An evaluation framework for pre-distribution strategies of certificates in VANETs

Michael Feiri
Services, Cybersecurity and Safety
University of Twente
The Netherlands
Email: m.feiri@utwente.nl

Jonathan Petit
Services, Cybersecurity and Safety
University of Twente
The Netherlands
Email: j.petit@utwente.nl

Frank Kargl
Institute of Distributed Systems
University of Ulm
Ulm, Germany
Email: frank.kargl@uni-ulm.de

***Abstract*—Security and privacy in vehicular communication are expected to be ensured by the pervasive use of pseudonymous certificates and signed messages. The design and establishment of necessary public key infrastructure and hierarchies of certificate authorities is ongoing in industry consortia, such as the Car-to-Car Communication Consortium. The privacy preserving dissemination of pseudonymous certificates is however still expected to be limited to single-hop exchanges between vehicles. This limitation to one-hop strategies might not be ideal, especially considering the importance of ensuring trustworthy stateless information exchange upon reception of the very first communication packets. We propose to investigate multi-hop pre-distribution strategies for certificates to significantly reduce this first encounter problem.**

I. Introduction and related work

A core requirement for effective vehicular communication is secure information exchange between vehicles. As the volatility of vehicular networks makes stable secure channels impractical, the commonly accepted solution for inter vehicle communication (V2V) is to use authenticated messages, based on a common vehicular public key infrastructure (PKI) and accredited certificate authorities (CA). Relevant standardization efforts at ETSI [1] and IEEE [2] have proposed appropriate protocols to implement such architectures. In order to additionally assure privacy for the passengers of vehicles in such architectures it is foreseen to issue multiple pseudonymous identities to vehicles, which can be switched according to given rulesets. The goal of providing multiple pseudonymous identities to vehicles is to provide location privacy to passengers.

The dissemination of certificates to vehicles is indirectly specified in ETSI and IEEE by means of direct inclusion of certificates in signed messages or through the possibility to explicit requests the inclusion of certificates. There are no universal rules that define the inclusion or omission of certificates, but the fact that certificates represent a significant amount of data makes it attractive to minimize the amount of certificate inclusions while maximizing the service quality. Service quality in this context is the ability to verify incoming messages of previously unknown vehicles as fast as possible. Waiting periods for exchanges of certificates after the first encounter of a vehicle in communication range need to be minimized. Existing research and suggestions in relevant standardization effort limit themselves to one-hope dissemination.

PKI systems, such as S/MIME [3], rely on similarly bootstrapping secure communication through an initial exchange of certificates between communication partners over not-yet-secured channels or messages. In case a communication partner is not available for the initial exchange of certificates it is possible to use a third party cache of certificates. This is possible because the trust in certificates does not depend on secure delivery but instead is solely hinged on (a chain or set of) trust anchors that certify the authenticity of the enclosed public keys. The concept of public cache server is popular for the related PGP/MIME [4] system, where keyservers are commonly relied on to deliver public key material along with cross certifications added by third party entities for the formation of a web-of-trust.

Communication system operating on public internet infrastructure can be expected have relatively stable connections and to tolerate varying amounts of latency to complete such an initial exchange of certificates to bootstrap secure communication. No matter if it is done end-to-end between endpoints or using caches located in keyservers. Vehicular communication on the other hand operates under more constrained conditions and under stricter requirements. Hidden station effect can prevent two way communication, the reachability of caches in RSUs or backend infrastructure (V2I) can not be assumed at all times, and the availability of certificate material must be guaranteed within reasonable latencies with respect to the beacon frequency and the relative trajectories of the moving vehicles.

Within the specific constraints of vehicular communication patterns, it is still possible to envision protocols that use caches for more effective dissemination of certificates. Also, another way to investigate dissemination of certificates beyond 1-hop neighborhood is to adapt protocols that propose to disseminate neighbor information through 2-hop piggybacking [5]. Such protocols have been specifically proposed for purposes of distributed congestion control (DCC) in vehicular communication networks. Both approaches will be investigated using analytical models to predict the suitability of these approaches to enhance the efficiency and effectiveness of certificate distribution in VANETs.

II. Requirements

Pseudonymous certificates are the foundation for both security and privacy in vehicular communication networks. Vehicles are expected to locally cache at least a small set of certificates to have the capability to immediately verify

the messages of all nearby vehicles even if the (chain of) relevant certificates are not included in every message. This can occur when a signed message only includes the digest of a certificate instead of the full (chain of) certificates in order to save bandwidth.

For the purpose of our analysis we assume that the size of a single certificate including compressed NIST P-256 ECDSA keys is 140 bytes [6]. One GiB of storage space could store approximately 7.669.584 certificates. Considering that in Europe alone an estimated number of more than 250 million vehicles are in use it becomes immediately obvious that pre-distributing all certificates is not a realistic option. A global estimate of motor vehicle registrations indicated about 1 billion vehicles in 2010. Assuming each vehicle would be equipped with a set of 100.000 pseudonyms to cover every possible 5 minute period over the course of a full year yields and upper estimate of 100 trillion pseudonymous identities. Storing this amount of pseudonyms would require about 12 EiB of storage. We assume as a requirement for our analysis that a vehicles on-board unit (OBU) are limited to a maximum of 1GiB of storage space for caches of certificate material.

