di Inforomatica e Sistemistica,
Università degli studi di Napoli Fedrico II,
Napoli, Italy
E-mail: mazzeo@unina.it

Manel Medina
Department of Computer Architecture,
Technical University of Cataloia (UPC),
Barcelona, Spain
E-mail: medina@ac.upc.edu

Massimiliano Rak
Dipartimento di Ingegneria dell’Informazione,
Seconda Università di Napoli,
Aversa, Italy
E-mail: massimiliano.rak@unina2.it

Jetzabel Serna
Department of Computer Architecture,
Technical University of Cataloia (UPC),
Barcelona, Spain
E-mail: jetzabel@ac.upc.edu

Copyright © 2010 Inderscience Enterprises Ltd.
Abstract: Vehicular ad hoc networks (VANETs) have evolved considerably over the last years, but despite the wide number of potential applications, VANETs also raise a broad range of critical security and privacy challenges. To achieve privacy, VANETs enforce the concepts of authentication and authorisation via public key infrastructures, relying on a large set of regional certification authorities with explicit cross-certification agreements to provide interoperability for vehicles and services. To avoid the burden of managing these cross-certificates, our research proposes the interoperability system (IS), an architecture to provide VANETs’ nodes with a security mechanism for mutually untrusted domains. The IS supplies vehicles with a trusted set of credentials by implementing a certificate status service and a security level evaluator. This paper shows that the proposed architecture can be used to implement a mandatory access control mechanism in two VANET scenarios with a protocol independent of the underlying communication system.

Keywords: authentication; authorisation; interoperability; security; VANETs.


Biographical notes: Valentina Casola is an Assistant Professor at the University of Naples Federico II. She received the Laurea degree in Electronic Engineering cum laude from the University of Naples, in 2001 and she received her PhD in Electronic and Computer Engineering from the Second University of Naples, in 2004. Her research activities are both theoretical and experimental and are focused on security methodologies to design and evaluate distributed and secure infrastructures. He published more than 30 papers in international conferences and journals.

Jesus Luna obtained his Engineering Diploma in Telecommunications and Electronics from the National Technical Institute (Mexico City), in 1995. Then, received an MSc in Computer Sciences from the Technical Institute of Higher Studies of Monterrey (Mexico City), in 2003. Finally, he obtained his PhD in Computer Architecture from the Technical University of Catalonia (Barcelona, Spain), where he graduated with honors in 2008. Currently, he works as a Senior Security Researcher in Barcelona Digital Centre Tecnològic and his topics of interest are grid/cloud security, trust and security for emerging technologies (Vehicular Ad-hoc Networks and Wireless Sensor Networks) and applied cryptography.

Antonino Mazzeo is a Full professor of Computer Architectures at the Computer and System Engineering Department of the University of Naples Federico II, Italy. He received the laurea degree in Electronic Engineering. His research activities include methodologies and tools for design/analysis of distributed systems; secure and real-time systems and dedicated parallel architectures. He published hundreds of papers in international conferences and journals.

Manel Medina is a Full Professor at the Technical University of Catalonia (UPC), since 1992. He was a Chief Innovation Officer of SeMarket and Security Projects Officer of Barcelona Digital Technological Center. He was the Head of esCERT-UPC, Spanish Computer Emergency Response Team and of the Internet Applications research center (UPC). He was the Head of cANet, research center of Internet Applications of the UPC and a full Member of
ESRIF (European Security Research and Innovative Forum) (since 2006) to advise European Commission about security research topics in the R&D funding programmes.

Massimiliano Rak is an Assistant Professor at the Second University of Napoli, Italy. He received the laurea degree in Computer Science Engineering from the University of Napoli Federico II, in 1999 and PhD in Computer Engineering from the Second University of Napoli, in 2002. His research activities include both theoretical and experimental issues, in the areas of performance evaluation of computing systems, parallel and distributed software engineering, security of information systems, autonomic systems, GRID and cloud computing. He published more than 40 papers in international conferences and journals, he is a member of many international committees.

Jetzabel Serna obtained her Bachelor’s Degree in Computer Systems Engineering from the Technical Institute of Tijuana (Tijuana, Mexico), in 2001. She received a Master of Sciences degree in Computer Science and Communications Engineering from the Gerhard Mercartor University (Duisburg, Germany), in 2006. Since 2006, she doing her PhD at the Technical University of Catalonia in the Computer Architecture Department (Barcelona, Spain), and working as a Research Assistant in the Network Security Group. Her topics of interest are security, trust and privacy in mobile environments.

