A NOVEL MODULAR BLACK-BOX ARCHITECTURE FOR SECURE VEHICULAR NETWORKS

M'hamed Chammem, Mohamed Hamdi and Noureddine Boudriga
Communication Networks and Security Research Lab., Sup'Com, University of 7th of November, Carthage, Tunisia

Keywords: VCS, Black-box, Investigation process, Information privacy, Secure access, Authentication.

Abstract: The emerging technology of vehicular communication systems (VCSs) raises a number of technical challenges that need to be addressed. Particularly, security ranks at the top of these challenges. In fact, the plethora of services that can be provided using VCSs introduces new communication scenarios that require special security services. This paper tackles the problems related to the storage of the evidences related to onboard security architectures. A special emphasis is made on the management of the events related to the features and history of the vehicle. In this context, a new black-box architecture is proposed. It consists in two basic modules: a main black-box and an auxiliary black-box. We show that this separation allows a better classification of the data records supported by the block-box. The interaction of the black-box with the other components of the VCS is also discussed. Due to the sensitivity of the event records, the input data flows pass necessarily through a security module which performs some key functions including event timestamping and security policy management. A specific public key infrastructure is also proposed to support our secure VCS architecture.

1 INTRODUCTION

The recent proliferation of the applications of Vehicular Communication Systems (VCSs) has been mainly rendered possible by the development of embedded electronic systems and wireless communication infrastructures. The particular features of vehicular networks mainly stem from the nature of the parties involved in the communication and also from the properties of the data. In fact, the entities that are part of a vehicular communications system are private and public vehicles, the road-side infrastructure, and authorities (the latter component being composed primarily as network entities). An authority will be responsible for the identity and credential management for all vehicles registered in its region (e.g., national territory, state, canton, metropolitan area), similarly to what is currently the case. Public vehicles (e.g. police cars) may have specific roles and be considered as mobile infrastructure.

This complex context raises two major security-related challenges: (a) the secure storage of the event records related to the different applications the vehicle is involved in and (b) the simultaneous provision of privacy guarantees and strong authentication mechanisms. The analysis of the different incidents that a vehicle can be subject to (e.g., crashes, thefts, masquerading) strongly depends on the solutions one can find for these challenges. The characteristics of VCSs make it difficult to manage the event records since these can be related to the applications in which the vehicle is involved or to some key manufacturing tasks. The event records should also be generic enough to be supported by the different actors involved in VCS transactions.

In this paper, we propose a new black-box architecture that supports the management of complex evidence records emanating from the different components of the VCS. It includes two major modules: the main black-box and the auxiliary black-box. The first is used to store highly-sensitive data that are intrinsic to the vehicle while the latter rather serves for the preservation of event records related to the applications to which the vehicle participates. A security unit is also devised to support the implementation of sophisticated operations including data timestamping and security policy management. According to the application of interest, appropriate access modes and privileges are granted to the authorized entities. Furthermore, a lifetime is defined for every event record category

Chammem M., Hamdi M. and Boudriga N. (2010).
A NOVEL MODULAR BLACK-BOX ARCHITECTURE FOR SECURE VEHICULAR NETWORKS.
In *Proceedings of the International Conference on Data Communication Networking and Optical Communication Systems*, pages 93-103
DOI: 10.5220/0002989400930103

depending on the sensitivity of the corresponding application. A Public Key Infrastructure (PKI) is developed to support the implementation of the proposed security architecture. A particular interest is given to the simultaneous provision of authentication and anonymity services.

The major contributions of the paper are given in the following:

1. The black-box concept is generalized to encompass the storage of data originating from various applications while it has been used, in the existing approaches, only to monitor incidents and crashes.
2. The consideration of two black-box modules (main black-box and auxiliary black-box) is suitable with the segregation of duties concept since the main black-box is accessed only by the manufacturer and the authorities mandated to perform post mortem investigation while the auxiliary black-box can serve to store data related to various applications.
3. The proposed vehicular PKI guarantees both authentication and anonymity services. It is also used to timestamp important events. It relies on simple operations, which makes it suitable with the computational and memory capabilities of the VCS components.
4. We address a case study showing how our system can be used in complex contexts (i.e., fleet management) to monitor various parameters ranging from the driver behaviour to the events that can occur to the vehicle.

The rest of the paper is structured as follows. Section 2 reviews the existing researches that have addressed the implementation of black-boxes for vehicular applications. We highlight the factors that make vehicular black-boxes different from those used in airplanes. Section 3 explores a set of typical applications that can be deployed on the basis of VCSs and sets the basic security requirements for these applications. Section 4 presents the secure black-box architecture that constitutes the core of our contribution. A functional description of the main modules and data flows is given in this section. Section 5 describes the PKI we introduced to support the security services related to the new black-box module. A case study illustrating the functionalities enabled by our black-box system is discussed in Section 6. Finally, Section 7 concludes the paper.

2 RELATED WORK

The black-box is becoming a mandatory component in modern vehicles. It can store a lot of useful parameters to analyze for possible investigation (Qiang Wu, et al., 2008). However, the functions implemented on the black-box are not enough sophisticated.

