Security and Privacy of Location-based Services for In-Vehicle Device Systems

Marcello Missiroli, Fabio Pierazzi, and Michele Colajanni
Department of Engineering "Enzo Ferrari"
University of Modena and Reggio Emilia
Modena, Italy
Email: {marcello.missiroli,fabio.pierazzi,michele.colajanni}@unimore.it

***Abstract*—Location-based services relying on in-vehicle devices are becoming so common that it is likely that, in the near future, devices of some sorts will be installed on new vehicles by default. The pressure for a rapid adoption of these devices and services is not yet counterbalanced by an adequate awareness about system security and data privacy issues. For example, service providers might collect, elaborate and sell data belonging to cars, drivers and locations to a plethora of organizations that may be interested in acquiring such personal information. We propose a comprehensive scenario describing the entire process of data gathering, management and transmission related to in-vehicle devices, and for each phase we point out the most critical security and privacy threats. By referring to this scenario, we can outline issues and challenges that should be addressed by the academic and industry communities for a correct adoption of in-vehicle devices and related services.**

***Keywords*—Location-based services; vehicle systems; security; privacy; eCall; black box**

I. Introduction

The recent diffusion of *in-vehicle devices*, also known as *black boxes*, allows the implementation of a large and not yet fully exploited set of location-based services for cars, such as emergency calls, insurance services (e.g., Pay-As-You-Drive [1]), navigation systems, car maintenance, place recommendation and traffic management. The presence of one or multiple in-vehicle devices is likely to become a mass phenomenon if we consider that they are becoming mandatory in some countries. For example, it is expected that all new cars will be equipped with black box devices for emergency call services starting from 2015 in Europe [2] (eCall system [3]) and from 2017 in Russia [4] (ERA-GLONASS [5]).

However, the diffusion of such services is not at all counterbalanced by an adequate awareness about system security and data privacy threats related to in-vehicle devices. Security can be threatened by a plethora of actors. For example, the service provider, the network operator or the manufacturer of the black box device may misuse gathered personal and location-based information. The in-vehicle device is a critical point by itself because it can be tampered and modified by an attacker to compromise the user security, or even the passengers safety if the black box is connected with the controller network of the vehicle. Finally, the device may be subject to user manipulation for fraudulent intents (e.g., sending fake information to reduce insurance costs).

Existing literature addresses these security threats focusing on specific scenarios, such as insurance [6] and emergency call [7] systems. Other research is related to the problem of locational privacy [8], while other authors consider vehicle safety problems [9]. However, no effort has been yet devoted to analyze the overall picture of the security and privacy threats connected to in-vehicle devices and related services, that represent the main focus of this paper. We consider the possibility of multiple coexisting and/or combined services that rely on the same in-vehicle device, and we give the following main contributions:

- we present the reference scenario, outlining the main components common to all location-based services relying on in-vehicle devices;
- we analyze the security threats affecting each component, and we detail the analysis by referring to popular black box based services (emergency calls and insurances), and we outline possible threats evolution if and when multiple services will be integrated into a single black box device;
- we propose the adoption of a unified in-vehicle device developed according to an open model (open standards, and open source) that we call *white box*, because this solution can support the convergence of multiple services on a single device while guaranteeing an adequate level of security for end users and service providers.

The rest of the paper is structured as following. Section II presents the comprehensive scenario related to in-vehicle device systems. Section III outlines the main actors involved in such scenario, and identifies the security threats related to system security and data privacy. Section IV analyzes the security of three different scenarios: emergency call services, insurance services, and a future scenario in which all services rely on a unified in-vehicle device. Section V compares the risks related to these three scenarios. Finally, Section VI describes the main conclusions.

II. System Overview

We propose a comprehensive scenario that identifies the main characteristics of location-based services relying on in-

