

# Analysis of Vehicle-Based Security Operations

---

**Jason M. Carter, Ph.D.**  
**Nathanael Paul, Ph.D.**  
Oak Ridge National Laboratory  
United States

**Jenny Zhang**  
National Highway Traffic Safety Administration  
United States

**Paper 15-0457**

## **Abstract**

Vehicle-to-vehicle (V2V) communications promises to increase roadway safety by providing each vehicle with 360 degree situational awareness of other vehicles in proximity, and by complementing onboard sensors such as radar or camera in detecting imminent crash scenarios. In the United States, approximately three hundred million automobiles could participate in a fully deployed V2V system if Dedicated Short-Range Communication (DSRC) device use becomes mandatory. The system's reliance on continuous communication, however, provides a potential means for unscrupulous persons to transmit false data in an attempt to cause crashes, create traffic congestion, or simply render the system useless. V2V communications must be highly scalable while retaining robust security and privacy preserving features to meet the intra-vehicle and vehicle-to-infrastructure communication requirements for a growing vehicle population.

Oakridge National Research Laboratory is investigating a Vehicle-Based Security System (VBSS) to provide security and privacy for a fully deployed V2V and V2I system. In the VBSS an On-board Unit (OBU) generates short-term certificates and signs Basic Safety Messages (BSM) to preserve privacy and enhance security. This work outlines a potential VBSS structure and its operational concepts; it examines how a vehicle-based system might feasibly provide security and privacy, highlights remaining challenges, and explores potential mitigations to address those challenges.

Certificate management alternatives that attempt to meet V2V security and privacy requirements have been examined previously by the research community including privacy-preserving group certificates, shared certificates, and functional encryption. Due to real-world operational constraints, adopting one of these approaches for VBSS V2V communication is difficult. Timely misbehavior detection and revocation are still open problems for any V2V system. We explore the alternative approaches that may be applicable to a VBSS, and suggest some additional research directions in order to find a practical solution that appropriately addresses security and privacy.

## **Section 1: Introduction**

Dedicated Short-Range Communication (DSRC) can support V2V and V2I communications; however, bandwidth and range limitations challenge integration of safety and privacy features. In order to ensure interoperability between different OEMs, vehicle safety messages (i.e., Basic Safety Messages or BSMs) must be trusted while protecting the identity of the driver or vehicle.

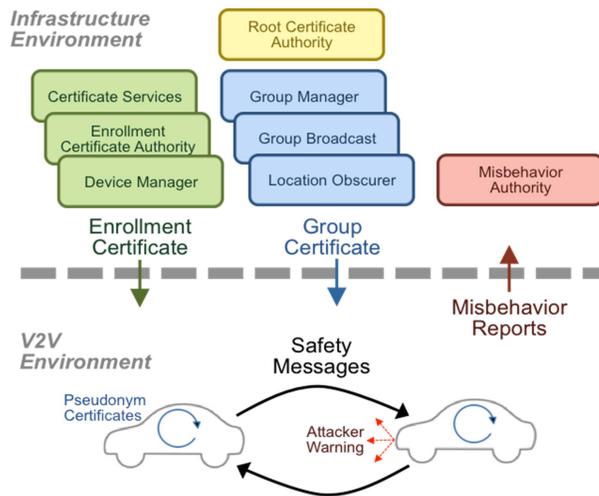
In a traditional public key infrastructure (PKI), participants create, receive, manage, and revoke certificates. A certificate encapsulates a participant's public key and identifies that participant within the system. Each participant signs data using their private key. When a message recipient receives a signed message, the recipient verifies the message signature using the sender's public key to ensure the message has not been altered. Assuming that the sender's private signing key has not been compromised or exposed, the recipient will trust that the sender signed and sent the received message.

The proposed Public Key Infrastructure (PKI) for the Intelligent Transportation System (ITS) Vehicle-to-Vehicle (V2V) safety initiative will be the largest PKI ever deployed. The PKI needs to address the basic security properties (authentication, integrity, and non-repudiation) of a traditional PKI while protecting individual privacy. In the rest of this document, assume that unless otherwise stated, a PKI refers to a PKI for use in a transportation infrastructure and will be used for V2V and V2I. As in most PKIs, revocation is

needed. Revocation typically requires participant identification. For this PKI, the revocation authority would be identifying certificates associated with a particular vehicle or device.

Participant population estimates in a PKI provide a foundation for network traffic, storage, and infrastructure analyses. Using a linear model of U.S. vehicle registration numbers from 2000 to 2012 [FHWA11], the number of registered vehicles in 2016 will be approximately 257 million; this includes public and private automobiles, buses, and trucks. The population of private and public vehicles will be dynamic; vehicles will be added and removed from the system for several reasons. U.S. vehicle population increases on average 1.97 million vehicles per year. This implies that more than 15 million new vehicles are purchased on average each year in the U.S. [NADA14]. When the V2V system is fully deployed, the VPKI system is expected to accommodate more vehicles as the overall U.S. vehicle population is projected to grow. Furthermore, the VPKI needs to manage certificates from the end-of-life, misbehaving, and/or malfunctioning vehicles in order to ensure the integrity of the V2V system and protect the remaining participants from mishaps. The 2011 Automotive Recycling Association Report estimated 12.61 million vehicles are recycled per year; this value is very close to our end-of-life vehicle projections (i.e., 12.96 million per year). The certificates in end-of-life vehicles may potentially be compromised and used maliciously. Vehicles that intentionally use compromised certificates maliciously, or unintentionally malfunction, are classified as misbehaving vehicles; this class of vehicles may cause mishaps intentionally or unintentionally based on their broadcast safety messages.

The deployment of a PKI system relies on a supporting infrastructure. The components and authorities within this infrastructure manage and distribute certificates so participants can communicate in a trustworthy way. However, addressing privacy concerns requires a different certificate management and distribution approach from a traditional PKI that uses inherently identifying credentials. A recently proposed Security Credential Management System (SCMS) for North America adds infrastructure components to provide privacy protection. [Whyte13] attempts to address privacy by building an infrastructure whose architectural design mitigates the possibility of an internal privacy breach, and this work is the basis for the current VPKI, the Security Credential Management System (SCMS) being explored for North America. Several promising alternative strategies have been developed that may allow



**Figure 1: Vehicle-Based Security System**

for a reduced level of infrastructure and associated communications with the vehicle. These include privacy-protecting group credentials, shared certificates, and functional encryption [Delgrossi12].