1 Introduction

Vehicular ad hoc networks (VANETs) are an emerging research area and one of the most relevant forms of mobile ad hoc networks (Fonseca and Festag, 2006). By the year 2010, it is expected that 40% of all vehicular components will be electronic and with this integration, VANET vehicles will be capable of storing and processing great amounts of information, including a driver’s personal data and geolocation information. A VANET vehicle (Figure 1) is equipped with processing, recording and positioning mechanisms with a potentially ‘infinite’ power supply.

VANETs enable car-to-car and car-to-infrastructure communication, thus communicating nodes are either vehicles or base stations that can exchange information; for the rest of this paper, these will be referred as car-to-car (C2C) and car-to-service provider (C2S) communications.

According to Plossl et al. (2006), Prevent-project (2008) and Raya and Hubaux (2005), VANETs’ messages can be classified in to three groups: warning (to prevent detected risky situations), traffic management and added value (to provide internet services). Despite VANETs sharing general features with conventional ad hoc networks, they have individual characteristics that are decisive in the design of the communication system (Zanella and Fasolo, 2006), which include

1. dynamic topology
2. mobility models
3. infinite energy supply
4. localisation functionality.
Unfortunately, a VANETs system can be vulnerable to security attacks, which may compromise the driver’s privacy (i.e. disclosing his personal data) and even cause life-threatening situations (i.e. false warnings resulting in road accidents). In a VANET, the network access is granted by default, and so messages sent by one node are ‘available’ to all other nodes that have joined the network, thus easing packets’ eavesdropping. One of the most important challenges in VANETs is related with finding proper techniques and architectural solutions to enforce security and privacy. The apparent trade-offs between these two concepts have been discussed on a broader level by Security vs. privacy (2008).

A connected vehicle is also able to run wireless cryptographic protocols (Hubaux et al., 2004) and to use X.509 v3 digital certificates from public key infrastructures (PKI) (Internet X.509 Public Key Infrastructure, 2002); these two features are becoming a common approach for implementing VANETs’ secure access to value added services (IEEE Std p1609.2). Available proposals envision a wide number of certification authorities (CA) (which act as trusted third parties within regional scopes) and cross-certification agreements to provide interoperability among these otherwise untrusted domains. Unfortunately, existing approaches are based on static and hard to manage trust relationships and certificates among the participants, resulting in security issues with vehicles needing to access up-to-date information about trusted CAs – authoritative for the vehicle’s location – to validate messages received on the road (just as shown in Example 1).

Example 1: Consider the scenario depicted in Figure 2 where a vehicle with a German electronic license plate (ELP) and a digital certificate issued by DE_{CA} travels to France and receives from another vehicle a warning message digitally signed by a certificate issued by FR_{CA}.

Figure 1 New vehicles will include a central computing platform network that can provide USB, Bluetooth, IEEE 802.11 interfaces or ethernet and may have features such as GPS, EDR – event data recorder (i.e. to store data for a vehicle’s crash reconstruction) – and radars.
Authentication in the previous example implies the following certificate validation process:

1. Cryptographic verifications over the certificate path (i.e. verifying the digital signature of each certificate)
2. Verifying each certificate’s validity period
3. Verifying that the first certificate in the chain is a trust anchor
4. Verifying the status of each certificate in the path to ensure that it has not been revoked or suspended.

The process just described is referred as basic path validation (Internet X.509 Public Key Infrastructure, 2002).

Because of the regional CAs used in VANETs environments, it is feasible to conclude that drivers will have a certificate issued by their own CA, therefore conveying a big interoperability problem when interacting with services and vehicles from others CAs. Returning to the previous example: how to perform the basic path validation process if

1. A trust anchor cannot be determined (FR_CA is unknown to the German driver).
2. Therefore, revocation information for the French driver cannot be validated? Is the originator of the warning authorised to generate this class of messages?

For the research presented in this paper, security and privacy issues in VANETs are related with the concepts of authentication and authorisation, and so they will be addressed by proposing an infrastructure called the interoperability system (IS), which focuses on the capability of providing reliable users’ identities to the different domains.
through the adoption of a policy-based approach. This process, called extended path validation (Internet X.509 Public Key Infrastructure, 2002), defines an approach that enables any entity (service providers and vehicles) to validate in real-time a digital certificate issued by any other CA even though they do not belong to the same trusted domain.

