Review of "Secure Crash Reporting in Vehicular Ad hoc Networks"

Xiaokai He
(xiaokai@cs.tu-berlin.de)

Seminar "Internet Security" ,
Technische Universität Berlin

WS 2009/2010 (Final Version of 12th January 2010)

Abstract

Recently, VANETs have been attracted a lot of attention by academia and industry. To make the communication really useful, some people have already tried to improve safety for such implementations. The following report is based on the paper "Secure Crash Reporting in Vehicular Ad hoc Networks" by Sumair Ur Rahman and Urs Hengartner [Sumair], which is published in March 26, 2007, appeared in Proc. of Third International Conference on Security and Privacy in Communication Networks (SecureComm 2007), Nice, France, September 2007. An automated crash reporting application named AutoCore is presented in this paper. To secure this application, a security infrastructure is needed. Therefore, the concept of Road-worthiness Certificates and these certificates in a practical scheme for the distribution of cryptographic vehicle credentials issued by regional transportation authorities are used. What also been presented in this paper include a decentralized scheme for conditionally anonymous, inter-vehicle communications, support of roaming and in the end an evaluation of the security infrastructure using AutoCore. In addition, this review is not only about this particular paper, but also contains some content in some other related papers in this area. Both of the background and related work in this area and the following newer research development and trend have been mentioned. Nevertheless, some cryptosystems have also been discussed here, to accomplish different task and requirement.

1 Motivation & Introduction

1.1 Motivation

It is not rare to suffer traffic jam because of some accident. Police needs time to collect the evidence from where the accident occurred before remove all the wreckage. Moreover, lack of the information for the accident always lead to the difficulty of the judgment of responsibility. To solve these problems, make the traffic more flexible and the judgments more reliable, an efficient framework that can collect the accident information quickly during or shortly after the incident is needed.

1.2 Introduction

The paper proposed a VANET application, AutoCore, to automatically records video and telemetry data in a crash for use during an investigation. After deployment of this application, the authority could use the information collected by it to determine liability in incidents and the police is able to remove the wreckage at crash sites quickly to improve the traffic. Furthermore, this application could also help determine liability in hit-and-run incidents.
From security perspective, several topics have been discussed in this paper, like maintaining vehicle location and identity privacy, providing conditional anonymity for vehicles reporting collisions, protecting the system against various attacks and ensuring the authenticity of reported data.

2 Background Work

To date, the design of suitable MAC layer protocol for VANET is the focal point of both industrial and academic research effort in vehicular safety communication over VANETs. Vehicular safety applications studied so far include collision avoidance, cooperative driving and traffic optimization [Maxim].

2.1 Challenges & Requirements

There are some requirements that have already been pointed out [Brayn]. Such as
Authentication versus Privacy, Availability, Low Tolerance for Errors, Mobility, Key Distribution, Incentives, Bootstrap.
And some challenges those remain open has been listed in the paper [Sumair], namely:

- The task of distributing the cryptographic credentials used by vehicles to sign and authenticate outgoing messages has been ignored
- Proposed key management schemes require a centralized database for the conditional anonymity of vehicles, introducing a single point of failure
- A concrete example of how these proposed techniques could be applied to protect a particular VANET application has been missing

2.2 VANET Security and Privacy

Some of the proposed solution include: Digital signatures as a building block, Tamper-proof device, Key management, Anonymous public keys, Authenticated session establishment, DoS resilience and Verification by correlation [Maxim].

2.3 Identifying Threats

2.3.1 Adversaries

The following classes of adversaries have been listed [Brayn] in increasing order of threat:

- Greedy Drivers, a greedy driver might try to convince the neighboring vehicles that there is considerable congestion ahead, so that they will choose alternate routes and allow the greedy driver a clear path to his/her destination.
- Snoops, encompasses everyone from a nosy next-door neighbor to a government agency attempting to profile drivers.
- Pranksters, include bored teenagers probing for vulnerabilities and hackers seeking fame via their exploits.