In Qiang Wu, et al., 2008, a vehicular black-box architecture is discussed. The architecture of the developed system can record and store analog video sequences compliant to H.264 only when the acceleration exceeds a limit value. When the car operates in normal conditions, the system does not record any information since the risk of traffic accidents is limited. However, if an emergency occurs, the system will start the video encoding and stores a series of H.264 files.

The block diagram representing this black-box is given in Figure 1. Apart from the camera and video decoding device, we observe the 3-axis accelerometer and a memory function. It should be noticed that the security functions has not been accurately addressed in this paper.

Since most of the black-box approaches that have been proposed in the literature for VCSs rely on Event Data Recorders, we accurately discuss this concept in the following subsection.

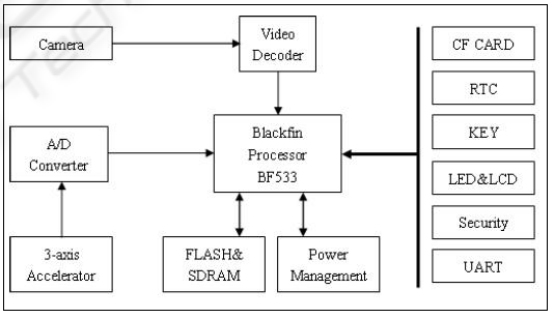

Figure 1: System block diagram of black-box, (Qiang Wu, et al., 2008).

2.1 EDR-based black-box Approaches

The integration of Event Data Recorders (EDRs) in a number of recently manufactured vehicles presents a different perspective on the assessment of the validity of passengers risk based on the Acceleration Severity Index 'ASI' (Gabauer, D.J., and Gabler, H.C., 2005). EDRs are capable of electronically recording data such as vehicle speed, brake status and throttle position just prior to and during an accident. The ability of EDRs to document the deceleration of a vehicle during a collision event is of particular interest. Another interesting feature

developed in this study is the ability of EDR to record the velocity profile of the vehicle during a collision event.

Other approaches rely on EDR technology to investigate the correlation between the ASI threshold limits and the potential for passenger injury in crash events. Gabauer, D. J., and Gabler, H. C., (Gabauer, D. J., Gabler, H.C., 2005) investigate a relationship between the ASI and injury to airbag-restrained occupants and has established a methodology for future studies.

Today, the complex computer systems in vehicles can store huge amount of data. The concept of black-box has been used for a long period in aircraft monitoring for recording information in the few minutes before a crash.

For years, this same concept has been widely used in the automotive field including crash investigation and accident scenario reconstruction (The Florida Senate, 2009 and Deborah Sapper et al., 2009).

In most vehicles, the EDR module is located in the airbag control module. The objective of this module is to monitor the crash scenarios and to deploy the airbags if needed. This module also contains several accelerometers. The EDR will record about five seconds of pre-crash data per type of vehicle. These data include vehicle speed, acceleration / deceleration, engine speed...

The EDR will also record the crashing phase, assessing different parameters every five milliseconds before impact. These data can be analyzed to calculate many parameters including the crash duration and impact velocity (Hampton C. Gabler and al., 2004).

Despite the abundance of the literature having addressed the EDR concept, several severe drawbacks can be noticed (Aleecia M. McDonald, Lorrie Faith Cranor., 2006):

1. The stored data are not structured according to their sensitivity making them viewable to everyone that accesses the black-box. This is not convenient to the real context where the vehicle is involved in many applications generating data with different security levels. The fact that the EDR is monolithic can be at the origin of confidentiality and privacy violations if the usage of the black-box is generalized to the monitoring of miscellaneous services.
2. The entities storing data into the EDR are not authenticated. Similarly, the stored events are not timestamped. These two facts prevents the use of the stored data as legal proofs. Cryptographic functionalities should be enabled on the EDR in order to ensure the authenticity and the integrity of the data retrieved by the event analyzer.
3. The data stored into the EDR are not prone to automated analysis. They present relevance only to experts that can decode appropriately these data. This constitutes a serious limitation since even the owner of the vehicle is unable to exploit the information stored in the corresponding black-box. Consequently, the usage of the black-box is confined to the analysis of serious incidents while it can be used for the storage of less harmful events such as the profiling of the driver behaviour or the vehicle state.

2.2 Black-box usage in Modern Vehicles

Black-boxes have many applications in vehicular networks. The most relevant usages of this technology are listed below.

1. Investigating accidents and crashes: The data recorded by EDR or the black-box just a few seconds before a crash are usually exploited by experts in the investigation process to delineate responsibilities and evidences. The recorded parameters are mainly related to vehicle speed, acceleration, braking, timestamp...
2. Training young drivers: Clemens Kaufmann and Christine Tureschek., (Clemens Kaufmann, Christine Tureschek., 2008) has a particular operating data recorded for evaluating the performance of young drivers during training sessions. This practice seems to be very helpful for improving driver training.
3. Detecting unauthorized modification of odometer parameters: Changing the odometer parameters reading is a crime that is unfortunately becoming a widely-performed practice. Some vehicle owners are not immune to this temptation. Black-box can provide proofs to ensure that the mileage is correct.
4. Detecting unauthorized modification of VIN: A unique identification number of vehicle (VIN) is assigned to each car. It is a unique identifier of 17 characters, defined by an international standard that identifies a vehicle uniquely. The bodies of law enforcement use these serial numbers to identify and retrieve cars or car parts that have been stolen. Automobile manufacturers use the VIN as part of safety recalls. The character identification number (VIN) can be considered as part of the black-box to indicate the vehicle manufacturing data, model, location of manufacture, and possibly more. The decoding of this issue is the process of deciphering that information. The VIN is also

used to access a report on the vehicle history (Carfax, 2010). Each report issued by CARFAX contains important information that can influence the decision of whether to buy a used car.