To perform the extended path validation in VANETs, the following two phases are required:

1. automatically perform the cross certification by an automatic policy mapping (i.e. comparison and evaluation of the certificate policies from the involved CAs) to build a dynamic CA federation
2. validate in near-real time a VANET certificate’s status.

Furthermore, the proposed IS will act as an attribute authority for any service provider implementing an identity-based access control mechanism that takes into account the driver’s privacy and liability (non-repudiation).

The reminder of this paper is organised as follows: In Section 2, related works on security architectures and solutions for VANETs are reported and in Section 3, a high-level view of an architectural solution proposed for the interoperability of different untrusted domains is presented. In Section 4, the contributed IS is presented and the extended path validation concept is widely explained. In Section 5, adoption of the proposed IS for the C2C and C2S scenarios will be demonstrated. Finally in Section 6, some conclusions are drawn and the directions for the future work are outlined.

2 State-of-the-art

VANET technology is a novel research topic that is currently in standardisation process and therefore works presented in this section rise mostly from academical and industrial worlds. The following paragraphs will cover the most important research related with VANETs’ authentication, authorisation and privacy issues.

In recent studies (Liu et al., 2007; Papadimitratos et al., 2007; Parno and Perrig, 2005; Plossl et al., 2006), the use of PKI and digital certificates have been proposed to provide a suitable solution to the authentication and authorisation challenges in VANETs. An efficient architecture for managing the whole certificate’s life cycle (issue, distribution, validation and revocation) has been found to be fundamental. In Papapanagiotou et al. (2007), authors presented a certificate validation scheme based on a distributed version of OCSP for authorisation and authentication in VANETs, which is capable of preventing known issues like the flooding of extended revocation lists. Unfortunately, privacy issues were not taken into account.

Raya et al. (2006) proposed a certificate revocation model consisting in a set of three protocols (revocation using compressed certificate revocation lists (RC2RL), revocation of the tamper-proof device (RTPD) and the distributed revocation protocol (DRP)), each one adapted to a specific VANET scenario. In RC2RL and RTPD, revocation occurs when the CA sends a message to the ‘revoked vehicle’; however, other relying parties (vehicles and service providers) do not receive these notifications, therefore opening a security gap on the whole VANET system. In the case of the DRP protocol, the
An interoperability system for authentication and authorisation

possibility of collusion attacks also remains open. Obviously, we have to consider that an attacker detection system, basic for the deployment of the mentioned family of protocols, has not yet been designed.

The SRAAC protocol proposed in Fischer et al. (2006) allows distribution of certificates, anonymous message authentication with quorum-based blinded certificate issuance, anonymity, revocation and isolation of misbehaving vehicles. SRAAC makes use of a digital signature algorithm called Magic Ink-DSS with shared secrets; however, the disadvantage of this model is that a vehicle detected as malicious will not be revoked in real time because its issued certificates (previously stored in their On Board Unit) will still be valid for some arbitrary time window.

A mechanism for access control using the Kerberos model was described in Moustafa et al. (2006). The authors proposed an authentication and authorisation mechanism to access offered services according to a previous subscription (token) so that afterwards the vehicle is authenticated at the highways entry points. This model is specific for highways environments, thus limiting its applicability.

From the investigation of the relevant related work, it must be remarked that VANETs’ authorisation research is still quite limited. In many distributed infrastructures, the adoption of a certificate delegation model is also proposed; the state-of-the-art proxy credentials (Neman, 1993) are a common technique used for delegation, where an entity A grants to another entity B the right for B to be authorised with others as if it were A. In other words, entity B is acting as a proxy on behalf of entity A. The computational grid is the most common scenario where proxy credentials are used for security delegation (Casola et al., 2007a; Housley et al., 2004).

