Don't Talk to Strangers
On the Challenges of Intelligent Vehicle Authentication

Alishah Chator and Matthew Green
Computer Science Department, Johns Hopkins University, Baltimore, MD, U.S.A.

Keywords: Authentication, V2V Communications, Privacy.

Abstract: Vehicle-to-vehicle (V2V) communications offer an unprecedented opportunity to increase driver safety. At the same time, the use of computer networking technologies raises new concerns around information security and privacy. Specifically, V2V communications systems provide the opportunity for malicious individuals to transmit false data, with unknown effects on future vehicle systems. A number of proposals have been advanced in order to add *authenticity* guarantees to V2V systems using cryptographic techniques. Unfortunately, many of these proposals have a number of side effects related to efficiency and driver privacy. In this work we discuss these tradeoffs and explain why it is challenging to achieve all desired properties in a single system. We then suggest alternative approaches that may be more realistic than current proposals.

1 INTRODUCTION

Vehicle-to-Vehicle (V2V) communication technology allows automobiles to exchange digital messages via short-range radio. This technology promises to dramatically improve driver safety by providing detailed information about nearby vehicles, including exact position and speed. By monitoring this information, communications-enabled cars can notify the driver of danger or take action to avoid a crash.

V2V communication offers many potential benefits. However, it also raises new concerns related to security, privacy and driver safety. Critical among these is the resilience of V2V systems to *malicious* transmissions, including messages designed to harm drivers or create unsafe traffic conditions. As vehicles become more automated and thus dependent on the accuracy of these transmissions, these opportunities are likely to be exploited. Consequently, one of the major requirements of a future V2V communication system is a means to *authenticate* that each V2V transmission originates with a legitimate transmitter.

The problem of authenticating V2V communications has been the subject of a great deal of academic research, much of it involving the use of cryptographic authentication technologies (Raya and Hubaux, 2005; Yousefi et al., 2006; Papadimitratos et al., 2006; Raya and Hubaux, 2007; Calandriello et al., 2007; Papadimitratos et al., 2008; Khodaei et al., 2014; Foo et al., 2015; Hamida et al., 2015; Khodaei and Papadimitratos, 2015; Khodaei and Papadimitratos, 2016). Indeed, in the United States these technologies have been developed to the point where they are being deployed in current vehicles (Hehn et al., 2014; Pleskot, 2017). However, it remains unclear whether these techniques are sufficient or appropriate to solve the security problems raised by V2V communications.

To understand what makes this problem particularly challenging, it is necessary to discuss the various requirements that face designers of V2V systems. In tandem with the need to authenticate messages, modern V2V systems are typically expected to satisfy two additional requirements. First, they must address potential concerns regarding driver privacy. Specifically, many governments have mandated that V2V transmissions should not allow for the tracking of vehicles. As a second requirement, V2V systems are expected to provide robust functionality in a challenging environment where many vehicles have limited network connectivity. This leads to three overall requirements, which we refer to as *authentication*, *privacy*, and (communication) *robustness*.

Unfortunately, as we show in this work, these requirements are fundamentally at odds. Achieving all three of these goals simultaneously requires that (1) receivers must be able to verify the identity of each transmitter and reject signals from bad actors, and yet (2) receivers should not be able to identify a specific transmitter, or even link different transmissions to the same vehicle, and (3) this process must not rely on

Chator, A. and Green, M.
Don't Talk to Strangers.
DOI: 10.5220/0006790205220528
In *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2018)*, pages 522-528
ISBN: 978-989-758-293-6

regular or even periodic updates issued from a central authority to the vehicle fleet. While it may be possible to achieve two of these goals simultaneously, achieving all three appears fundamentally difficult.

The implication of this is twofold. First, we believe this should motivate designers to reconsider the deployment of cryptographic authentication infrastructure, which can be very costly.[1] Secondly, we believe that manufacturers should begin to develop alternative techniques that filter out potentially malicious V2V communications *by examining the content of the messages*, rather than by relying on authentication data.

1.1 Cryptographic Authentication for V2V

A secure V2V communications system consists of several components. The most important is the On Board Equipment (OBE), a specialized computer that resides within each vehicle. This computer is connected to a radio transceiver and a Global Positioning System unit. In current V2V proposals, the OBE transmits "basic safety messages" that embed the vehicle's exact position and trajectory. These messages may be received by nearby vehicles, and used to display messages to the driver and/or (in future autonomous vehicles) assist in making driving decisions.

