Design principles for WG5 C-ITS short term certificate policy.

Introduction

Members of WG5 are uncertain about the future certificate policy in V2X communications and applications when it comes to balancing the interests of secure authentication versus the interests of privacy.

From a security perspective identifiers in V2X messages have been introduced in order to enable receiving stations to verify the reliability of the sender. From a functional point view point receiving stations need the identifiers to reliably link a sequence of received messages to one individual sender vehicle.

The drawback of enabling receiving stations to link messages to individual sender vehicles is the potential impact on the privacy of the sender vehicle driver. To reduce this privacy impact the ETSI specification requires two types of certificates, i.e. long term and short term certificates. Short term certificates contain pseudonym identities and they will alternate while driving.

The question is now raised in WG5 for the parametrization of the short term certificates. More precisely: when should short term pseudonym identities change?

This paper takes a use case approach as the guiding principle to answer this policy question.

What do Day One use cases need?

We will focus on use cases from two bundles of the Day One use cases. Within the V2I bundle we will focus on traffic lights interactions and within the V2V bundle we will focus on traffic safety messages.

1. Traffic light interactions

Typical traffic light interactions in Day One use cases are:

- GLOSA (Green Light Optimal Speed Advisory)
- Traffic light priority request (by designated vehicles)

Traffic light interaction is a local process. When a vehicle would receive optimal speed advices or requests for traffic light priority (or just needs to be detected) this typically would take place in a range of 500 meters from the traffic light or less. When it comes to the frequency of messaging this would be less demanding than what the ETSI G5 standard can deliver (i.e. 1 - 10 messages per second). Maybe one CAM message per second or even less would be enough for these use cases. This may be dependent of the complexity of the traffic and crossroad situation. This is the functionality viewpoint.

From a privacy point of view the question would be: is there a functional need that the traffic light installation can track the individual approaching vehicles? This would be a question for traffic engineers. One can expect that in the case of a traffic light priority request from a designated vehicle the tracking (“identification”) of the vehicle is a more likely requirement than for GLOSA.

Let’s assume that from a functionality point of view there would be freedom to change pseudonym identities right after every major crossing and there would be substantial traffic of equipped vehicles. If pseudonyms would change after every major crossing – and if time intervals would be long enough and if pseudonyms would not be reused - the trips of the vehicles could not be reconstructed by aggregation of all received CAM messages from individual vehicles.

2. V2V Traffic safety use messages

Typical traffic safety use cases that would benefit from V2V messages are:

- emergency braking light
- slow or stationary vehicle
- emergency vehicle approaching

The emergency braking light use case would justify frequent CAM messages broadcasting during the full braking operation (couple of seconds at most). Pseudonym identities would not change during this operation for obvious safety reasons.

The case of a slow or stationary vehicle would be the same for traffic safety reasons. However the duration time of a slow or stationary vehicle may be minutes or even hours. In these exceptional cases there would be no need for a pseudonym change until the exceptional situation is over.

Emergency vehicles are a special category of vehicles with privileges that gives them special authorizations in sending CAM messages. From a privacy point of view this category would be compelling only in case of VIPs being transported. Two modes of operations can be distinguished. In emergency status – when the priority lights are active – a different set of pseudonym identities could be used than during normal driving conditions. Upon changing the mode of operation and thus changing the set of short term certificates being used the CAM broadcasts could best be suppressed for a couple of seconds at least in order to prevent pseudonym identities from different sets to be linked as belonging to the same vehicle.

3. Use cases aggregation

Each vehicle (i.e. its ITS station) itself would determine the intervals of the broadcasted CAM messages depending on the traffic context. Changes of pseudonym identities typically would take place between distinct traffic contexts where functionality and traffic safety are not critical for the vehicle itself. This is the concept that the vehicle needs to be aware of its own driving and traffic context and is acting accordingly to be in control.