5. Addressing special needs: The use of vehicles by governmental poses specific problems and therefore requires careful management of the vehicle's history including the presence of multiple drivers per vehicle. Some information available in the black-box can allow the identification the behaviours of drivers and their parameters such as speed, acceleration, shock. The exploitation of such information can help in fleet management car (e.g., government, fire-fighters, rent) to better understand the history of cars.

2.3 Intrinsic Features of the Vehicular Black-box

Black-boxes have been widely as part of airplane security systems to store reliable proofs and evidences that can assist in investigation processes. The extension of this concept to the VCS context requires substantial modifications due to the particular characteristics of vehicular networks. In the following, we give the most important features of vehicular black-boxes.

1. The qualifications of the driver or driver are completely different. The drivers like the drivers of trains and boats have training and qualifications. They all have predispositions to drive in and drive safely.
2. Regulating the operation of airplanes, trains and boats is generally governed by national and international laws. This implies that maintenance procedures of equipment and safety procedures that tend toward universal repositories. Driver of the car does not have comparable qualifications to the requirements of the aerospace or marine. Cars drive on city streets, semi-urban areas and motorways. The space evolution of cars is particularly dynamic in terms of the evolution of other cars, pedestrians, etc.
3. Research and development of black-box for vehicles for over forty years, have provided some solutions including the implementation of electronic systems called 'Event Data Recorder'. The EDR is used to investigate in cases of traffic accidents and delineate the responsibilities of different actors involved in the accident.
4. Many countries do not exploit the data recorded by the EDR in accidents. It is important to note that many new cars contain an EDR is close to 100% (registered in 2009/2010).
5. Electronic systems in the car are seen by many drivers and users of the car, like electronic gadgets and not as professional solutions for driver assistance contrary to the perception of electronic systems of the aircraft, boat or train. The reliability of components and electronic systems is widely approved.
6. The vehicular system actors are many: manufacturer, vehicle owner, insurance, mechanic, engineering services Transportation (technical inspection), police, customs...
7. Manufacturers of cars tend to increase vehicle safety through two approaches:
   a. Enhanced Passive Safety: Passive safety for all that, the vehicle is designed to avoid serious injury (or death) to the driver and passenger of a car during an accident (e.g., reinforcement box, airbags, security belt)
   b. Enhanced active safety Active safety is everything in the vehicle and around the vehicle is designed to avoid the accident in automotive technology: electronics (ABS, ESP(electronic stability control), BAS - BAS • Traction...)
8. Many development ideas of black-box for vehicles. The basic idea is to capture a few seconds of data before and after the shock (the crash).
9. The vehicles of tomorrow must be designed to combine the active and passive safety (figure 2). The efficiency of passive safety systems are beginning to reach saturation. In contrast, active safety systems promote the potential of significantly improving the effectiveness of vehicle safety. Significant improvements can be obtained by combining the systems of active and passive safety (Claudia Kratzsch, Heidi Kroemker., 2009).

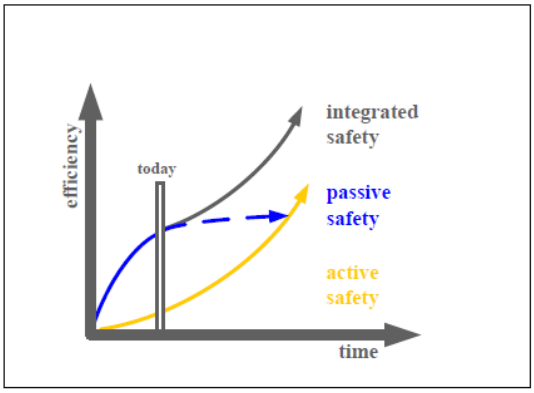

Figure 2: Efficiency of Integrated safety approach (Claudia Kratzsch, Heidi Kroemker., 2009).

3 SECURE ARCHITECTURE FOR VEHICULAR NETWORKS

In M. Chammem et al., (M. Chammem et al., 2009), we proposed a secure VCS architecture depicted in figure 3. In this section, we describe the components of this architecture and investigate the potential services that it can provide. We also set the basic security requirements for these applications.

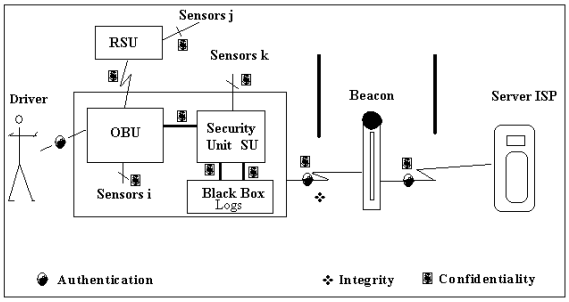

Figure 3: General architecture (M. Chammem et al., 2009).

3.1 Secure VCS Architecture

The key components of the secure VCS architecture developed in (M. Chammem et al., 2009) are cited in the following.

