Security Architectures in V2V and V2I Communication

Rens van der Heijden
Faculty of Electrical Engineering, Mathematics and Computer Science
University of Twente
The Netherlands
r.w.vanderheijden@student.utwente.nl

ABSTRACT

This paper discusses several proposed security architectures to solve the current problems in securing communication between vehicles. Through an analysis of the literature, requirements are derived and discussed, important security architectures are gathered and then compared using the derived requirements. This paper will also shortly discuss vulnerabilities, providing directions for future work.

Keywords

Vehicular Ad Hoc NETworks (VANETs), Security, Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I)

1. INTRODUCTION

Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communication systems are promising for increasing road capacity, avoiding accidents, providing web or entertainment services, and other applications [34, 40]. V2V refers to communication between vehicles and V2I refers to the communication between vehicles and other communication entities located within a fixed infrastructure. Because many of these transmit sensitive data such as identification, position, and speed of the vehicle, a high level of security and privacy insurance [26, 31] is a prerequisite for broad acceptation of these communication systems. Therefore, security in V2V and V2I communication is a field attracting considerable attention over the past few years. This paper provides a short overview of the main V2V and V2I security architectures that are currently available, and at the same time compares them using a set of derived requirements.

Although in 2006 some of the basic network and security features were standardized in IEEE 1609.2 [14] by the Institute of Electrical and Electronics Engineers (IEEE), many improvements to the security architecture have been proposed since then, because not all required features were included in those standards. In particular, privacy and key revocation applied in the Public Key Infrastructure (PKI) are topics that were left open [17, 22]. However, since then, various schemes [10, 11] and alternative security architectures [5, 7, 9, 16, 38] have been developed to address these issues. The purpose of the paper is to review the main currently available security architectures based on a combination of requirements established by various papers.

13th Twente Student Conference on IT June 21st, 2010, Enschede, The Netherlands.

One of the first V2V and V2I communication architectures was developed by the Vehicle Safety Communications Consoritium (VSCC). This consortium realized their project in the United States of America in two phases. The first phase, denoted as Vehicle Safety Communications (VSC) started in 2002 and ended in 2004 [36, 37]. The second phase, denoted as Vehicle Safety Communications 2 (VSC2) started in 2006 and ended in 2009 [38]. VSC focused on traffic safety related applications, such as avoiding accidents. VSC especially focused on the standardization of the communication architecture [26]. Security might not have been addressed sufficiently, though the VSCC proposed security improvements to the IEEE 1609.2 standard. Apart from VSC, other important projects in the area of security in V2V and V2I communication include Secure Vehicle Communication (SeVeCom) [12, 16, 18, 19, 20], funded by the European Commission, and Network on Wheels (NoW), funded by the German government [5, 7, 29]. SeVeCom started in January 2006 and its duration was planned for 4 years, while NoW started in 2004 and ended in May 2008.

The paper will address the following research questions:

1. What are the V2V- and V2I-specific requirements for secure networking?
2. Which architectures are available for securing V2V and V2I communications?
3. Are these security architectures able to fulfill these requirements?

For this paper, a literature study has been performed on two aspects: requirements and available security architectures. After this study, a qualitative comparison is made between the examined architectures, based on the set requirements. The requirements are ordered by type, while the current architectures are summarized. These summaries will contain the information needed for an analysis based on the requirements. The analysis is performed by requirement, discussing essential differences between each architecture in detail. This paper concludes by selecting a preferable architecture based on the performed analysis.

This paper is organized as follows. Section 2 answers the first research question by discussing the requirements associated with security in V2V and V2I communication. In section 3, an overview of the main currently available security architectures is provided to answer the second research question. The third research question is answered in section 4, where a comparison between the discussed security

architectures is provided. Finally, section 5 concludes and provides recommendations for future activities.

2. REQUIREMENTS

Many projects and papers have defined their own requirements for various purposes, including comparison of security architectures or cryptographic techniques, and providing solutions for specific applications. An important work by Plößl et al. [28] discussed core security requirements. However, these requirements have been refined since then.

This section presents a summary of the requirements for a security architecture for V2V and V2I communication systems. They have been divided into three groups: privacy, message security and network management. Privacy requirements aim to hide the identity of the user and prevent attackers to build a profile of the user behavior. Message Security requirements protect the sent messages against tampering, faking and inspection, protecting the network from unauthorized users and attackers. Network Management requirements provide further protection of the network and keeps it maintainable. A description of each requirement is given in the following subsections.

2.1 Privacy

Weak anonymity means that vehicles cannot be identified from the messages they send, and that these messages can only be linked to the sending vehicle within a certain time frame. This as opposed to **strong anonymity**, which requires that no messages are linkable to vehicles. However, this is impractical for many applications, which rely on sources to provide repeated information. If strong anonymity is enforced, these applications may become useless [24, 25]. Proposals have been made to implement weak anonymity through pseudonyms, allowing users to change pseudonyms to retain their anonymity. Thus, an attacker should not be able to connect different pseudonyms. Note that this requirement views anonymity from the network perspective: it does not require protection against an inside attacker, which has access to the secret data that the certificate authority (CA) controls [24, 25, 27, 35].

Location privacy means that the location of a vehicle over time should remain private. More practically, an attack on the privacy of a vehicle that uses a V2V or V2I communication system should not be easier than tracking it through other methods (such as following the vehicle). Lack of location privacy would allow those with a reasonable budget [6] to collect information about where users go and sell this information, causing a large invasion of the users' privacy, which hampers the deployment and acceptation of V2V and V2I communication systems [24, 27, 30, 35].

2.2 Message Security

Message authentication provides the possibility to a receiver to identify the sender of a message. This could also be accomplished through a pseudonym, to still be able to ensure the privacy of the sender [24, 25, 28, 30, 35]. Closely related to this requirement is **message integrity**, which allows the sender to check that the message is not modified. These two requirements are essential to ensure that received messages can be trusted to originate from the right source and are not modified on their route to the receiver [24, 25, 27, 28, 35].

