# Privacy-Aware Event Data Recorders: Cryptography Meets the Automotive Industry Again

*Constantinos Patsakis, Trinity College*
*Agusti Solanas, Universitat Rovira i Virgili*

## ABSTRACT

Vehicles are equipped with more technology with each passing day. Acronyms such as ABS (anti-lock braking system), EBD (electronic brakeforce distribution) or EPS (electric power steering) have become commonplace, and are used as synonyms for safety and comfort. On the contrary, others like EDR (event data recorder) are not as popular. EDR, commonly known as automotive black boxes, are devices used to collect data about a vehicle and its occupants, which can be accessed after an accident to clarify its cause. With the upcoming regulation of the National Highway Traffic Safety Administration requiring manufacturers to include EDR in all new vehicles, privacy advocates have raised some alarms related to the storage of and access to these data. In this article, we propose a novel privacy-aware solution for the EDR of modern vehicles. Our solution is based on modern cryptographic primitives like timed release encryption (TRE), and it guarantees the privacy of the vehicle's occupants while allowing the full functionality of EDR in case of emergency.

## INTRODUCTION

Safety is a priority of the automotive industry. Infrared night vision, and lane departure warning and traction control systems are just a few examples of devices that have joined forces with the more classic seatbelts and airbags to provide drivers and passengers with more safety. A diverse set of acronyms such as ABS (anti-lock braking system), EBD (electronic brake-force distribution), EPS (electronic power steering) and ESP (electronic stability program) have become commonplace, and are used by the automotive industry as synonyms for safety and comfort.

In addition to the above, modern vehicles come equipped with modern infotainment and positioning technologies like GPS. As a result, they have become very complex networks of autonomous embedded systems in which electronic contol units (ECUs) and sensors cooperate to create an electronic environment that makes the vehicle operate as a platform entity [2]. This complex network receives and processes information (i.e., measurements and functioning states) that allows it to control actuators that perform a plethora of tasks from regulating fuel injectors and reducing emissions to unlocking the brakes and improving stability. Also, a significant part of this information can be collected and stored in event data recorders (EDRs).

Vehicles are evolving toward increasing their connectivity, and can no longer be understood as individual entities whose inner networks and controllers are isolated from the outer world. With the growing use of communications among vehicles (i.e., V2V communications) and between vehicles and the infrastructure (V2I communications), vehicles have become active nodes that can send, receive, and relay data within a complex and global network [14]. Using vehicular ad hoc networks (VANETs), vehicles create mobile networks in which they exchange information ranging from infotainment to followed trajectories, and traffic and emergency warnings, which couldbe very relevant in the context of Smart Cities if security and privacy are properly guaranteed [16]. Recently, the automotive industry has started to embed systems that allow connection to the Internet from within the vehicle, thus offering onboard services like Facebook and Skype.

The transition of vehicles from merely mechanical to highly complex and intelligent automated machines reached its zenith with the Google driverless car. Thanks to its reliability, some states of the United States of America have granted it a driving license. The results point out that the Google car probably deserves the driving license since in tests of more that 300,000 km only two accidents were reported, and neither of them was caused by the driverless car.

### EVENT DATA RECORDERS

Generally, every new device, service, or gadget that the automotive industry includes in their vehicles is welcome by the public due to the fact that they make drivers' lives simpler, safer, and


0163-6804/13/$25.00 © 2013 IEEE

more comfortable. However, there are a few exceptions that have been cause for concern. That is the case of event data recorders (EDRs), also known as *automotive black boxes*.

Event data recorders are devices that have been used for decades in ships and airplanes. Their main goal is to record all the necessary information so that in case of severe accidents, specialists are able to reconstruct or even simulate the events that took place and understand the causes that led to an accident. Depending on the manufacturer and their intended use, black boxes are equipped with magnetic-tape or solid state storage. However, the latter has fewer moving parts, which translates into fewer maintenance issues and a lower risk of malfunction in case of severe crashes.

EDRs have been included in some vehicles since the 1990s. Current EDRs collect various information about the vehicle: vehicle speed, engine speed, force of the impact, steering input, airbag deployment lapse, accelerator position, brake status, seatbelt status, passenger's airbag, and so on. The vast majority of new vehicles are equipped with one EDR; according to the National Highway Traffic Safety Administration (NHTSA)[1] around 96 percent of 2013 cars are already equipped with EDR. Notwithstanding, the NHTSA is going to regulate this matter to make EDRs mandatory for new vehicles, starting from September 1, 2014.