Sensors: A set of sensors gathering various information about the external and internal environments of the vehicle are part of the communication system. The data provided by these sensors mainly serves not only to monitor the behaviour of the driver and the vehicle but also for the implementation of computer-assisted decision making systems inside the vehicle.

Onboard Unit (OBU): This component implements most of the computational tasks required to deploy the applications of the VCS. It generally consist of one or more processors or microcontrollers interacting through various specific bus technologies such as CAN(Controller Area Network), VAN, (Vehicle Area Network), LIN (Local Interconnect Network), FlexRay, MOST.

Security Unit (SU): The security policies related to the different actions related to the services involving the vehicle are managed by the SU. This component can be used to build trust relations between the components involved in vehicular transactions. It supports advanced security functionalities related to cryptographic protocols (e.g., PKI, anonymous certificates) and security policy management.

Black-Box: It is mainly used to store the proofs and evidences related to various vehicular transactions in a secure environment. It should implement appropriate policies in order to cope with the heterogeneity of the evidences that can relate to the driver behavior (e.g., payment receipts, velocity excess) or the vehicle state (e.g., incidents, identity modification)

Road Side Unit (RSU): The RSU acts as a relay between the driver, the vehicle, and the environment. It often consists in a data gathering and communication system related to the environmental data (e.g., traffic, atmospheric conditions, available services). It can also serve to advertise for some services and applications. Other possible usages of RSU are emergency handling and assisted driving.

Beacon: Performs the same functionalities as the RSU but it is resource-impoverished. The usage of beacons is often limited to detection and localization services.

Application and service provider (ASP): Various services can be provided on the basis a VCS. ASPs can be the source of various data such as news, multimedia content, location information, and advertisements.

3.2 Short-range and Long-range Communication Media in VCSs

Modern vehicles are increasingly relying on electronic devices to access/provide secure services across public communication networks. At the vehicle level, specific buses are used to ensure local communication between the various devices. Additional devices are also included into the vehicle so that it can communicate with other entities belonging to the VCS.

In the following, we review the most important bus technologies integrated in today's vehicles (Anthony Marino, John Schmalzel., 2007 and Milind Khanapurkar, et al. 2008).

Controller Area Network (CAN): developed by Bosh in the eighties. All sensors, actuators, and command devices have the same privilege level and are connected through a serial bus.

Local Interconnect Network LIN: used as an in-vehicle communication and networking serial bus between intelligent sensors and actuators. Other auto body electronics include air conditioning systems, doors, seats, column, climate control, switch panel, intelligent wipers, and sunroof actuators.

Byteflight: is used for safety-critical applications in motor vehicles. Byteflight is a TDMA (Time

Division Multiple Access) protocol that runs at 10Mbps over (2-WIRE or 3-WIRE) Plastic optical fibers in a bus, Star or Cluster configuration which provides an information update rate of 250uS.

FlexRay: is a high-speed serial communication system for in-vehicle networks using Point-to-Point links, at 10Mbps (Fault-Tolerant) over Un-shielded Twisted Pair or Shielded Twisted Pair cable. The FlexRay bus defines the Physical layer (Electrical and Optical) and Protocol. FlexRay is an extended protocol version of byteflight. Applications for FlexRay include; steer-by-wire and brake-by-wire.

Media Oriented Systems Transport (MOST): is the de-facto standard for multimedia and infotainment networking in the automotive industry. MOST defines a multimedia fiber-optic (low overhead, low cost) point-to-point network implemented in a ring, star or daisy-chain topology over Plastic optical fibers.

Long-range communication infrastructures are also required in VCSs to enable Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) data transmission. Multiple standards can be used to this purpose including Wifi, GSM, GPRS, UMTS, and WIMAX.

3.3 Security Requirements for Vehicular Communication

In this subsection, we point out the security needs related to secure service provision over vehicular networks (M. Chammem et al., 2009 and Maxim Raya et al., 2006).

- Authentication: The authentication process must verify the identity of the driver or the person authorized to drive the vehicle. Similarly, beacons should be authenticated in order to counter spoofing attacks.
- Integrity: The information and data from various sources of information should not be either altered or amended by an intruder. Relevant information from the sensors, computers OBU, RSU and SU systems and V2V and V2I communications should be protected against unauthorized modifications.
- Non-repudiation: It is important to ensure that the parties engaged in a V2V and V2I communication cannot deny that a transaction / communication took place.
- Access control: The vehicle systems are a means of transport belonging to individuals or legal entities. The possessive side is crucial. Access to systems is strictly controlled by means of increasingly secure.
- Confidentiality: The confidentiality of information must be ensured in all vehicle systems. Only authorized persons can access information, particularly in V2V and V2I communications.
- Accessibility: The vehicular systems have a long lifetime. The proper functioning of sensitive subsystems must be ensured throughout the lifecycle of the vehicle.
- Privacy: Vehicular systems are private. Their operations are governed by regulations and practices. The privacy of the driver and passengers is considered as an important aspect of security.
- Responsibility enforcement: Drivers of vehicles are fully responsible for their actions in the process of conduct. Vehicles should provide information to identify or assist in the attribution of responsibility. Authorities are generally entitled to the identification of responsibilities in case of accidents (police officers, insurance experts).
- Vehicle Tracking: The precise location of the vehicle has become useful information for vehicle safety in particular against theft and rangeland management.
- Proof and evidence management: During the movement of vehicles on roads and highways, some services require evidence to identify the vehicle in case of legal travel speed; accidents... The proof may include photography of the registration plate of the vehicle supported by a timestamp.

