ISSN: 1231-4005
e-ISSN: 2354-0133
DOI: 10.5604/12314005.1217298

DATA EXCHANGE IN A TACHOGRAPH SYSTEM AS THE ELEMENT OF THE CYBERSECURITY OF THE MODERN CAR

Michał Śmieja

University of Warmia and Mazury
Faculty of Technical Sciences
Department of Mechatronics
Słoneczna Street 46a, 10-710 Olsztyn Poland
e-mail: smieja@uwm.edu.pl

Marcin Rychter, Piotr Sułek

University of Life Sciences in Lublin
Faculties of Production Engineering
Department of Power Engineering and Transportation
Głęboka Street 28, 20-665 Lublin, Poland
e-mail: rychter@poczta.fm

Abstract

A numerous flows of data in the modern vehicle are necessary to maintain the complexity of systems included on-board. Unfortunately, along with the increase of the road security and many useful facilities there are arising vulnerabilities coming from cyberattacks and reliability of the communication systems. Because many components are based on highly advanced E/E technology, the security measures known from IT are more and more important. The data encryption mechanisms, used in IT for memory content and data transfer protection, are getting important in automotive. In the paper there are presented considerations connected with the cybersecurity of the vehicle, as a part of the transportation system, as well as the effect of the process of the production. In the article authors focused on the encryption of the communication between the tachograph device and the motion sensor. The normal operation of the interface tachograph-sensor follows the operation of pairing based on authentication and identification services. The pairing operation takes place in an authorized workshop and its goal is to check the legality of devices paired, and the so-called establishment of the session key, which contains encryption keys used for 3DES encryption. The description of data encryption for the motion sensor, presented in the article, is the example of the bunch of solutions required for the modern vehicle.

Keywords: *tachograph, motion sensor, cybersecurity, sensor pairing, encryption data*

1. Introduction

Despite the many legal and economic initiatives taken by governmental agencies responsible for the structure of the transport systems, a significant portion of the carriage is performed in road traffic. Flexibility and reliability of the road transport plays a basic role in this respect. Construction and operation of a modern truck, due to the numerous requirements in terms of energy consuming and ecology, is associated with the increasing use of electrical and electronic systems (E/E) to manage the components of the vehicle. Replacing many mechanical couplings used in the construction of older generations' vehicles with E / E systems significantly raises the possibility of modifications of the present in these couplings interactions and the optimization of the entire system. The production and operation of such devices differ from the traditional approach. They are based largely on the data exchange and processing and hence they face new IT-specific problems and threats. Many of these issues have been previously identified, and methods for resolving them were developed, outside the automotive industry. This reduces significantly the way for their implementation in these applications. The information channels between vehicle components are exposed to cyber-attacks, the objective of which is the interference with the operation of the vehicle by the impact on the processed data. The basic condition for the vehicle to be released for driving on the road is control in terms of the proper level of security of interaction with other objects in its environment. A special case in this respect is digital tachograph system. Unlike typical supervisory mechanisms, which are limited to control the technical condition of the vehicle itself, digital tachograph system considers a team of the vehicle / the driver as one object. Considering it, security challenges consist on preventing the falsifying of the tachograph records used to control the working time of drivers. Known attacks on the digital tachograph system are presented in [7, 10]. Appropriate protection against various types of attacks requires a variety of resources and a reference to the entire life cycle of the individual components and the whole system.