Because these messages may have safety implications, it is important to provide a means by which vehicles can distinguish authentic messages from malicious transmissions sent by unauthorized transmitters. The canonical method for cryptographic authentication uses *public key digital signatures*. In this scheme, users possess a *public key* and a *secret key*, where the former should be shared and the latter is hidden. Users may employ the secret key to *sign* arbitrary messages. The resulting signature can be verified using the public key. The fundamental challenge with authentication is distributing the public keys in a way that users are certain who a public key belongs to. A common strategy is to use *certificates*. A certificate is a digital credential that contains the public key of a user, and is in turn signed by a trusted authority known as a Certificate Authority. Certificates have a set time period during which they are considered valid. In some systems, there is a *revocation* process in place to invalidate certificates so the system can control who can send authentic messages.

The security of this approach therefore makes a key assumption: the key material needed to generate digital signatures will be available only to *approved* OBE devices, and will not be easy for a malicious party to extract from an OBE and duplicate. Because this last assumption is difficult to guarantee across millions of vehicles, this motivates a final requirement: if the cryptographic keys are extracted from an authorized OBE device by a malicious party, there exists a means to identify the invalid messages, and disable the stolen keys.

To make this effort more challenging, modern V2V security proposals add two additional requirements. First, individual messages sent by vehicles should not uniquely identify the vehicle. Moreover, it should be challenging to link two messages sent by the same vehicle at different locations. This requirement is intended to prevent the use of V2V communications as a means to track the location of vehicles. This privacy goal has been identified a critical requirement of deployed V2V security systems, and accounts for a substantial degree of the complexity of deployed proposals such as the U.S. government's proposed SCMS system (Hehn et al., 2014).

As a final requirement, today's V2V systems assume that network connectivity (from vehicles to the Internet, or to centralized authorities) is fundamentally unreliable. That is, many vehicles will not be able to connect routinely to a central authority in order to obtain additional key material. A V2V security system must function even without access to a reliable cellular network. We refer to this final property as *robustness*.

2 TRADEOFFS

As discussed above, an intelligent vehicular system must satisfy several distinct requirements that may not be easy be achieve simultaneously. We first enumerate these requirements, which we refer to as *authenticity*, *privacy* and *robustness*.

Authenticity. This is the property that communications between vehicles are trustworthy. Messages received from other vehicles are from exactly who they say they are from, and all the contents of the messages are accurate. Vehicles that are found to be misbehaving are detectable or removed from the network.

Privacy. The privacy requirement implies that vehicles are able to communicate without revealing information that could be used for tracking vehicles. In a private system, transmissions should not contain uniquely vehicle-identifying information, and multiple messages from the same vehicle should not be linkable. A common benchmark is that the system should not allow an adversary perform a stronger attack on privacy than it would be

[1] One proposal, called SCMS (Hehn et al., 2014), is expected to cost approximately $4 billion USD to deploy in the United States.

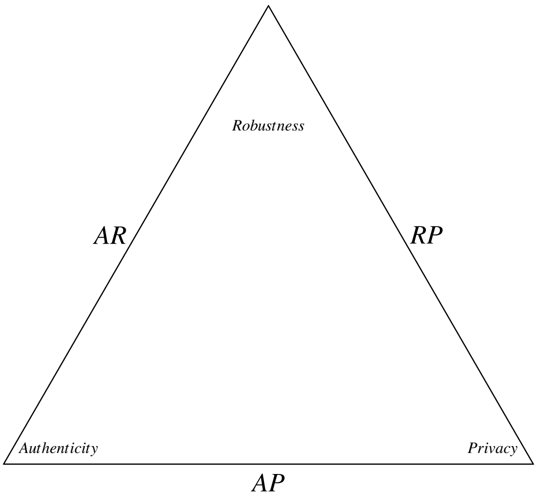

Figure 1: This figure illustrates the trilemma of the properties of Privacy, Authenticity, and Robustness in Intelligent Vehicle Authentication. At best, only two of these properties can be simultaneously offered. Consequently, as one attempts to maximlze two of these properties it will be at the cost of the third property. The sides AR, AP, RP represent achieving Authenticity and Robustness at the expense of Privacy, achieving Authenticity and Privacy at the expense of Robustness, and achieving Robustness and Privacy at the expense of Authenticity respectively.

able to in than the absence of the system.[2]

Robustness. We define Robustness as the property that the system remains operational and *secure* even in the face of low overall levels of connectivity to the network. A system with low Robustness requires that every vehicle has a stable fast connection to the network in order to operate correctly. A system that achieves high Robustness is one that can still offer all of its guarantees even if vehicles often have sporadic, slow, or even no connection to the network.