978-1-4799-5313-4/14/$31.00

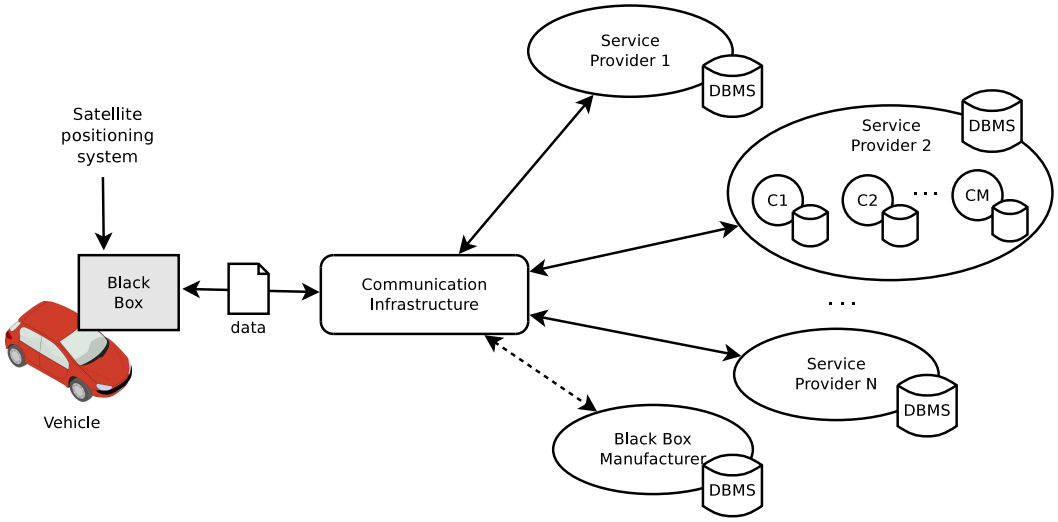

Figure 1. System overview of a black box based vehicle system for location-based services.

vehicle black box devices. In the scheme represented in Fig. 1, we consider a *vehicle* equipped with a *black box* that collects information about location, time and possibly other maintenance data (e.g., status of engine, airbags, and other mechanical and electronic components). These data are then transmitted through some *communication infrastructure* to one or more *service providers*. We can assume that each service provider stores data received from the black boxes of its customers into one or more private databases.

A service provider may be a single entity (e.g., *Service Provider 1* in Fig. 1), or it may consist of several separate *components* (e.g., *Service Provider 2* in Fig. 1 with components $C_1, C_2, ..., C_M$). For example, in emergency call services, these components correspond to local emergency safety points that receive an automatic help request from the black box device. In the case of an insurance service, the components might be different branches of the insurance company (e.g., IT infrastructure, billing, risk assessment).

In some cases, the service provider might not be interested in handling the infrastructure required for data collection directly because of setup and maintenance costs. In such cases, the black box manufacturer can collect data from the black box devices thus acting as a component of the service provider.

The key element of this scenario is represented by the in-vehicle device that collects and transmits information about the vehicle, the owner behavior, the driver(s) and so on. In order to fully understand the security analysis presented in Section III, it is necessary to describe the main components of the device, and how data are managed and stored by referring to the scenario outlined in Fig. 1.

A. Black Box Components

The specific hardware implementation of the in-vehicle device may vary depending on the supported services, but the components that are common to most black box devices are similar and reported in Fig. 2.

A *satellite receiver* pinpoints the exact spatial and temporal coordinates of the vehicle. Position tracking is based on existing satellite positioning systems (e.g., GPS or GLONASS [10]) that might be combined to obtain better coverage and precision [11]. Moreover, a timestamp can be obtained from the satellite data or from other protocols, such as GSM NITZ [12].

A *communication interface* allows the black box device to interact with the communication infrastructure in order to transfer data to the service provider(s). In most cases, the connectivity is provided through a SIM card integrated into the in-vehicle device, but other communication systems could be used as well.

A *user interface* on the vehicle dashboard allows the owner to interact with the black box device and/or to be informed about its status. It may include a power-on LED, or a button for manual activation of a service (e.g., for emergency call). In some cases, the black box integrates a USB interface that can be used to download its content.

Some *internal sensors* (e.g., an accelerometer) allow the black box device to collect more data or to prompt an automated response in presence of different events (e.g., a car crash). In other designs and prototypes, the black box can include even audio or video sensors.

An optional *vehicle bus interface* allows the black box to collect data from vehicle's sensors, or to send some signals to the vehicle control unit in order to interact with the car (e.g., remote door unlocking via vehicle bus, such as CAN bus [13]).