Message non-repudiation prevents a sender from falsely claiming he did not send a certain message. When coupled with liability identification, which defines that an authority should be able to resolve the users' anonymity under certain conditions, this requirement allows the appropriate authorities to trace abusive behavior [24, 25, 30].

Message confidentiality ensures that messages between two communicating entities (vehicles or road side units) cannot be read by a third party. This requirement is essential for applications that transmit identifying private data, such as credit card details, which can be used for applications such as automatic toll booths [24, 25, 28].

Error detection allows the architecture to detect malicious or erroneous transmissions from vehicles that are otherwise legitimate. It has been suggested that this can be implemented through some form of data verification, where the receiver can check a received message against similar messages and determine the validity of the data in the message. This can be used to detect malicious users, which may send a large amount of invalid data [2, 30].

2.3 Network Management

Efficiency means that the security architecture should take as little bandwidth and time as possible. This is essential for traffic safety applications that are used to ensure the safety of vehicle passengers, such as collision avoidance. Lack of efficiency in security will mean either that security will not be used or that traffic safety applications are not applicable or useful [17, 27, 28, 30, 35].

Liability identification, which is closely related to message non-repudiation, requires that messages concerning abusive behavior can be linked and used to identify the malicious user. It can also be used to detect malfunctioning On-Board Units (OBUs). The OBU represents a communication module that is installed and used by each vehicle that supports V2V and V2I communication. Without this security functionality, attackers can easily use the anonymity that the networks provide to remain undetected or untraced [25, 27, 35]. Together with non-repudiation, this allows the system to hold users accountable for their actions.

Flexibility defines that the security architecture should allow the developer and operator to determine which algorithms may be used, as well as allowing them to change these algorithms and perform updates to the system. High flexibility means that the system will not need to be replaced in the near future, while low flexibility might cause the deployment and adaptation of V2V and V2I communications to remain low until a more flexible architecture is developed, or allow many security and privacy attacks that are currently unknown [17].

Availability, which is also denoted as robustness, means that the architecture should be designed such that it is resilient to attacks that attempt to take down the network architecture. These attacks are commonly referred to as Denial of Service (DoS) attacks. In V2V and V2I communications, in addition to the usual DoS attack techniques used on the Internet, jamming is an efficient method. Defense against this type of attack is difficult [24, 25, 30].

Scalability is important when V2V and V2I communications become widespread. When this happens, V2V and V2I communications will rival or even surpass the Internet in terms of network size. The security solution should perform well under the given time- and bandwidth-constraints even when every car in a traffic jam on a major motorway is connected to the network [28].

3. SECURITY ARCHITECTURES

In this section, some main security architectures for V2V and V2I communication will be discussed. These security

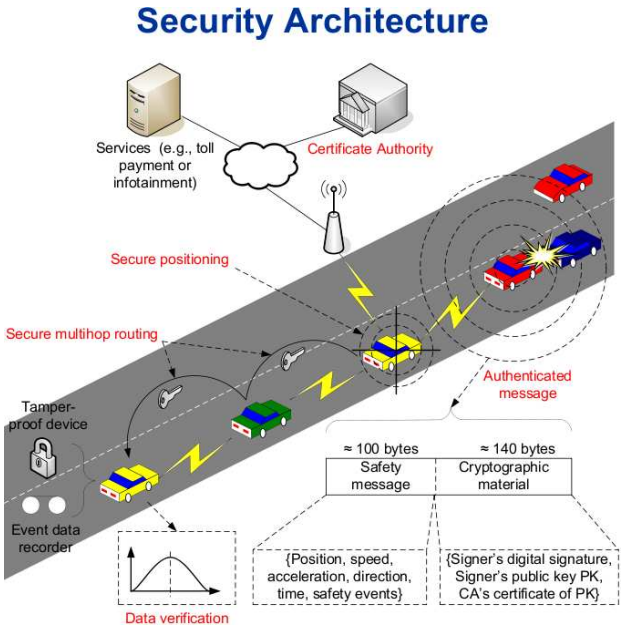

Figure 1. Illustration of a security architecture, taken from [5].

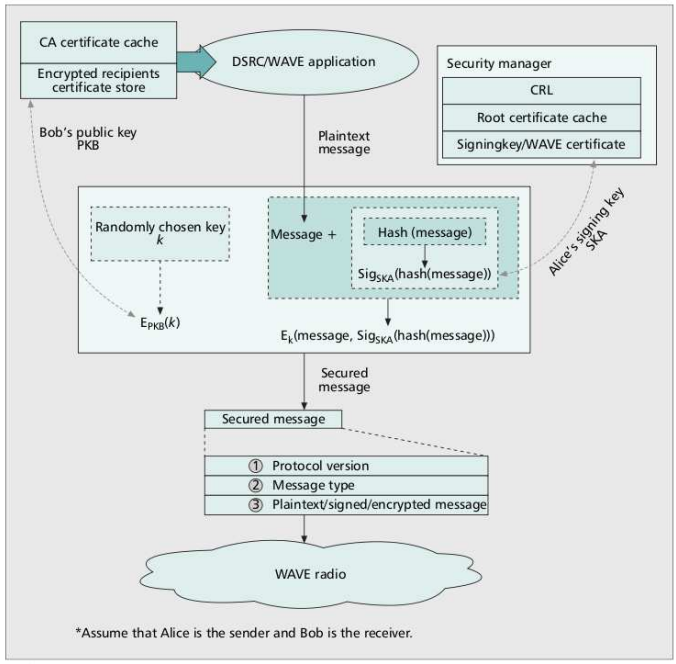

Figure 2. Illustration of the IEEE 1609.2 standard, taken from [22].

architectures are mainly developed by large vehicular networking projects that are carried out by several academic and industrial partners. The development process consists of roughly the same series of steps for each of the security architectures discussed here. First, a series of applications is identified. From these, characteristics and security requirements are derived, followed by an identification of the potential threats. For each of these, a security mechanism may be developed, or an existing solution may be used. The security architecture itself defines how these mechanisms will interact. To some extent, the V2V and V2I security components and their functionality are also determined by the security architecture [2, 18, 36].