As a final observation, it is important to note that these systems will have fixed hardware resources. Due to high tolerance requirements, this hardware will generally be much less performant than consumer grade hardware. This adds an additional bounding on the capabilities of a system, as processing power or storage will be limiting factors. We discuss these limits further below.

Now let us understand why these tradeoffs exist. Each of the sides of our triangle represents an extreme case where two properties are highly satisfied, but the third property is lacking.

AR. This represents a system with a high level of Authenticity and Robustness. Thus, this system can guarantee Authenticity even if vehicles often cannot interact with the network. In practice, an important feature of Authenticity is the exclusion of misbehaving vehicles. This requires updates from the network regarding which vehicles should not be trusted. In this situation, this list of revoked vehicle identities needs to be small and easy to process. However, introducing Privacy into the system will require more identities per vehicle or larger, more complex identities, both of which will dramatically increase the size or complexity of the revocation list.

AP. In a system that provides strong Authenticity and Privacy, valid messages can be considered trustworthy and communication does not jeopardize a vehicle's privacy. This results vehicles with a large number of or complex identities, which in turn means that the list of revoked vehicles can grow to be quite large or hard to process. This can only work in a highly connected network where vehicles can perform quick lookups on demand and only need to hold entries pertaining to a smaller time interval. In this setting Robustness is difficult to achieve.

RP. This side represents a system with Robustness and Privacy. Even under low connectivity guarantees, communications would not reveal significant information about vehicles or their driving behaviors. Clearly, Authenticity is difficult to achieve in this scenario. High privacy would require large revocation lists which could not be distributed effectively with the assumed network limitations. Thus, it would be difficult to inform vehicles about misbehaving parties and thus there would be little Authenticity.

3 EXAMPLE AUTHENTICATION SYSTEMS

To further clarify these tradeoffs, we will offer some examples of cryptographic vehicular authentication schemes.

3.1 Shared Key Authentication

Perhaps the most naïve implementation of vehicle authentication is to use a single cryptographic secret key that is shared across the entire vehicle fleet. Every vehicle would have the same identical key hardcoded into their onboard equipment. All messages signed

[2] For example, an attack than involves physically surveilling a specific car is acceptable, as even without this system it would result in a loss of privacy for that car. Similarly, the underlying basic safety messages might themselves leak identifying data; our goal should be that the authentication system does not offer further degradation.

by this key would be assumed to be authentic and trustworthy.

This scheme offers a great deal of privacy, since there is effectively no difference between messages sent by any vehicle. Indeed, as all messages are signed by the same key, it is impossible to link a message to a vehicle without the benefit of some auxiliary information. It also achieves Robustness as there is only one key, so there is little need for updates from the network. However, the tradeoff here is a very fragile Authenticity guarantee. Should a malicious individual obtain the key (perhaps by reverse-engineering the OBE), there is no way to renew security – effectively all vehicle transmissions become suspect.

3.2 Unique Key Authentication

An alternative approach would instead hardcode a single distinct (signing) key in each vehicle. This approach could provides both Authenticity and Robustness. However, it reduces Privacy, as vehicles are simple to differentiate. However, this means that the system is now able to identify misbehaving vehicles, and updates (revoking specific vehicles) from the network are feasible provided that keys are reasonably sized.

3.3 Rotating Key Authentication

Some proposals, including the Security Credential Management System (SCMS) – a proposed U.S. system for authentication in vehicle to vehicle networks (Hehn et al., 2014) – provision each vehicle with many distinct keys, which can be rotated as the vehicle proceeds. Provided the number of keys is sufficient, this reduces the probability that a single vehicle will be identifiable from the key or authentication data. (Effectively, each distinct key appears as a separate vehicle.) This way vehicles can be distinguished, but still difficult to track.

At present, the only proposals that are close to deployment (*e.g.,* SCMS) use the *rotating key* approach. In the next section we discuss one of these proposals in detail, and illustrate the limitations of this approach.