C-ITS would be considered to become a part of total vehicle functionality. A vehicle would selectively broadcast CAM messages as it wants or needs something in return from its traffic environment (either visibility or a service). This change of perspective for C-ITS deployment may contribute to design acceptable security and privacy parameters.

Why are security and privacy in conflict with each other?

As stated in the introduction the risk of tracking an individual vehicle is a result of the introduction of message sender identifiers. Without any information that can be linked to message senders the total C-ITS system would become unreliable and unusable. The introduction and use of multiple pseudonym identities is a privacy enhancing technique and creates an extra threshold to link all movements from an individual vehicle to this very vehicle. At the same time it introduces a new security risk, the so-called Sybil attack. In fact this risk would weak the required reliability of the C-ITS system. This is described below.

A specific security argument for the reduction of the number of concurrently valid short term certificates

A pretty well known risk in C-ITS G5 networks (or more generally VANETs, Vehicle Ad hoc NETworks) are the so called Sybil attacks. The threat is that an individual vehicle can claim and may use up to ten or twenty different identities every one or two seconds. A typical exploit of this risk would be a rogue vehicle broadcasting multiple identities such as to gain traffic priorities which would be achievable only by its environment being deceived and assuming this one single vehicle representing a much higher number of vehicles at the same time at the same spot. This risk can be compared to the impact one can have in social media by increasing and using his or her number of identities (accounts).

Sybil attacks are very hard to detect in C-ITS as the traffic is moving and location and time messages inherently contain physical noise and inaccuracies. Therefore algorithms are practically not able to detect such a rogue vehicle faking multiple identities at the same time.

From a security perspective the optimal number of concurrently valid short term certificates for an individual vehicle would be just one. This would be a one to one relationship. In C-ITS a one to one relationship for vehicle and identifier is limited to long term certificates. In general one could say the higher the number of valid certificates: the higher the impact of potential abuse will be.

An alternative control to reduce the risk of the exploit of Sybil attacks would include activation or active revocation of short term certificates. So far revocation of short term certificates has not been in scope of the ETSI standard.

Eric Verheul recently suggested the IFAL approach for C-ITS pseudonym certificates. In the IFAL approach (acronym for Issue First Activate Later) each pseudonym certificate would be only valid for a very short period, e.g. 10 minutes. Pseudonym certificates can be issued by the vehicle manufacturer in one batch (requiring around ≈ 40MB of storage) for a long period, e.g. 10 years, but in inactive mode. That is, the vehicle does not yet completely possess the required private keys in the pseudonym certificates. The remaining parts of these private keys are periodically, e.g. quarterly, provided to the vehicle by the Pseudonym Certificate Authority (PCA). With the use of more or less standard cryptographic techniques, this can be done quite conveniently. To this end, the pseudonym Certificate Authority only needs to periodically send 16 bytes of data to the vehicle. This can for instance be done by SMS. As this data is not confidential it can even be broadcasted through roadside equipment or even be broadcasted over the Radio Data System (RDS). Further use of more or less standard cryptographic techniques would only require a simple Trusted Element in the Onboard Unit of the vehicle only having two keys (a signing key and a symmetric key). The underlying idea here is that the actual signing operation related to the pseudonym certificates is a joint effort done by the Trusted Element and the Onboard Unit where the latter part is not security critical. Central in IFAL are three parameters that are policy relevant: total lifetime (e.g. 10 years), lifetime of certificates (e.g. 10 minutes) and refreshment period (e.g. quarterly). With these parameters one can define different policies whereby one can establish various balances between reliability, privacy and efficiency. This balance is thus both configurable and transparent which can be an important advantage in the future EU Data Protection Authorities assessment of the ITS standard.