- Industrial Insiders, Attacks by insiders are particularly insidious, and the extent to which vehicular networks are vulnerable will depend on other security design decisions.
- Malicious Attackers, deliberately attempt to cause harm via the applications available on the vehicular network.

Another classification of attacker is introduced in three dimensions [Maxim]:
Insider vs. Outsider, Malicious vs. Rational, Active vs. Passive.

2.3.2 Attacks

Some of the more likely attacks has been listed as followed [Brayn]: Denial of Service (DoS), Message Suppression Attacks, Fabrication Attacks, Alteration Attacks.

2.4 Design of a Security Framework for VANETS

Most safety application concepts follow a general pattern: Collect sensor information and broadcast vehicles own status to neighboring vehicles via routine or event safety messages. The following Applications have been listed out in 'FleeNet' [Wilfried], namely:

- Cooperative driver-assistance applications
- Local floating car data applications
- User communication and information services

Some design options has been pointed out [Maxim]:

- Each vehicle possesses a large set of certified anonymous public keys
- Keys have short lifetimes
- Pseudonyms replaces vehicle identities
- Authentication of real identities is required for liability related messages
- Police abuse can be prevented by distributing the law enforcement authority
- Secure positioning guarantees position correctness

2.5 Dedicated Short Range Communication

In 1999, the U.S. Federal Communication Commission allocated 75MHz of Dedicated Short Range Communication (DSRC) spectrum at 5.9GHz to be used exclusively for vehicle-to-vehicle and infrastructure-to-vehicle communications. 5.9 GHz Dedicated Short Range Communications for Wireless Access in Vehicular Environments (DSRC/WAVE, hereafter simply WAVE), as specified in a range of standards including those generated by the IEEE P1609 working group, enables vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) wireless communications. This connectivity makes possible a range of applications that rely on communications between road users, including vehicle safety, public safety, commercial fleet management, tolling, and other operations [IEEE].

3 Cryptography Scheme

In this paper, in order to protect the system, three major cryptography schemes are used: the blind signature cryptosystems, the short signatures and the digital credentials.

3.1 Blind Signature Cryptosystems

The Blind Signatures Cryptosystems is first introduced for untraceable payments [David]. Two key digital signature systems combined in a special way with commutative style public key systems. It allows realization of untraceable payments systems, offer auditability and control with increased personal privacy together.

3.2 Short Signatures

Short digital signatures are needed in such environments as VANETs those with strong bandwidth constraints. Two most frequently used signatures schemes, RSA [Rivest] and DSA [FIPS], produce relatively long signatures compared with the security they provide. One of the short signature scheme had been introduced based on the Computational Diffie-Hellmann assumption on certain elliptic and hyperelliptic curves [Dan].

3.3 Digital Credentials

Applications that involve the electronic transfer of credentials, value tokens, profiles, and other sensitive information are quickly gaining momentum. Digital Credentials are the digital equivalent of paper documents, plastic tokens, and other tangible objects issued by trusted parties. At the same time, they are much more powerful than their physical counterparts. Digital Credentials also provide much greater security [Stefan].
Anonymous credential systems allow anonymous yet authenticated and accountable transactions between users and service providers [Jan].
In vehicular security, the vehicle uses credentials issued by regional authorities via roadside access points, to get the Road-worthiness Certificates.

4 Main Contributions

4.1 AutoCore

AutoCore is an automated collision reporting application. It established the connection between following concerned entities:

- Drivers
- Governmental Transportation Authorities
- Courts of Law
- Law Enforcement Authorities
- Roadside Access Point Operators

The System consists of control software, secure storage and a software interface to onboard positioning, imaging and telemetry sensors. The necessary components of the system include a Tamper-Prof Device (TPD), a positioning system such as Differential GPS, cameras and a WAVE-like communication interface for inter-vehicle and vehicle-to-infrastructure communication.
In such an application, the vehicles are divided into two classes, Primaries and Witnesses. They send two types of messages, Collision Beacons and Witness Beacons. Collision reports are delivered to law enforcement authorities by Witnesses.