4 ENHANCED BLACK-BOX ARCHITECTURE FOR VCS

In this section, we introduce a new black-box architecture for VCSs. We first describe the modules constituting this black box. Then, we discuss the typology of the events that can be stored.
Figure 4 illustrates the functional architecture of the proposed enhanced black-box architecture for secure vehicular communication system. We mainly consider two black-box modules: a main black-box and an auxiliary black-box.

- Main black-box (MBB): used to store the essential parameters of the vehicle including VIN. Three data flows can be thought of to store data in this module. The first flow (1) serves to

upload the features generated at the manufacturing phase to the MMB using a privileged access. The second data flow (2) relates to events generated by the sensors embedded in the vehicle. This encompasses the information about incidents including crashes and airbag deployment. The third data flow (3) concerns the events generated by the OBU without direct human intervention. For instance, physical damages occurring on the OBU as well as driving anomalies fall into this category. It is noteworthy that all the data stored in the MBB are (relatively) timestamped by the SU without the intervention of external timestamping servers.

- Auxiliary black-box (ABB): This module is used to store data related to the applications in which the vehicle is involved. Unlike the information stored on the MBB, ABB entries have a finite lifetime and cannot excess a storage space quota. This is necessary due to the panoply of potential applications that can enrich modern VCSs. The security policies regulating the storage of these application data are also stored in the ABB. Three data flows can be considered with respect to the ABB. The first flow (4) corresponds to data that pass through the Data Recording Module (DRM) and that may originate from the application provider platform or from a local passenger. These events do not require authentication by the SU. The second data flow (5) is similar to (4) except that the stored information passes through the User Authentication Module (UAM) prior to the DRM. It is used for sensitive application and user data. The third data flow (6) concerns the security policies that are stored on the ABB. Such information must be authenticated since the addition or the modification of security policies is restricted to authorized users.

The alert reader would have noticed that the MBB and the ABB are physically separated in the sense that no communication occurs between them. This is perfectly sound since these two modules are accessible by different entities. On the one hand, write access to the MBB is hardly restricted to the manufacturer, in the initialization phase, while read access is restricted to the transportation regulation authorities, in the operating phase. A tamper-proof capability is also made available to prohibit write access through the privileged access port (even to the manufacturer) once the vehicle is in the operating phase (i.e., has passed the initialization phase). On the other hand, access modes are richer for the ABB since different scenarios, depending on the available applications should be considered. More practically, data stored in the ABB can be, for example, (partially) retrieved by the owner, a private company (in the case of fleet management), and also experts authorized by regulatory courts.

Through the previous discussion, it appears that the SU is a mandatory interface to write data into the black-box modules. Basically, the SU supports four access modes:

Privileged access: The SU enables this special mode to manage the basic characteristics and parameters of the vehicle. Privileged write access is granted only to the manufacturer, during the initialization phase, in order to store the VIN. However, read access should be possible to the entities authorized to verify the authenticity of VIN (such entities are often agencies under the control of the department of transportation).

Sensor events: Modern vehicles are richly equipped with sensors based on various technologies (e.g., temperature sensors, velocity sensors, contact sensors, light sensors). Depending on its sensitivity, the information gathered by these sensors are stored either in the MBB or in the ABB. With the development of sensing and networking technologies, a trend that will probably be developed in the near future is to inter-connect the embedded sensors.

Passenger events: Since the driver and the passengers are able to interact with the OBU, the corresponding events should be handled by the SU in order to perform authentication and timestamping procedures. Different passenger clearance levels should be defined in order to deploy access control policies to the SU according to the source privilege.

Application events: When interacting with the available applications, several event records should be stored to serve as proofs or evidences. Such records range from payment receipts to timestamping tokens. To promote fairness between the multiple applications, lifetime and space quota policies should be enforced by the SU.

In the privileged access mode, a user should be authenticated before inserting modifications to the SPMM. The possible actions that can be made:

- Add a new policy
- Modify an existing policy

A policy is defined as follows:

Security_policy = {lifetime,protection_type,access_mode}
Protecting_type:= enciphered,signed,hashed
Access_mode Є {users_class} x {read,write}
User_class:= owner | driver

The owner car associate the data related to a given application to specific security policy. The maximum