An *internal storage* allows the device to store the data collected from the satellite receiver, the internal sensors and/or from the vehicle bus interface, such as the vehicle locations history. A detailed description of data management adopted

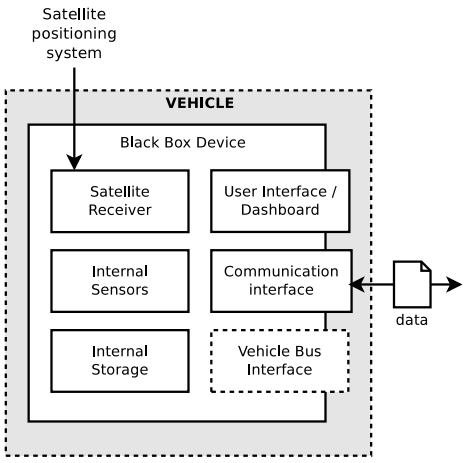

Figure 2. Main components of an in-vehicle black box device.

by in-vehicle device systems is presented below.

B. Data Management

Data management is a critical process concerning the entire flow from the internal storage of the black box device to the service provider database(s). Data management varies substantially on the basis of supported services. Nevertheless, we can identify the main features that characterize most in-vehicle black box services with respect to:

- data set,
- data lifetime and storage,
- data transmission.

All location-based services for in-vehicle device systems collect a *minimum set of data* consisting of: vehicle identification number, location (e.g., GPS coordinates), and timestamp. In addition to this minimum set of data, the black box might also collect *extra data* depending on supported services. For example, insurance services may require information about vehicle diagnostics (e.g., brakes and tyres condition, number of fastened seatbelt).

Collected data are usually stored inside the in-vehicle device and, when required by the service protocol, transmitted to the service provider that stores the data in its private databases. Depending on the specific service, the amount and type of data stored in the black box and in the service provider database may vary. For example, data may consist of raw vehicle locations or it may be aggregated data (e.g., information about miles driven per month that is used by a pay-per-use insurance company to bill its customers). In some emergency call systems (e.g., eCall [3]), the internal storage of the black box can store only data referring to the last three vehicle positions, and the service provider must only store anonymized information about car accidents.

In all services, data transmission between the black box and the service provider is a *two-way communication*: data collected by the black box is transmitted to the service provider for storage and elaboration; other signals might be sent from the service provider to the in-vehicle devices (e.g., signals for remote door unlocking, or a request for the vehicle position in anti-theft systems). The trigger for data transmission towards the service provider is *automatic*, and it can be prompted either periodically (e.g., once a day) or on an event basis (e.g., after a car accident). In some services, data transmission could also be triggered *manually* by the vehicle owner (e.g., emergency calls). The main difference from the security point of view refers to the possibility that communications may be activated only by the in-vehicle device or even by external triggers.

III. System Security

We analyze privacy and security of systems that rely on in-vehicle devices with respect to the scenario presented in the previous section. We identify the following actors:

- the *vehicle owner*, that equipped his/her vehicle with a black box device;
- the *service provider*, that offers one or more services to the vehicle owner, and that collects and stores data received from the in-vehicle black box;
- the *network operator*, that manages the communication infrastructures required for data transmission;
- the *black box manufacturer*, that built the black box installed inside of the vehicle;
- an *external attacker*, that is interested in accessing data gathered, stored in the black box and in the service provider databases.

The system security involves both the *privacy* of the vehicle owner data (e.g., locations history), and the *integrity* of data transmitted to and managed by the service provider.

One of the main assets that must be protected in such systems is the information about the *vehicle locations history*, that is usually stored in the black box internal storage and/or in the service provider's database(s). Indeed, from such data it is possible to infer some private information about the vehicle owner/driver [14]–[16] such as identifying his/her home, workplace and typical journeys. Hence, it is of utmost importance to study proper mechanisms to prevent information leakage in such systems.

The vehicle owner/driver might try to *tamper with the in-vehicle device* in order to alter the information stored in or transmitted to the service provider (i.e., compromising data integrity). For example, in insurance services the vehicle owner (directly or through the help of a mechanic) might try to alter information stored in the black box in order to deceive his responsibility in a car accident; or he may try to alter the information about the number of driven miles in order to pay a lower insurance premium [6].

The service provider collects the data received from the black box device into one or more databases. In order to guarantee the vehicle owner privacy, the service provider should collect all and only the information needed to provide

the required service. Unfortunately, the provider might try to illegitimately get some extra information from the black box device depending on its sensors and available functions (e.g., unauthorized voice recording). Proper protocols that allow the vehicle owner to identify *illegitimate data transmission* should be investigated.

Since the vehicle owner cannot deactivate the data transmission from the black box device, he must at least be notified when the black box device is transmitting data (e.g., through a led in the user dashboard). Moreover, another threat for the vehicle owner privacy is that the service provider might sell the collected information to external third parties.