First the IEEE 1609.2 standard is discussed, followed by three main security architectures for V2V and V2I communication systems. These are: Vehicle Safety Communication (VSC), Secure Vehicle Communication (SeVeCom) and Network on Wheels (NoW), which are respectively developed in the United States, the European Union and Germany. VSCC significantly contributed to the IEEE 1609 standard, including its security component, IEEE 1609.2. However, the security component of VSC has focussed on a specific branch of applications, namely those to improve road safety [37]. The current communication standard contains only weak security (defined in the 1609.2 standard [14]) and provides no privacy.

All of the discussed security architectures solve the authentication problem with a common solution; the Public Key Infrastructure (PKI). This solution requires the security architecture to define a way to assign and distribute certificates, which can be used to check that a message is indeed from the specified source. An example of such an architecture can be seen in Figure 1, which illustrates the basic PKI elements as well as some other desirable mechanisms such as secure positioning, data verification and multi-hop communication. The Certificate Authority (CA) takes care of the distribution of certificates. Note that an OBU is located in each vehicle and a Road Side Unit (RSU) is represented in Figure 1 as the base station that is wirelessly communicating with vehicles driving on the road. The message structure and size may be different, but the important elements (in particular, the signer's signature) remain the same. An important problem with the PKI solution is that sending a message with a certificate means that the sender may be identified by it at any point. To solve part of this privacy issue, multiple certificates are assigned to the same vehicle. This method may be denoted differently in the presented security architectures. In VSC, it is called Anonymous Certificates, while SeVeCom and NoW call it Pseudonyms. Other important PKI issues relate to assigning and revoking certificates. The security architectures provide different solutions and these will be discussed in the following subsections.

3.1 IEEE 1609.2

The current version of the IEEE 1609.2 standard was approved 8 June 2006 and defines many implementation details for the basic security features [14]. These security features are not complete, as papers written since then have pointed out. However, this paper will discuss the features shortly before moving on to more recent solutions. The main topic of IEEE 1609.2 is authentication of messages. This process is illustrated in Figure 2. It shows how the sender (Alice) secures a message, by first hashing the message, followed by a signature and an encryption with a random key. This random key is encrypted with the public key of the receiver (Bob) and then appended to the message. The signing key, which is used to create the signature, is stored in the security manager of the sender, while the public key of the receiver is retrieved from the CA.

For message authentication and integrity, the Elliptic Curve variant of the Digital Signature Algorithm (DSA), ECDSA, is proposed to sign and verify public messages. To communicate private messages, the current standard symmetric encryption algorithm, Advanced Encryption Standard (AES) [3], is used. To communicate the AES key, it is en-

Figure 3. VSC message format, taken from [36].

crypted using Elliptic Curve Integrated Encryption Scheme (ECIES) and transported with the message [14]. The difference between ECDSA and ECIES is that the latter is an application of ECC to encryption, while the former is an implementation of DSA using ECC. The mathematics behind Elliptic Curve cryptography (ECC) are based on a very complex problem related to Galois Fields [15] and is not of interest for this paper. However, Elliptic Curve cryptography has a core advantage in key size: they are generally an order of size smaller than the standard RSA keys for the same level of security. RSA (which stands for Rivest, Shamir and Adleman, the researchers that first published it) [32] is one of the most commonly used methods of asymmetric encryption and signature generation, based on integer factorization, while DSA [4] is the standard algorithm to sign messages based on primes and modular arithmetic. The required signatures for a Road Side Unit (RSU) may be distributed manually, to prevent an attacker from obtaining such a certificate [21].

As we can see in the summary above, as well as the standard document [14] and the analysis paper by Laurendeau & Barbeau [21], IEEE 1609.2 does not consider any privacy requirements for public messages and thus does not provide location privacy, which is assumed to be amended to the standard at a later date [14]. Much emphasis is placed on securing the transmitted messages, but not on other requirements such as liability identification or data verification.

3.2 VSC: Vehicle Safety Communications

The VSC project, which ended in 2004, is slightly older than the IEEE 1609.2 standard discussed in section 3.1, to which it provided large contributions [8]. However, contrary to IEEE 1609.2, the security component of the VSC project defines a more detailed security architecture and proposes on how to fill the gaps in this architecture with future research. A security layer on top of the existing 3-layer communication stack is defined. The existing stack consists of a physical layer (IEEE 802.11p radio), a link layer (IEEE 802.11p Media Access Control (MAC)) [13] and a newly developed network and transport layer. Above the security layer, VSC defines the Safety Application Layer, which is included in the standard mainly for the purpose of data verification by the safety applications. A general scheme for data verification is not discussed [36].

The VSC security architecture considers three important issues: authentication and certificate distribution, revocation and updating, and privacy. Various other issues are discussed but not solved, and some are not addressed at all. These issues can be connected to the requirements in a fairly straight-forward manner.

3.2.1 Authentication & Certificate Distribution

In VSC, a number of possible methods for obtaining initial certificates are proposed, though no decision is made. New certificates may be assigned in a similar manner as the update distribution. A hierarchy for managing certificates is described in VSC, which separates government and consumer OBUs into separate hierarchies. The government runs its own CA to distribute certificates for RSUs and OBUs of public safety vehicles like police cars. This hierarchy is expected to be similar to the governmental hierarchy (ie. national, state and county level CAs). VSC does not consider privacy requirements to be applicable to these certificates. Consumer devices receive certificates from CAs run by the OBU manufacturers [36]. The advantage of this scheme is that it is harder for an attacker to obtain a certificate that is meant for public safety vehicles.

The signature algorithm that will be used to generate and validate certificates is the ECDSA, resulting in relatively low security overhead, especially when compared to RSA or DSA, for the same level of security. Signature generation and authentication time is estimated to be sufficiently low as to not have a large impact on system performance. The structure of a typical user-generated message is illustrated in Figure 3. Note that a message from a public safety vehicle would look different, as this type of vehicle does not have privacy requirements [36].