In the case of severe accidents in which drivers and passengers can be seriously injured, the data collected by the EDR can help to determine the cause of the accident, and can be used to prove the negligence or innocence of drivers and manufacturers facing prosecution. Consider, for example, a simple scenario in which after an accident, the driver claims that his/her injuries were caused by the malfunction of the seatbelts. In this situation, it could be possible to check the information collected by the EDR to assess whether the driver had the seatbelt fastened when the accident occurred. Also, in more complex scenarios, like one in which two vehicles collide in a country road without witnesses, both drivers might blame each other, and the EDR of both vehicles could be used to determine the real responsibility for the accident.

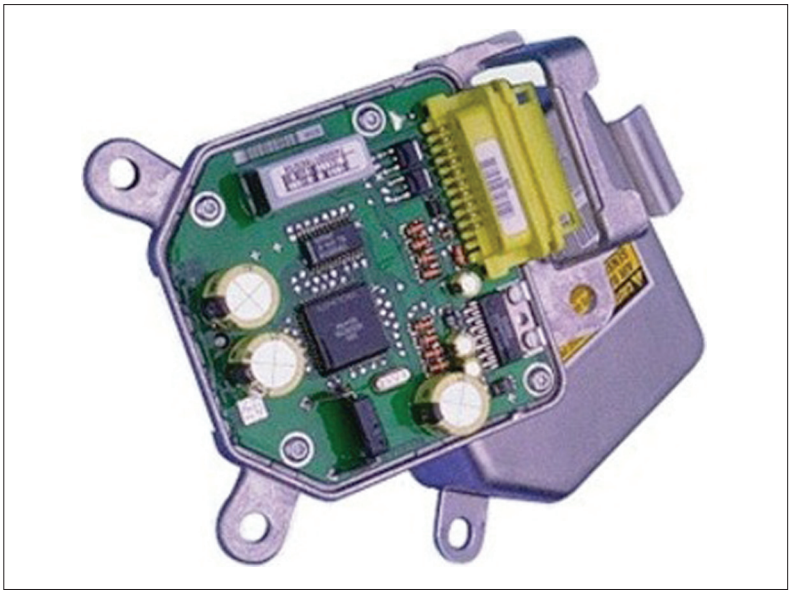

**Figure 1.** *Regular event data recorder (EDR), also known as automotive black box. Source: autoblog: http://www.autoblog.com/2012/12/07/white-house-clears-way-for-nhtsa-to-mandate-vehicle-black-boxes/.*

## EDRs and Privacy

A considerable number of privacy and security issues have appeared due to the growing complexity of the electronic systems that govern modern vehicles and the increasing use of communication technologies within them. Thus, it could be said that the benefits of the new technologies incorporated into vehicles are not without a risk. We can analyze the privacy and security risks from two perspectives regarding the context in which the attack is conducted: in-vehicle attacks and remote attacks. In other words, we might distinguish the attacks that understand the vehicle as an isolated entity and those that take advantage of the fact that modern vehicles are connected to a variety of different networks.

In the first scenario, the main in-vehicle networks are using LIN and CAN, which are protocols that do not support any kind of security mechanisms by default; hence, they are prone to many attacks [5]. Numerous attacks stem from faulty implementations of encryption mechanisms, enabling automated, unauthorized, and arbitrary access to the vehicle [1].

In the second scenario, it has been shown that there are many vulnerabilities that take advantage of entry points that modern vehicles have, such as Bluetooth or dedicated short-range communications (DSRC). Moreover, important vulnerabilities have been found in long-range wireless access, and many attacks exploiting broadcast channels and addressable channels have been developed [3, 8]. In light of the above vulnerabilities disclosure, as well as others, the U.S. Department of Transportation recently issued a Request for Information, highlighting the risks for Homeland Security [4]. Projects like EVITA[2] and works like [12] try to promote new, more security-aware vehicle frameworks.

Regarding EDR, if we consider them individually, they can hardly be seen as a security risk, since they are not used to control any critical system of the vehicle. However, if an attacker could gain access to a vehicle (locally or remotely), he/she could obtain very sensitive information about the vehicle, and, by extension, about the driver. Black boxes have been widely used in ships and airplanes for decades with success, but in these cases there are no privacy concerns. The main reason is that ships and airplanes follow predetermined routes, which are governed by strict rules. On the contrary, if an attacker gets access to the information stored by an EDR, he/she could be able to reconstruct the route followed by the vehicle and extract a lot of private information, such as where the driver works, with which people the driver communicates, his/her eating preferences, what kind of entertainment he/she enjoys, or even if he/she has health problems.