Apart from authentication, authorisation and delegation, privacy is also an important issue for VANETs. In Aijaz et al. (2006) and Parno and Perrig (2005), authors gave a detailed analysis of general system attacks on inter-vehicle communication (IVC) and described the main challenges in securing vehicular networks, pointing out other important system requirements (i.e. privacy). Potential implications of missing privacy are exposed in Dötzer (2005) and the author proposes to use centrally assignd digital pseudonyms. Beresford and Stajano (2004) defined a system where vehicles change pseudonyms in a certain region pointed by the system, this region being where a lot of vehicles are within the communication range (Dötzer, 2005). A disadvantage of the latter appears when there are not enough vehicles changing pseudonyms within a region. To overcome this problem, Golle et al. (2004) proposes self-assigned digital pseudonyms that take a set of measures while changing them: synchronising pseudonym change, introducing gaps (silent periods) and changing pseudonyms when nodes are in the region (this was also considered in Gerlach (2006) by defining them as mix-contexts in addition to frequently changing the pseudonyms and protecting the centralised mapping that intend to increase anonymity). Gerlach and Güttler (2007) provided an improvement of mix-contexts considering anonymity over randomly changing pseudonyms in certain intervals. CARAVAN (Gerlach, 2007; Sampigethaya et al., 2007) proposes a random silent period in order to hamper linkability between pseudonyms just as considered in other architectures already mentioned.

In Choi et al. (2005), authors proposed a system to balance auditability and privacy in VANETs based on symmetric cryptographic primitives and two different sorts of pseudonyms (short and long term). A study of practicability in pseudonymity deployment and implementation was done in Fonseca et al. (2007), where possible solutions were represented as a combination of existing pseudonymity algorithms.
In Lu et al. (2008), authors defined a protocol for conditional privacy preservation by proposing short-time anonymous key generation in order to minimise their number and ease their management. Road side units (RSUs) are in charge of generating the short-time keys and above these entities is found the trusted authority (TA), ultimately responsible for issuing RSUs’ certificates. In Lu et al. (2008), a mechanism based on different levels of privacy is also presented; it is based on a combination of levels of authentication, anonymity and unlinkability, which are a very interesting approach to cope with the privacy issues found by our research.

In summary, most of the research and proposed solutions for privacy mainly focus on the use of pseudonyms and algorithms for changing them. Because of the common belief that pseudonyms are important for VANETs’ overall security and are quite beneficial for protecting users’ identity, the architecture to be introduced in Section 3 is fully compatible with these solutions.

3 Architecture of a security framework for VANETs

Despite its importance, at the state-of-the-art there is no real architecture or standard for solving VANETs’ security issues mentioned in previous sections. In this paper, we propose a framework that can be adopted by any car to implement interoperable and secure authentication mechanisms in VANETs.

The contributed framework uses a PKI infrastructure, but allows final users (vehicles into the VANET) to perform authentication in any untrusted domain by dynamically enabling interoperability among different CAs without explicit agreements (i.e. cross certification). Such a model will be called a CA federation. To illustrate our proposal, we will refer to two use cases introduced in Section 1: the C2S and C2C. Even though the protocols, data and security features of the reference scenarios are quite different from an architectural point of view, we will manage them in a very similar way: in both cases, we propose the introduction of an IS acting as a trusted third party and, able to authenticate digital certificates by providing access credentials that will be used afterwards for authorisation purposes. The IS solves the problem of managing explicit trust relationships by enabling a dynamic trust establishment through the evaluation of a digital certificate’s security level. The rest of this paper will further detail the IS architecture and the security evaluation methodology being used.

Because a VANET service provider needs to protect the access to its services, we can talk about authorisation decisions based on access control policies defined by commercial aspects. On the other hand, a car does not offer a service, but still has to share information for other VANET’s nodes, therefore requiring the protection of the driver’s private information. To face the latter problem, we propose the implementation of a mandatory access control (MAC) mechanism (Bell, 2005) on the vehicle by assigning security labels to the personal data that is being managed: the access will be granted if the security level of the requestor is equal or higher than the security level denoted by the data’s label. This feature will be further explained in Section 5.2.

3.1 Use cases

In the C2S scenario (Figure 3), a vehicle needs to be able to access any authorised service available on the road, even in ‘untrusted’ domains, those being serviced under
a different CA. As shown in Figure 3, the vehicle uses the base stations (i.e. stations along the road that offers a wireless network access to the car) to access external services offered by service providers hosted by infrastructure nodes. The problems to address in this scenario are:

1. How does the service authenticate the car?
2. How does the car authenticate the service?
3. Which service can the car access (service authorisation)?
4. Which driver’s data the service can access (car authorisation)?
5. What happens when the connections are lost (car are in fast movement, therefore connection cannot be considered stable)?
6. How to perform authentication and authorisation when a car moves between two different domains?