To reduce the supporting infrastructure size and to increase a vehicle's independence from the infrastructure, ORNL has been investigating the potential for a Vehicle-Based Security System (VBSS) to provide security and privacy at the scale of a fully deployed V2V system. Figure 1 is an overview of the operations and components in our VBSS concept.

Communication between the infrastructure components does happen but is not illustrated. Instead of a trusted authority issuing ephemeral certificates, the proposed VBSS uses group credentials, and they facilitate short-lived pseudonym certificate generation on the vehicle. Vehicles form groups, and a vehicle will sign a message using its group signing key while maintaining anonymity. Unlike a traditional PKI message, in order to verify a message, a recipient does not need to know who exactly signed a message.

Group credentials also integrate mechanisms to add and remove participants in an efficient way; this feature can be used for vehicle revocation.

This paper outlines the VBSS structure and its operational concepts; it examines how a vehicle-based system might feasibly provide security and privacy, highlights remaining challenges, and explores potential mitigations to address those challenges. We suggest some additional research directions that will further validate a vehicle-based approach to V2V credential management.

## Section 2: Towards a Feasible VBSS

A PKI that addresses privacy must also scale to meet the needs of the U.S. vehicle population. In a PKI, identifying a signer is counter to the goal of maintaining a driver’s (signer’s) privacy. We assume that a driver wants to ensure the safety messages they transmits cannot be used to expose private details about that individual’s movements. If a vehicle used a single private key to sign every safety message, then the associated, publicly available, certificate could be used to identify that driver’s safety messages. Such a PKI must manage over 250 million identifying credentials. Scaling to manage this many credentials is a significant challenge. Short-lived pseudonym certificates have been adopted as a way to obfuscate an individual’s identity; numerous pseudonyms are used by each driver, multiplying the credential management challenge.

There are many potential cryptographic approaches to achieving a PKI that addresses privacy and scalability. These include functional encryption, shared certificates, and group signatures [Delgrosso12]. Although functional encryption in Vehicle Ad-hoc NETWORKS (VANETs) has recently received attention [Huang09], the maturity of the technology lags behind the other two approaches.

With shared certificates, a collection of vehicles (sharing group) share a single unique private key to sign safety messages. The verifying certificate of all vehicles within the sharing group provides equal anonymity; however, revoking a single bad participant will have the collateral effect of revoking all the members in the sharing group. To mitigate this collateral damage, each vehicle is given multiple keys. A new shared private signing key can be selected from the “backup” keys when the signing key being used is revoked. With this scheme, all of a vehicle’s signing keys could be revoked without any evidence of the vehicle’s misbehavior (i.e., a vehicle that unintentionally has behavior that does not conform to an expected adjudicated behavior). While no one has data on the expected or actual misbehaving vehicle rate, we anticipate that the number of misbehaving vehicles will be large requiring extensive mitigation of the collateral damage effect.

Group signatures have been prototyped in VANETs, although they can be computationally demanding. However, other work shows that the computational burden of group signatures does not preclude its use in vehicular networks: Instead of using group credentials to sign each and every message, they could be used to anchor ECDSA certificate trust [Calandriello11]. The group signatures are combined with Elliptical Curve Digital Signature Algorithm (ECDSA) signatures to decrease computational and network consumption. With this strategy, the vehicle acts as a subordinate certificate authority and generates its own ephemeral ECDSA certificates: each vehicle signs a generated ECDSA public key with its group signing key.

The combined use of ECDSA and group signatures is shown in Figure 2. In Figure 2, Alice creates a BSM and signs that BSM with a private pseudonym ECDSA signing key,  $k_A$ . This yields the signature  $\text{Sig}_{k_A}$  (BSM). In this example, Alice also signs the pseudonym certificate with her group signing key and attaches the corresponding signature,  $\langle A \rangle_G$ . Then, Alice sends the message and signatures to Bob. If Bob has received a message from Alice in the past, then Bob will trust the message once he verifies the BSM’s signature. If Bob has not previously received a message from Alice, Bob will first verify the group

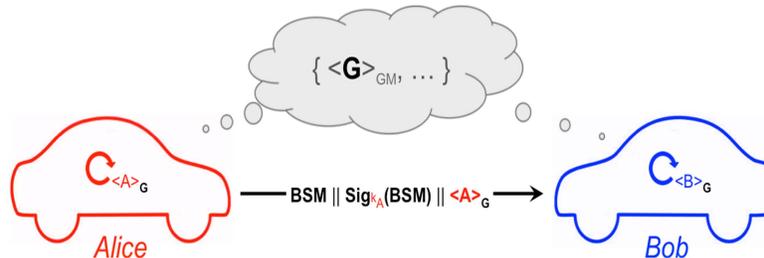


Figure 2: Two Vehicles Communicating Using Group Signed Pseudonyms

signature of the pseudonym,  $\langle A \rangle_G$ , by using the group public key. Then, Bob can check the BSM signature using  $\langle A \rangle$ . The circular arrow in Figure 2 signifies the vehicle's ability to generate pseudonyms. Pseudonyms can be created on-demand or in small, custom-sized batches. When a sender transitions to a new pseudonym certificate, the BSM recipient must obtain and verify that certificate prior to authenticating messages.

### Section 3: A Group-Based VBSS

In a group signature scheme, a group manager has a role similar to a root certificate authority [Chaum91, Ateniese00, Bellare05]. Any party in the PKI may receive a message signed by a particular group member. If the message recipient is in the same group as the message sender, then their common group public key can be used to authenticate the message. If the message recipient is in a different group from the message signer, he or she must first obtain the sender's group public key and then verify the message (We anticipate that it will be feasible to store all group public keys on a vehicle, and every vehicle starts with all group public keys). Group signatures are anonymous: the group public key, or certificate, only identifies the group and not an individual. When verifying a message, the recipient verifies that the message signer was a valid group member when they signed the message, but no additional identifying information about the message signer is learned.