We assume that the network operator is semi-honest, also known as *honest but curious* [17], that is, he does not modify transmitted data, but he may be interested in reading it. Hence, he might *eavesdrop* and collect the data transmitted between the black box device and the service provider. Moreover, whenever the black box connects to the network to transmit data (usually through a SIM Card), the network operator is always capable of detecting the vehicle position, and might save its locations history.

We also consider that the black box manufacturer might be interested in illegitimately receiving some data collected by the black box device that he produced and that is installed in the owner's vehicle. Hence, the hardware and software functionalities of the black box device must be properly audited and certified by an external third party that must verify the inability to activate extra services or to illegitimately collect data through some backdoor or covert channels [18], [19].

Moreover, it is likely that the black box manufacturer is responsible for the release of *software/firmware upgrades*, to fix bugs or to enable new services on the black box device. Vulnerabilities in the software upgrade system might be exploited by the vehicle owner or by an external attacker to *tamper* with the in-vehicle device. On the other hand, a black box without any software upgrade capability may be subject to design errors, and may be vulnerable to attacks that cannot be fixed without a device upgrade.

An external attacker may be interested in *tampering with the in-vehicle device* for several reasons, such as tracking the owner's vehicle, getting information about past journeys, and/or receiving extra data from the black box sensors (e.g., voice). We distinguish two types of tampering: *hardware* (e.g., by physically substituting the black box with another similar-looking but malicious device) and *software* (e.g., malware injection by exploiting a software bug). Indeed, the attacker may try to exploit vulnerabilities in the black box software and/or in the software upgrade process, or he may try to violate the black box manufacturer servers in order to compromise legitimate software updates.

We highlight that if the device tampering is successful, and the black box is connected to the vehicle control system (e.g., via CAN bus), then this tampering action may cause safety threats to the passengers or simplify vehicle theft.

Moreover, the external attacker might also be interested in *violating the service provider databases*, because they contain data related to all the customers. For example, insurance companies that offer advanced pay-per-use services usually rely on in-vehicle devices to collect the vehicle locations history of all their customers, in order to determine their profile risks. If the service provider collects all data in a single centralized database that is not well protected, then it becomes a really interesting target for external attackers.

IV. Services Security

The first security analysis is focused on two existing location-based service scenarios: *emergency call services* and *insurance services* that are provided through *proprietary black boxes*, that is, each service provider requires the installation of a separate black box device. Furthermore, we consider that the trend of having one black box for each service may not represent the most viable option in a future when location-based services will be widely adopted. Hence, we devise also a third scenario in which all service providers rely on a single, standard in-vehicle device: the *unified black box*.

A. Emergency Call Services

Emergency call services rely on the in-vehicle device to detect when a car is involved in an accident, with the goal of rapidly dispatching help requests. In this scenario, the service provider usually consists of a network of *Public Safety Answering Points* (PSAPs) that are responsible for requesting the intervention of the public rescue services (e.g., ambulance, police, firefighters). Typically, the PSAPs correspond to call centers that answer to emergency telephone numbers (e.g., 112 in Europe).

An example of emergency call service is eCall [3], a European automated car safety system that will be adopted by the European Union, Iceland, Norway and Switzerland. The development of eCall started in 2006, and recently the European Parliament approved a decision [2] mandating that every new European vehicle manufactured after October 2015 must install an eCall black box. Similarly, the emergency call service ERA-GLONASS [5] will become mandatory in Russia from 2017 [4].

In general, an emergency call service relies on a black box device that uses:

- a satellite receiver to determine the vehicle position;
- the mobile network to transmit data, and to initiate the call with the PSAP;
- a microphone and a speaker to support a voice call.

The in-vehicle device is usually in a "dormant" state, that is, it is disconnected from the mobile network and it does not transmit any data. When dormant, the black box collects

location data in the internal storage and it is able to detect whether the vehicle is involved in an accident (e.g., in eCall this is done by monitoring the internal accelerometer and the status of the vehicle airbags). If an accident is detected, the device connects to the mobile network within few seconds, and dials the emergency telephone number (e.g., 112 in Europe) with the "emergency call flag" set. The network operator recognizes the emergency call, and forwards it to the nearest PSAP. The in-vehicle device also transmits to the PSAP a set of data that is considered useful for the rescue services. For example, the minimum set of data transmitted by eCall has been defined by the European standard CEN15722 [20] and consists of:

- a message identifier;
- a vehicle identification number;
- the last three positions of the vehicle, in terms of GPS coordinates with timestamp;
- the direction of the vehicle, detected by the black box accelerometer, and helpful to determine the vehicle lane at the moment of the accident;
- number of passengers with fastened seatbelt.