4.2 Threat Model

Two kinds of the threat that the application mentioned before has to face are listed below.

4.2.1 Privacy Threats

Privacy here means conditional anonymity. Vehicles broadcasting VANET application messages cannot be tracked or identified, while accident investigators remain able to identify vehicles in case of an accident.

- Vehicle Positioning An attacker may attempt to track the movements of a vehicle by listening to the message that it broadcasts.
- Vehicle Identification Driver expects to be identified only when they are within visual range. The ability to track the movements of a vehicle without seeing it is considered a violation of privacy. [Zimmer]
- Leaked Collision Report Data Collision Report Data should not be viewed by unauthorized entities. It would be considered a privacy violation if low enforcement authorities, other drivers, roadside access points or the GTA could freely view the reports.

4.2.2 Security Threats

Here we give the definitions of some of the securing threats mentioned above.

- Denial of Service:
  An adversary could overwhelm vehicles by flooding them with false application beacons, rendering the communication channel, AutoCore and any other dependent applications useless. Nevertheless, a GTA's certificate refresh services can also be attacked by flooding garbage data. What also has been mentioned is signal jamming, the most basic type of attack in almost all VANET security literature. The adversary can simply jam the communication channel used by vehicles and RAPs, rendering any dependent applications useless and preventing critical information from reaching vehicles and RAPs.
- Message Suppression:
  A driver either physically disables his inter-vehicle communication system or modifies the application to prevent it from either sending or responding to application beacons.
- Message Fabrication/Alteration:
  A prankster might fabricate or replay altered messages to force on-scene vehicles into recording collision data. Would result in bogus data being collected by vehicles and making its way up to law enforcement authorities, wasting valuable communication, processing and storage resources.
- Key/Certificate Replication:
  An adversary would seed to undermine the system by replicating a single vehicle's identity across several vehicles. Can confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents.
- Rogue Roadside Access Points (RAP):
  A rogue RAP could compromise the authenticity of collision reports, because AutoCore makes use of RAPs as CRCs for the delivery of this data. It can prevent law enforcement authorities from obtaining necessary evidence for an investigation or leak valid vehicle credentials.

4.3 Security Infrastructure

Here described how to use a TPD to store secret data and protect the integrity of AutoCore software in vehicles. And also each of the four types of cryptographic elements used by this infrastructure and an efficient scheme for the roaming of vehicles.

4.3.1 Tamper-Proof Device

Protection of sensitive data stored in vehicles. Similar to a Trusted Protection Module (TPM), the device is passive, it can generate key pairs and perform signing operations, but does not run software. A TPD guarantees that the generated private keys never leave the device. TPDs contain sensors that can detect tampering and erase all the sensitive information protected by the device. It resists not only software-based attacks, but also hardware-based attacks. However, the exact design of a TPD is still defined as a future research.

4.3.2 Certificate Authorities

There are several certificate authorities can support the infrastructure, like following:

- Vehicle Manufacturers: Vehicle Identifier Number (VIN)
- Governmental Transportation Authorities: Electronic License Plates, Anonymous Credentials

4.3.3 Vehicle Identifiers

To uniquely identify vehicles, a identifier consists of a signing key pair (VID_{Pu}, VID_{Pr}) and a corresponding certificate VID_{Cert}, which contains information uniquely identifying the vehicle and that binds this information to the vehicle's public key VID_{Pu} has been used.

4.3.4 Road-worthiness Certificates

$RoadWorthy_{cert}$ is issued to a vehicle by its manufacturer or authorized inspection authorities, to prove that the vehicle has been inspected and approved for road-worthiness.