To form a group, a group manager must be designated and several public parameters chosen. When a potential participant requests assignment to a group, the participant's private pseudonym signing key must either be self-generated or generated by the group manager. In earlier work [Ateniese00], a group member takes part in an interactive group join protocol and receives a membership certificate tuple: a signature in the form of a pair,  $(A_i, e_i)$ ;  $A_i$  is computed as part of a zero-knowledge proof (ZKP) that shows that the prospective member knows a secret value, and random prime integer,  $e_i$ , usable for member revocation. The group manager creates groups, manages revocations, and identifies group members when needed by revealing a particular signatory. Using the group membership certificate, a participant sends and signs messages. Message verification proves the message signer is part of the group; no other details are provided by the sender.

The number and size of groups is a design choice. Some of the factors that might be used in determining how the U.S. vehicle population is partitioned include: geographic boundaries, vehicle manufacturer, and vehicle make. In other PKI systems, designers have created revocation mechanisms that can address vehicle recalls. Similarly, large subsets of a vehicle population can be revoked directly by removing an entire group when the group partitioning strategy is designed properly.

Table 1 details an example nation-wide group design in the U.S. In this design, there are fifteen thousand groups (and 15,000 corresponding group public keys). This design facilitates recalling a specific make and model of a vehicle in certain geographic regions. In the Table, Local Group Size accounts for all the groups within one of the fifty geographic regions, a state.

Description	Quantity
U.S. States	50
U.S. Automobile Manufacturers	30
Manufacturer Models	10
Groups	15,000
System Participants	250,000,000
Participants Per Group	16667
Local Group Size	300

**Table 1: Notional VPKI Group Design (U.S.)**

One issue with the group credential approach is internal privacy. The group manager can determine who signed a message using the signature and the information it retains about the entire group, a breach of internal privacy. However, internal privacy could be enhanced by splitting the group manager into two logical (or physical) entities; the collusion of both entities would be needed to identify a particular message signatory. In the most recent SCMS specification document [SCMS14], a Trusted Platform Module (TPM) was suggested to isolate and protect linkage authority operations, and this could be done in the same machine. A similar approach could be used to provide internal privacy for the group credential approach.

**Group Revocation.** Three alternative approaches to revoke a group member using Certificate Revocation List (CRL) are considered. A CRL is a list that grows and shrinks to ideally contain all those participants that could possibly be acting in the system and should be ignored. In one approach, the group manager

issues a CRL to identify revoked participants. The CRL also contains updated group public keys [Ateniese02]. Each unrevoked user uses the same CRL to identify revoked participants and verifies new messages. These CRLs have high overhead and transmission bandwidth costs. More specifically, verification is linear to the number of revoked participants, and the CRL is proportional to the number of revoked participants [Ateniese02]

In a more recent approach, a revocation list is issued that includes each revoked participant's private key [Boneh04]. This approach may allow an adversary to link messages to a single vehicle. This linking weakness is eliminated in another scheme at the cost of increased computation [Nakanishi05].

In a different approach [Camenisch02], each group public key characterizes its members by accumulating individual, identifying member values; however, the final accumulated value cannot be used to identify any single member. When a group member signs a message, their signature contains a proof, verifiable using the group public key, that some member of the group generated the signature. A group member can be removed, or revoked, from a group. The group manager revokes the member by removing their identifying number from the accumulated value included in the group public key. Although the revoked group member can still sign messages, message recipients will not be able to authenticate the message using the new group public key, since the individual has been removed from the group. New group public keys must be distributed efficiently to all participants that may receive a message from the revoked participant to facilitate this revocation alternative .

#### **Section 4: Trusted Hardware**

The cryptographic operations for VBSS will require high performance on-board vehicle computation to sign messages at 10Hz and verify messages at 1000Hz. In research trials, 400 MHz [DOT811492D], 1 GHz, and 3 GHz (i.e., a desktop CPU [DOT811492D]) processors have been used to experimentally evaluate system performance requirements. Exact hardware computational requirements are yet to be established. However, due to added computational burden from group signatures, the VBSS concept may require a custom Application Specific Integrated Circuit (ASIC) to perform trust-critical computation along with another processor (or a core) for additional general computation. We anticipate a 10-15x speedup with new ASICs.

We discuss three possible options for protecting on-board security elements and increasing computation: a TPM, the ARM TrustZone [ARM09], and a Hardware Security Module (HSM). Of these three options, TPMs will not meet the needs of VBSS, since they are resource-limited in computation and I/O. For instance, the ST19NP18-TPM can store only nine keys [ST13]. TPMs often interface over the Low Pin Count (LPC) bus (33 MHz). This limited interface can potentially create a bottleneck for computation. While TPMs are resource constrained, they are an attractive option with an estimated cost of about \$1 [Kursawe04].

If ARM chips are used for computation (over 50 billion ARM chips have been produced [ARM14]), the ARM TrustZone architecture could potentially meet VBSS requirements. ARM TrustZone is a proprietary trusted computing architecture that is integrated in many modern ARM chips. In the ARM TrustZone architecture, applications execute in two zones: a Secure World and a Normal World. Sensitive computations are executed in the Secure World. However, when multiple applications execute in the Secure World, establishing trust among secure world applications will add complexity to the system. Some manufacturers are already making automotive compute platforms based on ARM chips [NVIDIA15].

An HSM is a separate and distinct trustworthy computing device. Depending on the HSM, it may have more mitigations against physical tampering, and it may have more powerful computational capabilities. Depending on the features, it may meet VBSS message signing, message verification, key management, and policy enforcement operational constraints. HSM cost varies from the IBM 4765 [IBM4765] that costs several thousand dollars to HSMs for more specific applications cost less. For this application, a custom design produced at scale should be cheaper than more general HSMs; the cost should be feasible for connected vehicle technology. Additional HSM experimentation is needed to verify HSM suitability.

#### **Section 5: VPKI Revocation Goals**

The trust among vehicles will depend on the effectiveness of misbehavior detection and revocation subsystems within the PKI. With imperfect revocation, vehicles may trust an untrustworthy BSM. Traditional CRLs attempt to address all abnormal actors. There are three basic problems with this approach: first, list growth; second, determining when an actor on the list can be removed; and third, checking the list efficiently. These basic problems are particularly hard to contend with in a large, dynamic

environment. There are several properties of this environment that may call for examination of different methods to revoke misbehaving vehicles:

**Area of Concern:** Vehicles are only concerned about those vehicles that are immediately within their range (e.g., 300m to 1000m range for DSRC is realistic); this area is small, and it is always changing.