[1] *http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety*

[2] *http://evita-project.org*

*In several applications we want to grant access to the data after a given period of time. This means that we encrypt a message so that it can be decrypted after a certain point in the future (but not before).*

In addition, an important problem with current EDRs is that they are not fully standardized, so, for example, it is not clear which information is going to be collected and for how long it will be stored. NHTSA might have made the first step toward their standarization; nevertheless, the least requirements can be exploited by manufacturers. First, the proposed standard for EDRs sets a minimum duration of 5 s before the crash but no maximum after it, so given the low cost of storaging, EDRs could record for hours or days after such an event. Second, NHTSA's standard requires the recording of 15 data elements and another set of 28 data elements optionally, if they are present. Nevertheless, this standard does not prohibit manufacturers from recording even more elements, such as audio, video, or geospatial data.

Even with the existing EDRs, there is a lot of information that can be extracted. More advanced EDRs, which can be considered more invasive as well, enable storing the GPS location of the vehicle, sending the EDR information on the Internet, and contacting services in case of emergency.[3] The latter EDRs are also being used by many insurance companies in exchange for reduction in insurance costs or in order to promote more security services.[4] Such EDRs can identify various maneuver types, and use this information to profile the driver's skills and behavior. This way, "good drivers" can pay less in the future, and "bad/risky drivers" will have to pay more [15]. Nevertheless, such policies expose drivers' and passengers' privacy greatly [11]. Finally, proposed EDR extensions as in [6], where authorities can arbitrarily query EDRs remotely, generate even more citizen monitoring issues.

Moreover, the computerization of vehicles and the wide adoption of the Internet could make us speculate that the automotive industry would try to promote a model in which the EDR would be connected through the Internet and would store their information in an online database owned by the manufacturers. In such case manufacturers would play the role of a "trusted party," and if they misbehave, users' privacy requirements can be bypassed without their consent. On the other hand, if the user is the one who manages these data, he/she could tamper with the data to take advantage in case legal actions are taken after an accident occurs. More important, if the data are fully controlled by the driver (i.e., they can only be accessed with the driver's consent), if the driver is severely injured or dead the data cannot be obtained, and the EDR become useless.

Therefore, the questions that arise from the above are:

- Who owns the data collected by an EDR?
- Who manages the data collected by an EDR?
- Who is responsible for storing the data?
- How much data are stored?
- How will the data be stored and accessed?
- For how long will the data be stored?

All these questions are clearly related to the right to privacy of drivers and passengers. The privacy concerns about the current EDRs of vehicles, from one of the creators of IEEE 1616, T. Kowalick, is that law enforcement authorities, insurance companies, and even criminals could collect information about the driver's identity and his/her driving habits, trying to trap him/her with this information. Currently, accessing this information is in many cases quite easy through a car's OBD-II port and widely used automotive software [9].

In addition, recent developments in the automotive industry enable manufacturers to go even one step further with EDRs. For example, in its latest models, BMW has the automatic *teleservice* call feature, which automatically gathers all service-related data and sends them to a local dealership for analysis, and if the car requires maintenance, it arranges an appointment.[5] This way, the information about the vehicle and its driver, which is private in several ways, is transferred to the manufacturer.

Although manufacturers that collect these data could misbehave and obtain sensitive and private information about drivers, we do not support the idea of considering manufacturers the main privacy threat. The privacy issue resides in the fact that there is no actual protection within an EDR, and attackers that get access to the vehicle can use EDR to collect very sensitive information. Thus, the protection of EDR pursues several goals:

- Protect the privacy of drivers against unauthorized intruders and (authorized) manufacturers
- Guarantee the proper use of EDRs in case of accidents
- Guarantee the correctness and integrity of the data stored in EDRs

## Timed Release Encryption

Encryption has a wide range of applications in computer science and telecommunications, mainly to permanently secure our data from unauthorized entities. However, in several applications we want to grant access to the data after a given period of time. This means that we encrypt a message so that it can be decrypted after a certain point in the future (but not before).

We can find a clear application of this kind of scheme in bidding processes. The bidders place their bids and want to be sure that they are sealed in such a way that they cannot be opened before, for example, three days. Another application of the same concept is the case in which someone writes a diary and wants to enable everyone to read it after at least 50 years so that all the people mentioned have passed away. With the aim to address this kind of problem, the concept of time released encryption (TRE) was proposed.

TRE was introduced in May 1993 [10]; however, the original approach was based on trusted third parties (TTPs). On the contrary, modern approaches use what we call *time-lock puzzles* (i.e., computational problems that cannot be parallelized and require a precise amount of CPU time to be solved). The non-parallelization requirement is essential in order to avert entities with access to many processing resources, like clusters, taking advantage of others that do not.