4.3.5 Electronic License Plates

ELPs serve the same purpose as physical license plates. ELPS consist of a signing key pair (ELP_{Pu}, ELP_{Pr}) and a corresponding certificate ELP_{Cert}, which binds the vehicle's VID_{Pu}, contained in VID_{Cert}, to its public key ELP_{Pu} under a digital signature produced by the vehicle's home GTA. The certificate is valid for the duration of the vehicle's registration, and there is also a renew protocol for ELP be introduced in the paper.
The renewal protocol for ELPs is showed in Figure 2 [Sumair].

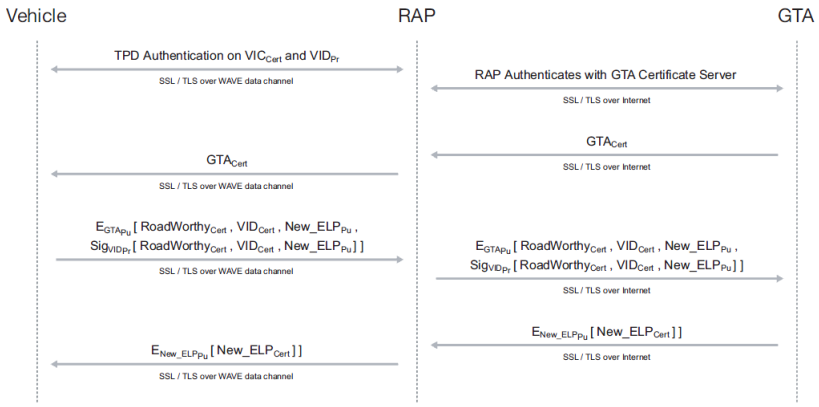

Figure 2: Protocol for the renewal of ELPs

4.3.6 Anonymous Credentials

Anonymous Credentials consist of a signing key pair $(AnonCred_{Pu}, AnonCred_{Pr})$ and a certificate $AnonCred_{Cert}$ covering $AnonCred_{Pu}$. The certificate is issued by a GTA and contains no public information that could be used by an unauthorized observer to identify the vehicle. Vehicles will possess a set of Anonymous Credentials and use the signing key $AnonCred_{Pr}$ of a credential to sign outgoing AutoCore messages. The corresponding certificate $AnonCred_{Cert}$ accompanies such a message. To avoid tracking of a vehicle based on $AnonCred_{Cert}$, the vehicle changes credentials often using a variable-frequency key changing algorithm.
To ensure the conditional anonymity of vehicles, a blind signature scheme is used for the certification of Anonymous Credentials by GTAs. The Advantage of this scheme is that a GTA cannot learn a vehicle's $AnonCred_{Pu}$'s while being ensured that the vehicle's identity can be recovered.
The renewal protocol for Anonymous Credentials is showed in Figure 3 [Sumair].

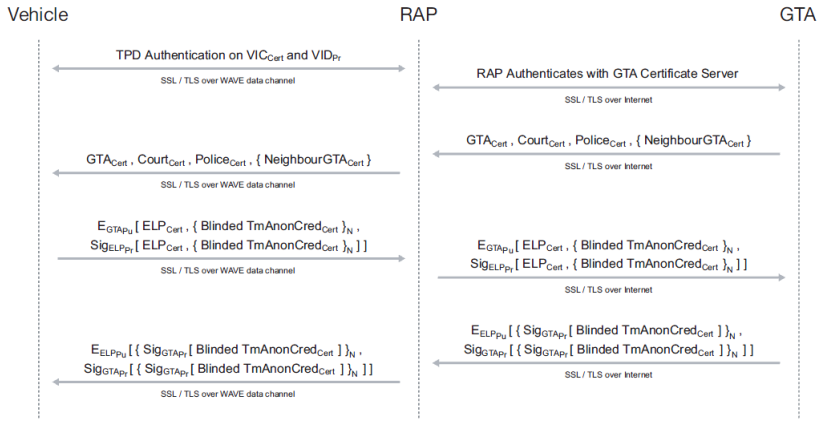

Figure 3: Protocol for the renewal of Anonymous Credentials.