**Population of Concern:** For most drivers, the subset of vehicles that they will encounter over the life of their vehicle will be significantly smaller than the set of all participating vehicles. In other words, most traditional CRL-identified actors are irrelevant for particular drivers. The core challenge is the variation in participating vehicle travel patterns in the U.S. Some drivers will encounter significantly more actors on the CRL than others; therefore, placing restrictions on which misbehaving vehicles are added to the CRL based on geography may cause drivers to trust vehicles they should not.

**Immediacy of Concern:** Of those vehicles within our area of concern, V2V systems should only focus on vehicles whose trajectory will bring them close to our immediate position; a vehicle may be in our area of concern but its trajectory may never pose a safety problem to our vehicle.

**Duration of Concern or Duration of Misbehavior.** Malfunctions may occur in the devices that provide data to include in safety messages and in devices used to corroborate vehicle misbehavior. Malfunctions may be short-lived. In the case of a short-lived malfunction, it would be a huge inconvenience for the driver to have to re-enroll in the VPKI for something that was caused by environmental factors.

The misbehavior and revocation goals for a PKI follow. Many of these goals may not be completely achievable in a system of this scale:

*Correct detection and classification of participants.* In an ideal system, the false positive (incorrectly labeling a vehicle as misbehaving when it is not misbehaving) rate is zero. The false negative rate (not labeling a vehicle as misbehaving when it is misbehaving) is also zero. If there are too many false positives, drivers may ignore safety warnings. With too many false negatives, the opportunity for accidents grows but well-behaved participants may never notice the existence of the unrevoked bad actors. In both cases, trust erodes. In addition to perfect actor classification, an ideal system should correctly identify unintentionally misbehavior and intention misbehavior.

*Immediate removal of misbehaving participants.* This goal relates to the immediacy of revocation – ideally, detection and revocation happen simultaneously along with notifying the remaining participants in the system of the revocation. In short, identified misbehaving vehicles are immediately unable to interact with others in the PKI; there is no delay. With a system of this scale, this goal cannot be met.

*Removed unintentional abnormal actors can immediately rejoin after their vehicle is fixed.* If an unintentional misbehaving vehicle is revoked and then fixed, the driver would expect that the vehicle's communication would be restored. Authenticating the unintentional misbehavior is important; this relies on correct detection and classification of participants, and it may be difficult to do.

*Upon one or more revocations, remaining non-revoked vehicles continue to function without interruption or extra work.* When a vehicle is revoked, the good vehicles that remain should be able to participate in the PKI without interruption and without extra work (except CRL use). In some potential VBSS schemes [Tengler07, White09, Haas09], a normal non-misbehaving vehicle may have to do some amount of extra work to remain in the system. When comparing revocation systems, the amount of extra work that a non-misbehaving vehicle must perform to remain part of the PKI is a potential metric of comparison.

## **Section 6: Misbehavior Detection: From Local to Global**

The number of vehicles that will be revoked over some defined time period is a valuable estimate when determining the feasibility of a vehicular credential management system. In a traditional PKI, revocation strategies are used to handle inappropriate or malicious use of credentials. In a VPKI, revocation strategies are needed to address malfunctioning vehicles, as well as malicious vehicles that could cause vehicle mishaps. Since this system has not been realized or simulated at scale to our knowledge, estimates are hard to derive and justify. Four classes were identified to stratify the broader estimation problem. These numbers are used to estimate the degree to which revocation will be required in the VPKI being considered for the U.S.

*Malicious vehicle.* Total elimination of malicious actors is improbable. A malicious participant may avoid detection by learning how global misbehavior detection is performed, for instance the period of time over which misbehavior reports are retained. We hypothesize vehicle credential compromise will be very difficult initially based on the diversity of vehicles, hardware, access points, and communication protocols.

The security posture in this domain makes it hard to estimate the likelihood of certificate compromise. We anticipate that this number will be low compared to the population of malfunctioning vehicles.

*Malfunctioning vehicles.* Electronic components typically fail early in their lifecycle due to manufacturing defects that escaped quality control and much later when the device reaches its time-to-failure. In between those times, component failure rates remain fairly constant. Component failure rate is also hard to estimate, since many of the components used in these systems are still being developed. Depending on a component’s function, it may be possible for the vehicle to self-validate information and avoid broadcasting inaccurate BSMs. Assuming that this capability is possible, we anticipate that the number of resulting revocations will be low.

*Environmental-Impacted Malfunctioning Vehicles – vehicles whose component accuracies are affected by environmental conditions.* Environmental conditions could lead to a wide range of issues. We do not estimate the impact here.

*End-of-life Vehicles:* This class of vehicles presents a dilemma: on one hand, we can assume that these vehicles have been completely removed from the system; on the other hand, parts are routinely harvested from end-of-life vehicles and security credentials are potentially valuable resources for bad actors. When the credentials do have value, attackers may harvest certificates from end-of-life vehicles, and then find a way to use them to broadcast targeted messages. We estimated that there are approximately 1 million end-of-life vehicles per month. Identifying these vehicles and revoking them is a challenge.

Previous estimates put the total population estimates from these three vehicle populations at a relatively low value [Whyte13].

Figure 3 identifies the infrastructure entities involved with misbehavior detection and revocation. The operations involved in misbehavior detection and revocation start with local misbehavior detection and misbehavior reporting. Misbehavior reports are generated by a vehicle that detects an anomalous safety message; the message has a prescribed format; it is encrypted and sent through the infrastructure to the

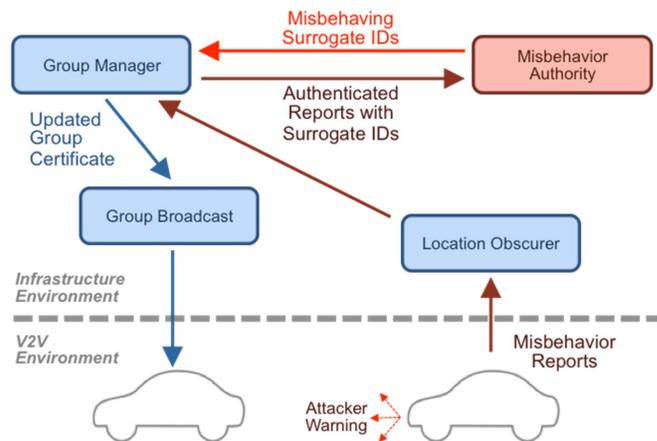


Figure 3: Misbehavior Reporting and Group Certificate Updates

group manager. Global misbehavior detection operates on a collection of misbehavior reports. Finally, group credentials must be modified and redistributed to the participant population.