2. Safety and security of tachograph system

The functioning of the numerous objects is more and more based on the processing of the increasing number of information. Communication mechanisms allow the system to function in interaction with other systems, however, with the risk of unwanted interference in their information assets. The problems of the IT system reliability are considered generally in two categories related to the cause of potential disfunction. The first group of technics leading to prevent the improper functioning is defined as IT safety. It is related to internal technical influences on the system improper functioning or its harmful effects on the ambient environment. Data encryption to improve IT the safety is not always beneficial, because it is by nature resulted in a significant increase in the software complexity, difficulties in debugging and the processing slow down. Safety mechanisms on are based primarily on the errors-free software development, control mechanisms, detection of unwanted events and using mechanisms (where possible) preventing the negative effects of the error and its deepening or restoring to normal functioning. An example of a safety element may be the “watch dog” mechanism. Watchdog restores the system by performing the reset operation. The safety optimization of it is carried out by setting the refresh time of the watchdog timer, so that the effects of temporary dysfunction on the system were mitigated as much as possible. In the case of (described below) the security, if there has been interference, the system should put on hold and signal the fact of its occurrence. Safety requirements in the automotive are described, among others, in a standard ISO 26262 [4]. The main objective of the digital tachograph system on board is the supervision and control function. Therefore, in that case the most important is the security, as the way of counteracting malicious / adverse impacts on system by interfering in the communication mechanisms between its elements. In terms of security, OSI security architecture refers to such terms as security attack, security mechanism, security service [11]. At the end user environment, stage of the motion sensor life cycle [10] the main threat is so called active type of security attack. The consequence of such an attack may be undesirable modification of the content of the data stream between the motion sensor and the tachograph, in order to falsify information about the vehicle speed and distance. Passive type of security attack is a type of attack in which the transmitted data are disclosed, but not modified. Passive type of security attack could pose a threat at the stages where the confidential data are transferred (e.g. Encryption keys). In order to repel security attacks, there are security mechanisms, which implement so-called security services such as: authentication (message origin authentication, entity authentication), data confidentiality or data integrity [2]. Basic security mechanism used in the system of digital tachographs is encryption. The elements of the tachograph system use so-called symmetric and asymmetric decipherment algorithms. Encryption scheme of data exchange between the card, the tachograph and motion sensor is presented in Fig. 1.

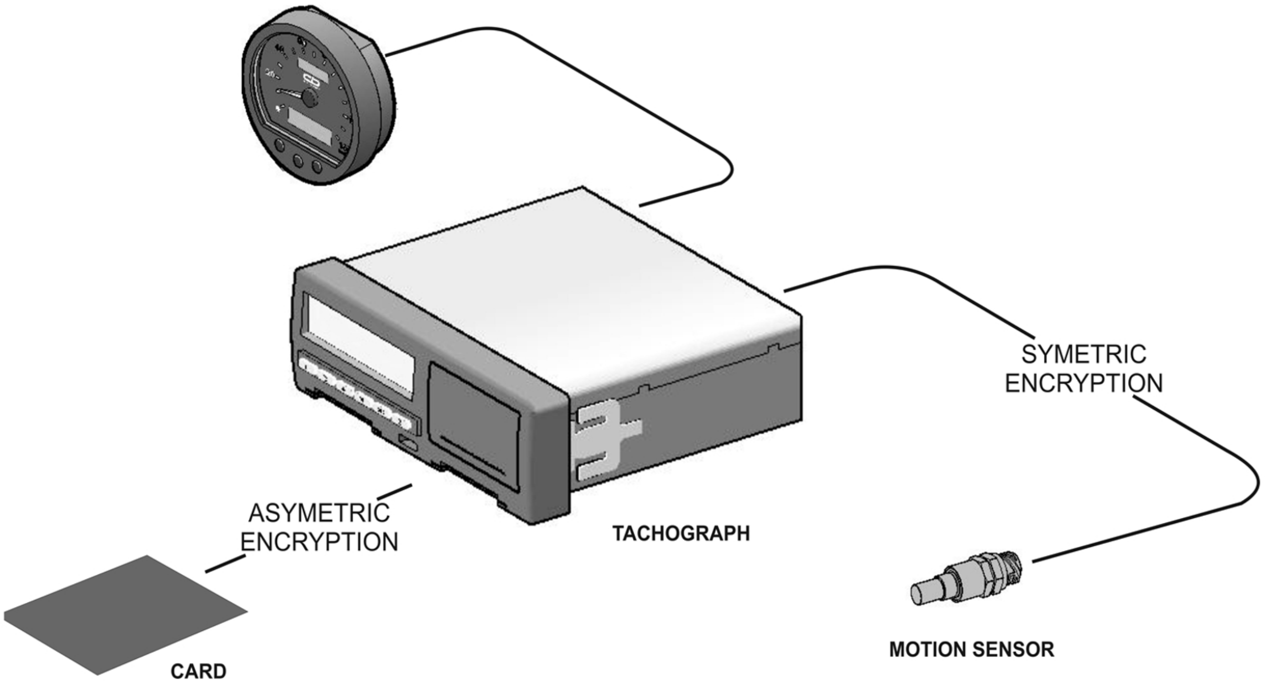

Fig. 1. The scheme of a tachograph encrypted data exchange

Due to the different nature of interfaces card-tachograph and tachograph-sensor, they use different encryption. Since the tachograph must be able to work with multiple cards (workshop card, drivers cards, inspector cards), data transmitted via interface tachograph-card is encrypted asymmetrically using public and private keys. A pair of sensor-tachograph functions a fixed connection that may be break up only in case of tachograph or motion sensor change (the malfunction, tachograph of sensor type upgrade), so that the symmetrical encryption is used.