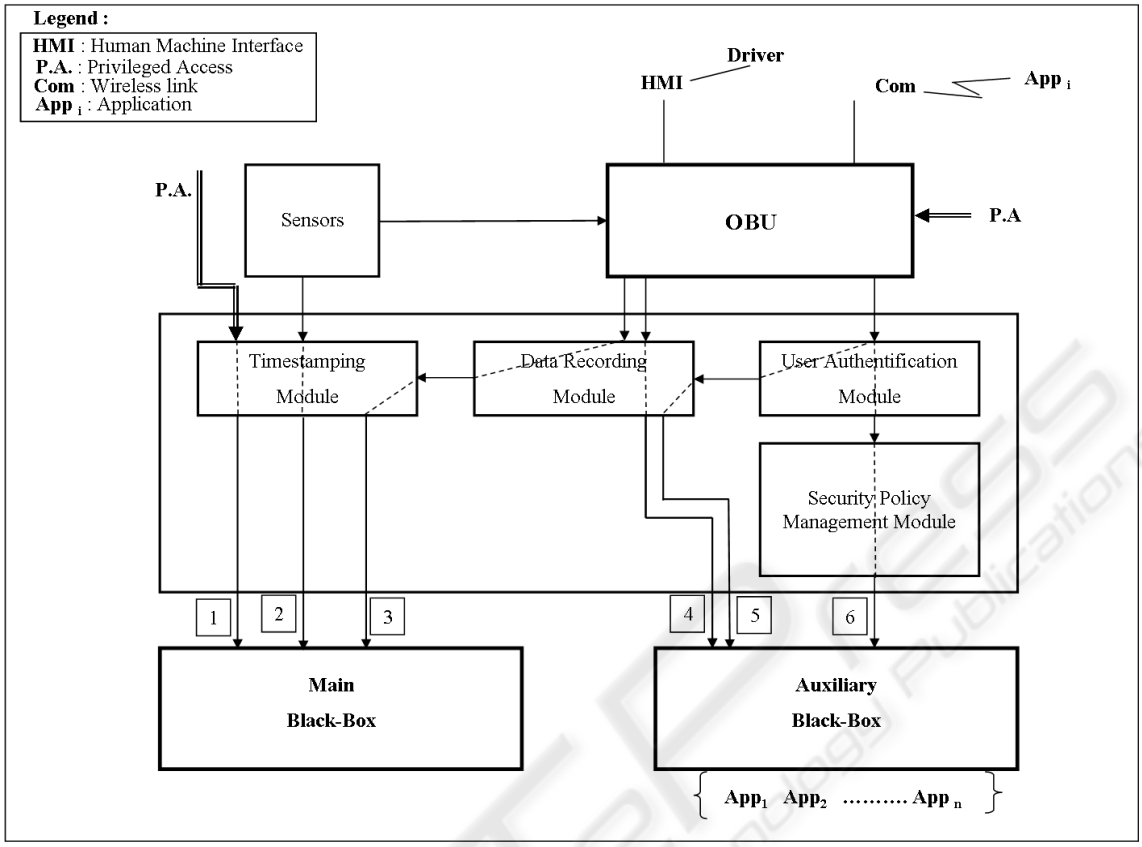

Figure 4: Enhanced black-box architecture.

storage space that can be record for this data should also be declared.

Association:= data,security_policy,storage_space

Then the record corresponding to the data of interest exceed the maximum storage space; a rotation policy is applied to preserve the most recent records.

5 VEHICULAR PKI ARCHITECTURE

Clearly, in the architecture introduced in the previous section, the black box is the focal component that will be used to look for trustable evidences regarding past events. To implement a mechanism allowing the preservation of such evidences, we introduce a new PKI that adapts to the specific features of vehicular networks. It relies on the encryption scheme proposed by Franklin and Boneh (D. Boneh and M. Franklin., 2001).

Vehicles and RSUs should be able to authenticate themselves and at the same time use disposable pseudonyms for vehicles so that their activities and communications are not tracked by parties that are eavesdropping on them. We also need to make certain that there is a verifiable trail between the pseudonyms and the real identities of the vehicle and that only a common, Trusted Authority (TA) is able to verify that trail in case of a dispute.

Unfortunately, existing PKI solutions are not convenient to our context because of the following reasons:

- Traditional PKIs are not very flexible in providing user specified levels of privacy due to rigid pseudonym (common name) assignments
- The size of the asymmetric keys used in existing cryptosystems do not allow the implementation of bandwidth-efficient protocols
- Existing signature algorithms do not allow the fulfillment of both authentication and anonymity preservation

To overcome these limitations, we propose the use of a modified asymmetric cryptosystem where public keys are substituted by arbitrary strings. The scheme proposed by Boneh and Franklin uses a bilinear map

$$\mu: \Gamma_1 \times \Gamma_1 \rightarrow \Gamma_2,$$

where Γ_1 and Γ_2 are cyclic groups of order p for

some large prime p. In particular, satisfies that $\mu(aP,bQ) = \mu(P,Q)^{ab}$ for all $P,Q \in \Gamma_1 \cdot \Gamma_1 \cdot \times \cdot \Gamma 2$ and $a,b \in \mathbb{Z}_p \mathrm{Z}^2$.

Weil and Tate pairings on elliptic curves are two fast and efficient ways of constructing such bilinear maps. In addition to encryption, we need the ability to provide non-repudiation in a cost-effective manner. In order to achieve non-repudiation with relatively meager computational requirements, we have chosen to employ a function which combines signing and encryption operations and also produces smaller ciphertext as compared to 'sign and then encrypt' strategies. Such features are not provided by D. Boneh and M. Franklin (D. Boneh and M. Franklin., 2001).