In other emergency call services, the minimum set of data may be extended with other information that may be useful in case of a car crash (e.g., vehicle diagnostics). We highlight that in emergency call services the black box does not store the entire vehicle history, but only data referring to the last few positions.

After the emergency phase, an anonymous record of the accident is forwarded and stored in a *centralized database*, where it can be used by the service provider for statistics purposes (e.g., to determine the efficiency of the emergency service).

By referring to the security threats presented in Section III, we identify the main threats that may affect emergency call services:

- An external attacker may try to *tamper with the in-vehicle device* to be able to track the vehicle and record all passenger conversations via the microphone connected to the black box.
- The service provider or the black box manufacturer may try to *illegitimately activate the device* in order to track the vehicle and/or listen to the passengers conversations.
- An external attacker may try to *eavesdrop* emergency calls by violating the GSM protocol [21] in the proximity of a PSAP.

In the emergency call scenario, the vehicle owner does not have any benefit in tampering with the in-vehicle device. Moreover, it is unlikely that an external attacker tries to violate the service provider databases because they do not contain really critical information about the vehicle owners.

B. Insurance Services

Many insurance companies are encouraging their customers to install a black box device in exchange for more convenient premium costs. Some common insurance related services include:

1) *event data recording*;
2) *anti-theft* (passive and active);
3) *pay-per-use* (basic and advanced).

Depending on the insurance contract, the vehicle owner might enable one or more of these services.

In event data recording service, the in-vehicle device monitors vehicle positions and diagnostics (e.g., brakes and seatbelt status, steering angle, airbag condition). If an accident is detected by the black box sensors, then the data about the vehicle positions and diagnostics are dumped locally in the internal storage of the black box, and they are manually collected by the insurance company in order to determine the degree of driver's responsibility.

Anti-theft services may be either passive or active. In passive anti-theft, the black box is used only to locate or track the stolen vehicle. In active anti-theft services, the black box device is also connected to the vehicle actuators in order to take to some extent remote control of the vehicle (e.g., to slowdown the vehicle or to prevent ignition).

The pay-per-use insurance contracts, also named Pay-As-You-Drive (PAYD [1]), determine different premium costs on the basis of how the vehicle owner drives. In basic PAYD services, the black box collects only aggregated information such as number of total driven miles. On the other hand, in the advanced PAYD services the in-vehicle device collects the full vehicle locations history, and periodically transmits it to the service provider. All the gathered vehicle locations data is stored both inside the black box internal storage and in the service provider's databases, and it is afterwards elaborated by the insurance company to infer the driver's risk profile that will determine the premium cost for the vehicle owner on the basis of how, when and where he drives.

OnStar [22], a subsidiary of General Motors, is a black box manufacturer that builds and manages in-vehicle devices that can be used by insurance companies to offer all the previously described services.

By referring to a scenario in which an insurance company offers event data recording, advanced pay-per-use, passive and active anti-theft services, we identify the following main security threats:

- An external attacker may try to *violate the insurance databases*, because they contain a lot of detailed and personal information about all customers, along with the full history of vehicle locations.
- An external attacker may also try to *tamper with the in-vehicle device* in order to track the vehicle or read stored information (i.e., a large set of locations history);

since the anti-theft system is connected to the vehicle actuators, the attacker may also try to harm the driver and the passengers [9].

- The black box manufacturer may try to activate *illegitimate data collection* in order to gather information about the vehicles that equip the black box devices that he produced.
- The user may try to *tamper with the in-vehicle device* in order to pay lower insurance premium costs (e.g., by reducing the number of driven miles by obfuscating the GPS signal [6]); or he might try to alter black box data in order to avoid responsibility in case of an accident.
- The service provider (i.e., the insurance company) may try to make the customer pay more than he deserves by manipulating the data used for the computation of the premium costs (e.g., total number of miles driven).
- If the car is stolen, a thief (i.e., an external attacker) may try to tamper with the black box device in order to disable the anti-theft systems (i.e., tracking and remote vehicle control).