3. Data exchange security in the life cycle of motion sensor

The use of symmetric encryption of data in motion sensor-tachograph interface extends the security issue beyond the normal operation of the tachograph system. The figure 2 shows the construction of a hi-tech motion sensor that meets EAL4+. The connector (1) connects the motion sensor with the cable to the vehicle unit. It also contains the interface to the vehicle unit (data interface) and the power supply. The crimping (2) links the connector with the body (3). Inside of the body, the Printed Circuit Board PCB (4) performs the logical security functions of the sensor. It is connected with the Hall sensor for motion detection speed signal interface (5).

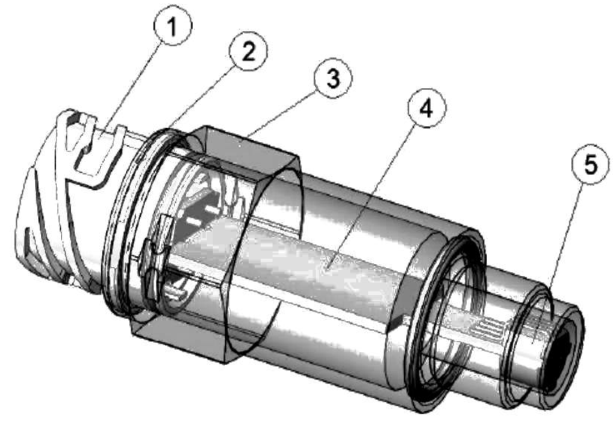

Fig. 2. The motion sensor DTMS (BogArt)

Exchange of the vehicle movement data between the motion sensor and the tachograph is done by serial communication and analogue signal as described in detail [10]. Redundant nature of such data transmission, unlike many systems, is not resulted from safety considerations, but from the security. Although the content of information transmitted in both channels is the same, unlike many redundant systems, it is not possible to operate the device if one of the interfaces is defected. The purpose of the dual channel is mutual control of the data transmitted in each of them individually. The difference in content transmitted by the analogue and digital channel is considered as the damage or an attempt for externally modifies the motion data delivered to tachograph. According to the applicable regulations, the operation of the vehicle is in such a situation prohibited. In order to counteract active security attack, ISO 16844 requires a symmetric encryption of transmitted data according to the algorithm Triple Data Encryption Standard (3DES), using two encryption keys [8]. The normal operation of the interface-tachograph sensor follows the operation of pairing based on authentication and identification services. The pairing operation takes place in an authorized workshop and its goal is: to check the legality of devices paired, and the so-called establishment of the session key, which contains encryption keys used for 3DES encryption. The time from the moment of the pairing execution, until next pairing, is called a session. The end of the session, e.g. as a result of damage and/or replacement any of the elements of the tachograph / sensor requires another pairing thus the next session begins.

4. The process of preparing the motion sensor for exploitation

Proper preparation of the sensor to the correct pairing requires a number of technical and organizational activities in accordance with the procedures defined in the key management and key provisioning structure [1, 3]. The main participants are producers of motion sensors, tachograph manufacturers, cards manufacturers, certification bodies and institutions coordinating the flow of information. At the final stage of the manufacturing process, the manufacturer sets the sensor extended serial number containing the basic information about the place and date of manufacturing, type of sensor, the manufacturer code (according to the marking European) and the sensor serial number. The extended serial number Ns is public and as such is sent (in plain text), along with the generated pairing key Kp (encrypted) to the relevant Member State Certification Authority (MSCA). MSCA encrypts Kp with Master Key (Mk), received from the European Root Certification Authority (ERCA). Extended serial number is encrypted by MSCA with an identification key (Kid) key calculated from master key. Encrypted Ns and Kp are stored in non-volatile memory of the motion sensor. In this state, the motion sensor is ready for installation in the vehicle. In order to perform encrypted data exchange resistant to security attacks, master key Km is also transmitted in two separate parts (Kmvu, Kmwc) to tachograph manufacturer and cards manufacturer.

