V2X Security & Privacy: The Current State and Its Future

André Weimerskirch
escrypt Inc.
315 E Eisenhower Parkway, Suite 008
Ann Arbor, MI 48108, USA
+1-734-418-2797, andre.weimerskirch@escrypt.com

ABSTRACT

Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication is currently a focus of research and standardization in the USA, Europe and Asia. It is believed that V2V safety applications are able to reduce traffic fatalities significantly. Data security was identified as a major technical aspect to resolve before potential deployment. In particular, communication security and privacy are main aspects to consider but also physical security of the microcontroller, key injection, privacy mechanisms implemented by government agencies, and policy questions around security. This article provides an overview of the current state and of open issues.

INTRODUCTION

The US Department of Transportation (DOT) plans to decide in 2013 whether vehicle-to-vehicle (V2V) safety applications will be deployed in the near future. A main challenge is data security and privacy to protect communication and to protect vehicle passengers' privacy. The American VSC3 (Vehicle Safety Communications 3) project funded by the US DOT is designing, evaluating and selecting security solutions and will implement a model deployment within the next two years. Also the European Car-to-Car Communication Consortium (C2C-CC) and several European projects (e.g. PRE-DRIVE, simTD, and PRESERVE) intensified research and development of security solutions for V2X. The results of these projects will be introduced to the American IEEE 1609.2 security standard [1609.2] and to the currently created European ETSI V2X security standard. Several Asian countries, including Japan and South Korea, also develop such systems.

The American projects and the American standard IEEE 1609.2 focus on V2V safety applications and single-hop V2I communication. The V2I communication provides a communication channel to a security server that is required to load security credentials for V2V safety communication. DSRC radios installed in vehicles broadcast heartbeat messages that include information such as geographic location, timestamp, and speed. In case of safety-related events, heartbeat messages might include further information, e.g. an electronic brake light flag indicating an emergency brake of the transmitting vehicle. The European approach is broader at this time and includes multi-hop geo-networking applications. The European standard is currently developed by ETSI.

It appears today that the US and Europe implement different approaches: the US projects focus on V2V safety communication security, and single-hop V2I communication is required to load security credentials that are necessary to execute secure V2V safety communication. Proprietary applications based on DSRC single-hop communication according to IEEE 1609 might be implemented as well. The European approach does not focus a single area but considers security for V2V safety applications (single-hop and multi-hop) as well as non-safety applications and V2I applications (single and multi-hop) altogether.

STATE-OF-THE-ART

Communication Security

IEEE 1609.2 describes the basic security protocol. Basic safety messages (BSM) are signed using ECDSA-224 and certificates are issued using ECDSA-256. Each message is signed (to detect alteration of a message on the receiver side and to make sure that the message originates from a valid sender), and a certificate, certificate digest (a truncated hash value of the certificate), or certificate chain (a list of certificates that represents the certificate hierarchy) is attached. By default 10 heartbeat messages are broadcast per second but advanced channel congestion mechanisms might reduce the broadcast rate. First results suggest attaching a full certificate once or twice per second but no thorough research results are available; it appears reasonable to define the rate of attaching a full certificate in terms of messages rather than time to account for channel congestion mechanisms.

Recent changes in the IEEE 1609.2 draft include the use of implicit certificates. These certificates reduce size of a packet significantly that includes signature and sender's certificate, and implicit certificates speed-up verification at receivers' side if both message and sender's certificate are verified. However, implicit certificates require using ECDSA-256 to sign messages if root certificates are set to a key length of 256 bits.

Messages can be encrypted using ECIES-256. In the current IEEE 1609.2 standard, such encryption is mainly envisioned for vehicle-to-infrastructure (V2I) communication. V2I communication is envisioned to be used rarely compared to V2V heartbeat messages.

The involved cryptographic operations are computationally expensive. Table 1 provides an overview of ESCRYPT's IEEE 1609.2 software implementation performance in terms of cryptographic operations on a 400 MHz PowerPC. It is foreseen that a DSRC unit will broadcast 10 packets per second and receive several hundred packets per second. Therefore the American VSC-A/VSC2 project suggested a verify-on-demand (VoD) approach [KW11]. Only messages are verified that will have an impact on safety applications, and all outgoing messages are signed. This approach reduces the load considerably to a few verifications per second. Note that this approach might not be used for all application architectures and needs to be considered carefully before being applied.

