Poster: Establishing Dynamic Secure Sessions for Intra-Vehicle Communication Using Implicit Certificates

Fikret Basic
Institute of Technical Informatics
Graz University of Technology
basic@tugraz.at

Christian Steger
Institute of Technical Informatics
Graz University of Technology
steger@tugraz.at

Robert Kofler
R&D BMS
NXP Semiconductors Austria
GmbH Co & KG
robert.kofler@nxp.com

Abstract

With the data traffic being ever-more growing in present intra-vehicular networks, it is becoming increasingly important to secure the vital communication sessions. To enable secure communication for resource-constrained devices, it is necessary to provide a design that is both secure and light in its delivery. This can be achieved with implicit certificate schemes, however, most design proposals are based on the use of the static key derivations with keys tied to the certificates, and hence, are more vulnerable to data exposure attacks. In this work, we present a solution based on the use of the Station-to-Station (STS) protocol with the implicit certificates, offering a dynamic key derivation with perfect forward secrecy. We try to bridge the gap between the conventional schemes and offer a design that can be further extended and used under different constrained architectures.

1 Introduction

Security in modern vehicles is becoming increasingly important due to the increase of the number and complexity of electronic control units (ECUs). This is especially important in electric vehicles where additional elements, such as charging stations, can offer a weak link between the outside world and the internal vehicle system. Here, it is important to consider the performance limits of common ECUs, while not affecting the level of security. Failure in providing an adequate security might leave backdoors open that attackers can exploit, but otherwise, increasing the security complexity might interfere with the overall system's performance, which can impact the safety of the vehicle and its driver.

This work focuses on the use of implicit certificates, specifically the Elliptic Curve Qu-Vanstone (ECQV) schema [1], to offer a flexible security architecture, while still considering the ECUs' constraints. The implicit certificates allow for an *implicit authentication* between parties by public key reconstruction. They have seen a recent surge in interest by the research community in the automotive [5, 4], but also the Internet of Things (IoT) [3], domain, due to their smaller overhead when compared to the traditional certificates.

Limits of existing approaches: While providing a full security suite, the mentioned research studies fail to properly address the key vulnerabilities. They lack the perfect forward secrecy (PFS) property, i.e., that each subsequently derived key is protected from the exposure of a previous key. While the derivation and protection of the asymmetric keys are usually securely handled, the derivation of the symmetric session key often gets neglected. This line of key derivation (KD) falls under the static KD, in which the session key is tied to a certificate session, rather than just the communication session. Any kind of exposure of the security configuration, e.g., private keys, could compromise all the messages from that certificate session, since they all use the same key.

Our contribution: To increase the security of the in-vehicle networks, and limit any potential key exposures to only individual communication sessions, we propose a general design for the dynamic KD of symmetric keys. The design is aimed at the ECQV-based schemes and relies on the Station-to-Station (STS) protocol to provide the PFS [2]. This work can be seen as an extension of the studies presented by Puellen et al. [5] and Pollicino et al. [4]. It provides a dynamic property where each individual communication session is covered by a unique key with a high-enough entropy in relation to the previous keys. While being primarily targeted for the intra-vehicle networks, the proposed KD and session establishment protocol can be used with any similar system that utilizes the ECQV architecture, e.g., also as an extension to the solutions presented for the IoT networks [3].

2 STS with Implicit Certificates

The proposed design is based on a centralized architecture, in which each individual ECU needs to be properly authenticated before they can interact with other ECUs that are also part of the same in-vehicle network. Such authentication process is handled by a central secure gateway (SG) [3, 5]. The SG is also responsible for the communication control with external networks, e.g., cloud, allowing only for the validated services to be connected. After the devices are authenticated, the SG generates and exchanges the certificates and key reconstruction data that are afterwards used for the inter-ECU communication without the SG's involvement.

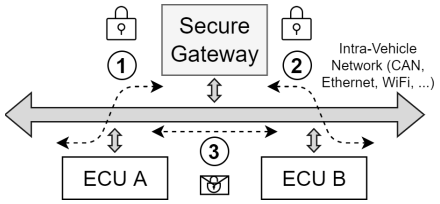

Figure 1. Intra-vehicle implicit certificate exchange.

Figure 1 illustrates the exchange sequence of security configuration messages. Steps ① and ② cover the authentication and registration process for individual modules [5]. This process is independent of the KD and the secure session establishment, which follow afterwards. What is important, however, is that all the devices that participate in the secure session need to have previously been registered with the main SG, i.e., they need to possess certificates. During ③ an ECU (either A or B) sends a request to the other party where they mutually authenticate each other based on the implicit certificate, and simultaneously generate a symmetric key.