In most PKI implementations, each user only has one certificate, which it sends with every message. Since the same certificate will be included in all messages with a specific party, this leads to a privacy concern: these messages can easily be linked together. Unfortunately, in V2V communications this risks that distributed radio receivers could link messages together and thus reconstruct the path of individual vehicles as they move around a city.

4 CASE STUDY: LIMITATIONS OF THE ROTATING KEY PARADIGM (SCMS)

SCMS uses a PKI infrastructure to authenticate messages transmitted by vehicles. However, the system incorporates several mechanisms to enhance the system's privacy guarantees. We summarize these below:

Using many certificates for each vehicle. Rather than assigning one long-term certificate to each vehicle, SCMS provisions each transmitter with several thousand distinct and unlinkable certificates. Vehicles are expected to "rotate" certificates periodically, ensuring that the same certificate (and public key) is not used for a long time. Certificate rotation changes the identifying information associated with the transmission, and makes it difficult to link different sightings of the same vehicle.

Ensuring certificates cannot be linked by insiders. While using multiple certificates improves the privacy of the system against outside parties, it leaves open the possibility of tracking by the authorities who issue the certificates. Consequently, SCMS breaks the public key infrastructure into two distinct authorities in the SCMS backend, the *Pseudonym Certificate Authority* and the *Registration Authority*. *Pseudonym Certificate Authority* will only know that a vehicle is requesting certificates, but not what those certificates look like. *Registration Authority* knows what the individual certificates look like, but has no idea which certificates belong to which vehicle. Assuming the two authorities do not collaborate or share information, the resulting design protects users even against tracking by insiders.

Adversarial or unexpected behavior can be controlled. In a normal PKI system, controlling undesired behavior is handled by publishing the certificate of the offending user in a public "revocation list". However, due to SCMS's privacy properties, each user has thousands of certificates that must be revoked. Moreover, the privacy requirements of SCMS require that these certificates do not reveal the vehicle identity. To address this concern, SCMS provides two additional capabilities:

1. **Tracing.** When vehicles detect suspicious messages, it can report the behavior to a special backend entity called the *Misbehavior Authority*. Then, the SCMS entities collaborate to perform a tracing procedure to find the vehicle that sent the offending message. These entities can also obtain a 'seed value' that can link all of the certificates of this vehicle.
2. **Revocation.** Once the Misbehavior Authority identifies an offending vehicle, SCMS can revoke

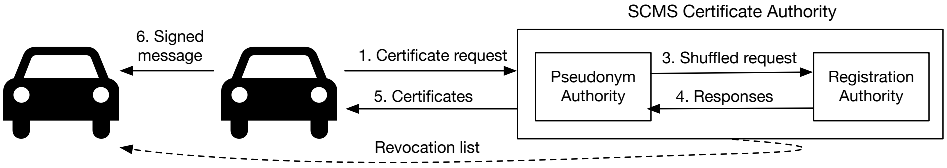

Figure 2: Overview of the SCMS Architecture.

this vehicle by blacklisting it from obtaining new certificates and notifying other vehicles not to trust communications from this vehicle. To achieve the latter, each V2V participant must be able to identify all of the certificates of every revoked vehicles. The process of revoking a vehicle reduces to broadcasting a list of expandable seed values for all revoked vehicles. Every car in the system can now examine incoming certificates to see if they contain one of the revoked serial numbers.

By only requiring one seed value per vehicle, the system hopes to provide Authenticity even with a weak connection to the network. Thus, it would also provide Robustness.

However, we will now discuss how in the designers' effort to provide all of Privacy, Authenticity, and Robustness SCMS resulted in weak amounts of each.

Weak Privacy. In order to limit the size of the revocation list, each vehicle only has about 20 valid certificates per week. Assuming certificates are rotated while driving to avoid tracing, this will lead to certificate reuse. Given that the typical U.S. driving pattern involves repeatedly traversing the same road segments (*e.g.,* while commuting) this certificate re-use can be used for linking certificates back to a vehicle and extracting information about driving behavior. The technology used for broadcasting Basic Safety Messages (BSM) is also relatively easy to eavesdrop (Reyzin et al., 2017), as it is relatively inexpensive to capture all BSMs sent by vehicles within a significant radius. This would allow a few malicious parties to amass a significant body of data about vehicles in a given geographical area, which could be further processed to de-anonymize drivers and identify individual commuter paths. Additionally, there does not seem to be any real method to prevent collusion of the various insider entities to trace vehicles. Thus, the system structure offers little benefit in return for its complexity.