In our solution, each vehicle and RSU has a unique identifier ID_{id}. These identifiers include the designation of the entity as a vehicle or RSU; e.g. *IDv* = (*vehicle*||*identifier*). We envision that these identifiers can be certified at regular periods (say annually) by a TA. If any certificate is revoked the TA notifies all the RSUs in the system, so RSUs have to only store Certificate Revocation List (CRL) entries that are less than a year old. Vehicles never have to download any CRL, which provides for huge savings in communication costs. Moreover, we use the following notations:

- d_v; d_I : Secret key corresponding to ID_v and ID_I; respectively.
- K_I : Secret key assigned to the RSU *I*.
- TS_i : Timestamp at time *i*.
- , : Public and private keys assigned to a vehicle by *TA* as part of their certificates.
- *sigEncrypt* (sigencryption) and *sigDecrypt* (sigdecryption) refer to identity-based operations while *rsaEncrypt*, *rsaDecrypt*, *rsaSign* and *rsaVerify* refer to operations that use the RSA algorithm. In some places we breakup *sigEncrypt* and *sigDecrypt* to its subfunctions *Sign*, *Encrypt*, *Decrypt* and *Verify*. Additionally, we use *aesEncrypt* and *aesDecrypt* to denote symmetric cipher operations using the AES cipher.

Our process is conducted according to three phases:

Setup Phase: The TA conducts the setup phase of the cryptosystem and computes the relevant system parameters (*params*) and the master secret *s*. Both of these are then distributed to all the RSUs in the system. The TA also generates a random secret key K_I for each RSU I and distributes it to that RSU.

The TA keeps a copy of this key in its database to help in future arbitration proceedings. The TA provides each vehicle with its unique vehicle identifier (ID_v), public key certificate certifying this identifier and including a public and private key (Pub_v and Pvt_v) generated using classical algorithms like RSA. Additionally each vehicle is provided with all the public system parameters (*params*) of the identity-based cryptosystem.

Pseudonym Generation: We assume that RSUs have up-to-date CRLs and that they will only issue a new pseudonym only if the vehicle's credentials have not been revoked. When a vehicle needs to get a new pseudonym, it engages a RSU as follows:

$$
\begin{aligned}
ID_v^i \quad &: \quad M = \langle Cert_v, TS_j, ID_v^i, rsaSign_{K_{pvt}^v}(ID_I \| ID_v^i) \rangle \\
ID_v^i \rightarrow ID_I \quad &: \quad C = sigEncrypt_{d_v^i}(ID_I, M) \\
ID_I \quad &: \quad M = \langle Cert_v, TS_j, ID_v^i, U \rangle = sigDecrypt_{d_I}(C) \\
& \quad rsaVerify_{K_{pub}^v}(U, ID_I \| ID_v^i) \\
& \quad T = aesEncrypt_{K_I}(ID_v \| TS_{j+1})) \\
& \quad ID_v^{i+1} = \langle vehicle \| T \| ID_I \| TS_{j+1} \rangle \\
& \quad d_v^{i+1} = Extract(ID_v^{i+1}) \\
ID_I \rightarrow ID_v^i \quad &: \quad rsaEncrypt_{K_{pub}^v}(ID_v^{i+1} \| d_v^{i+1} \| TS_j)
\end{aligned}
$$

Secure Communication: Our system provides an implicit credential in the form of the pseudonym for secure communication between all entities. The pseudonym includes a time-stamp indicating the last time some infrastructure point validated the credentials of a vehicle. Each vehicle could set its trust threshold as per the user's choice, in deciding how old pseudonyms they want to trust. Once that choice is made, we can simply validate the identity-based signature on the message to verify that the vehicle using the pseudonym actually has the private key corresponding to it. The private key could only have been generated by a RSU (or the TA) who has the master secret s. The implicit authentication provided by our pseudonyms is communication efficient because it eliminates the need for certificate exchange between vehicles and also does not require the vehicles to download any CRL.

Non-repudiation: In case of a dispute involving vehicles one can try to locate the cause of the incident based on the messages exchanged between vehicles. Vehicles can log messages into some-kind of a black-box like device and turn these messages over to an arbiter. We assume for simplicity that the arbiter is the same as the TA and has access to the secret key database (containing secret keys of the RSUs). Suppose vehicle ID_b hands over a message M and corresponding signature hU;Wi stating it was sent by vehicle pseudonym ID_i a to pseudonym IDi

b. The arbiter will validate if the message indeed was created and signed by IDi a, intended for IDi b and then will decipher as to which real vehicle ID's these pseudonyms belong to. This mechanism works as follows:

1. $M = ID_a^i \| ID_b^i \| m$
2. Check that ID_a^i and ID_b^i are in M
3. If $Verify(M, U, V, ID_a^i) == true$, continue
4. We write $ID_a^i = \langle vehicle \| T \| ID_I \| TS_{j+1} \rangle$
5. $K_I = KeyLookup(ID_I)$
6. $ID = \langle ID_a \| TS_{j+1} \rangle = aesDecrypt_{K_I}(T)$
7. Check that ID contains the same TS_{j+1} as in ID_a^i
8. ID_a is the real identity of the sender.
9. Repeat steps [4..8] with ID_b^i to get recipient.

The advantage of this scheme is that no special storage is required in either the vehicles or the infrastructure for each pseudonym. The message M containing the source and destination pseudonyms and signature are the only things that need to be stored to settle any disputes. Further, the original identities of the vehicles can be re-created only by a TA with valid legal cause for such action.