Figure 2 shows the sequence steps of our proposed protocol. The calculations are based on the elliptic curve (EC) mathematical properties. Certain equations are mirrored, with $z \in \{A,B\}$. Random numbers are derived with $X_z \in_R [1,...,n-1]$. G is the EC generator point, with n being the used EC order. $Cert_z$ is an assigned certificate.

Random integers guarantee the unique KD input with:

$$XG_z = X_z * G \tag{1}$$

Likewise, the symmetric session keys are calculated with a KD function (KDF), e.g., a hash-family $H(*)$ function, as:

$$K_S = KDF(X_A * XG_B) = KDF(X_B * XG_A) \tag{2}$$

This STS derivation uses an encryption function to validate the party's trustworthiness, denoted with $Enc_{key}(*)$. The verification of the messages starts with the decryption $Dec_{key}(*)$ followed by the verification EC function with the respective public key Q_z. The public keys are calculated as:

$$Q_z = H(Cert_z) * Decode(Cert_z) + Q_{SG} \tag{3}$$

Security evaluation: The protocol is secure against passive attacks. Only the valid parties are able to derive the correct premaster secret. The used symmetric encryption protocol for signed message exchange needs to be of sufficient length (128 or 256 bits). The protocol is also secure against active attacks. Any change in the parameters during the transmission will result in either the wrong premaster secret calculation or an error during the verification processes. As mentioned, STS offers the PFS. To maintain this property, the protocol needs to be initiated in every new session. Even if compromised, an adversary would need to know every individual session-derived random secret (from Figure 2: X_A & X_B) to be able to derive the individual keys. The mathematical properties of the implicit certificates and the EC guarantee the authentication process correctness [1, 3, 5].

Preliminary performance evaluation: A reference model was implemented and evaluated against a static KD model with EC digital signature algorithm (ECDSA) found under common implicit certificate deployments [3, 4]. The

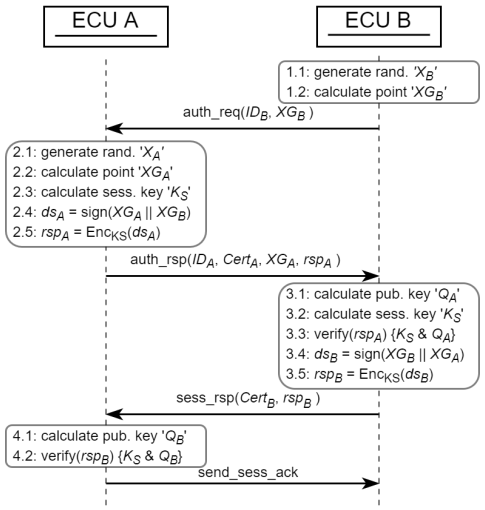

Figure 2. STS protocol based on the implicit certificates.

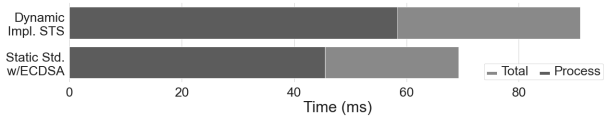

Figure 3. Performance of the process run and transfer time of the STS schema and a static ECQV KD model.

tests were done between two Raspberry Pi 4 that communicate over a serial link. The evaluation models were implemented in Python using the *fastecdsa* library. Figure 3 shows the mean measured time after a hundred test runs, with the proposed STS schema showing only a slight overhead increase over the compared ECDSA static model.

3 Conclusion

In this work, we have presented a design for an in-vehicle secure session establishment protocol for systems that are based on the ECQV architecture. The protocol utilizes the STS properties to allow for a dynamic session establishment. For the next step, we plan to optimize and integrate the proposed protocol design into a test environment focusing on the in-vehicle communication to depict a real-world scenario. The presented protocol will be evaluated against other certificate and KD schemes on performance and security level.

Acknowledgments

This work was done within the funding project "EFRE-top: Securely Applied Machine Learning - Battery Management Systems" ("SEAMAL BMS", FFG Nr. 880564).

4 References

[1] M. C. *SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)*. Certicom Corp., 2013.

[2] W. Diffie, P. C. Van Oorschot, and M. J. Wiener. Authentication and authenticated key exchanges. *Design, Codes and Cryptography*, 1992.

[3] D. A. Ha et al. Efficient Authentication of Resource-Constrained IoT Devices Based on ECQV Implicit Certificates and Datagram Transport Layer Security Protocol. In *Proc. of the 7th SoICT Conf.* ACM, 2016.

[4] F. Pollicino et al. An experimental analysis of ECQV implicit certificates performance in VANETs. In *IEEE 92nd VTC2020-Fall*, 2020.

[5] D. Puellen et al. Using Implicit Certification to Efficiently Establish Authenticated Group Keys for In-Vehicle Networks. In *Proc. of the 11th IEEE VNC Conf.*, 2019.