A VANET’s vehicle is able to request any available infrastructure service, but also can offer ‘services’ to other vehicles: for example, a police car requesting a vehicle’s driver information and current speed. In these C2C scenarios (Figure 4), a vehicle will need to authorise other vehicles to access its information (including the driver’s private data). To achieve this goal, a driver can decide which personal information can be accessible and the minimum required security level to do this. A brief summary of the problems to solve are:

**Figure 3**  C2S components
1. How can the cars authenticate each other?
2. Which data can be shared among vehicles?
3. What happens when communication is lost?
4. How to perform authentication and authorisation when cars belong to two different domains?

Both cases put in evidence that the VANET infrastructure can be seen as two different networks: a peer-to-peer network of cars made of unreliable and dynamic connections and the network’s infrastructure offering services to the cars. The C2S scenario models the communication between these two networks, while the C2C scenario represents peer-to-peer communication.

3.2 An architectural model for VANET security

Current state-of-the-art authentication and authorisation mechanisms for VANETs have been derived from traditional ones (as PKI for authentication and policy-based access control mechanisms for authorisation); however, many particular problems remain open: issues with unreliable communications and brief connections require a special care and cross certification agreements between untrusted domains are hard to manage in VANETs. The former problem relates with the VANETs’ nature itself: interleaves of ‘communication silent’ due to infrastructure’s failures are likely to occur along with very short connections with other cars or infrastructures because of the car’s speed. A well-designed VANET protocol should implement optimised messages where security
An interoperability system for authentication and authorisation

(i.e. digital signature mechanism and cryptosystem being used) and performance (i.e. signature size and encryption time) are balanced to cope with these unreliable and short connections.

The protocols we propose are designed in order to take into account the VANET requirements (i.e. unreliable and short connections) at design level and independently from the (proprietary) technology involved. As a consequence, the solution we propose has been designed with a performance-oriented approach just as illustrated in Section 5.

On the other hand, the problem of cross certification agreements is due to the future deployment of VANETs, which will result in the creation of several PKIs, each one usually installing its own CA and thus giving birth to a large set of different and untrusted security domains (based on the authors’ experience at least one-per Member State in the EU). This represents one of the biggest interoperability problems that could arise among all VANET users and therefore one of the major security challenges to be faced before building this wide distributed infrastructure. In other words, this problem is related to the definition of a trusted PKI infrastructure able to guarantee a secure degree of interoperability among all the involved VANETs’ CAs. In practice there are two commonly accepted approaches that provide interoperability between different security domains based on PKI technology:

1. Involved CAs explicitly build a trusted domain by defining a new CA hierarchy through cross certification techniques. In this case, each CA explicitly trusts the others and therefore is able to accept their certificates.

2. Involved CAs do not build an explicit trusted domain, but interoperate through a ‘federation’: any CA belonging to the federation implicitly trusts the others, thanks to the definition of a well-established policy-based framework.

Even if the explicit trusted domain (first approach) is an attractive solution, it is not always possible to implement in practice because of the required agreements between the involved organisations, along with administrative overheads and technical problems that arise.

Previous issues should be addressed by VANET’s protocols, but at the state-of-the-art they are not. For this reason, we have proposed an interoperability system for VANETs to be able to work in these networks with independence of the underlying protocols, thanks to the use of a personal agent (PA) software associated to each car. With this contribution, we are able to cope with both of the problems mentioned at the beginning on this section: short connections and complex elaborations are managed via a PA acting on behalf of the car that created it by means of a delegation model. A car’s PA activates to interact with the interoperability system in the ‘wired’ network and to keep the car and session status. If the car disconnects for any reason before receiving a response from the infrastructure, then as soon as it reconnects and re-authenticates to the IS, its PA returns along with the validation reply.

To cope with cross-certification issues, the proposed IS implements the concept of CA federations. In a CA federation, the members agree on a minimum set of security requirements that must be fulfilled by all of them to interoperate. These minimum requirements are usually a subset of the CA’s certificate policy and can be audited at any time by the other members of the same federation. If a new CA wants to participate in the federation, then its CP must pass through an ‘accreditation’ process to ensure compliance with the minimum requirements or, in other case, to assess the candidate in which
provisions (individual rules from the CP) should be improved to become a member. Once the accreditation process has been passed, the new member CA’s root certificate is added to a trusted repository (usually hosted by the federation itself like in The International Grid Trust Federation (2008)). Instead of distributing new sets of cross-certificates to all the VANET’s nodes, it is only necessary to let them know how to access the CA federation’s repository in order to update their local copies of trusted CAs.

