Internet of Trucks and Digital Tachograph – Security and Privacy Threats

Marc Sel · Dusko Karaklajic

PwC - Enterprice Advisory - Belgium
{marc.sel | dusko.karaklajic}@be.pwc.com

Abstract

Integration of digital tachographs with emerging technologies, such as Intelligent Transport System (ITS) or fleet management system, extends the initial mission of tachographs. In addition to supporting the enforcement of social and commercial rules, they improve driver experience and increase transport and maintenance efficiency.

On the other hand, trustworthiness of information provided by these "smart" tachographs remains crucial to accurately reflect drivers' activities and prevent fraud. In this article, we analyse how the new trends in digital tachograph technology, such as wireless communication, integration with the ITS and satellite positioning systems, change the security and privacy threat landscape.

1 Introduction

Tachographs have been introduced to improve road safety by supporting the implementation of rules related to driving and rest periods, working time, or maximum speed of a vehicle. Such rules not only improve road safety, but also prevent unreasonable driver working conditions, and foster fair competition. The tachograph equipment has been regulated since 1970 and the current regulation in place is Council Regulation (EEC) No 3821/85 on recording equipment in road transport. So far, the regulation has been adapted multiple times in order to follow technological progress, reduce fraudulent activities, improve efficiency, and cost-effectiveness.

One of the main drivers for improved regulation is the breach of social rules by the transport organizations motivated by commercial interests. By using procedural and technical means to breach the tachograph rules, the organizations and drivers themselves are trying to gain competitive advantage. According to [EC144-11] there are several thousand heavy duty vehicles driving on the trans-European network with manipulated tachograph equipment. On the other hand, in addition to fostering the enforcement the social rules, frequent adaptations of the regulatory framework aim at improving transport efficiency, reducing the costs and the administrative burden by reducing the number of document issuances. To that end, [EC451-11] defines a set of goals to be achieved by the new generation of digital tachographs:

- Remote communication with tachographs for control purposes;
- Automated recording of precise location of a vehicle through global navigation satellite system (GNSS);
- Integration of digital tachographs in Intelligent Transport Systems;

N. Pohlmann, H. Reimer, W. Schneider (Editors): Securing Electronic Business Processes, Springer Vieweg (2014), 1-9

- Merged functionalities of driver cards with driver licence to increase security and reduce administrative burdens.

Given that the trustworthiness of tachograph data remains crucial to accurately reflect drivers' and vehicle behaviour, security of the entire digital tachograph ecosystem must be carefully considered. Even more, since the data in scope includes personal, localisation and behavioural information, privacy protection arises as an important aspect as well. This article discusses how the security and privacy threat landscape is changing with the evolvement of hyper-connected and multi-functional smart tachographs and highlights the most critical impacts.

The rest of the paper is organized as follows: Chapter 2 describes the tachograph ecosystem and lists the system actors. While Chapter 3 introduces the concept of smart tachographs and related emerging technologies, Chapter 4 analyses how the new concepts affects the security and privacy threat landscape. Finally, we conclude in Chapter 5.

2 Digital Tachograph System

The core elements of a tachograph system are shown in Figure 1.

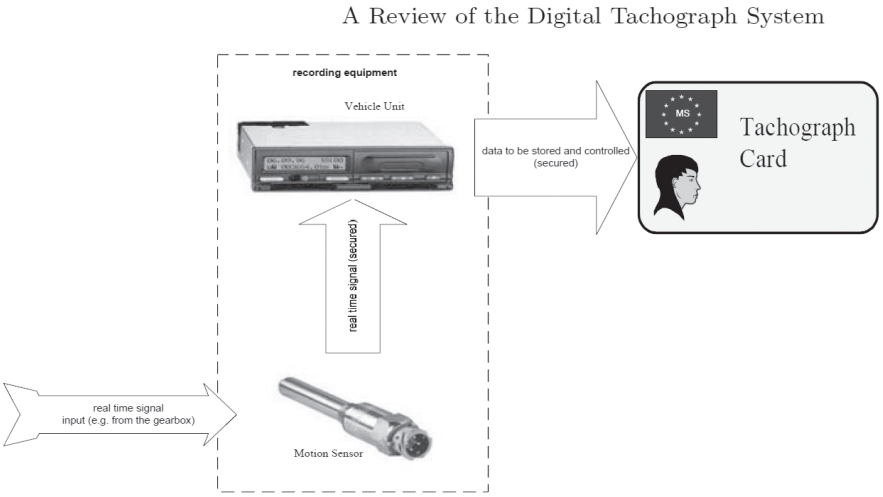

Fig. 1: Core elements of a tachograph system [FULE06]

It consists of the recording equipment, including a vehicle unit and a motion sensor, and a number of tachograph cards used to represent the system actors. It can be observed that today's tachograph is an off-line system. PKI is used for security, but there are no revocation checks done. In what follows, we explain these main building blocks in more detail.