The pairing process, shown in Fig 3 begins with the insertion of the workshop card (which a part of the master key Kmwc) in the tachograph. The master key parts KmVU and Kmwc can trigger a master key Km and identification key Kid. On the request of the tachograph, the sensor sends unencrypted extended serial number Ns. Using the generated identification key Kid, the tachograph encrypts Ns with Kid and sends encrypted Ns to the motion sensor. The positive result of the comparison of the encrypted Ns stored in the memory of the motion sensor and the one received from the tachograph allows continuing pairing. In the next step, encrypted (in MSCA) with master key Km pairing key Kp is sent to the tachograph where it is decrypted with master key Km generated in the tachograph. Thanks to this operation, the tachograph and sensor have the same pairing key Kp. For the session to be the final result of the pairing, tachograph generates a random session key Kses that will be used to encrypt and decrypt messages exchanged between the motion sensor and tachograph during the session. Than the tachograph encrypts Kses with Kp and sends it to the motion sensor. Motion Sensor, after Kses decryption with Kp, can use Kses to encrypt and decrypt data in the same way as the tachograph.

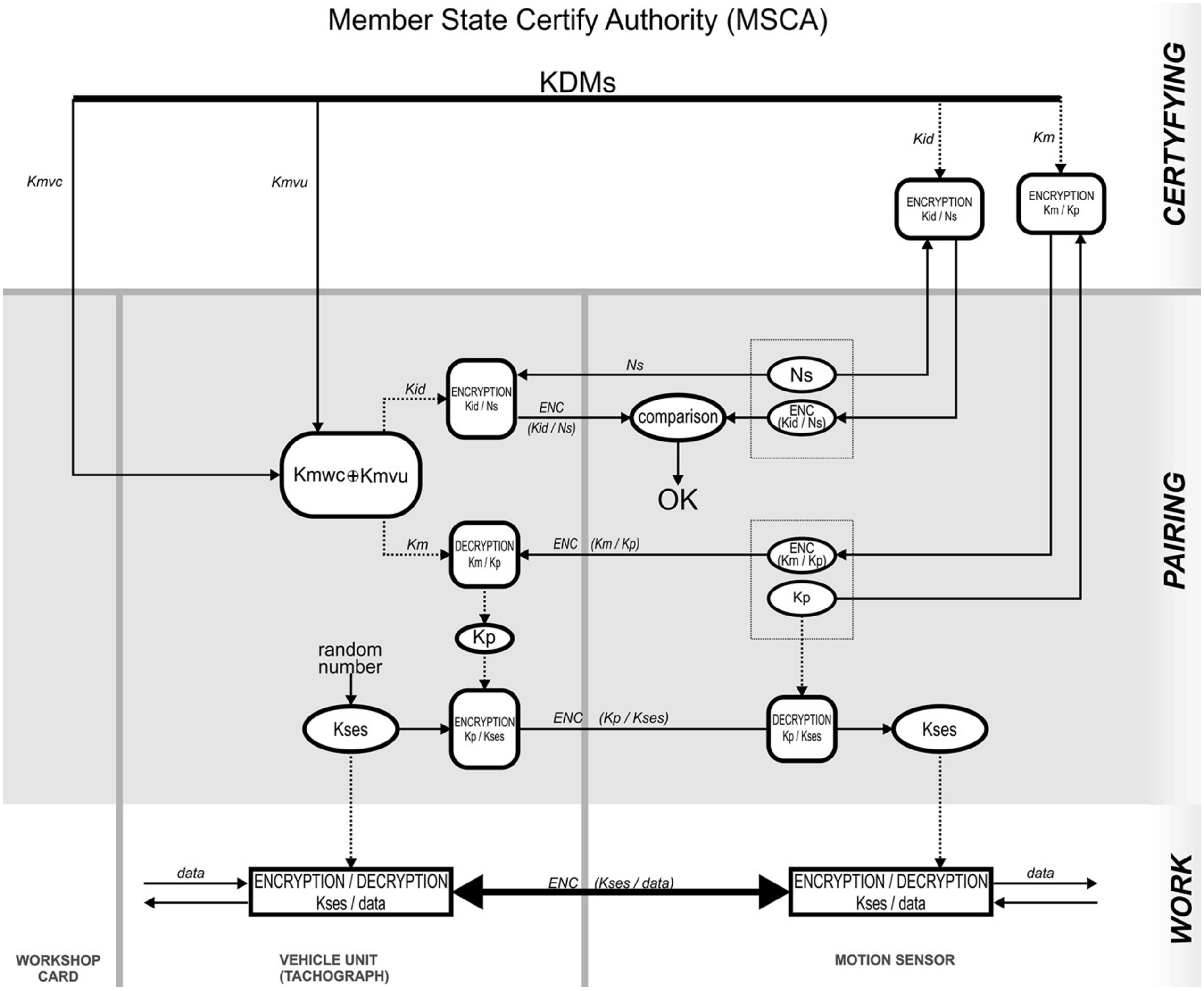

Fig. 3. The scheme of pairing motion sensor-tachograph

5. Summary

The modern approach to the protection of the subsystems of the vehicle as well as their components becomes more and more complex, so from the point of view of the product lifetime and existing threats. Due to the nature of numerous components, based on highly advanced techniques of E/E, the importance of safeguards known at IT is increasing. Developed earlier data encryption mechanisms used to secure the content of electronic storage and network communication plays increasingly significant role in automotive. Presented in the article description of data encryption for the motion sensor is just a single example of group-wide solutions required by the equipment of the E/E of a modern vehicle. A characteristic feature of such solutions is, apart from purely technical matters, organizational actions relating to e.g. the distribution and security of encryption keys. The robustness of an electronic circuit is not limited to its normal operation. Appropriate security measures must be applied in a much broader scope. The expected steps for further raise the level of safety and reliability of the vehicles provide digital tachograph systems redundancy extension by additional verification of tachograph records by external devices. Already known solutions allows taking of the vehicle motion data from the ABS or an independent GPS receiver. The current legal regulations in this respect [5, 6] does not specify precisely the redundant