3.2.2 Revocation & Updating

Because a PKI is used, revocation of certificates is an issue. The security architecture needs to define a way to detect malicious OBUs, which may be created by attackers or caused by a malfunctioning software component, and prevent these OBUs from sending malicious data into the network. Detecting malicious OBUs that hold a certificate is not in the VSC scope. It is assumed that some verification method will be used to detect malicious information. The project documents do suggest that the Safety Application Layer should be used to validate data. A common way to prevent malicious nodes from using the network is to use a Certificate Revocation List (CRL), which simply publishes lists of revoked certificates. The VSC project also hints to this solution, but it does not recommend its mandatory use. The main objection to using CRLs is the fact that their size drastically increases over time, especially because expired certificates should also be revoked. However, other solutions may be yet more challenging. CRL distribution could be provided the same way as providing the OBU with new certificates and software updates, or simply by using broadcasts. In the former case, all of this information should simply go through an encrypted connection from the CA to the OBU, using some encryption method, or through a separate secure channel [36].

3.2.3 Privacy

The VSC project discusses seven schemes to protect privacy, from which anonymous certificates is found to be the best trade-off between privacy, management complexity and containment of malicious OBUs. In the successor of VSC, VSC 2 [38], a group-based protocol is used, an approach that is also outlined in VSC. This protocol uses probabilistic verification and allows a configurable level of privacy and is referred to as the zero-trust model [33, 39]. However, in VSC, anonymous certificates are used to prevent any receiver in the network to build a consistent profile of a vehicle, since the target vehicle switches certificates periodically. A method to switch between these certificates is not defined. To allow a CA to revoke rights of a malicious device, anonymous certificates should be linkable by the appropriate authorities. To protect a vehicle from attackers from inside the CA, certificates should be blindly signed and a scheme is described to make it computationally infeasible to link a large amount of certificates. Access should also be restricting through appropriate procedures [22, 36].

3.3 SeVeCom: Secure Vehicle Communication

The SeVeCom project is an European project that was specifically set up in order to develop a complete security architecture. The project planned to provide a significant amount of input to the European Telecommunications Standards Institute (ETSI), Intelligent Transport Systems (ITS) Technical Committee working group 5, which will standardize a new security architecture [1, 5]. It assumes that a vehicle has an Event Data Recorder (EDR), a Tamper Proof Device (TPD) and some device for a global navigation satellite system such as GPS [23]. The EDR is used to record any liability-related data, both from vehicle sensors and received communication, while the TPD is used to contain all the vehicle's secrets, which include an electronic license plate and key pairs. The TPD should also have its own battery and clock, which it uses to perform all the security tasks for the vehicle. This includes signing and verifying digital signatures, encryption and decryption, and key management. As its name suggests, the TPD should be protected against tampering. Only authorized personnel should be allowed to modify it [20].

In addition to these vehicle components, the security architecture consists of a series of modules that provide security functionality, as show in Figure 4. The modules discussed here are: the secure communication, the identification & trust, the privacy management, the in-car security and the tamper evident security module. It should be noted that the SeVeCom security architecture is designed to be as modular as possible, and it is not unthinkable that modules will be modified to contain additional security features or different algorithms at a later date. Each described component has several goals and interacts with the other components. These relations are illustrated in Figure 4.

The **secure communication module** facilitates all communications between vehicles. Through the network protocol, four types of messages may be sent: insecure, authenticated, confidential and secure messages. Insecure messages are comparable with plain text messages over the Internet; they do not contain any protection. Usefulness of these messages is limited; most applications require knowledge about who is the sender. For these, authenticated messages can be used. Typically, a Message Authentication Code (MAC) is used to ensure authenticity and integrity of the message. Authenticated messages are generally used for beaconing, transmitting the information about the vehicle under some pseudonym. To prevent receivers from reading a message, confidential messages can be used. Secure messages are both encrypted and authenticated, in either order. In both cases, confidentiality can be achieved by using a standard encryption scheme [20]. For efficiency reasons, an approach that uses symmetric session keys is desirable, since asymmetric encryption is computationally expensive, especially when large chunks of data are transfered (ie. updates, CRLs and so on). There are schemes available for key-exchange for both group and single receivers, though a previously agreed key could also be used. This module also provides secure routing based on location (georouting), and the transmission of messages that are persistent on some location for a specified amount of time or hops (geocast).

The **identification & trust module** is the module that handles everything concerning the management of identities. It manages the identity of the vehicle and the credentials to authenticate the vehicle's messages (identity management) and is in charge of checking the authenticity of received messages (trust management). Part of this module is also the PKI and the CAs that distribute and revoke certificates. The certificates in SeVeCom are simply managed by the CA belonging to the governmental region in which they are assigned. Exclusively CAs can link the pseudonyms of users, which they can use to revoke all certificates of a particular user [24]. In addition to these procedures, SeVeCom defines mechanisms for detecting rogue and misbehaving nodes. This happens through correlation of the data. Once sufficient information has been gathered, SeVeCom provides three methods for revocation; through the TPD, through compressed CRLs and through a distributed protocol. In particular the use of a distributed protocol has advantages, since it can be used without direct access to the CA. Revocation through the TPD simply disables the target vehicle's TPD, so it can no longer sign messages. Compressed CRLs are similar to normal CRLs but use some optimizations that also apply to VSC (if used with CRLs). The distributed protocol, simply called Distributed Revocation Protocol, allows vehicles to communicate and accuse a vehicle that misbehaves. If sufficient accusations are made, messages from that vehicle are ignored. When possible, a report to the CA is made [12, 20].