4.3.7 Travel between GTA Jurisdictions

To extend the scheme to allow vehicles to communicate with vehicles and infrastructure certified by other GTAs, enabling communication while traveling outside the home GTA's jurisdiction is necessary. This is somehow like the roaming topic in wireless communications, vehicles need to acquire the Anonymous Credentials from a Foreign GTA. And the Foreign GTP should be capable to verify the old Anonymous Credentials from the Home GTA of the vehicles. There should also have some kind of registration mechanism when the vehicle approaching the border of the next GTA.
Including $HomeGTA_{Cert}$ in messages increases overall message size. In case the communication channel is congested, a Vistor could add $HomeGTA_{Cert}$ only to a subset of its sent messages.

4.4 Securing AutoCore

Describes how to used the security infrastructure to protect AutoCore communications.

4.4.1 Securing Inter-Vehicle Communications

Here we use Anonymous Credentials which has introduced before, to ensure the authenticity of AutoCore messages and guarantee non-repudiation of these messages. The

method here is Anonymous Credentials.

4.4.2 Securing Vehicle to Infrastructure Communications

Communication between vehicles and infrastructure is required for the delivery of data. This kind of communication is secured using standard mutual authentication and secure data transfer protocols, such as SSL/TLS [RFC] with client authentication.

4.4.3 Securing AutoCore Collision Reports

In order to guarantee the integrity of the collision reports and prevent the abuse of information contained in them, two processes have been used here. One is the certificate of the Anonymous Credentials, which is issued by government. The other is the public key which is issued by police. This insured the report is readable, only both of these departments think it's necessary.

4.5 Security Analysis

Analysis if the system has met the following requirements:

- Authentication
  All messages produced by vehicles are signed with their current $AnonCred_{Pr}$ and authenticated using the corresponding $AnonCred_{Cert}$.
- Data Consistency
  In AutoCore, data consistency is provided by having AutoCore correlate Collision Beacons with sudden braking or a sudden change in direction by the host vehicle. In addition, if more than one vehicle equipped with AutoCore is involved in a collision, it is possible to correlate Collision Beacons sent by these vehicles by checking the timestamps and locations included in the messages.
- Non-repudiation
  A vehicle cannot claim to be a different vehicle, because it signs messages with its own private keys.
  A vehicle cannot deny having sent messages because a message is signed with $AnonCred_{Pr}$, which belongs to the vehicle and was generated by the vehicle in the first place. Timestamps included in each message guard against message replay attacks.
- Privacy
  In this solution, vehicles send messages in an anonymous way, which defends against vehicle identification or positioning attacks. However, this anonymity is conditional, that is, in the case of an accident, it must be possible by authorities to revoke this anonymity.
- Real-time Constraints
  This aspect depends on choosing a suitable cryptosystem for each of the cryptographic elements.

4.6 Choice of Cryptosystems

To reduce overhead, cryptosystems with short signature and key sizes are needed. ECDSA is chosen for most of the signing key pairs, and BBLS, blind signature scheme based on the BLS short signature scheme is used in signing key pair used by GTAs for certifying Anonymous Credentials. Elliptic Curve Integrated Encryption Scheme (ECIES) is chosen for encrypting a car's identity.

For ECDSA, a public key size of about 20 bytes is chosen, which results in signatures of 40 bytes. For BBLS, a public key size of about 75 bytes is chosen, which results in signatures of size about 25 bytes. For ECIES, a public key size of 20 bytes has been chosen. All these choice of key sizes had been tested in experiments, that they result a reasonable delay, which stay in the board of Real-time Constraints, and meanwhile, also provide a protection for the AutoCore that strong enough.

5 Follow-up Work

Since this paper is not only related to "secure crash reporting", which has not so many work followed, but also focus on the common topic in security field in VANETs, it's helpful for us to have a look at what happened after that.