signal source, however they set clear the follow-up direction. Another expected modification of the transmission systems is to replace the existing 3DES encryption algorithm with more secure AES and increase the encryption strength by extending the length of the encryption key. The inevitable consequence of the progressive expansion of the data protection schemes is the additional overhead of electronic systems that provide transmission. Taken from [9] example demonstrates the fact that twice-longer encryption key results in 4-times longer processing time. The IC manufacturers address this issue by IC performance increase through, among others, the increase of internal clock frequency. Extra phenomenon driving the application of encryption mechanisms can be high growth of Internet of Things technology and related microcontrollers with built-in hardware encrypting peripheral devices.

Acknowledge

The article funded under the project entitled "Development of innovative manufacturing technology of motion sensors to a new generation of digital tachographs, according to the common criteria EAL4 +". The subsidy contract No. UDA-POIG.01.04.00-28-004/11-00 under the measure 1.4 Support special projects of the priority axis 1. Research and development of new technologies, Innovative Economy Operational Programme 2007-2013.

References

[1] Bishop, J.W., Nordvik, J.P., *Digital Tachograph System European Root Policy Version 2.1,* European Communities, 2009.

[2] *Data communication networks: open system interconnection (OSI); security, structure and applications*, Recommendation x.800, The International Telegraph And Telephone Consultative Committee, Geneva 1991.

[3] *Digital tachograph system European root certification authority certification practices*, Statement Version 1.0 European Communities 2004.

[4] Riso, S., Temple, C., Arendts, B., Metz, P., Enser, B., *Functional Safety in accordance with ISO 26262*, ZVEI-German Electrical and Electronic Manufacturers Association e.V., Frankfurt am Main, Germany 2012.

[5] *Rozporządzenie Komisji (UE) nr 1266/2009* z dnia 16 grudnia 2009 r.

[6] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 165/2014* z dnia 4 lutego 2014 r.

[7] Rychter, M., *Budowa i zastosowanie systemu tachografii cyfrowej*, Wydawnictwo ITS, Warszawa 2011.

[8] Stallings, W., *Cryptography and network security principles and practice fifth edition,* Prentice Hall, 2011.

[9] Soja, R., *Automotive Security: from Standards to implementation,* Freescale White Paper.

[10] Śmieja, M., Rygiewicz, A., *Information system safety in a context of automotive applications,* Journal of KONES, Vol. 16, Warsaw 2012.

[11] Wolf, M., Weimerskirch, A., Wollinger, T., *State of the Art: Embedding Security in Vehicles,* Hindawi Publishing Corporation, EURASIP Journal on Embedded Systems Vol. 2007.