C. Unified Black Box Services

Present black box based services rely on single-service, proprietary and generally incompatible devices (e.g. the German Sparkassen Direkt [23] insurance service and LKW-Maut toll payment systems), often based on proprietary protocols, sometimes patented, and with limited available documentation. If a vehicle owner subscribes to multiple services, he is forced to install several independent black box devices on his vehicle, which is expensive and impractical. Hence, we discuss a future scenario in which all service providers rely on a unified standard device called *unified black box* (UBB). This is the most likely scenario because it is rather unrealistic to have, for example, three separate black boxes in the same vehicle for the emergency call, insurance and traffic monitoring. Similarly, the users cannot accept to re-install a different device for any change of insurance contract or emergency provider. Interoperability between different standards will also become an important factor, especially in Europe. Indeed, the interoperability tests between the emergency call services eCall and ERA-GLONASS are already underway [24].

Emergency call black boxes mass production will drive costs down, and proprietary black box devices will become economically unfeasible. We therefore realistically expect that black box design will converge to the UBB, that will be able to support not only all mandatory emergency call system requirements, but will also be used for several other services (e.g., insurance and traffic management). To this purpose, it will be equipped with several hardware interfaces, it will be prone to software upgrades and remote configuration.

While this scenario has positive implications for both end users and service providers in terms of costs and usability, it might introduce higher security and privacy risks. For example, the requirement to support different services and to guarantee service interoperability implies the presence of several hardware ports (e.g., USB, different vehicle buses) and multiple entry points (e.g., HTTP), thus introducing multiple attack paths. Moreover, a malicious software provider could be interested in accessing data stored in the unified black box, but related to services offered by different providers (e.g., an insurance supporting a basic pay-per-use service that receives only odometer data could be interested in reading the vehicle positions).

The use of closed-source hardware and software development model for the UBB is not useful to guarantee a high security standard for such critical elements of the system. An approach relying on proprietary and undocumented protocols follows a "security by obscurity" policy, that is not considered a good practice. A radically different solution would be to embrace an open approach [25], where the hardware, firmware and software of the black box is made available to third parties for inspection, audit and upgrade proposals. We argue that this is the best solution to guarantee to both users and service providers that no backdoor, undocumented features or other security flaws are hidden in the black box. Furthermore, a large community of auditors ensures a fast process for the discovery and patching of vulnerabilities.

To summarize our position, we believe that the best solution to have a secure and trustworthy unified black box is to create a *white box*, that is, an open system substituting the proprietary in-vehicle devices currently used.

The full design of a white box is out of the scope of the paper, but we outline some important guidelines that must be taken into account in its design. First of all, data encryption should be adopted at different levels, in order to secure data communications (e.g., SSL), the internal storage of the in-vehicle device, and the service providers databases [26], [27]. Each service provider will run its own application on the white box, and each application should run in a separate *sandbox* environment. The white box operating system should expose proper APIs that can be called by the service providers applications in order to interact with the white box (e.g., get GPS position, write on internal storage, communicate with vehicle bus). The access to the APIs must be properly regulated through ACLs (access control lists). Prior to the installation on the white box device, the user must be able to view the ACL permissions required by each service provider application. All operations and data communications should be properly logged, in order to be able to audit the device functioning and detect misuses. Moreover, software updates of both the white box operating system and of the service provider applications must be verified with digital certificates and signatures, in order to prevent installation of malicious or unauthorized software. It would also be convenient to consider the adoption of *trusted computing* hardware and software solutions (e.g., [28], [29]) in order to guarantee the correct execution of expected services and to prevent user and provider tampering and misbehavior.

TABLE I
COMPARISON OF RISKS RELATED TO DIFFERENT DEVICES

Attacker	Means	Emergency call		Insurance		UBB	
		$\mathcal{R}$	$\mathcal{F}$	$\mathcal{R}$	$\mathcal{F}$	$\mathcal{R}$	$\mathcal{F}$
Vehicle owner	device tampering to alter data	- - - -	- F - -	A B C -	E F G H	A B C -	E F G H
Service provider	unauthorized service activation	A - C D	- - - -	A B C -	E - G H	A B C D	E - G H
Black box manufacturer	backdoor	A - C D	- F - -	A B C -	E F G H	A B C D	E F G H
Network operator	data eavesdropping	- - C -	- - - -	- - C -	E - G H	- - C -	E - G H
External attacker	device tampering	A - C D	- - - -	A B C -	E - G H	A B C D	E - G H