Local misbehavior detection is a vehicle’s intrinsic ability to use on-board hardware (e.g., vehicle-resident sensors) and software to detect safety messages that do not conform to physical reality. This locality is opposite a global system where a central networked system performs misbehavior detection. Local misbehavior detection can be done using software that detects simple safety message anomalies, or in a more complex system corroborate information collected from a vehicle’s organic sensors (e.g., radar, lidar, sonar) with received safety messages to determine irregularities more accurately. In global misbehavior detection, other infrastructure components (e.g., a RSU or misbehavior authority) determine if a vehicle is misbehaving.

In recent work, using vehicle-resident sensors, researchers have explored attacker-warning systems that can be used independently or in conjunction with misbehavior reporting and revocation [Calandriello11]. The attacker-warning concept that we outline can extend the range of a vehicle’s inherent warning sensors; on-

board sensors may have line-of-sight range or be blocked by surrounding vehicles. Attacker warnings need to be within the range of DSRC communications. One of the challenges in realizing an attacker-warning system is trust. Much of the information is provided by sensors whose readings may be suspect (e.g., GPS). Additionally, this is a consensus-based concept without a central trusted authority; this is a significant obstacle. A conceptual attacker warning might employ three operations:

1. Local, or inherent, misbehavior detection
2. Warning transmission: Vehicles and roadside equipment should broadcast warning messages over DSRC to other vehicles in their area of concern. The following information may be important for vehicles able to receive these warnings:
  - The actor's pseudonym certificate. Although these certificates are short-lived, one or two certificates may be sufficient to span the time over which the warned vehicle may encounter the actor.
  - Report time. Due to immediacy of concern and duration of misbehavior, it may be appropriate to limit a warning message's valid time.
  - Reporter position. A vehicle's location changes and may not impact a given situation. This proximity information may help validate the warning or the need to consider the warning. While this could impact privacy, there may be ways to not report the position globally but use this information locally.
  - Consensus information. As a measure to improve warning system trust, warning recipients could rebroadcast validated warning messages with an updated confidence value. Warnings with higher confidence should be more trustworthy.
3. Warning processing: Vehicles should be able to receive and evaluate warnings, and then use these warnings in conjunction with safety messages to improve their safety posture.

There are motivations to combine several approaches. A vehicle can enforce a local policy based on local misbehavior detection. Local misbehavior adjudication helps use valuable DSRC resources more efficiently, decreases the computation required during global adjudication, and it has the potential to reduce global misbehavior detection errors.

Since the effectiveness of using any revocation scheme is unknown in this large-scale VPKI deployment, an incremental approach to handling misbehavior may be worth consideration. In this incremental approach, local misbehavior detection is the most critical; an attacker-warning system might be introduced next; finally, misbehavior reporting to a global authority might be required to improve the overall trustworthiness of the system at the expense of significant communication and processing overhead.

Each misbehavior report contains details from one or more safety messages that the vehicle used to determine local misbehavior. The reporting vehicle must sign all reports to avoid malicious reports from being processed; encryption may also be necessary to maintain the confidentiality of the reporter. In our conceptual VBSS, misbehavior reports flow through a network traffic obfuscator, similar to one that was previously introduced [Whyte13]. Reports are then handed off to the group manager. The group manager verifies the report using the appropriate version of the group certificate making sure the reporting vehicle has not been removed from the group. Then, the group manager will "open" a signed BSM to identify the misbehaving vehicle that signed that BSM and assign it an ephemeral proxy identifier. The purpose of the proxy identifier is to provide a way for the misbehavior authority to aggregate reports on a specific vehicle and not have secret information on a particular driver. A collection of reports on a vehicle does not automatically imply misbehavior; therefore, the misbehavior authority should know as little as possible about the identity of the vehicles it is analyzing in the aggregate. Proxy identifiers will be short-lived, so they do not become unique persistent identifiers and allow the misbehavior authority to break the privacy of vehicles that are found to be behaving correctly. Authenticated reports with a proxy identifier are then passed to the misbehavior authority.

The Misbehavior Authority is responsible for gathering misbehavior reports globally from all the participants in the connected vehicle system. Ideally, the misbehavior authority should be a central entity within the infrastructure; however, misbehavior authorities that are collocated with distributed group managers should be investigated. Global misbehavior detection algorithms are an open area of research [Delgrossi12]; however, one critical property of these algorithms will be their true positive and true negative rate.

Once the misbehavior authority has identified misbehavior, the group manager will remove that vehicle from the group by distributing updated public data including an updated group certificate that will disallow revoked vehicles from continued participation. A removal operation is performed for each validated misbehavior report. In other words, the number of operations necessary to update the trust elements in the

system is linear in the number of revoked vehicles. After a number of removals have been made, group certificate updates will be distributed to system participants. However, the size and number of trust elements is fixed with groups.

## Section 7: VBSS Revocation

If a BSM sender or receiver has an outdated group certificate, messages sent between the parties may not be verifiable. This issue holds with many of the group signature schemes. One way to address this issue is to assign vehicles to multiple groups. Assume that a given vehicle is a member of two groups. If one of its two group public keys is old, then the user can use the other corresponding private signing key to create message signatures that can be authenticated. Alternatively, assume both group public keys are old (i.e., the group manager has revoked at least one member in each group). The user may not be able to communicate with other users that are using the most recent public group keys.

As a possible alternative to addressing unsynchronized public key updates, we propose that revocation be staggered. For example, rather than each group member storing a single group public key for a given group, the group member stores the current group public key and the previous group public key. If a group member updates her group public key, she can then verify messages from senders that have updated to the latest group public key, and she can also verify messages from senders who use the previous group signing key. By staggering group public key updates, the immediacy of user updates can be relaxed.