[3] *http://news.mercedes-benz.co.uk/uncategorized/mercedes-benz-ecall-faster-help-at-a-crash-scene.html*

[4] *Such as OnStar: https://www.onstar.com and AcuraLink: http://owners.acura.com/acuralink*

[5] *http://www.bmw.com/com/en/owners/service/teleservices/automatic_teleservice_call/introduction.html*

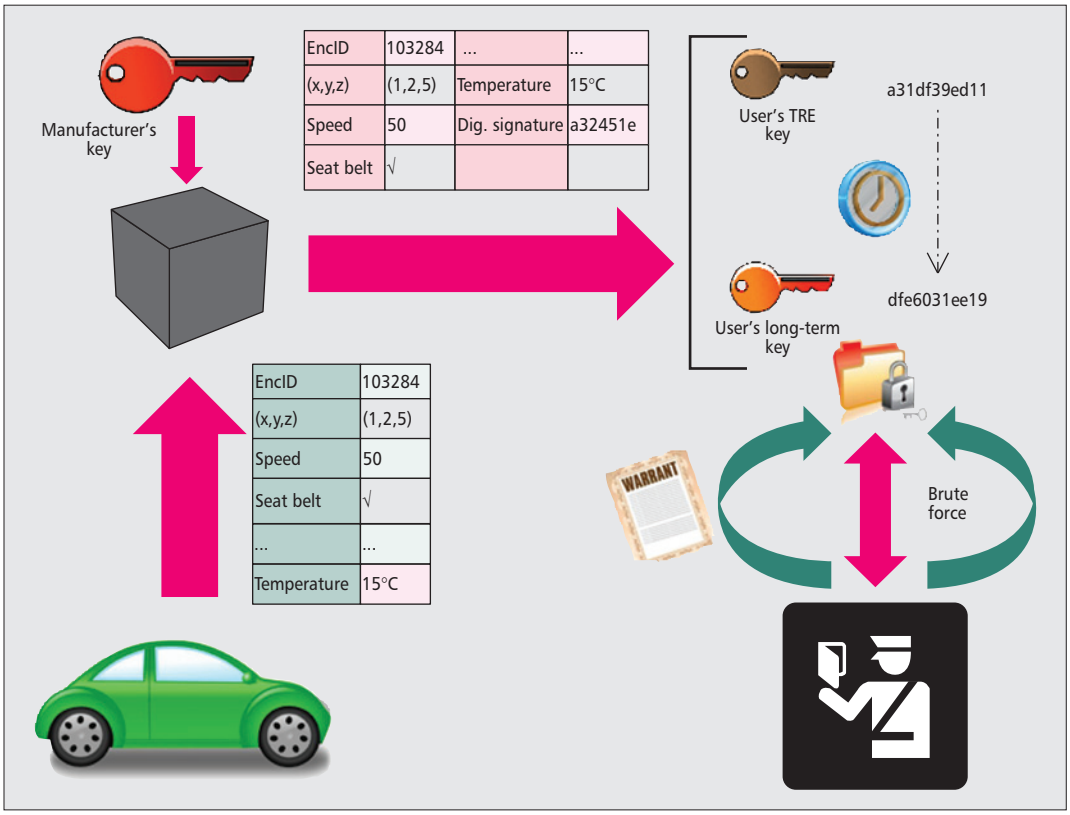


**Figure 2.** *The vehicle EDR collects data and generates vectors* **v** *signed with the key of the manufacturer. These records are encrypted using TRE and stored in the short-term storage. Records in the short-term storage can be decrypted by solving the time-lock puzzle.*

*Protecting the privacy of drivers (i.e. by preventing the access of others to the data stored in EDR) could be easily done. A simple solution to the problem would be to encrypt the data locally with a key only known by the driver.*

Several time-lock puzzles are based on the RSA encryption algorithm [13]. In a general scheme that releases an encrypted message $m$ in $T$ s, the procedure works as follows. First, we pick two large prime numbers, $p$ and $q$, and calculate their product, $n = pq$, and its Euler's totient, $\phi(n) = (p - 1)(q - 1)$. Then we compute $t = TS$, where $S$ is the number of square operations modulo $n$ per second that the potential receivers could perform. Next, we pick an encryption algorithm $E$ and a key $K$, and we encrypt the message $m$ with algorithm $E$ and key $K$ to obtain

$$C = E_K(m)$$

Afterward, we pick a random number $a \bmod n$ and compute

$$C' \equiv K + a^{2^t} \bmod n$$

Finally, we publish the parameters:

$$(n, a, t, C, C')$$

The only way to solve this puzzle (i.e., find the value of $K$ to decrypt $C$ and obtain the original message $m$) is to take $a$ and perform $t$ square operations modulo $n$. Note that parallelizing this procedure is not possible, and any gain obtained in the process would be compensated by the communication costs. This way, we can ensure that the encrypted message will not be disclosed before the desired period of time.