Figure 5 shows that a VANET can be modelled as a distributed system composed by base stations offering wireless connection to cars, a certificate authority and a set of server providers hosting the VANET services. It is worth to notice that cars belonging to different domains also must have certificates issued by different CAs. As shown in Figure 5, the model we propose creates a PA for each car and uses the IS as an intermediary between the certificate verifiers (vehicles and service providers) and the issuing CAs, by managing (retrieving, elaborating and updating) the information needed to create a dynamic CA federation. As mentioned before, the IS is independent from the underlying VANETs’ communication protocols.

**Figure 5** The proposed security architecture for VANETs (see online version for colours)

4 The interoperability system

The goal of the interoperability system is to build a dynamic federation of CAs by evaluating their certificate policies, thus enabling the extended path validation of digital certificates from mutually untrusted domains. The IS must perform two main tasks:

1. online validation of the certificates’ status
2. evaluation of the issuing CA’s security level.

To achieve its goal, the IS should be comprised of

1. a certificate validator to verify the certificate’s status in near real-time
2. a PKI evaluation system to obtain the security level provided by a CA.

The certificate validator uses a high-level OCSP responder (Myers et al., 1999) to provide in near-real time the status information of certificates issued by any member of the CA federation. Trust issues with these OCSP servers are solved considering the use of
authorised responders digitally signing the OCSP responses with a certificate from the same PKI hierarchy of the OCSP client (i.e. the driver’s CA). OCSP is a request–response protocol that greatly benefits the performance of VANET-like systems, just as shown by European projects like CertiVeR (CertiVer project, 2005).

About the second component, the PKI evaluation system, we have adopted the reference evaluation model (REM) for evaluating a CA’s security level (global security level (GSL) in REMs terminology) as illustrated in Section 4.1. This approach is based on the formalisation of a certificate policy to determine if the corresponding CA is compliant with the federation’s minimal security requirements and to quantitatively evaluate its particular security level. In this way, it is possible for the proposed IS to dynamically build a CA federation for VANETs. As mentioned before, the CA’s security level can be used afterwards to enforce privacy by performing authorisation decisions based on a mandatory access control model just as illustrated in Section 5.2. As introduced in Section 4, a final component of the proposed architecture, the PA, is co-located with each relying party (vehicle or service provider) to perform authentication and authorisation decisions even in presence of communication failures.

Section 5 explains in further detail how the different elements of the proposed architecture interoperate in order to perform the extended path validation in both the C2S and C2C scenarios.

4.1 Dynamic CA federation using the REM

The interoperability system helps building dynamic CA federations because it allows a client to evaluate ‘on-the-fly’ a certificate policy from an unknown CA, thus establishing if its security level corresponds to the requested security features.

The methodology used to evaluate the security level provided by a CA and decide to create a dynamic trust relationship with it is the REM (Casola et al., 2007b). Its main goal is to provide an automatic mean to state the security level provided by an infrastructure; REM has been widely adopted in the past to dynamically build CA federations (Casola et al., 2007a, c). The methodology defines

1. how to express in a rigorous way a security policy (a certification policy in our particular case)
2. how to evaluate a formalised policy
3. how to state the provided security level.

With REM, any policy is represented through an XML tree containing all its provisions as intermediate nodes and leaves.

In Figure 6, the three phases of the REM methodology are shown: policy structuring, policy formalisation and policy evaluation.
The goal of the *structuring* phase is to associate an enumerative and ordered data type $K_i$ to the $n$ leave provisions of the policy. A policy space $P$ is defined as $P = K_1 \times K_2 \times \ldots \times K_n$, i.e. the vectorial product of the $n$ provisions $K_i$. For example, the provision *KeyLenght* can assume the following ordered values: 128 bits, 512 bits, 1024 bits and 2048 bits. The space is defined according to a policy template that strongly depends on the application context.

The main goal of the *formalisation* phase is to turn the policy space $P$ into an homogeneous space $P'$. This transformation is accomplished by a normalisation and clusterisation process that allows to associate a local security level (LSL) to each provision. For example, if a policy has a KeyLenght of 512 bits, it will be associated to the LSL = 2 and the normalised vector is $(1,1,0,0)$. After that, the provisions may be compared by comparing their LSLs.