Table 1: IEEE 1609.2 Crypto Performances (PowerPC@400 MHz)

Operation	**Time**
ECDSA-224 Signature Generation	7 ms
ECDSA-224 Signature Verification	27 ms
ECIES-256 Encryption	28 ms
ECIES-256 Decryption	21 ms

Privacy

Privacy is a main concern for deployment of V2X. Privacy needs to be distinguished as follows:

1. *Privacy against 3rd party entities*: It is widely agreed that anonymity and long-term unlinkability of broadcast messages is required for a successful DSRC deployment. Anonymity disallows any identifier in messages that can be linked to the vehicle, such as license plate number and VIN. Long-term unlinkability makes sure that two messages broadcast at time-intervals far apart (say, at different days) cannot be linked to avoid tracking of vehicles and to avoid that behavior patterns can be derived [WHHL10]. The agreed approach is to regularly change pseudonyms. For instance, pseudonyms can be changed after a given time period (say, 5 minutes), or during special events (e.g. each time a vehicle's engine is started).
2. *Privacy against authorities*: there are several mechanisms available to provide privacy against authorities. However, any mechanism that provides a technical barrier against privacy abuse will limit the control over the network [LHH08]. Therefore such mechanisms are not considered for deployment. It is recommended to implement privacy on an organizational level by splitting the ability of authorities to recover privacy sensitive information. For instance, two authorities must collude to recover any information of a given DSRC certificate. Such design proposals are available, and they would allow sharing power by assigning V2X authorities such as Registration Authority (RA) and Certificate Authority (CA) to different parties.

It is currently debated if and to which extent the broadcast of location information affects the vehicle passengers' privacy. The European Data Protection directive [EU95] provides guidance but it is unclear which technical design satisfies the directive. A main obstacle appears the tension between the requirement of a safety system to be always enabled to function properly and to broadcast location information in plain text, and the inability to control who will receive the information.

Certificate Management and Revocation

Certificates need to be issued and certificates need to be regularly renewed. Furthermore, there must be mechanisms to revoke certificates. A variety of mechanisms are available:

- *Issue certificates*: a certificate authority (CA) issues certificates for DSRC units. The role might be split into a CA and a registration authority (RA) to introduce an organizational mean of privacy protection.
- *Renew certificates*: certificates need to be renewed regularly to provide new certificates for the privacy mechanism of changing certificates. New certificates could be requested via DSRC road-side-units (RSU), if available, or large bulks of certificates could be loaded during vehicle service. Certificates can be encrypted before loading them to a DSRC unit and only decryption keys could be provided regularly via DSRC RSUs.
- *Revocation*: revocation is necessary to remove DSRC units from the system (e.g. after misbehavior occurs). Revocation can be performed with two mechanisms:
    - *Distribution of certificate revocation lists (CRL)*: the CA lists all certificates to be removed in a CRL and distributes the CRL to all DSRC units. DSRC units then do not accept packets anymore from senders that use revoked certificates. Since each DSRC unit is equipped with multiple certificates, an efficient

mechanism is required to identify all certificates of a DSRC unit with a single entry [HHL09].

    - *Denial renewal of certificates*: the CA creates a CRL but does not distribute it to DSRC units. However, if a revoked DSRC unit requests new certificates, the request is denied.

- *CA Hierarchy:* the hierarchy can be highly flexible. For instance, there might be root CAs for Europe and for the US. Sub-CAs might be deployed per state and nation, and there might also be sub-CAs per vehicle manufacturer. It is crucial though that minimum requirements for CAs are defined to allow interoperability. A flat hierarchy is superior in terms of performance, especially for V2V safety applications.
- *Connectivity:* connectivity between DSRC units and CA is needed to enable security. At deployment, this connectivity might be provided by Cellular connection or by DRSC RSUs. In case of RSUs, it is foreseen that a relatively small number of RSUs is sufficient that can then grow with higher OBU penetration rates.
- *Bootstrapping and key injection:* OBUs need to be initialized during or after production. A cryptographic credential needs to be injected in a secure environment, and then this credential will be used to load further credentials (e.g. pseudonym certificates). The key injection process by car makers and OBE suppliers needs to be implemented in such a manner that all parties satisfy minimum security requirements, and that 3rd parties cannot forge bootstrap in order to acquire valid credentials. However, it can be assumed that parties want to implement the key injection based on available processes (e.g., for the car maker vehicles' electronic immobilizer credentials), and that these parties implement this very differently today.