## Our Privacy-Aware EDR

Protecting the privacy of drivers (i.e., by preventing the access of others to the data stored in EDR) could easily be done. A simple solution to the problem would be to encrypt the data locally with a key known only by the driver. This approach solves any privacy problem; unfortunately, the problem that arises is that in the case of a serious accident the driver might die and would not be able to provide the decryption key to the authorities. After all, the main role of EDR is to provide information regarding severe accidents, and in these cases, a plain encryption scheme makes EDR useless.

Our scheme for privacy-aware EDR seeks to find the right balance between the privacy of drivers and passengers and the effective use of EDR by authorities in case of an accident. Therefore, our proposal allows authorized parties (i.e., authorities, insurance companies, vehicles manufacturers, etc.) to have access to the data stored by EDR without the intervention of the driver in emergency situations *only* (e.g., after an accident). Moreover, our scheme grants them access to the *latest* recorded values only. The complete log file is only available to the driver. Hence, authorities can gain access to old data only if drivers consent.

We assume that with the sustained reduction of the cost of solid state storage solutions, vehicles' EDRs could store all their information in such devices. Hence, our solution considers two different kinds of storage: short-term and long-

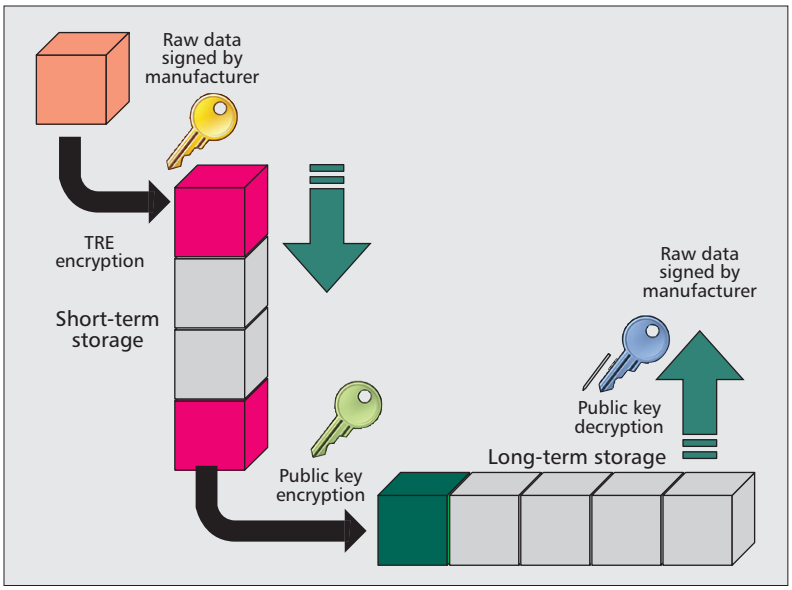


**Figure 3.** *Short-term and long-term storage schemes: When the short-term storage is full, the oldest TRE-encrypted record is encrypted with a public key scheme and transferred to the long-term storage.*

term. Different encryption mechanisms are used in either case to provide the necessary privacy to the driver. For short-term storage we use a timed release encryption scheme with algorithm $E$, which has a release period of $T$ days. On the other hand, for long-term storage, we use a public key algorithm $E'$, with keys $e$ and $d$ for encryption and decryption, respectively.

At regular intervals (e.g. every 10msec) the EDR creates a vector $\mathbf{v}$ that contains the values that have to be stored. Apart from these data, the EDR appends two more values:

- [*EncID*], a unique record identifier, generated from a crypto-counter [7] that is keyed by the manufacturer and initialized with different values for each vehicle.
- [*VIN*], the vehicle identification number. The resulting data vector is signed by the manufacturer (by using a regular signature scheme Sig(·) and private key $P_k$ embedded in the EDR), and the output for each record is:

$$m = (EncID, VIN, \mathbf{v}, Sig_{P_k}(EncID|VIN|\mathbf{v}))$$

This record $m$ is the one to be protected by our privacy-aware EDR. As stated above, we cannot use a simple encryption scheme because it could make EDR useless. Thus, in our approach, the EDR takes the record $m$ and encrypts it using TRE and a key provided by the driver. As a result, a record $c$ with a release period of $T$ days is obtained and stored in the short-term storage (refer to Fig. 2 for a graphical representation of this procedure).