Weak Authenticity. The revocation list is specified to have a fixed upper limit of about 10,000 vehicles. This means only 0.004% of the vehicles on the road can be revoked. This seems to be a drastic underestimation, and once this limit is reached Authenticity is completely lost.

Weak Robustness. The system requires vehicles to replenish their set of certificates approximately every three years. This will be a serious issue for regions that have weak or no connection to the network. A separate issue is with the revocation of certificates. If SCMS relies of user reporting for identifying misbehaving transmitters, then areas with low connectivity will have potentially long delays before misbehavior reports are filed. Similarly, vehicles may not receive up to date lists of revoked vehicles. The result being that misbehaving units pose a much more serious risk to users in low connectivity areas.

Further Hardware Limitations. Additionally, the limited hardware resources available to vehicles in the SCMS further bound the achievable amount of these properties. By increasing the number of certificates delivered to a vehicle, one could improve the privacy of the resulting system. At the same time, a larger number of certificates results in higher resource requirements at all vehicles (for both certificate storage and revocation data), and reduces the number of vehicles that may feasibly be revoked. Many of these hardware limitations result from the requirement that all vehicles will be mandated to be part of SCMS. Thus, the equipment must be cost effective to be included in the full range of vehicles.

5 ALTERNATIVE APPROACHES

We now discuss some alternative approaches that take different positions on the tradeoff between Privacy, Robustness, and Authentication.

C2C-CC. Europe has proposed an alternative to SCMS called C2C-CC (Schoch, 2012). The key difference is that there is no mandate. The service is opt-in, and likely will support only high-end vehicles that already have cellular communications built in. This frees the specification from having its hands tied supporting a broad range of hardware limits. By sacrificing Robustness in this way, the European version avoids the Authenticity and Privacy pitfalls faced by SCMS, and achieves better amounts of both.

Advanced Cryptographic Techniques. There are existing cryptographic techniques that solve many of SCMS's issues. Anonymous Credentials (Camenisch and Lysyanskaya, 2003) allow for authentication without having to reveal the entire certificate. Thus a single certificate can be used repeatedly without risk of linkage. Group signatures (Boneh et al., 2004) allow any member of a group (i.e. vehicles participating in V2V) to prove group membership without revealing which member is actually doing the signing. Both of the above technologies support having a trusted party able to trace and revoke users. Unfortunately, usage of these tools requires generous hardware resources and still require occasional network connectivity.

Content-based Filtering. An alternative to cryptographic authentication is to instead filter incoming messages by examining their content, and comparing this to other data received directly at the vehicle's sensors. One could consider this approach as applying a form of spam filtering to incoming messages. In this paradigm, messages would be given a score ranking them by credibility, and then actions would be taken based on this score. This approach could complement an existing authentication system, with authentication data passed to the scoring system as one form of input. In practice, this approach is likely to prove necessary even if cryptographic authentication is widely deployed. We believe that automakers and researchers should focus on designing these systems.

5.1 Summary of Schemes

Figure 3 offers a illustrated summary of the tradeoffs made by the discussed authentication systems.

6 CONCLUSION

By examining various methods to provide vehicle authentication, it is clear that there is an unavoidable set of tradeoffs. Thus, we must accept that no proposed system will be perfect. It is our opinion that Privacy cannot be compromised on, as Intelligent Vehicle systems have the potential to expose a dramatic amount of personal information for all citizens. It is very likely that resulting systems will then have to compromise on Authenticity.

Our fundamental takeaway is that *regardless of which cryptographic system we choose*, intelligent vehicles will have to carefully weigh the trustworthiness of messages that they receive and not depend heavily on the authentication data. More succinctly, the only data that can be trusted safely is that which comes from a vehicles own sensors. Trusted agencies may be able to pin certificates into vehicle equipment in order to provide some credible external information to these vehicles.