As an illustration, using the terms High, Medium and Low in a very loose fashion:

- choosing a total lifetime of **10 years**, a certificate lifetime of **one minute** and a refreshment period of **one day** one would get setup that has high reliability and privacy but that is less efficient as the PCA has to send refreshment updates on a daily basis.
- choosing a total lifetime of **10 years**, a certificate lifetime of **one minute** and a refreshment period of **three months** one would get setup that has high privacy but medium reliability and that is reasonably efficient as the PCA has to send refreshment updates only on a quarterly basis
- choosing a total lifetime of **10 years**, a certificate lifetime of **ten minutes** and a refreshment period of **three months** one would get setup that has medium reliability and privacy and that reasonably efficient as one has to send refreshment updates only on a quarterly basis
- choosing a total lifetime of **10 years**, a certificate lifetime of **ten minutes** and a refreshment period of **ten years** one would get setup that has medium privacy but low reliability due to the effective lack of refreshment but that is very efficient as one does need to send refreshment updates at all.

An interesting property of this setup is that it allows to have several pseudonym certificate policies next to each other where it is left to vehicle owner and the relying party to accept a policy or not. That is, there is no need to only accept one pseudonym certificate policy. Although one could regulate minimal requirements on policies from both privacy (e.g. certificate lifetime at most 30 minutes), reliability (refreshment period at least quarterly) but also on safety (certificate lifetime at least 5 minutes). With respect to the latter; very short pseudonym certificate lifetimes, of say one minute, increase the risk of Sybil attacks and thus public safety. In this way one can motivate certain choices on certificate lifetime based on proportionality, an important principle in European privacy law.

Irrespective of the policy chosen, at any moment in time only *one* pseudonym certificate would be valid (active) in the IFAL setup. Pseudonym certificates cannot be reused implying that the IFAL approach would mitigate the risk of Sybil attacks even if a practical implementation would allow 2 concurrent pseudonym certificates for reasons of traffic safety context (change of pseudonym certificate would be too risky in a specific second or specific minute).

Solution direction

In many industries both security practices and privacy practices take risk based approaches. In information security and cyber security practices risk based approaches have a long tradition. In Information privacy (data protection) the risk based approach is now taking off in the EU and will become more common after the recent adoption of the GDPR.

Instead of balancing the conflicting security interest versus the privacy interest we would advocate for balancing each of the interests versus the business risk. The business approach is common and best practice in the fields of security management and privacy management. A first impression of this approach was given in the examples of the use cases.

So far all stakeholders involved in C-ITS have tried to achieve security and privacy objectives for the total C-ITS ecosystem. This approach may initially have looked very promising but some major resulting obstacles have turned out very hard to overcome which was confirmed in the breakthrough working groups in the C-ITS Platform last year (WG4 and WG5).

In the outline below both security and privacy will be balanced against business risk. Common and required design principles such as proportionality and necessity can only be applied when balanced against specific business cases. This is the recommended approach to convince the Data Protection Authorities as well.

Security and Privacy by Design steps

As stated before C-ITS should rather be positioned as part of the total tomorrow's vehicle functionality. C-ITS (an ITS-G5 Wifi-P based VANET) will not be the only connectivity option nor will it be the only in car sensor technology being deployed. The developments of autonomous functions in vehicles as well as 4G/5G cellular networks can be taken into account and will make this approach for C-ITS future proof. The following is a list of viewpoints for design steps that would be opportune now.

1. What *sensor technology* will be available and affordable and can complement C-ITS for specific vehicle functions? Sensor technology can reduce the frequency of C-ITS messages as well as contribute to the reliability of the individual vehicle and the reliability of the VANET around the vehicle's location. The privacy impact needs to be assessed specifically for the designed case including the use of all aggregated vehicle data. For the sake of liability it also seems reasonable that a vehicle gives priority to its own sensors if there is conflicting information with external sensors based on C-ITS.

2. What *alternative connectivity option* will be available and affordable and can complement to the C-ITS G5 wifi-p networks? The use of 3G, 4G (and 5G networks when available) can contribute to a *hybrid V2X connectivity* approach and will make V2V and V2I connectivity more robust. Both connectivity options would need to be

aggregated when it comes to assessing the risks for personal data loss (privacy) and for traffic safety and traffic flow (security). From a control perspective both network technologies can complement each other when it comes to mitigating risks of network unavailability or saturation.