We assume that the short-term storage has capacity for a predefined number $n$ of TRE-encrypted records. For example, if we want to store data for an hour and we generate a vector every second, the short-term memory will store at most 3600 TRE-encrypted records: $\{c_1, c_2, \ldots c_{3600}\}$. When the short-term storage is full and a new TRE-encrypted message arrives (e.g., in our example $c_{3601}$), the oldest TRE-encrypted message stored in the short-term storage (e.g., in our example $c_1$) is popped, releasing the necessary space for the next record to be stored. The popped message $c_1$ will be re-encrypted with a public key cryptosystem $E'$,

$$[c_1' = E'_e(c_1)]$$

and the resulting record $c_1'$ is transferred to the long-term storage where only the driver will be able to decrypt it by using his/her private key $d$. (Fig. 3 provides a graphical representation of this procedure).

By using TRE, records in short-term storage could be decrypted by authorities in case of accident, and public key cryptography guarantees that records in long-term storage are only accessible to the driver. Thus, the privacy of our scheme could ease the storage of more sensitive data like location data without the opposition of privacy advocates.

An implementation of this scheme has been made in Python to evaluate the performance of the scheme. The code has been tested on a typical desktop PC; on average, 0.041 ms is needed for each encryption with AES, the RSA key generation needs around 0.011s, and for the encryption of each vector with TRE, we need around 4 ms. More precisely, in order to store each vector, on average 4.76 ms are needed, with a maximum of 5 ms and standard deviation 0.2 ms. Given that vehicle EDRs typically store the values at rate not more than 10 ms, the processing cost can be considered at least affordable. Additionally, we should highlight that the scripting nature of Python slows down many computations. Nevertheless, the precessing overhead does not introduce a cost which is above the needed timeframe of 10 ms; hence, we can deduce that the proposed model can be efficiently implemented in an embedded system.

## Threat Model and Discussion

Each of the methods used in our scheme provides a new layer of security against several attacks, discussed next.

The first thing we do with the data sent from the vehicle is to append an [*EncID*] and the [*VIN*]. The addition of these fields to the vector of data $\mathbf{v}$ is crucial, as they enable tracing whether a record has been injected or removed (e.g., by the driver). The VIN guarantees that the EDR belongs to a given vehicle and cannot be replaced, and the crypto-counter creates a sequence of pseudo-random values that cannot be duplicated by another entity (without knowing the generation key). Note that an attacker might try to copy and paste signed vectors from other vehicles. However, the combination of the crypto-counter and the chassis number makes our privacy-aware EDR immune to such attacks. A graphical representation of this possible attack is given in Fig. 4.

Afterward, the next step is to sign the data with the manufacturer's key. After this step the message gains authenticity and integrity and cannot be tampered with. The combination of the crypto-counter, the chassis number, and the signature of the manufacturer guarantees that nei-