In a traditional PKI, participants may submit certificates to a central authority to check whether they are on the CRL. CRLs may be broadcast to users, so users can check the certificates they receive locally. CRL updates are usually promulgated using delta lists to decrease the amount of communication overhead. When short-lived certificates are used, a central authority can utilize a blacklist to identify those participants whose certificate expirations should not be extended or renewed. The primary issues with these traditional approaches are list management (additions and removals), list size, and list distribution. CRLs have global context: all participants must have knowledge of the complete list since they may interact with a revoked participant.

In a group-based VBSS, the group manager can identify a message sender, since they can “open” a de-identified group signature on a pseudonym certificate. Their role can be split to further distribute the trust elements and make it harder to break privacy, but ultimately when a misbehaving vehicle has been identified its privacy is assumed to be forfeit.

Misbehavior reporting, adjudication, and revocation synchronization challenges exist in the real-time and distributed V2V environment. Because the identification and revocation of a bad participant is not immediate, we now examine how delayed revocation impacts a group revocation system. Figure 4, depicts the evolution of the V2X environment over a period of time where two vehicles have been reported as misbehaving and subsequently revoked from the group. While this figure illustrates some of the synchronization challenges in a VBSS based on groups, other designs [Whyte13] may be susceptible to synchronization issues. In the Figure, time progresses from left to right; the dotted arrow delineates the state of the infrastructure environment (top) and the state of the vehicular environment (bottom). For simplicity, all vehicles are part of one group. Both environments start in a good state (green) at the left: all parties are using group certificate one (GC1).

In VBSS, vehicle revocation can only occur when misbehavior has been reported, and the misbehavior authority classifies the identified vehicle as misbehaving. These actions will not occur instantaneously. In the Figure, there is a time gap between the Vehicle A misbehavior report and misbehavior adjudication and creation of GC2. Since we have perfect hindsight and Vehicle A is truly misbehaving, the trust state of the V2V environment is degraded at the point in time when Vehicle A started misbehaving – Vehicle A will be

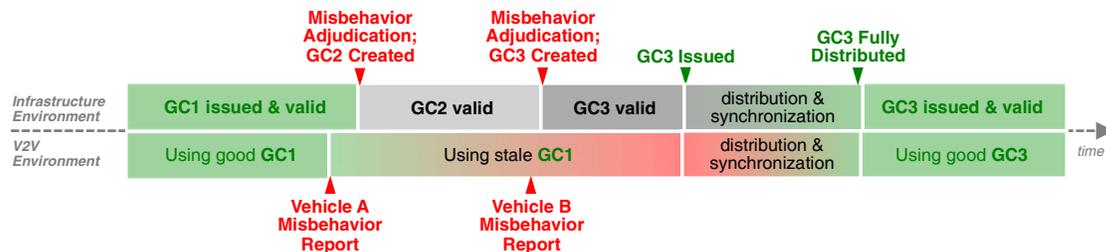


Figure 4: Misbehavior Reporting and Revocation Synchronization

trusted by other vehicles, but it will be transmitting potentially untrustworthy messages that will be verified by recipients. The gradual transition from green to red in the lower portion of the Figure illustrates the effect of this state; more and more vehicles encounter the misbehaving vehicle and will trust its broadcast safety messages. In an ideal system, this transition would not exist; however, misbehavior reporting, misbehavior adjudication, and distribution of updated credential will require time. Decreasing the transition from green to red and back to green is a goal.

When a vehicle is revoked, the group public key must be updated. The infrastructure may not issue new group certificates every time a vehicle is revoked. The propagation of new group certificates consumes communication resources and time.

The gray color in the Figure indicates the time period when the infrastructure's group certificate state differs from the group certificate's state in the V2V environment, because GC2 was not issued by the infrastructure. After the second misbehavior adjudication has been integrated into the group certificate, GC3 is ready to be issued. The group manager then re-issues updated group certificates on a schedule to minimize synchronization problems. Once new credentials are released, vehicles and roadside equipment can transmit these updates to vehicles that have not received the update yet.

In the Figure, the trust of the system is degraded from the time the first vehicle misbehaves until GC3 has been fully distributed. At this point, both environments are synchronized. Any group-signed messages the misbehaving vehicles broadcast will not be verifiable using the updated credentials.

To protect against misbehaving vehicles that have not been revoked, local misbehavior detection is a potential first line of defense. During the distribution and synchronization period, the system gradually returns to a fully trusted state. Certificate caching can be introduced to alleviate the problem of unsynchronized group certificates. Let  $GC_x$  be group certificate  $x$ , and let each vehicle cache two GC versions:  $GC_{x-1}$  and  $GC_x$ . We assume the sender is using pseudonyms generated using their most recent GC. Each signature includes a signed identifier (e.g., the value one for a message signed by  $GC_1$ , the value two for a message signed by  $GC_2$ , etc.). A vehicle can quickly check if it has the most recent GC by checking the identifier.

We consider six abnormal cases where four GC versions have been issued ( $GC_1$ ,  $GC_2$ ,  $GC_3$ , and  $GC_4$ ), where  $GC_4$  is the most recent GC. In each case, vehicle A is sending a basic safety message to a receiver, vehicle B. Both vehicles can store up to two certificates. To enable communication between two vehicles, they must have at least one  $GC_x$  in common.

**Case 1: Functioning with Old Certificates.** Both vehicles have cached  $GC_1$  and  $GC_2$ . Vehicle B can validate vehicle A's message. If vehicle A has not been revoked, their interaction is equivalent to the case where the most recent update is  $GC_2$  despite both vehicles being out of synchronization with the infrastructure. If vehicle A has been revoked,  $GC_3$  or  $GC_4$  should reflect their removal from the group. However, in their current state vehicle B's trust will be misplaced. To remedy this situation, B should update to  $GC_4$  as quickly as possible.

**Case 2: Delay in Revocation.** Both vehicles have  $GC_3$  and  $GC_4$ . B can validate A's message. It is possible that A could have been reported as misbehaving, but a new update has not been issued – this case must be handled by local misbehavior detection.