Performance and Physical Security

It was described above that communication security in V2X requires computationally expensive cryptographic operations. It seems that an advanced generic automotive processor (around 1 GHz embedded microcontroller) is able to calculate at most 100-200 digital signature generations and verifications per second. However, V2V safety applications will broadcast 10 messages per second, and a vehicle will receive 1,000 or more messages per second. There are two approaches available to process such a high amount of messages: (1) only messages that might impose an actual impact to a vehicle are processed, or (2) dedicated security hardware to process all messages is applied. The first approach, called Verify-on-Demand (VoD) in the VSC-A project, was mentioned above. This approach was proven to work well in the VSC-A project for 60 vehicles, and it is supported by the IEEE 1609.2 standard draft. However, this approach might not work with all application architectures. For instance, it is unclear if VoD works with ETSI's architecture. ETSI defines a local dynamic map (LDM) that stores information about the neighborhood of a vehicle. Applications then use data from the LDM. However, it is then unclear how to apply a VoD mechanism since information in the LDM can be derived from more than one received message. On the other hand, the VoD mechanism is highly flexible; advanced applications might require a faster processor or a multi-core processor that is able to verify several messages in parallel.

The second approach is based on the assumption that all messages shall be verified before they are further processed (verify-all). Only a dedicated security controller (ASIC) is able to handle the number of required cryptographic operations, in particular ECDSA signature verifications. The European projects EVITA and OVERSEE design secure vehicle architectures, and PRESERVE [P11] is developing an ASIC. It makes sense to include dedicated security features such as secure key storage in the ASIC. In particular, no secret keys shall ever be used or stored outside of the secure controller in a vehicle's electronic system. A similar architecture is defined for the PC world by the TPM specification [TCG]. The following describes an example: a DSRC unit creates key pairs, sends the public keys to the CA, and the CA then issues certificates. Due to privacy, the DSRC unit will actually request hundreds or thousands of certificates at the same time. If a security controller is used, the controller will generate the key pairs, output the public key in plain text, but output the private key only in encrypted format to be stored in an external device since the security controller cannot hold thousands of private keys. Only the security controller is then able to load and decrypt the private key. The security controller's interface will not provide a function to output the private key in unencrypted format.

The use of a dedicated security processor provides advantageous. However, the actual security gain is unclear. On one hand, attacks on a DSRC radio can be mounted by manipulating the DSRC radio's input and by manipulating sensor output or by injecting manipulated data packets to the vehicle's communication bus (e.g. via the easily accessible OBD-II port). A dedicated security controller is not able to counter these attacks, but only a holistic vehicle security architecture avoids such attacks. Also the CA design can counter attacks: instead of providing hundreds or thousands of certificates to the DSRC unit, the CA could encrypt those certificates and provide encrypted certificates to the DSRC unit. These are useless unless the DSRC unit regularly requests a decryption key for the encrypted certificates. This design makes sure that a compromised DSRC unit never has access to more than a few certificates. The downside of a dedicated security controller is its cost, thus making attractive a security design that does not assume a security controller in vehicles or in DSRC units.

CONCLUSIONS & OPEN ISSUES

The security design for V2X is currently finalized to enable deployment of V2V safety applications. While many details need to be worked out, the overall design is stable and well understood. However, a few issues remain open – some of these issues allow advanced applications and increased performance whereas other issues need to be resolved before deployment is possible.

Epidemic Information Spreading: data can be distributed in V2X systems using V2V multi-hop communication, i.e., DSRC units re-broadcast received data after reception. Preliminary research suggested that a single RSU in a metropolitan area suffices to spread a CRL within a few hours. However, such a mechanism must be made reliable and channel congestion must be countered.

Geo-Networking: at this time, V2V safety applications are the main focus of security projects in the US and Europe. However, also extended applications are considered, including multi-hop geo-networking applications (including multi-hop safety applications). Security mechanisms need to be refined yet for such applications.