The main goal of the *evaluation* phase is to pre-process the $P'$ vector of LSLs in order to represent it by a $n \times 4$ matrix whose rows are the single provisions $K_i$ and the number of columns is the chosen number of LSLs for each provision. For example, if the number of LSL is four and the LSL associated to a provision is $l_2$, the row in the matrix associated to the provision in the matrix will be $(1,1,0,0)$. Finally, a distance criterion for the definition of a metric space is applied. REM adopts the Euclidean distance among matrices:

$$d(A,B) = \sqrt{\sigma(A-B,A-B)}$$

where $\sigma(A-B,A-B) = \text{Trace}((A-B)(A-B)^T)$

To define the GSL, $L_{P_x}$, associated to the policy $P_x$ must be introduced in some reference levels according to the following metric function:

$$L_{P_x} = \begin{cases} L_0 \text{ if } d_{l_0} \leq d_{l_0} \\ L_1 \text{ if } d_{l_0} < d_{l_0} < d_{l_2} \\ L_2 \text{ if } d_{l_2} \leq d_{l_0} < d_{l_2} \\ L_3 \text{ if } d_{l_3} < d_{l_0} < d_{l_4} \\ L_4 \text{ if } d_{l_4} < d_{l_0} \end{cases}$$
where \( d_{i,o} \) are the distances between the references and the origin of the metric space (denoted as \( O \)). This function gives a numerical value to the security level.

In summary, REM’s goal is to evaluate the GSL or security level associated with a CA through the evaluation of its certificate policy so that trust decisions can be taken.

5 Authentication and authorisation in VANETs

The interoperability system can offer its services in any distributed infrastructure; nevertheless, its implementation should deal with the failures of the communication layers and in particular with the inherent VANET’s mobility. Let us take for example a vehicle that moves from one base station to another, the management of secure messages is still required to preserve the privacy and keep the status of a service request (even if the communication is lost). These issues are addressed by assuming that the communication between vehicles and infrastructure are asynchronous and a PA is associated to each car.

The PA works on behalf of a car in the infrastructure, any car creates and delegates its own PA to authenticate and authorise any request and to preserve its status in case of network disconnections. Furthermore, it is responsible to communicate with the proposed interoperability system to validate digital certificates by performing the extended path validation.

In the next subsections, we will illustrate how the PA and the IS are adopted to authenticate and authorise drivers to access a service provider (C2S scenario, Section 5.1) and how to authenticate and authorise drivers to access other car’s data while preserving driver’s privacy (C2C scenario, Section 5.2).

5.1 C2S secure access

To implement the asynchronous protocol introduced in previous sections, we have proposed an approach based on agents that are able to keep the status associated to a session/request even when the connection is lost.

The proposed protocol is depicted in Figure 7. There is a special server infrastructure (it is assumed to be offered by the road infrastructure) whose aim is to accept vehicle’s signed requests towards a specific service being offered and to create a PA associated to each request. When a PA is created, its identification number (PAid) is returned to the vehicle to acknowledge the request and to let it know how to manage a disconnection due to a communication failure. A final acknowledge message closes the previous asynchronous exchange. From this point on, the PA will work on the infrastructure on behalf of the vehicle that requested the service. The first time a car requests a service, the PA will do the following:

1. perform the basic path validation and invoke the interoperability service to get the GSL\(_{\text{client}}\)
2. compare the GSL of the driver (GSL\(_{\text{client}}\)) against the GSL of the requested service (GSL\(_{\text{server}}\)) to complete the authentication step through an extended path validation
3. enforce the authorisation mechanism (authorisation handler) with the GSL and the service access control policies
forward the car client request to the service provider after authentication and authorisation

store the results that will be forwarded to the car client even if it has lost the connection.

For the subsequent requests, the vehicle will sign them and enclose its PA_id, which is then verified by the server infrastructure to return the respective stored results.

One of the requirements addressed by this protocol is that connections must be short and only few messages should be exchanged. We are able to meet this by adopting an asynchronous approach: messages exchanged inside the VANET network, that is, between the car and the server infrastructure (grey boxes in Figure 7), are short and never require a complex behaviour. The PA, which resides on the server and communicates with other components using the service to service (S2S) network, has the role of managing the complex elaborations. To complete the exchange, a car sends the request message by attaching its PA_id. In this case, security is granted due to the certificate delegation model between the car and the PA. Following the asynchronous approach, if the client sends a request before the result is available, the server simply will not return any result.