**Case 3: Partially Unsynchronized Old Sender.** A has  $GC_1$  and  $GC_2$  in its cache; B has  $GC_2$  and  $GC_3$  in its cache. B can validate A's message using  $GC_2$ . If A has not been revoked, the exchange is equivalent to the case where the most recent update is  $GC_2$ . If A has been revoked in  $GC_3$  or  $GC_4$ , then B's trust will be misplaced. In all situations, B can notify A that its certificates are out of date since it had to use an outdated certificate to validate the pseudonym. This should cue A to pull the  $GC_4$  update (from a road-side unit or nearby vehicle) and generate new pseudonyms. This case is the main reason more than one GC is cached. B could not verify A's messages if B could only store the latest GC,  $GC_3$ . With the caching of GCs, A and B can still communicate.

**Case 4: Partially Unsynchronized Old Receiver.** Vehicle A has  $GC_2$  and  $GC_3$ ; vehicle B has  $GC_1$  and  $GC_2$ . B can only verify A's signatures if A is using old pseudonyms; this would be abnormal for A. If A were using updated pseudonyms, B will not be able to authenticate A's pseudonyms. In the first case (A uses  $GC_2$ ), B would still be unaware that it needs to update its certificate but could continue communicating with A; in the later case, B will know to update its certificate when it finds  $GC_3$  was used.

**Case 5: Unsynchronized Old Receiver:** A has  $GC_3$  and  $GC_4$ ; B has  $GC_1$  and  $GC_2$ . B cannot verify any signed messages from vehicle A. This does not mean that vehicle A's messages are untrustworthy. The signature identifier is a cue for B to check for an updated GC.

**Case 6: Unsynchronized Old Sender.** A has  $GC_1$  and  $GC_2$ ; B has  $GC_3$  and  $GC_4$ . B cannot validate messages from A. This may mean that A's messages cannot be trusted, or if A is trustworthy it is due to B not having  $GC_2$  in its cache. The signature identifier cues B to obtain an updated group certificate.

Significant communication savings may be possible by using group certificate revocation strategies instead of more traditional certificate revocation lists. When a new vehicle joins a VBSS, it will receive an initial load of group certificates that enable it to authenticate the vehicles within its geographic area. However, only being able to communicate to vehicles in its own geographic area may be insufficient for vehicles that travel outside of their local area. How groups are determined and established is an important area of research. The design must incorporate several factors including the type of large-scale revocation (e.g., recalls) that might be required, laws, and the capabilities of stakeholders to perform certain group manager functions. One possible configuration involves dividing the vehicle population by states, manufacturer, and model.

Because the size of the group certificate is fixed, the storage needed for all of the group certificates is the constraining factor. A group certificate is approximately 900 bytes [Calandriello11] (could potentially use smaller key sizes for reduced certificate sizes). We can use this information to reason about how many groups a VBSS should support. Based on our notional group partitioning strategy, vehicles must store 15,000 group certificates to cover the entire U.S. This will be unnecessary for almost all vehicles in the system. However, if these certificates were stored on the vehicle, the total storage capacity needed would be approximately 13 MB. If we cache the previously used group certificate, then the total amount of storage would be almost 27 MB. These certificates are public and not identifying, so they do not need to be stored in memory whose access is restricted to trusted software and hardware. Our concept includes a mechanism for distribution of trust updates; therefore, storage of this number of group certificates may not be necessary.

**End-of-life vehicles.** Scaling to address end-of-life vehicle revocation is difficult. As previously noted, there are approximately 1 million vehicles that reach their end-of-life each month in the U.S. Adding these vehicles to a traditional revocation list is prohibitive. To address these vehicles in a group PKI, group certificate size remains fixed independent of the number of updates. The group update distribution process benefits from the fixed group public key size. Traditional CRLs grow linearly in the number of vehicles. In a traditional PKI approach, accommodating end-of-life revocations will make revocation infeasible.

## Section 6: Conclusion

Traditional PKIs have been designed and used for specific types of problems where privacy is not a concern (e.g., email). This lack of privacy is an issue for a vehicle PKI. Parties in a traditional PKI will exchange keys and later send and receive messages. When a recipient verifies a message, they assume that the sender is trustworthy. In a vehicle PKI, a receiver must trust the sender without identifying the sender – the sender should remain anonymous. This is a challenging problem at a large scale, and a different way of approaching the problem is needed. To provide privacy at a large scale, we suggest the use of a group-based approach for VBSS. Our initial analysis shows that using groups in a vehicle PKI helps mitigate some of the issues that we see in other systems.

A great deal of work has been done to address vehicle security and privacy; however, more work and field trials are necessary. Trustworthy hardware may be required on all connected vehicles to protect credentials; it will certainly be necessary to protect a group signing key and the pseudonym generation process in a VBSS. The BSM transmit and receive rates envisioned in high density V2V environments may require high performance trustworthy hardware in vehicles. This system's trust is predicated on the acceptable operation of a misbehavior detection and revocation system. The right balance of local and global misbehavior detection is critical, and more misbehavior simulation and experimental results will help us establish what will be an acceptable operational state. By integrating group certificates, VBSS may address some of the revocation overhead issues in a system of this size; staggered (or cached) group certificate updates offer additional benefits.

An operational VPKI that provides an acceptable level of security and privacy would be a groundbreaking achievement. We are optimistic about the possible solutions VBSS offers: Putting pseudonym generation in the vehicle has benefits; the inherent privacy preserving properties of group signature cryptography mitigates certain types of infrastructure growth. We encourage research that enables a vehicle to produce its own ephemeral certificates while protecting privacy. Using groups, vehicle privacy is maintained through the anonymity afforded by a group. As vehicle PKI research and technology becomes more focused, the unique challenges this environment presents will be addressed and the promise of safer vehicles will be realized.

## Acknowledgements

This research was funded by the National Highway Traffic Safety Administration (NHTSA). To date, NHTSA has posed questions and provided insight that has helped guide this work. We would also like to thank Lawrence MacIntyre and Jarilyn Hernandez, our colleagues at the Oak Ridge National Laboratory, for their valuable feedback on this research.