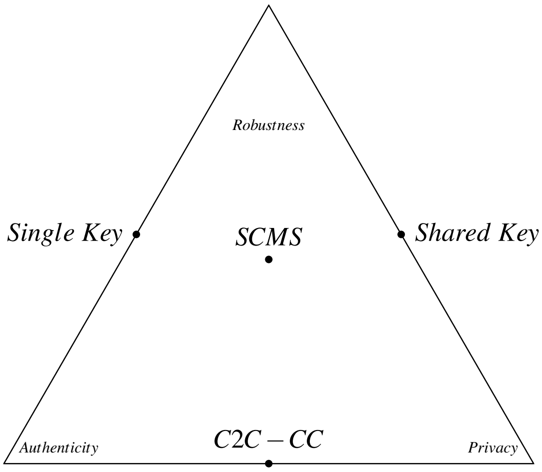

Figure 3: This figure visualizes how the different classes of systems we discussed sacrifice one property to maximize the other two, SCMS notably attempts to attain all 3 properties, but this hurts its ability to offer any of the properties. We did not include a *Group Signature* or *Anonymous Credential* based system on this diagram as it is potentially able to achieve high amounts of all 3 properties, but requires significantly more hardware resources.

Given these conclusions, we believe that the current directions in Intelligent Vehicle Communication and Authentication have serious issues. Given the high cost of these deployments and the potential risk of relying on them, we believe that widespread deployment of cryptographic authentication systems needs to postponed until more thought is given to what a reasonable model for what communication looks like. In fact, designers of these systems should operate with the assumption that authentication may not be provided. While the immediate deployment of systems such as SCMS seem to be on hold at the moment (Eggerton, 2017), it is still concerning that these problematic technologies are on the cusp of widespread implementation.

REFERENCES

Boneh, D. et al. (2004). Short group signatures. In *Advances in Cryptography—CRYPTO 2004*. Springer-Verlag.

Calandriello, G., Papadimitratos, P., Hubaux, J.-P., and Lioy, A. (2007). Efficient and robust pseudonymous authentication in vanet. In *Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '07, pages 19–28, New York, NY, USA. ACM.

Camenisch, J. and Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In *SCN '03*, pages 268–289.

Eggerton, J. (2017). Report: Trump to Withdraw Proposed V2V Mandate. Available at http://www.broadcastingcable.com/news/washington/report-trump-withdraw-proposed-v2v-mandate/169789.

Foo, E., Djamaludin, C., and Rakotonirainy, A. (2015). Security issues for future intelligent transport systems. In *2015 Australasian Road Safety Conference*, Gold Coast, Qld.

Hamida, E. B., Noura, H., and Znaidi, W. (2015). Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, 4(3):380–423.

Hehn, T. et al. (2014). Vehicle safety communications security studies: Technical design of the security credential management system. Final report, Crash Avoidance Metrics Partnership and National Highway Traffic Safety Administration (NHTSA).

Khodaei, M., Jin, H., and Papadimitratos, P. (2014). Towards deploying a scalable & robust vehicular identity and credential management infrastructure. In *Vehicular Networking Conference (VNC), 2014 IEEE*, pages 33–40. IEEE.

Khodaei, M. and Papadimitratos, P. (2015). The key to intelligent transportation: Identity and credential management in vehicular communication systems. *IEEE Vehicular Technology Magazine*, 10(4):63–69.

Khodaei, M. and Papadimitratos, P. (2016). Evaluating on-demand pseudonym acquisition policies in vehicular communication systems. In *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet*, IoV-VoI '16, pages 7–12, New York, NY, USA. ACM.

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., and Hubaux, J.-P. (2008). Secure vehicular communication systems: design and architecture. *IEEE Communications Magazine*, 46(11).

Papadimitratos, P., Gligor, V., and Hubaux, J. (2006). Securing vehicular communications-assumptions, requirements, and principles.

Pleskot, K. (2017). 2017 Cadillac CTS Now Standard With V2V Technology. Available at http://www.motortrend.com/news/2017-cadillac-cts-now-standard-v2v-technology/.

Raya, M. and Hubaux, J.-P. (2005). The security of vehicular ad hoc networks. In *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*, SASN '05, pages 11–21, New York, NY, USA. ACM.

Raya, M. and Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. *J. Comput. Secur.*, 15(1):39–68.

Reyzin, L. et al. (2017). RE: Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126).

Schoch, E. (2012). Securing Cooperative ITS: C2C-CC's Pilot PKI. 6th C2C-CC Forum.

Yousefi, S., Mousavi, M. S., and Fathy, M. (2006). Vehicular ad hoc networks (VANETs): Challenges and perspectives. In *2006 6th International Conference on ITS Telecommunications*, pages 761–766.