Figure 7 Asynchronous C2S provider communication protocol
5.2 C2C secure access

In the asynchronous C2C scenario (Figure 8), the message originator is the car client, while the message’s target becomes another vehicle (the car server). The latter can delegate its operations to its own PA (just like the one used by the server infrastructure explained in Section 5.1). Notice that in Figure 8, we assume that the car server has already created its own PA to keep the state of the car client’s request even if the communication link among them is lost.

In this scenario, the following interactions occur:

1. The car client sends a message to the car server (i.e. asking for road conditions) and receives a request ID.
2. The car server sends a request to its PA to validate the car client certificate.
3. The car server’s PA performs the extended path validation of the car client’s certificate (Cert_{client}), evaluates its GSL (GSL_{client}) and locally stores it.
4. The car server requests the results of the certificate evaluation (GSL_{client}). On the basis of this GSL and on a mandatory access control mechanisms, it can authorise the access to the service and if granted, it will prepare and keep the service’s results.
5. In the last part of the protocol, the car client requests the service’s results.

As in the previous case, the asynchronous approach helps us to face the VANET performance requirements: all messages exchanged inside the VANET network (between any car and the server infrastructure) are short and never imply complex elaborations (see grey boxes in Figure 8). From this design phase, we can also note that to improve overall performance, the GSL comparison and authorisation processes (currently taking place inside the car server) can be delegated to the PA if few resources are available. Furthermore, the PA can also cache the policy evaluation’s result and associate it to a known CA, thus avoiding the re-evaluation of a known policy in the future.

When a car server receives the car client’s GSL (GSL_{client}), a mandatory access control (MAC) is applied over the driver’s personal data. This authorisation model is based on two basic rules (Bell, 2005):

1. the simple security property states that a subject at a given security level may not read an object at a higher security level (no read-up)
2. the *-Property (read star-property) states that a subject at a given security level must not write to any object at a lower security level (no write-down) and may only append new data to any object at a higher security level.

As introduced in Section 3, the basic idea behind the proposed authorisation mechanism is to assign a security label to each data of the driver’s personal information. This label will represent the minimum GSL required to enforce MAC’s simple security property, just as shown in the Example 2.

**Example 2**: Let us suppose a car server in which driver’s personal data has been assigned the security labels (GSLs) shown in Figure 9. If a car client’s GSL_{client} = 5, then it will be able to access both the car server’s public (GSL_{client} > GSL_{public}) and emergency data (GSL_{client} = GSL_{emergency}), but not its private one (GSL_{client} < GSL_{private}).
Finally, it is worth to highlight that the drivers’ real identity is not further compromised with our proposal because PAs can be created according to the pseudo-identification mechanism used by the VANET (i.e. pseudonyms).

Figure 8  Asynchronous C2C communication protocol

Figure 9  In the proposed authorisation mechanism, driver’s personal data is labelled with a minimum required security level (GSL)
6 Conclusions

In this paper, we have presented a framework and its corresponding architecture to cope with security and interoperability problems appearing in VANET environments requiring the use of multiple regional CAs. The first part of this research has analysed how important the concept of interoperability is for VANET’s authentication and authorisation, which ultimately translates into potential risks for the overall security and privacy.

The second part of this research introduced the interoperability system (IS) in charge of validating in near-real time the driver’s certificate via the online certificate status protocol (OCSP) and quantitatively evaluating its security level through a technique known as the reference evaluation methodology (REM). The latter value can be used to enforce a mandatory access control model proposed to protect the driver’s personal data, which has been previously labelled with the minimum security level required to access it. The process just described was named extended path validation and in this paper, we have proposed a protocol to implement it in two widely used VANET scenarios: C2C and C2S communication. Thanks to the use of a PA component in each node, and it is possible for the proposed mechanisms to be independent of the VANET’s underlying communication protocols and to keep the state of a vehicle’s request, therefore avoiding communication problems caused by mobile nodes disconnecting from the network by any reason.

Future work will be aimed at doing the required simulations to evaluate and analyse the performance and costs of using the proposed protocol into a VANET environment, using for example an underlying routing protocol like VITP (Dikaiakos, 2007). Even though in this paper we have commented the basics about using the IS for enforcing VANET’s privacy, our future work also will focus in providing a more in-depth study of this feature by comparing it with other privacy enhancing mechanisms. Finally, we would like to begin extrapolating the proposed architecture and protocol to other MANET environments with analogous privacy requirements, that is, Smartphone-to-Smartphone communication.

References


An interoperability system for authentication and authorisation