5.1 Tradeoff between Privacy and Accountability

One of the important issues in this area is the tradeoff between the privacy of the drivers and the accountability of misbehaving vehicles.

5.1.1 Privacy-Preserving Protocols for VANETs

This protocol has been introduced by Mike Burmester [Mike] to balance the tradeoff between privacy and accountability in a VANE. Both pairwise and group communication among vehicles in the network and communication between a vehicle and the road infrastructure has been considered. They use symmetric and public key operations with help of a frequency changed pseudonyms to protect the communication.

5.1.2 Secure and Efficient RSU-aided Privacy-Preserving Protocol

For reduced the heavy signature and authentication overhead caused by asymmetric cryptography, they tried to take advantages in using symmetric cryptography and build another protocol [Xiaodong].

5.2 Data Verification

There are two kinds of data verification been introduced by Soyoung [Soyoung] : Two-directional data verification and Time-based data verification for reliable regional traffic data propagation.
The two-directional data verification approach uses vehicles in both driving directions of a two-way road as two separated media channels. A traffic message will be transmitted through both channels. A recipient vehicle verifies the message integrity by checking if data received from both channels are matched. This approach exploits the fact that it is difficult and costly to have two collaborative vehicles on both driving directions in the same region.
The time-based data verification approach only uses vehicles in the opposite driving direction to propagate a traffic message by first issuing its public key commitment and later the actual traffic message. It relies on the time delay between these two messages and the mobility of vehicles to protect data integrity.

5.3 Other Aspects

Such topics like performance enhancement, secure VANET-based road traffic control system and secure VANET-based toll collection system have also been discussed.

6 Conclusion

The paper is well thought out and described many aspects of the security area in VANETs. It pointed out the main problem and tried to solve them in an application that use several techniques. It focused on the secure crash reporting system, but contributes here is not only useful for this scenario, but also for the other scenarios in VANETs. During reading this paper, I have also collected some other related information from other paper, to make it clear, how the security in VANETs has been concerned more and more, and how the old ideas being improved and new ideas come up. This paper has also included a set of typical cryptosystems, which can also use in other applications.

References

[Sumair] Sumair Ur Rahman, Urs Hengartner: *Secure Crash Reporting in Vehicular Ad hoc Networks*;

[Brayn] Brayn Parno, Adrian Perrig: *Challenges in Securing Vehicular Networks*;

[David] David Chaum: *Blind Signatures for Untraceable Payments*;

[Maxim] Maxim Raya, Jean-Pierre Hubaux: *The Security of Vehicular Ad Hoc Networks*;

[Mike] Mike Burmester, Emmanouil Magkos, Vassilis Chrissikopoulos: *Strengthening Privacy Protection in VANETs*;

[Soyoung] Soyoung Park, Cliff Zou, Damla Turgut: *Reliable Traffic Information Propagation in Vehicular Ad hoc Networks*;

[Xiaodong] Xiaodong Lin: *Secure and Privacy-Preserving Vehicular Communications*;

[Zimmer] M. Zimmer: *Personal Information and the Design of Vehicle Safety Communication Technologies*;

[Dan] Dan Boneh, Ben Lynn, Hovav Shacham: *Short Signatures from the Weil Pairing*;

[Wilfried] Wilfried Enkelmann: *FleetNet - Applications for Inter-Vehicle Communication*;

[Stefan] Stefan Brands: *A Technical Overview of Digital Credentials*;

[Jan] Jan Camenisch, Els Van Herreweghen: *Design and Implementation of the idemix Anonymous Cerdential System*;

[IEEE] IEEE Std 1609.2^{TM} – 2006: *IEEE Trial-Use Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages*;

[RFC] Network Working Group Request for Comments: 5246: *The Transport Layer Security (TLS) Protocol Version 1.2*;

[FIPS] FIPS PUB 186-3: *FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION Digital Signature Standard (DSS)*;

[Rivest] R.L. Rivest, A. Shamir, and L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*;