V. RISK COMPARISON

We are interested in summarizing and comparing the security and privacy risks related to emergency call, insurance, and unified black box (UBB) devices and services. For each possible threat, we report in Table I two risk parameters: the *reward* $\mathcal{R}$ and the *feasibility* $\mathcal{F}$. The reward $\mathcal{R}$ represents the set of information that can be accessed (or modified) if the attack succeeds. In particular, the reward $\mathcal{R}$ might consist of one or more of the following data (ordered by increasing sensitivity):

- (A) *vehicle diagnostics*;
- (B) *full vehicle locations history*;
- (C) *real-time vehicle position* (i.e., vehicle tracking);
- (D) *audio recording*.

The feasibility $\mathcal{F}$ represents a set of conditions that might facilitate the attack. It might consist of one or more of the following conditions (ordered by increasing relevance):

- (E) *frequent data transmission*, because it might facilitate the attack and complicate its detection;
- (F) *physical access* to the in-vehicle device, because it facilitates tampering attempts;
- (G) *presence of a high number of interfaces and built-in functions*, because they might introduce multiple points of attack;
- (H) *presence of services that can be called from the external*, because they represent possible targets of attack that can be exploited without requiring physical access to the in-vehicle device.

From Table I, we can observe that in the emergency call scenario there is no reward for the vehicle owner if he tampers with the in-vehicle device. On the other hand, for other attackers the reward even includes the audio recording of the passengers conversations, that represents a highly sensitive data. However, in most cases the feasibility of the attacks in the emergency call scenario is low, because the emergency call black box transmits data only in the case of accidents (event-based activation) and offers a limited number of interfaces and functions.

In the insurance scenario, the vehicle owner may try to tamper with the black box device to alter vehicle diagnostics (e.g., for neglecting responsibility in case of a car crash), or vehicle locations history and/or tracking (e.g., for paying lower insurance premiums). For other attackers, the rewards include the vehicle diagnostics, the full vehicle locations history, and the possibility of getting the location of the vehicle. In general, the feasibility of the attacks in the insurance scenario is higher with respect to emergency call, because the insurance black box usually exposes services that can be accessed from the external, and offers a high number of interfaces and functions.

As expected, the rewards $\mathcal{R}$ and the feasibilities $\mathcal{F}$ related to the UBB case are always equal to or higher than those referring to emergency call and insurance private black boxes. The motivation is that a UBB manages data related to several services through multiple hardware and software interfaces, each possibly representing a different point of attack. Similarly, the risks of tampering attempts of a UBB device increase greatly because it collects and stores several interesting data for an attacker.

These motivations, in addition to the augmented complexity of the UBB, lead us to propose the adoption of a *white box* that must be based on open standards and known APIs (Section IV-C). A similar architecture can increase the overall system security [25], because it becomes verifiable thanks to an open source design and implementation approach. Moreover, this open approach allows to share the efforts related to development, debugging and auditing among a large group of contributors.

VI. CONCLUSIONS

The growing popularity of in-vehicle devices to collect data about user-related information allows the realization of novel interesting services. We propose a comprehensive study to describe the security and privacy threats affecting these services by initially analyzing two classes of existing location-based services (i.e., emergency call and insurance) assuming a proprietary black box device for each service. Furthermore, we analyze the impact from a security point of view of using the same unified black box for multiple services that we expect to be a common case in the near future.

We conclude that most security and privacy issues can be addressed by adopting an open architecture for the unified in-vehicle device (that we call white box), where it is possible to verify the compliance of the device behavior with respect to the service contract terms and to perform independent audit

to guarantee the necessary level of security. The diffusion of similar white box devices may be the catalyst to create an ecosystem for the proposal of a plethora of interoperable and trustworthy location-based services for the end users.

REFERENCES

[1] J. Bordoff and P. Noel, "Pay-as-you-drive auto insurance: A simple way to reduce driving-related harms and increase equity," *Hamilton Project Discussion Paper*, 2008.

[2] "Report on the proposal for a regulation of the European Parliament and of the Council concerning type-approval requirements for the deployment of the eCall in-vehicle system and amending Directive 2007/46/EC," February 2014. [Online]. Available: http://www.europarl.europa.eu/

[3] "European emergency call system (eCall)," http://ec.europa.eu/digital-agenda/ecall-time-saved-lives-saved, visited in May 2014.