3. What *alternative privacy enhancing technology* can be considered, e.g. attribute based credentialing (ABC)? The just completed independent assessment of Eric Verheul confirms that today's best of breed ABC vendor technologies and the ABC4Trust framework are not ready yet for the large scale ITS deployment. They may have a future role in ITS when they are ready to meet ITS requirements for computing power performance and communication bandwidth.

4. What *cryptographic optimizations* are possible in today's ETSI C-ITS standards that would improve the ITS privacy and security posture? The IFAL approach for pseudonym certificates described by Eric Verheul is such an optimization that may fit within the ETSI requirements and ETSI standard and is based on conventional and accepted cryptography. The certificate policy parameters will be pseudonym certificate life time (e.g. 10 minutes), activation intervals (e.g. 3 months) and issuance interval (e.g. 10 years). There would be room in the certificate policy to differentiate the pseudonym certificate parameters according to vehicle categories (e.g. emergency vehicles, private cars, etcetera). As hinted above, further cryptographic optimizations can also simplify the required vehicle Trusted Element in C-ITS and thereby its (cost) efficiency.

Conclusion and follow up

Two new perspectives have been presented here for the pseudonym certificate policy. Both perspectives are compatible with each other.

1. Optimize the current ETSI standard with the IFAL pseudonym certificate principle as described by Eric Verheul. Pseudonym certificates will be used only once and are valid for only 10 minutes. This will significantly reduce the privacy impact as well improve the reliability of the V2X network against Sybil attacks. The optimization also includes the introduction and simplification of the vehicle Trusted Element which will improve the (cost) efficiency of V2X networks.

2. Create a functional ITS model that would specify and justify the need for CAM messages. They would be based on specific and prioritized use cases in traffic safety or traffic optimization. That would give a solid basis to configure vehicle parameters for CAM messages broadcast frequency and message intervals as well as to specify the acceptable pseudonym certificate change.

By thus taking the principles of Privacy by Design and Security by Design to the next level the C-ITS platform may prepare to reach out to the European Data Protection Authorities (Article 29 Working Party) for a formal opinion on the C-ITS standard.

Short term actions in this solution direction that can be undertaken would be:

1. Make a design for a simple in car Trusted Element that can connect to both the LTCA and PCA and that can manage the full set of pseudonym certificates for 10 years ahead.
2. Plan one or more field trials in a Proof of Concept for testing IFAL and smart functional pseudonym certificate change management in real traffic conditions.

References

- Article 29 WP opinion on anonymisation (and pseudonymisation) - 2014 :

  http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

- GDPR –legal text expected to be officially published on 25th May 2016 :

  https://www.dlapiper.com/en/us/insights/publications/2016/04/final-text-of-the-gdpr-finally-available/

- Article on strength of privacy protection in V2X with pseudonym certificates - 2010:

  https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui.inst.100/institut/mitarbeiter/wiedersheim/wons2010-tracking.pdf

- Car2Car and PRESERVE security architecture with concept of the pseudonym management module - 2014 :

  https://www.preserve-project.eu/sites/preserve-project.eu/files/PRESERVE-D1.3-V2X_Security_Architecture_V2.pdf

- Detecting Sybil attacks in vehicular networks – Journal of Trust Management 2014

  http://journaloftrustmanagement.springeropen.com/articles/10.1186/2196-064X-1-4

- Eric Verheul's presentation on IFAL and ABC4Trust for ITS for Dutch ITS security round table on 10 May 2016

  http://www.ditcm.eu/images/ITS_Ronde_tafel_/Security/meeting_100516/presentaties/ABC4Trust%20in%20ITS%201.1%20PUB.pdf

Gilles Ampt – 17 May 2016