The **privacy management module** is an extension of the identification & trust module and is in charge of applying pseudonyms, ensuring that the vehicle retains a certain level of privacy (pseudonym application). It will also decide when to change pseudonyms, to strike a balance between connectivity, efficiency and privacy (pseudonym management). For this, a known method called mix zones is used [20]. Pseudonyms may be provided by an entity different from the CA and consist of the entity's identifier and signature, along with a public key and lifetime. New pseudonyms may be requested from a provider whenever needed [24]. It could be possible that the privacy management module allows a configurable level of privacy. When changing a pseudonym, it is important to note that all the lower level protocols (in the Internet protocol stack, these would be IP or MAC addresses) should also change their identity. If this does not happen, these addresses would allow an attacker to trace a vehicle regardless of what measures it took to protect its identity [20].

The **in-car security module** is still subject of research and is thus not yet worked out. However, the goal of this module is simple: to prevent unauthorized users from executing code on other OBUs. This is implemented through two components: a firewall and an intrusion detection mechanism. The firewall component is straight-forward, as its goals are comparable to those of firewalls that are used on general-purpose machines, protecting the car's systems from attacks coming from the network. Specific to V2V and V2I communication systems, the firewall should also maintain consistency between the car's internal systems (for example, use the car sensors to check data). The intrusion detection mechanism should detect hardware tampering and establish trust between various hardware components. This, combined with the tamper evident security module, protects the system from hardware level attacks [20].

The **tamper evident security module** is the component that controls the secret data of the vehicle, ie. private keys, certificates and the vehicles long term identity. It is in control of all security operations, which are calculated in the TPD. This protects the system against hardware attacks and makes sure that the keys will never leave the

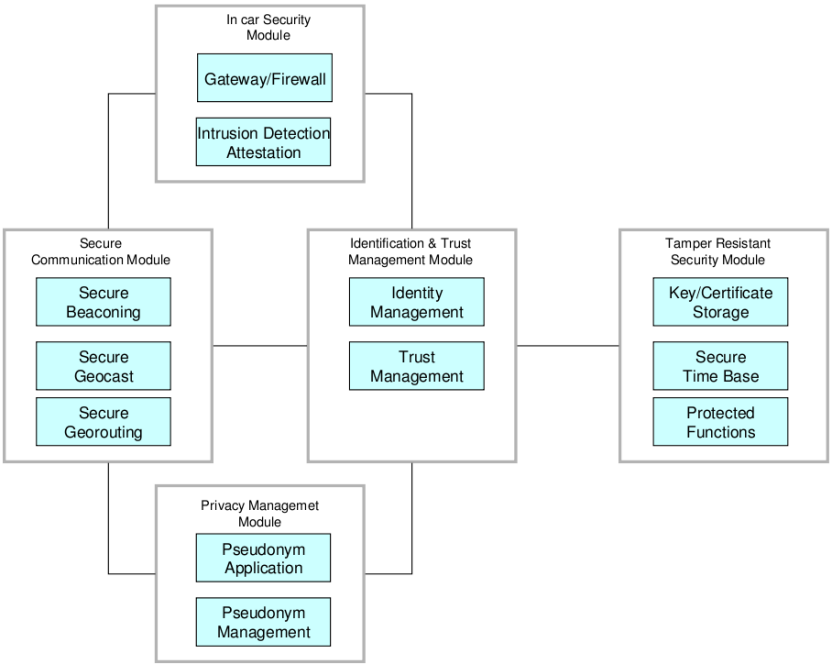

Figure 4. SeVeCom architecture components, taken from [20].

TPD, as well as protecting against tampering. In addition, this module contains a battery and a reliable time source, both included in the TPD. These are used to add a timestamp to the message. SeVeCom explicitly chooses not to include GPS in the module, as it is vulnerable to attacks on the GPS signal (GPS spoofing) as well as not being essential. Similarly, GPS cannot be used for the secure timing required for cryptographic calculations [12, 20].

It is also proposed by SeVeCom members to increase the availability of communication through spreading out over various distinct wireless technologies, such as Ultra-Wide Band (UWB), Bluetooth and the Global System for Mobile communication (GSM), apart from the default IEEE 802.11p technology. This provides additional availability and protects the system against jamming/DoS attacks aimed at the IEEE 802.11p technology. Note that when an attacker jams all these wireless technologies, availability will still suffer [31]. Note however that this technique is not mentioned in the SeVeCom security architecture document [20].

The current SeVeCom proposal uses ECDSA for cryptographic purposes. It also includes various other signature schemes, such as RSA, in its comparisons. Results indicate that ECDSA has reasonable performance for both key size and generation and verification speeds. The latter two properties are highly desirable in V2V and V2I communications, considering the high speed and time constraints. Though ECDSA is not the fastest, its small key size makes it the recommended algorithm for now [20, 12].

3.4 NoW: Network on Wheels

The Network on Wheels (NoW) project is another recently completed project. It was active between 2004 and 2008, funded by the German government and the automotive industry in Germany. Like VSC, NoW focuses on the standardization of the entire communications architecture rather than just the security aspect. It is suggested that the project's results will be combined with SeVeCom and other projects to create a single architecture, which will be standardized by ETSI [5].

This paper focuses on the Organizational and Component View of the NoW security architecture, which is described along with various other views in the paper that presents the NoW security architecture [8]. This view reasonably resembles the other two architecture descriptions, allowing for simplified comparisons between each section. The components that NoW uses are divided in two groups; Security Infrastructure and Node, defining where they run, respectively. As the name implies, security infrastructure components provide an infrastructure that the consumers' nodes may use. The infrastructure contains the following components: Communication Security, Juridical and Executive Authorities, Inspection Site and the Registration Authority. The node contains a defensive component (data assessment & intrusion handling), a component that handles revocation, a mechanism to use and change pseudonyms, testing and certification components, and the vehicles (secret) registration. The node and infrastructure components interact as defined in the Functional Layers view [8]. This extra information is omitted here. Instead, the general layout of the security architecture, also shown in Figure 5 is in the following subsections.

3.4.1 Security Infrastructure

The **communication security** component contains the necessary PKI to facilitate the use of certificates to sign messages. This module covers the basic security requirements; authentication, integrity and non-repudiation, when combined with the revocation mechanism. A mechanism that generates pseudonyms for a node to use is also assumed to be provided. This component also contains mechanisms to test the system and detect errors in the system, as well as attacks.