[4] "Law on legal status, function and structure of ERA-GLONASS system," December 2013. [Online]. Available: http://eng.kremlin.ru/acts/6489

[5] "Russian emergency call system (ERA-GLONASS)," http://era-glonass.com/, visited in May 2014.

[6] C. Troncoso, G. Danezis, E. Kosta, J. Balasch, and B. Preneel, "PriPAYD: Privacy-friendly pay-as-you-drive insurance," *IEEE Trans. Dependable and Secure Computing*, vol. 8, no. 5, pp. 742–755, 2011.

[7] C. Geuens and J. Dumortier, "Mandatory implementation for in-vehicle eCall: Privacy compatible?" *Computer Law & Security Review*, vol. 26, no. 4, pp. 385–390, 2010.

[8] A. J. Blumberg and P. Eckersley, "On locational privacy, and how to avoid losing it forever," *Electronic Frontier Foundation*, 2009.

[9] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway *et al.*, "Experimental security analysis of a modern automobile," in *Proc. 31st IEEE Symp. Security and Privacy*, 2010, pp. 447–462.

[10] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer, 2007.

[11] G. Heinrichs and J. Windl, "Combined use of GPS and GLONASS: A new era in marine navigation and positioning," in *Proc. 11th Int. Tech. Meeting of the Satellite Division of the Institute of Navigation (ION GPS)*, 1998, pp. 2081–2090.

[12] J. C. Ewert and M. Stuempert, "Method and device for providing a mobile station with network identity and timezone (NITZ) information," US Patent App. 11/718,493, Nov. 3, 2004.

[13] W. Lawrenz, *CAN system engineering*. Springer, 1997.

[14] J. Krumm, "Inference attacks on location tracks," in *Pervasive Computing*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2007, pp. 127–143.

[15] R. Dewri, P. Annadata, W. Eltarjaman, and R. Thurimella, "Inferring trip destinations from driving habits data," in *Proc. 12th ACM Workshop on Privacy in the electronic society*, 2013, pp. 267–272.

[16] M. U. Iqbal and S. Lim, "A privacy preserving GPS-based Pay-as-You-Drive insurance scheme," in *Symp. GPS/GNSS (IGNSS)*, 2006, pp. 17–21.

[17] O. Goldreich, *Foundations of Cryptography: Volume 2, Basic Applications*. Cambridge university press, 2004.

[18] G. J. Simmons, "Subliminal communication is easy using the DSA," in *Advances in Cryptology – Eurocrypt '93*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 1994, vol. 765, pp. 218–232.

[19] S. Zander, G. J. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Commun. Surveys and Tutorials*, vol. 9, no. 1-4, pp. 44–57, 2007.

[20] C.-D. Bârcă and S. Dumitrescu, "eCall: minimum set of data (MSD)," *Journal of Information Systems & Operations Management*, vol. 3, no. 2, pp. 428–439, 2009.

[21] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," in *Advances in Cryptology - CRYPTO 2003*, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2003, pp. 600–616.

[22] "OnStar Corporation," https://www.onstar.com/, visited in May 2014.

[23] "Sparkassen Direkt, insurance company," https://www.sparkassen-direkt.de, visited in May 2014.

[24] R. Oorni, R. Hautala, T. Laakko, and E. Meilikhov, "eCall cross-border tests between Finland and Russia," in *19th ITS World Congress*, 2012.

[25] J.-H. Hoepman and B. Jacobs, "Increased security through open source," *Communications of the ACM*, vol. 50, no. 1, pp. 79–83, 2007.

[26] R. A. Popa, C. M. S. Redfield, N. Zeldovich, and H. Balakrishnan, "CryptDB: protecting confidentiality with encrypted query processing," in *Proc. 23rd ACM Symp. Operating Systems Principles (SOSP)*, 2011, pp. 85–100.

[27] L. Ferretti, M. Colajanni, and M. Marchetti, "Distributed, concurrent, and independent access to encrypted cloud databases," *IEEE Trans. Parallel and Distributed Systems*, vol. 25, no. 2, pp. 437–446, 2014.

[28] S. W. Smith, *Trusted computing platforms: design and applications*. Springer, 2005.

[29] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in *Proc. 19th ACM Symp. on Operating Systems Principles (SOSP)*, vol. 37, no. 5, 2003, pp. 193–206.