Misbehavior Detection: misbehavior detection is currently researched for all V2X applications. Misbehavior detection includes detection of malicious nodes as well as detection of defect nodes. It seems reasonable that misbehavior detection needs to be closely linked to applications since only applications are able to evaluate the trustworthiness of a specific application packet. At this point it is clear that the sender should perform an outgoing validity check to avoid broadcast of defective sensor data, and incoming messages shall be checked for plausibility. A global misbehavior detection is able to detect misbehavior that exceeds a local range (e.g. if the same certificate is used in different locations at the same time). While it is straight forward to define the over-the-air message format for reporting misbehavior, introducing actual detection mechanisms is an open research issue. First approaches to detect misbehavior locally were described in [GVG09].

Physical Security and Security Controller: while the standardization of the actual mechanisms does not need to be standardized, it makes sense to define minimum requirements and to standardize a security function API. It might also be useful to introduce a level of trustworthiness for DSRC units (expressed in the units' certificates) that display the implemented level of physical security. The receiver is then able to evaluate trustworthiness of received packets.

Aftermarket and Here-I-Am Units: most security research and design was performed for V2V safety and for on-board units. While many results can be used and the same mechanisms can be applied in most cases, it is essential to understand the differences and to design and implement aftermarket devices accordingly. Here-I-Am (HIA) devices broadcast position and possibly speed but they do not receive messages and they do not provide warnings to their users. HIA units are not necessarily connected to a vehicle system. A typical example are units (e.g. cell phones) carried by cyclists in order to inform and warn vehicle drivers. Aftermarket and HIA devices can be turned off and therefore the requirements in terms of privacy might significantly differ to vehicle on-board units. The actual implementation might be the same as it is for on-board units since many aftermarket and HIA devices are connected to the Internet, thus easing the request of security credentials.

Bootstrapping: the general approach to bootstrapping, i.e. the initial key initialization of a new unit, is clear. However, it is unclear how to implement bootstrapping if there are a variety of car makers and suppliers included. Even more, aftermarket devices will need to fulfill the same or similar requirements. While all unit producers need to implement bootstrapping mechanisms that fit to their production process, the mechanism needs to fulfill minimum security requirements such that no illegitimate units can be introduced. Note that minimum requirements include cryptographic and organizational aspects as well as policy regulations.

Security Policies: security mechanisms need to be supported by policies that define ground rules. In particular, revocation of DSRC units requires security policies. It needs to be defined in which case a DSRC unit will be revoked, and how a DSRC unit will be re-installed after it was revoked (e.g., does the vehicle need to be presented to police or DMV; what will be the action against manipulation; and how will falsely revoked units be identified). Further required security policies include minimum requirements of DSRC units (e.g., in terms of physical security) and limitations of the use of DSRC transmissions for unrelated reasons (e.g., speed information of DSRC broadcasts may not be used by police for any reasons).

REFERENCES

[EU95] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[GVG09] Mainak Ghosh, Anitha Varghese, Arobinda Gupta, Arzad Kherani, Skanda Muthaiah, *Misbehavior Detection Scheme with Integrated Root Cause Detection in VANET*, Proceedings of the Sixth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2009). ACM, Beijing, China, September

2009.

[HHL09] Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET. Proceedings of the Sixth ACM International Workshop on Vehicular Ad Hoc Networks (VANET 2009). ACM, Beijing, China, September 2009, pp. 89-98.

[1609.2] IEEE P1609.2/D5, Draft Standard for Wireless Access in Vehicular Environments – Security Services for for Applications and Management Messages, 2011.

[KW11] Hariharan Krishnan, André Weimerskirch, "Verify-on-Demand – A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication", SAE 2011, World Congress, April 12-14, 2011, Detroit, USA.

[LHH08] Kenneth P. Laberteaux, Jason J. Haas, and Yih-Chun Hu. Security Certificate Revocation List Distribution for VANET.*Proceedings of the Fifth ACM International Workshop on VehiculAr Inter-NETworking* (VANET 2008). ACM, San Francisco, CA, September 2008, pp. 88-89.

[P11] PRESERVE – preparing secure V2X communication systems. http://www.preserve-project.eu/

[TCG] Trusted Computing Group, TPM Main Specification, available at http://www.trustedcomputinggroup.org/resources/tpm_main_specification

[WHHL10] André Weimerskirch, Jason J. Haas, Yih-Chun Hu, and Kenneth P. Laberteaux. Data Security in Vehicular Communication Networks. *VANET Vehicular Applications and Inter-Networking Technologies*. Edited by Hannes Hartenstein and Kenneth P. Laberteaux. John Wiley & Sons, Ltd., March 2010.