The **registration authority** and the vehicle manufacturers together run a registration system that determines the long-term identity of a vehicle. They both assign this unique identity to the user's OBU and the registration of

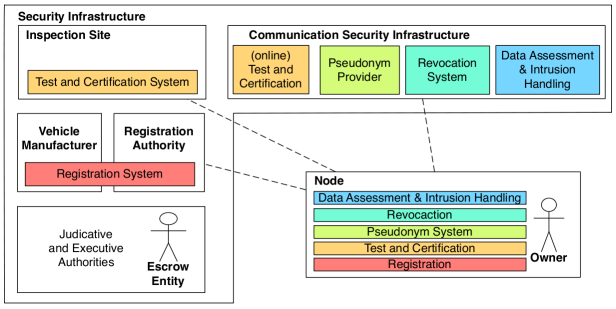

Figure 5. NoW Organizational and Component View, taken from [8].

the user and his vehicle with the correct authority.

The **inspection site** is the part of the architecture that performs intrusion detection, together with what the nodes do in a distributed manner. It may be required for users to test and certify their OBU to receive certificates. This component attempts to guarantee correctly a functioning system, using the Communication Security component to determine this.

The juridical and executive **authorities** manage access to the network. They include police and the court, and can permanently remove users from the system, or punish violations of rules.

3.4.2 Nodes

The **data assessment and intrusion handling** component is the local counterpart of the same functionality that the communication security component delivers through the network. Together, they protect the network against attacks based on misinformation and faulty nodes that transmit incorrect data. This is achieved through simple low-level checks, which are called plausibility checks in NoW [2, 8].

The **revocation** component provides local revocation services. It makes sure that messages signed with revoked certificates are not accepted and could even provide a self-revocation service for when the tamper-proof device is compromised, or when a critical malfunction is detected.

Location privacy is ensured to some extent through the **pseudonym system** component, which decides when to change between pseudonyms and maintains a cache for them. An algorithm to change pseudonyms, called mix contents, is also defined in NoW. This algorithm requires that sufficient similar vehicles are present and close enough, where similarity is determined through the possible attributes in the message contents. The algorithm should be improved by the use of a minimal stable time, in order to avoid the situation that vehicles constantly switch pseudonyms.

The **test and certification** component contains tests to ensure the stability of the system, together with basic tools to verify certificates. The hierarchy for certificates is not provided. This component also allows that some vehicles receive special privileges or functionality. For example, the system can be configured to instantly recognize police cars or ambulances and notify the drivers on a road to make room. This component also provides multi-hop authentication, splitting the message in a mutable and immutable part. The mutable part is altered and signed by during each hop, while the immutable part (the actual data) remains intact. Note that in order to build a trusted forwarding chain, as defined in NoW, a lot of additional certificates need to be signed [7, 8].

Finally, the **registration** component contains a TPD to store the vehicles' long term identity and private keys. It communicates with the registration authority for this purpose. Through this communication, the component should also be able to revoke the long term identity if tampering is detected [7, 8].

4. COMPARISON OF SECURITY ARCHITECTURES

In this section, the security architectures discussed in the previous section will be compared separately on each requirement. Each of the comparisons are presented separately as follows; first, it is established which of the architectures implement the feature. If more than one architecture contains the feature, differences will be discussed.

4.1 Privacy

4.1.1 Weak anonymity

Weak anonymity is a requirement that, when addressed, allows the user to have guaranteed anonymity within a certain time frame. This guaranteed anonymity is achieved in NoW by providing an algorithm called mix contents [6]. Though both VSC and SeVeCom identify the necessity of such an algorithm, only NoW defines one, while SeVeCom refers to an older algorithm called Mix Zones [20]. Each architecture applies some form of pseudonyms to ensure the anonymity of the certificates used to sign messages, as described in section 3. To protect privacy while authenticating messages, the adaptive anonymous authentication protocol has been designed. It allows a configurable amount of privacy by specifying which servers are trusted; all servers, private only, public only, or no servers at all. The protocol uses a probabilistic method to verify certificates through a group of vehicles that use V2V communication [33, 39].

4.1.2 Location privacy

The solution provided by each architecture for the location privacy requirement is based on pseudonyms. These pseudonyms, which are also used to provide weak anonymity, provide sufficient protection of messages to keep the user's privacy as safe as it would be without VANETs from attackers in the network. However, VSC is the only architecture that goes into detail about which procedures and methods may be used to shield the user from inside attackers [36].

4.2 Message Security

4.2.1 Authentication & Integrity

Each architecture contains these basic security requirements and implement it in a similar, standard fashion: a PKI is used. Each of them recommends the use of the ECDSA, which is cited to have the smallest keys while still maintaining sufficient verification speed [5, 12, 20]. SeVeCom, which allows symmetric cryptography to be used for their confidential messages, notes that these keys can also be used to ensure integrity through Message Authentication Codes, without mentioning a specific algorithm.

Each architecture defines a CA hierarchy along governmental lines, such that every country, state and region have their own CA and are responsible for their own users. VSC also defines a separate CA for consumers that lets the manufacturers of the OBUs manage the certification

of their own users. The advantage of this approach is that public safety vehicles are the only vehicles managed by the government, which makes it harder for an attacker to obtain a public safety certificate, with which an attacker could cause significant disruption or advantages over other traffic [36]. However, privately managed data may be more vulnerable to privacy violation by the OBU manufacturers or inside attacks by employees of this manufacturer. NoW defines an additional authentication mechanism, that allows the receiver to see which vehicles retransmit a packet, through a trusted forwarding chain. This chain is built by repeatedly signing the message [8].

4.2.2 Non-repudiation

Non-repudiation is an important security property that is desirable to protect the network from malicious users. The SeVeCom project provides this through an Event Data Recorder (EDR) that is assumed to be available. It also takes secure positioning into the picture, which provides firmer guarantees on the correctness of the recorded information [12]. NoW claims to provide non-repudiation but does not explicitly define a mechanism to permanently record relevant messages. VSC only defines a circular buffer that records data in a certain time frame, which protects it against some replay attacks but does not provide non-repudiation, unless the data can be saved to non-volatile storage.