Another requirement exists relative to a baseline of bandwidth consumption for the simple inclusion of certificates in every message sent by vehicles. For the purpose of our study we only investigate periodic beacon messages. Combined with a synthetic channel model and estimates of average vehicles densities this allows us to calculate probabilities for channel load and packet loss under various protocols. To derive meaningful metrics of application level service quality, we calculate the expected awareness quality (AQ) [7] for the awareness of nearby vehicles in a safety relevant area of 300 m around vehicles. A penalty for increased latency between the first encounter of a new vehicle and the first successfully verifiable secured message is implicitly included in the AQ metric. Any pre-distribution scheme should improve the AQ compared to the baseline case of including full certificates in all periodic messages. Ideally, a new pre-distribution scheme would also provide improved AQ over certificate omission schemes such as Neighbor-based Certificate Omission [8] and Congestion-based Certificate Omission [6].

A third requirement for a new pre-distribution scheme is to not influence the privacy of passengers by not compromising the unlinkability of pseudonyms used by a vehicle. This is a relevant aspect due to the basic fact that pre-distribution will leak the expected future location of vehicles and their pseudonym. Even under hierarchic, geographic, or temporal scoping rules, it should be hard for an attacker to link pseudonyms as belonging to a single vehicle. We assume an attacker model that matches common expectations of not being too powerful in terms of network coverage and not being mobile enough to outright follow a tracked vehicle.

III. Solutions and future work

The solution space for certificate pre-distribution can be partitioned into three broad techniques, all of which will be augmented with directional scoping:

- n-hop dissemination.
- store-and-forward dissemination.
- probabilistic dissemination.

These techniques emphasize different forwarding methods, but are essentially all based on pushing information where it is expected to be needed. The opposite approach of pulling information that might be needed along a given trajectory would require the ability to accurately predict the positions of vehicles that are far outside communication range and to broadcast pull requests beyond the intended trajectory. Both aspects are deemed prohibitive for efficient use of the available communication channels.

To ensure the unlinkability of pseudonyms it seems intuitively plausible to not pre-distribute multiple pseudonymous certificates that belong to the same vehicle, as this creates a link between the two identities. On the other hand, the model of an attacker against location privacy assumes that a local mobile follower can watch pseudonym changes anyway. It is even possible to argue that the pre-distribution of valid pseudonym certificates without claiming the actual presence of users of these certificates enlarges the size of the k-anonymity group without having a negative effect on the service quality through an introduction of phantom vehicles.

An attractive opportunity to implement pre-distribution of certificates in VANETs presents itself in the context of proposed DCC systems [5]. Such systems optimize channel utilization by aiming to maintain a constant channel busy ratio (CBR). A CBR value below the ideal target value can be interpreted as an indication of unused bandwidth. An optional service quality enhancement scheme such as pre-distribution of certificates could be a useful consumer of such unused bandwidth.

As future work we will develop an analytical model that allows us to model the AQ of different push dissemination strategies for certificate pre-distribution, and compare the effectiveness and efficiency against existing inclusion and omission schemes. Additionally, we will investigate the impact of certificate pre-distribution on location privacy and possible interactions with DCC systems.

References

[1] ETSI TC ITS, "ETSI TS 102 731 v1.1.1 - intelligent transport systems (ITS); security; security services and architecture," Standard, TC ITS, 2010.

[2] IEEE, "IEEE 1609.2v2 - Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages," 2011.

[3] B. Ramsdell, "Secure/multipurpose internet mail extensions (s/mime) version 3.1 message specification," 2004.

[4] M. Elkins, "Mime security with pretty good privacy (pgp)," 1996.

[5] T. Tielert, D. Jiang, Q. Chen, L. Delgrossi, and H. Hartenstein, "Design methodology and evaluation of rate adaptation based congestion control for vehicle safety communications," in *VNC*, 2011, pp. 116–123.

[6] M. P. Feiri, J. Y. Petit, and F. Kargl, "Evaluation of congestion-based certificate omission in vanets," in *Proceedings of the IEEE Vehicular Networking Conference (VNC 2012), Seoul, Korea*. USA: IEEE, November.

[7] R. K. Schmidt and T. Leinmüller, "A spatio-temporal metric for the evaluation of cooperative awareness," in *18th World Congress on Intelligent Transport Systems*, 2011.

[8] E. Schoch and F. Kargl, "On the efficiency of secure beaconing in vanets," in *Proceedings of the third ACM conference on Wireless network security*, ser. WiSec '10. New York, NY, USA: ACM, 2010, pp. 111–116.