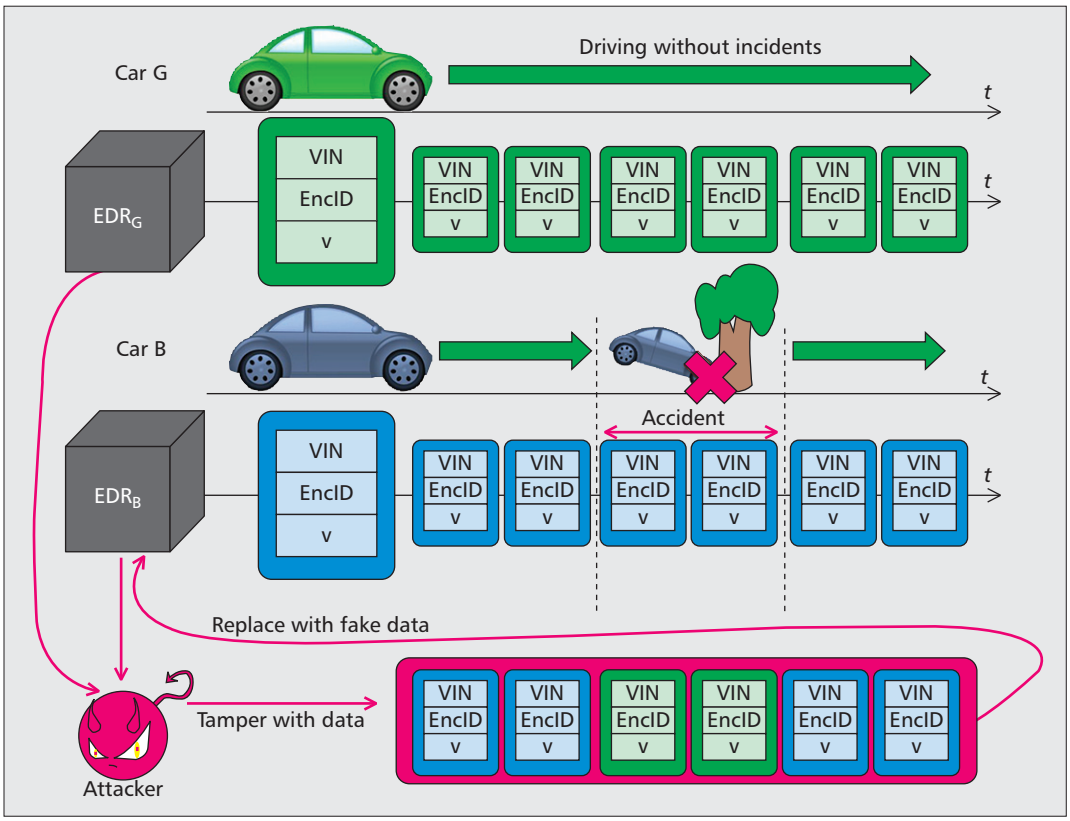


**Figure 4.** *Graphical scheme of a possible attack. After having a crash with his/her car, the attacker might try to tamper with the EDR data to cover the accident by replacing the piece of data of the accident with data from another EDR.*

ther the driver nor an attacker can tamper with the data without being detected.

The time release encryption used in short-term storage allows authorities to access the complete short-term log files of the EDR in, at most, $n \times T$ days (where $n$ is the number of records in the short-term storage) or in $T$ days if $n$ systems are used in parallel to decrypt each record individually (note that the decryption of each individual record cannot be parellelized due to the very properties of time-lock puzzles). This is a very important property of our scheme, as it prevents anyone from trying to invade drivers' privacy indiscriminately without any good reason and computational resources. The fact that the authorities could gain access to the data in $T$ days if they have a cluster with $n$ nodes guarantees that trying to invade someone's privacy is costly and should not be done unless it is really necessary. This prevents massive and indiscriminate violations of drivers' privacy.

Finally, for long-term storage we propose the use of a public key encryption algorithm since it provides more security to the data. Vehicles are quite often left unattended for long times, which means that attackers might have physical access to them. An attacker might try to access the vehicle log files stored in the EDR without the driver's consent while the car is unattended. In this situation, if we use symmetric cryptography instead of public key cryptography, the attacker could manage to start the vehicle and steal the symmetric key that would be loaded in the memory of the EDR. Recent side channel attacks, like timing or power analysis attacks, would enable an attacker to access the key or part of it. On the contrary, in the case of public key algorithms, we have two keys, one for encryption and one for decryption. Therefore, the attacker can only gain access to the encryption key (which is in memory), but not to the decryption key. Hence, the long-term storage in our privacy-aware EDR remains secure.

For some reasons such as criminal investigations, authorities might need to access older data — something that current versions of EDRs do not support. In such situations our privacy-aware EDR with long-term storage might help. Considering that the data in long-term storage is encrypted with a public key cryptosystem, the driver has to collaborate with the authorities to decrypt them. If the driver is not collaborative, authorities should apply the legal framework at their disposal to address the situation.

*Considering that the data in the long-term storage is encrypted with a public key cryptosystem, the driver has to collaborate with the authorities to decrypt them. If the driver is not collaborative, authorities should apply the legal framework at their disposal to address the situation.*

## Conclusions

Finding the right balance between safety and privacy is a tough problem, especially in the context of the automotive industry in which safety is a must.

The great technological advances that are included in modern vehicles open the door to great opportunities to improve the driving experience, and the safety of drivers and passengers. However, if the proper measures are not taken, using such technologies could put the privacy of people in jeopardy.

*Drivers and passengers can protect their privacy and, at the same time, gain full advantage of using black boxes. In addition, authorities and manufacturers can access the data they really need in case of accident so as to improve the safety of drivers.*

In this article, we have analysed the case of event data recorders, commonly known as black boxes. We have shown that due to the use of this technology along with Internet and wireless communications, a number of attacks could be executed to steal information and endanger the privacy of the users of the vehicle. Also, we point out that drivers have no protection against the misuse of those data.

With the aim to cope with the privacy issues related to EDRs and, at the same time, guarantee their full functionality in case of accidents, we have proposed a cryptographic scheme that uses time release encryption (TRE) and public key cryptography (PKC). Thanks to the use of PKC, users have full control over their long-term stored data. In addition, by applying TRE on the short-term stored data, authorities and manufacturers can decrypt the information in case of accidents, and other large scale attacks are prevented by the high computational cost they would impose. As a result, drivers and passengers can protect their privacy and, at the same time, gain full advantage of using black boxes. In addition, authorities and manufacturers can access the data they really need in case of accidents in order to improve the safety of drivers.