6 CASE STUDY

We consider the case of a fleet management system deployed by a private transportation company in order to monitor the behaviour of the drivers. We suppose that the vehicle is equipped with sensors allowing the measurement of the following information:

- Vehicle speed (wheel-based)
- Vehicle speed (from tachograph)
- Accelerator pedal position (0–100 %)
- Total fuel used (litre since life time)
- Fuel level (0–100 %)
- Engine speed
- Total engine hours (h)

Obviously, this application interacts with other services defined by the regulation authority such as highway fee payment. Using the proposed architecture, the black-box usage scenarios in this situation are as follows:

- Two privilege levels should be defined on the SU: one for the monitoring administrator and the other for the driver. The administrator is granted read access to the data listed above while the driver is able to define a security policy so that the payments receipts related to highway fees are stored in the black-box. Appropriate lifetimes should obviously be set according to the local laws and guidelines.
- Information related to the monitoring service as well as the highway fee payment is stored into the ABB. Since the data related to the driver behaviour is collected by local sensors, it should not be authenticated. However, the payment receipts should be signed by the payment server. It is important to mention that this latter should also preserve a payment proof, which should be different from the one sent to the client (driver) since it includes the signatures of the different RSUs the vehicle has crossed as well as the signature of the driver. In fact, the identity in this case is composed by the pseudonym (authenticating the driver) and the vehicle identity (that can be RFID tag).
- The data stored in the ABB, and related to the monitoring service, should be encrypted using a symmetric key configured by the administrator.

7 CONCLUSIONS

In this paper, we developed a novel black-box architecture for applications provided on vehicular networks. The major advantage of our approach is that it allows the definition of multi-level security policies to protect the data stored within the back-box. The proposed architecture allows a better segregation of duties during the data analysis phase since a main black-box has been considered for long-term storage while an auxiliary black-box is used for medium-term and short-term storage. Space quota and lifetime policies are therefore used to support this reasoning.

REFERENCES

Qiang Wu, Kebin Jia, Xuwen Li., 2008. Study on Vehicle Video Blackbox with Acceleration Sensitive Function, *International Conference on MultiMedia and Information Technology*, p.833-836.

Gabauer, D. J., and Gabler, H. C., 2005. Evaluation of Acceleration Severity Index Threshold Values Utilizing Event Data Recorder Technology, *Transportation Research Record: Journal of the Transportation Research Board, No. 1904*, Transportation Research Board of the National Academies, pp. 37-45, Washington, DC.

Claudia Kratzsch, Heidi Kroemker., 2009. Vehicle-To-Vehicle Communication For Enhanced Integrated Safety, *21st International Technical Conference on the Enhanced Safety of Vehicle*, June 15–18, Stuttgart, Germany.

The Florida Senate, 2009. Committee on Commerce, Issue Brief 2010-305 *Automobile Event Data Recorders*. October 2009.

Clemens Kaufmann, Christine Tureschek., 2008. Connecting Black Box Data and Driving Behaviour Observation for Better Understanding of Driving Behaviour, *European Conference on Human Centred Design for Intelligent Transport Systems* - Lyon, France, April 3-4, 2008

Maxim Raya, Panos Papadimitratos, Jean-Pierre Hubaux., 2006. Securing Vehicular Networks, *Poster at IEEE Infocom2006* (Infocom April 2006), Barcelona, Spain.

Deborah Sapper, Henry Cusack, Lisa Staes., 2009. Evaluation of Electronic Data Recorders for Incident Investigation, Driver Performance and Vehicle Maintenance, Project #BD549-50, *Center for Urban Transportation Research University of South Florida*, September 2009.

Aleecia M. McDonald , Lorrie Faith Cranor., 2006. How Technology Drives Vehicular Privacy, *A Journal of Law and Policy for the Information Society*, Volume 2, Issue 3, http://www.is-journal.org/

Mhamed Chammem, Mohamed Hamdi, and Noureddine Boudriga,. 2009. A Platform for Secure Multi-Service Vehicular Communication, *Int. Conference on Ultra Modern Telecommunications (ICUMT'09)*, 12-14 Oct, 2009, St Petersbourg, Russia.

Milind Khanapurkar, Dr. Preeti Bajaj, Dakshata Gharode., 2008. A Design Approach for Intelligent Vehicle Black Box System with Intra-vehicular communication using LIN/Flex-ray Protocols, *IEEE International Conference on Industrial Technology*, Sichuan University, Chengdu, China, April 21-24, (IEEE ICIT 2008)

Hampton C. Gabler and al., 2004. Use of Event Data Recorder (EDR) Technology for Highway Crash Data Analysis, *National Cooperative Highway Research Program*, Project 17-24, Final Report

John Pierowicz, Daniel P. Fuglewicz, Glenn Wilson., 2004. Development of Requirements and Functional Specifications for Crash Event Data Recorders, *Final Report, December 2004 USDOT* Contract: DTFH61-01-C-00182, Task Order Number: BZ82B007

Anthony Marino, John Schmalzel., 2007. Area Network for In-Vehicle Law Enforcement Applications, *SAS 2007 - IEEE Sensors Applications Symposium* San Diego, California USA, 6-8 February 07

Carfax, 2010. Vehicle Identification Number, a CARFAX vehicle history report, *Website http:// www.carfax.com/*, Last visit February, 26, 2010.

D. Boneh and M. Franklin., 2001. Identity-based encryption from the Weil pairing, *Lecture Notes in Computer Science*.