4.2.3 Confidentiality

Confidentiality is to keep transmissions secret, which is essential for some VANET applications that transmit identifying information such as automatic tolling and certificate updates. VSC explicitly does not provide confidentiality, reasoning that it has not identified any applications that absolutely require it. These applications fall outside the domain of VSC, which focuses on safety applications. Another argument put forth was that broadcasts are inherently harder to secure [36]. NoW also does not provide confidentiality in its set of features. SeVeCom defines a system for confidentiality. It performs this through encryption of the transmitted messages. It should be implemented through some standard key-exchange protocol or a previously agreed key, a symmetric (session) key should be set up. For key-exchange protocols, the pseudonyms can be used. A specific protocol is not decided on, but the Station-to-Station, based on Diffie-Hellman, is used as an example [20].

4.2.4 Error detection

Both NoW and SeVeCom indicate that data verification should be used to detect malicious users and malfunctioning OBUs. NoW implements data verification through two levels of plausibility checks [5], while SeVeCom only recommends its use. VSC already provided a scheme which could be used to implement data verification, allowing data to be checked in the application layer to retain genericness [36].

4.3 Network Management

4.3.1 Efficiency

Since the solutions of each of the three architectures have similarly structured messages, their efficiency is roughly the same. SeVeCom also provides optional confidentiality, which puts it in a disadvantage in terms of overall efficiency. NoW's implementation of multi-hop authentication requires more bandwidth and is thus less efficient. NoW, SeVeCom, IEEE 1609.2 and VSC all recommend the use of the ECDSA to provide signing services to the network, considering its efficiency in terms of bandwidth. NoW does not consider it proven to be sufficiently scalable; SeVeCom has tested some algorithms and concluded ECDSA was the best choice for now [17, 20]. Since IEEE 1609.2 uses public certificates, it is the most efficient of the discussed architectures, but also the least feature-rich.

4.3.2 Liability identification

Liability identification, the requirement that allows an authority to link a vehicle's pseudonyms, is defined by each of the discussed projects. Each also defines that strict conditions should be placed on when the authority may link the pseudonyms. VSC explicitly defines that it should be computationally expensive for the authority to compute the linking between pseudonyms [36], to protect the user against mass-surveillance. None of the architectures describe an algorithm or method to link the pseudonyms, though this makes sense as the pseudonyms are not bound to a specific cryptographic method either.

4.3.3 Flexibility

A major advantage of the VSC architecture is that it performs data checking in its Safety Application Layer, which allows the application designer to define different policies. These policies can define how strict security should be, or pick out messages that can be skipped (for example, when the communication type is not supported) [36]. SeVeCom allows similar measures for both confidentiality and the signing of messages [20]. It also emphasizes the ability to adapt the security architecture quickly. NoW provides some more detail in how the system should be implemented in a vehicle.

4.3.4 Availability

NoW considers a general transmission medium to be used, rather than some specific protocol (which is DSRC, in the case of VSC). It specifically allows the use of other layers for the purpose of communication [8]. These proposals have also been made by SeVeCom members [29], but has not been inserted into the standard. VSC does not discuss the issue of availability. The risk of using other mediums is that it hurts the privacy of the user, since the medium might not support a dynamic address (for example, the MAC address of a network card of a general purpose computer is fixed). As discussed in SeVeCom, it is required that these addresses be changed somehow whenever a pseudonym change occurs [20].

4.3.5 Scalability

Scalability is a hard to match requirement without precise definition of which algorithms will be used. Like efficiency, this requirement is matched roughly equally by each architecture, with possible exception of NoW. NoW has a number of procedures that have the potential to slow the system down; data checking and the trusted forwarding chain may hurt scalability. With sufficient availability and small signatures, as currently defined, the security architectures do not have to worry about bandwidth as much as before.

5. CONCLUSIONS & FUTURE WORK

In this paper, an analysis of three security architectures for VANETs was performed. The analyzed architectures, NoW, SeVeCom and VSC, were first described and then compared based on the requirements that were established. The requirements were split into three groups according to their goals: privacy, message security and network management. Notably, all discussed architectures apply similar means to achieve message authentication and use the

same asymmetric cryptographic algorithm (Elliptic Curve Cryptography), citing its small key size and relative speed as major advantages. SeVeCom provides a very powerful and general baseline architecture, providing all the basic requirements, but lacks the description of critical details. NoW supports some very useful security features and algorithms that provide a higher level of privacy and authenticity. However, VSC still provides superior privacy protection. On the other hand, VSC does not specify all the security features, such as availability, with the level of detail that the other security architectures specify. In addition, their contributions have already proved to be very useful for the IEEE 1609.2 standard. The results obtained by the SeVeCom and NoW projects will be considered as input for standardization by ETSI ITS WG5. As future activities in this area one could consider large experimental trials where the SeVeCom, VSC, VSC2 and NoW security architectures, or security components could be implemented and verified in sufficiently large and realistic V2V and V2I field tests. Depending on the results of these field trials, conclusions could be derived on which of the security architectures or security components can be recommended for further standardization or for the enhancement of the existing IEEE 1609.2 and ETSI security specifications.

6. REFERENCES

[1] 7th Framework Programme. GeoNet website. Online Resource: http://www.geonet-project.eu/, last accessed: 23 May 2010.

[2] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller. Attacks on inter vehicle communcation systems - an analysis. In *3rd International Workshop on Intelligent Transportation*. WIT, 2006.

[3] Federal Information Processing Standards. Advanced encryption standard. Technical report, National Institute of Standards and Technology, 2001.

[4] Federal Information Processing Standards. Digital Signature Standard (DSS). Technical report, National Institute of Standards and Technology, 2009.

[5] M. Gerlach. C2X security and privacy - standardization NOW. Presentation slides. Available from: http://www.network-on-wheels.de/, last accessed 29 March 2010.