## Disclaimer and Acknowledgments

This work was partly funded by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-0004 "ARES," project TSI2007-65406-C03-01 "E-AEGIS," project TIN2011-27076-C03-01 "CO-PRIVACY," and the Government of Catalonia under grant 2009 SGR 1135.

Agusti Solanas is with the UNESCO Chair in Data Privacy, but he is solely responsible for the views expressed in this article, which do not necessarily reflect the position of UNESCO or commit that organization. Agusti Solanas thanks the Department of Mathematics of the University of Roma Tre, Italy, where he was doing a research stay while this article was written, and he is grateful for the financial support of the Spanish Ministry of Education, Culture and Sport with the José Castillejo Grant CAS0200/2012.

## References

[1] E. Biham *et al.*, "How to Steal Cars — A Practical Attack on Keeloq," *CRYPTO 2007*, 2010.
[2] A. W. M. Bonnick, *Automotive Computer Controlled Systems: Diagnostic Tools and Techniques*, Automobile Electronics, Taylor & Francis Group, 2001.
[3] S. Checkoway *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," *USENIX Security*, 2011.
[4] FBO, Cyber Security and Safety of Motor Vehicles Equipped with Electronic Control Systems, Solicitation Number: Dtrt57-11-ss-00007, tech. rep., Federal Business Opportunities, 2011.
[5] T. Hoppe, S. Kiltz, and J. Dittman, "Security Threats to Automotive Can Networks — Practical Examples and Selected Short-Term Countermeasures," *Proc. Computer Safety, Reliability, and Security (SAFE-COMP)*, 2008, pp. 235–48.
[6] J.P. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles," *IEEE Security Privacy,* vol. 2, no. 3, 2004, pp. 49–55.
[7] J. Katz, S. Myers, and R. Ostrovsky, "Cryptographic Counters and Applications to Electronic Voting," *Advances in CryptologyEurocrypt 2001*, 2001, pp. 78–92.
[8] K. Koscher *et al.*, "Experimental Security Analysis of A Modern Automobile," *IEEE Symp. Security and Privacy*, Oakland, CA, 2010, pp. 447–62.
[9] T. M. Kowalick, *Black Box: What's under Your Hood?*, MICAH, 2005.
[10] T. C. May, Timed-Release Crypto, http://www.hks.net/cpunks/cpunks-0/1460.html, Feb. 1993.
[11] P. R Mueller, "Every Time You Brake, Every Turn You Make — I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information," *Wis. L. Rev.*, 2006, p. 135.
[12] C. Patsakis and K. Dellios, "Securing In-Vehicle Communication and Redefining the Role of Automotive Immobilizer," *SECRYPT*, 2012, pp. 221–26.
[13] R. L. Rivest, A. Shamir, and D. A. Wagner, "Time-Lock Puzzles and Timed-Release Crypto," tech. rep./memo MIT/LCS/TR-684, MIT Lab. for Computer Sci., Feb. 1996, (Revision 3/10/96).
[14] T. Schütze, "Automotive Security: Cryptography for Car2x Communication," tech. rep., Rodhe & Schwarz, Mar. 2011.
[15] T. Toledo, O. Musicant, and T. Lotan, "In-Vehicle Data Recorders for Monitoring and Feedback on Drivers' Behavior," *Transportation Research Part C: Emerging Technologies*, vol. 16, no. 3, 2008, pp. 320–31.
[16] A. Martínez-Ballesté, P. A. Pérez-Martínez, and A. Solanas, "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible," *IEEE Commun. Mag.*, vol. 51, no. 6, June 2013.

## Biographies

Constantinos Patsakis (patsakik@scss.tcd.ie) is a research fellow at Trinity College. He received his B.Sc. in mathematics from the University of Athens, Greece, and his M.Sc. in information security from Royal Holloway, University of London. He received his Ph.D. from the Department of Informatics of the University of Piraeus. His main areas of research include cryptography, security, and privacy.

Agusti Solanas (agusti.solanas@urv.cat) is a researcher at URV. He received his M.Sc. degree in computer engineering from Universitat Rovira i Virgili in 2004 with honors (Outstanding Graduation Award). He received a Diploma of Advanced Studies (Master's) in telematics engineering from Universitat Politècnica de Catalunya in 2006 and a Ph.D. in telematics engineering from UPC in 2007 with honors. His main fields of activity are privacy and security. He has authored over 90 publications. He is a member of the ACM.