## Section 7: References

- [Al-Fuqaha07] A. Al-Fuqaha and O. Al-Ibrahim. Geo-encryption Protocol for Mobile Networks. *Computer Communications*. 30(11-12):2510-2517. Sept. 2007.
- [ARM09] ARM. ARM Security Technology: Building a Secure System using TrustZone Technology. Available at [http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C\\_trustzone\\_security\\_whitepaper.pdf](http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf). 2009.
- [ARM14] ARM. <http://next100billionchips.com>. Internet Archive Wayback Machine. July 15, 2014. Available at <https://web.archive.org/web/20140715212213/http://www.next100billionchips.com/>.
- [Ateniese00] G. Ateniese, J. Camenisch, M. Joye, and G. Tsudik. A Practical and Provably Secure Coalition-resistant Group Signature Scheme. In *Proceedings of the 20th Annual Crypto Conference (CRYPTO)*. August 2000.
- [Ateniese02] Giuseppe Ateniese, Dawn Song, Gene Tsudik. Quasi-Efficient revocation of Group Signatures. *Financial Cryptography*. March 2002.
- [Bellare03] Mihir Bellare, Daniele Micciancio, Bogdan Warinschi. Foundations of Group Signatures: Formal Definitions, Simplified Requirements, and a Construction Based on General Assumptions. In *Advances in Cryptology – EUROCRYPT 2003, Lecture Notes in Computer Science (LNCS) Vol. 2656, E. Biham ed, Springer-Verlag, p. 614-629*. May 2003.
- [Bellare05] Mihir Bellare, Haixia Shi, Chong Zhang. Foundations of Group Signatures: The Case of Dynamic Groups. In *Topics in Cryptology – CT-RSA 2005, Lecture Notes in Computer Science (LNCS) Vol. 3376, A. Menezes ed, Springer-Verlag, 2005*.
- [Boneh04] Dan Boneh and Hovav Shacham. Group Signatures with Verifier-Local Revocation. In *Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS)*. p. 168-177. October 2004.
- [Calandriello11] Calandriello, G.; Papadimitratos, P.; Hubaux, J.-P.; Lioy, Antonio, "On the Performance of Secure Vehicular Communication Systems," *Dependable and Secure Computing, IEEE Transactions on*, vol.8, no.6, pp.898-912, Nov.-Dec. 2011. [Camenisch02] Jan Camenisch and Anna Lysyanskaya. Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In *Advances in Cryptology – CRYPTO 2002, Lecture Notes in Computer Science (LNCS 2442)*. p. 61-76. September 2002.
- [Chaum91] David Chaum and Eugene van Heyst. Group Signatures. In *Advances in Cryptology – EUROCRYPT 1991 (LNCS 547)*. p. 257-265. April 1991.
- [Delgrossi12] Luca Delgrossi and Tao Zhang. Vehicle Safety Communications. *Wiley*. 1st ed. October 2012.
- [DOT811492D] DOT. Vehicle Safety Communications – Applications (VSC-A). Final Report: Appendix Volume 3 Security. *CAMP*. DOT HS 811492D. Sept. 2011.
- [FHWA11] Federal Highway Administration's Office of Highway Policy Information, Highway Statistics Series, <http://www.fhwa.dot.gov/policyinformation/statistics/2011/>. September 2011, Accessed 2014.
- [Haas09] Jason J. Haas, Yih-Chun Hu, Kenneth P. Laberteaux. *Security and Communication Networks*. John Wiley & Sons, Ltd. September 2009.
- [Help14] HelpScout. 75 Customer Service Facts, Quotes & Statistics. Available at <http://www.helpscout.net/75-customer-service-facts-quotes-statistics/>.

- [Huang09] Dijiang Huang, Mayank Verma. ASPE: attribute-based secure policy enforcement in vehicular ad hoc networks. In *Ad Hoc Networks*. 7(8):1526-1535. November 2009.
- [IBM4765] IBM. IBM 4765 PCIe Cryptographic Coprocessor. Available at [https://www-03.ibm.com/security/cryptocards/pciecc/pdf/PCIe\\_Spec\\_Sheet.pdf](https://www-03.ibm.com/security/cryptocards/pciecc/pdf/PCIe_Spec_Sheet.pdf).
- [Kursawe04] Klaus Kursawe. Trusted Computing and its Applications: An Overview. In *ISSE 2004 – Securing Electronic Business Processes*. Springer. September 2004.
- [Nakanishi05] Toru Nakanishi and Nobuo Funabiki. A Short Verifier-Local Revocation Group Signature Scheme with Backward Unlinkability from Bilinear Maps. In *ASIACRYPT 2005*. Springer-Verlag, LNCS 3788. p. 533-548. December 2005.
- [NADA14] NADA. NADA DATA Annual Financial Profile of America’s Franchised New-Car Dealerships. [www.nada.org](http://www.nada.org). 2014.
- [NHTSA14] National Highway Traffic Safety Administration (NHTSA), USDOT. U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication for Light Vehicles. *Press Release*. Available at <http://www.nhtsa.gov/About+NHTSA/Press+Releases/2014/USDOT+to+Move+Forward+with+Vehicle-to-Vehicle+Communication+Technology+for+Light+Vehicles>. February 3, 2014.
- [NVIDIA15] NVIDIA. Buy Jetson TK1 DevKit. Available at <https://developer.nvidia.com/jetson-tk1>.
- [Raya06] Maxim Raya, Daniel Jungels, Panos Papadimitratos, Imad Aad, Jean-Pierre Hubaux. Certificate Revocation in Vehicular Networks. *LCA Technical Report*. 2006.
- [ST13] STMicroelectronics. ST19NP18-TPM Data Brief. Available at [http://www.st.com/st-web-ui/static/active/en/resource/technical/document/data\\_brief/DM00039003.pdf](http://www.st.com/st-web-ui/static/active/en/resource/technical/document/data_brief/DM00039003.pdf). November 2013.
- [Tengler07] Steve Tengler, Scott Andrews, Ronald Heft. Digital Certificate Pool. *U.S. Patent US20070223702 A1*. Sept. 2007.
- [White09] Robert G. White, et al. Privacy and Scalability Analysis of Vehicular Combinatorial Certificate Schemes. In *Proceedings of Consumer Communications and Networking Conference*. January 2009.
- [Whyte13] William Whyte, Andre Weimerskirch, Virendra Kumar, Thorsten Hehn. A Security Credential Management System for V2V Communications. In *Proceedings of the Vehicular Networking Conference (VNC)*. December 2013.