[6] M. Gerlach. Assessing and improving privacy in VANETs. In *4th Workshop on Embedded Security in Cars*. ESCAR, 2006.

[7] M. Gerlach. Use cases for a vehicular network security system, draft version 1.0. Technical report, NoW: Network on Wheels, 2007.

[8] M. Gerlach, A. Festag, T. Leinmüller, G. Goldacker, and C. Harsch. Security architecture for vehicular communication. In *5th International Workshop on Intelligent Transportation*. WIT, 2007.

[9] M. Gerlach, F. Friederici, A. Held, V. Friesen, A. Festag, M. Hayashi, H. Stübing, and B. Weyl. Pre-Drive C2X, deliverable d1.3, version 1.0: Security architecture. Technical report, 7th Framework Programme, 2009.

[10] Y.-C. Hu and K. P. Laberteaux. Strong VANET security on a budget. In *Workshop on Embedded Security in Cars*, 2006.

[11] D. Huang and M. Verma. ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. *Ad Hoc Networks*, 7(8):1526–1535, November 2009.

[12] J.-P. Hubaux, S. Capkun, P. Papadimitratos, and M. Raya. Securing vehicular communications. Presentation slides. Part of SeVeCom project.

[13] IEEE 802.11 Working Group. *IEEE P802.11p/D3.0, Draft Amendment for Wireless Access in Vehicular Environments (WAVE)*, 2007.

[14] IEEE P1609.2 (1556) Working Group. *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, 2006.

[15] A. Jurisic and A. Menezes. Elliptic curves and cryptography. *DOCTOR DOBBS JOURNAL*, 22:26–37, 1997.

[16] F. Kargl. SeVeCom Deliverable 2.1-App.A, version 1.2: Baseline security application. Technical report, 6th Framework Programme, 2009.

[17] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: Implementation, performance, and research challenges. *IEEE Communications Magazine*, 46(11):110–118, November 2008.

[18] R. Kroh, A. Kung, and F. Kargl. SeVeCom Deliverable 1.1, version 2.0: Vanets security requirements final version. Technical report, 6th Framework Programme, 2006.

[19] A. Kung. SeVeCom Deliverable 2.1, version 2.0: Security architecture and mechanisms for V2V/V2I. Technical report, 6th Framework Programme, 2007.

[20] A. Kung. SeVeCom Deliverable 2.1, version 3.0: Security architecture and mechanisms for V2V/V2I. Technical report, 6th Framework Programme, 2008.

[21] C. Laurendeau and M. Barbeau. Threats to security in DSRC/WAVE. In *5th International Conference, ADHOC-NOW*. Springer Berlin/Heidelberg, 2006.

[22] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. S. Shen. Security in vehicular ad hoc networks. *IEEE Communications Magazine*, 46(4):88–95, April 2008.

[23] National Space-Based Positioning, Navigation, and Timing Coordination Office. Global positioning system website. Online Resource: http://www.gps.gov/, last accessed: 4 June 2010.

[24] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux. Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11):100–109, November 2008.

[25] P. Papadimitratos, V. Gligor, and J.-P. Hubaux. Securing vehicular communications - assumptions, requirements, and principles. In *Workshop on Embedded Security in Cars*. ESCAR, 2006.

[26] P. Papadimitratos, A. Kung, J.-P. Hubaux, and F. Kargl. Privacy and identity management for vehicular communication systems: A position paper. In *Workshop on Standards for Privacy in User-Centric Identity Management*, 2006.

[27] K. Plößl and H. Federrath. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards & Interfaces*, 30(6):390–397, 2008.

[28] K. Plößl, T. Nowey, and C. Mletzko. Towards a security architecture for vehicular ad hoc networks. In *1st International Conference on Availability, Reliability and Security*. ARES, 2006.

[29] M. Raya and J.-P. Hubaux. The security of vehicular ad hoc networks. In *ACM Workshop on Security of Ad Hoc and Sensor Networks*. SASN, 2005.

[30] M. Raya and J.-P. Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[31] M. Raya, P. Papadimitratos, and J.-P. Hubaux. Securing vehicular communications. *IEEE Wireless Communications Magazine*, 13(5):8–15, 2006. Special issue on Inter-Vehicular Communications.

[32] RSA Laboratories. PKCS #1 v2.1: RSA Cryptography Standard. Technical report, RSA Laboratories, 2002.

[33] K. Sha, Y. Xi, W. Shi, L. Schwiebert, and T. Zhang. Adaptive privacy-preserving authentication in vehicular networks. In *First International Conference Communications and Networking in China*, pages 1–8. Citeseer, 2006.

[34] M. L. Sichitiu and M. Kihl. Inter-vehicle communication systems: A survey. *IEEE Communications Surveys*, 10(2):88–105, 2008.

[35] A. Studer, E. Shi, F. Bai, and A. Perrig. TACKing together efficient authentication, revocation, and privacy in VANETs. In *IEEE Secon 2009 Proceedings*. IEEE, 2009.

[36] Vehicle Safety Communications Consortium. Vehicle safety communications project -final report-. Technical report, United States Department of Transportation, 2005.

[37] Vehicle Safety Communications Consortium. Vehicle safety communications project task 3 final report, identify intelligent vehicle safety applications enabled by dsrc. Technical report, United States Department of Transportation, 2005.

[38] Vehicle Safety Communications Consortium 2. Vehicle safety communications - applications VSC-A first annual report december 7, 2006 through december 31, 2007. Technical report, United States Department of Transportation, 2008.

[39] Y. Xi, K. Sha, W. Shi, L. Schwiebert, and T. Zhang. Probabilistic adaptive anonymous authentication in vehicular networks. *Journal of Computer Science and Technology*, 23(6):916–928, 2008.

[40] H. Zhu, R. Lu, X. Shen, and X. Lin. Security in service-oriented vehicular networks. *IEEE Wireless Communication Magazine*, 16(4):16–22, 2009.