2.1 Recording Equipment

The recording equipment consists of two main components:

- *Motion Sensor*, which measures axel rotation from where speed and distance travelled by a vehicle can be derived. The Motion Sensor is attached to the gearbox and uses a simple

communication interface to provide its measurements to the Vehicle Unit for further processing.
- *Vehicle Unit*, which is meant to be embedded in the central console of a vehicle, and is used to record, store, display, print and output data related to the vehicle and its driver. It can be observed that only physical communication with the VU is possible. There is no wireless interface of any kind present.

The communication between a Motion Sensor and a Vehicle Unit is established via an authenticated and encrypted channel. The detailed data exchange and communication protocols between these two components are specified by the ISO 16844-3 standard.

2.2 System Actors

Actors in a digital tachograph system include the European Commission as regulator, the European Root Certification Authority (ERCA), the Member State's competent authority and their operational CA's, as well as their national Card Personaliser. Additional actors that rely on tachograph smart cards are drivers, workshops (for calibration purposes), vehicle owners (typically companies) and law enforcement authorities. Card management, including issuance, renewal and revocation, as well as the security aspects, is the responsibility of the national competent authorities. Tachonet is used to avoid "card shopping" across the EU, since prior to issuing a card, the competent authority will query all other authorities whether the applicant already obtained a card in another country.

The following four types of smart cards are used:
- *Driver card*, personalized per driver containing the driver's records;
- *Control card,* providing access to the data stored in the system, available only to the law enforcement authorities.
- *Company card*, providing a company access to the data stored in the vehicle unit's memory, e.g. to provide compliance evidence to a national authority with regard to respecting the safety rules (driving the truck with a driving card in place, respecting driving and resting time, etc);
- *Workshop card*, used for the calibration of the tachograph parameters such as vehicle tire size. It is only issued to certified workshops.

For the detailed description of the data model used by the smart cards listed above, we refer the reader to the EU directive [EC02]

3 Smart Tachographs and Emerging Technologies

Ever increasing demands to improve the efficiency and user friendliness of the digital tachograph systems while decreasing the costs, drive the development of new use cases and integration scenarios. The integration with the Intelligent Transport System (ITS) could prevent the duplication of processes and synergy with vehicle on-board units, such as road tolling, fleet management or satellite positioning units. Sharing of information and resources between various in-vehicle applications can enable new and improve the existing functionalities at reduced operational costs. As stated in [ITAP10], the intention is to promote the digital tachograph into "the essential core telematics element in the ITS station of the vehicle concerned".

ITS refers to information and communication technology applied to transport infrastructure and vehicles in order to improve transport safety and efficiency, as well as to improve drivers' experience. An overall ITS architecture presented by ETSI in [ETSI10] is shown in Figure 2. Its main building blocks are vehicles, road side units and a network infrastructure. In the further analysis, we focus on the vehicle unit (ITS-S (Vehicle) in Figure 2).

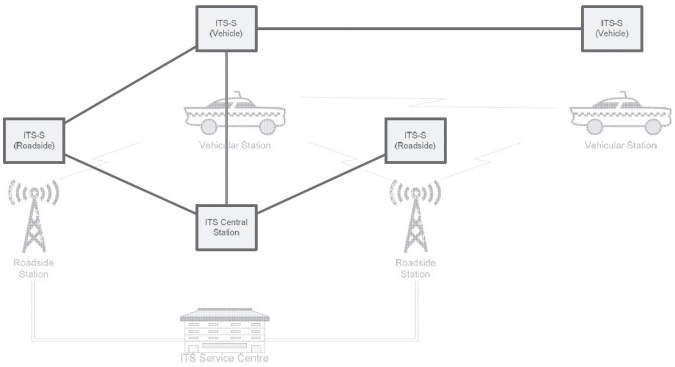

Fig. 2: ITS Architecture [ETSI10]

The scenario in which we analyse security and privacy risks assumes that the information provided by digital tachographs is integrated with other in-vehicle applications, for example automatic gear shifting [ECIA11], automatic keeping of distance and breaking, and communication with the remote parties and service providers such as road-pricing authorities, insurance companies and emergency services as shown in Figure 2. Further, in addition to the integration with the ITS, it is assumed that the future digital tachograph system includes a satellite positioning sensor and a wireless interface for remote control, as envisioned in [EC451-11]. In what follows, we denote such tachograph as a *smart tachograph*.

The next section analyses security and privacy threats to smart tachographs.

4 Security of digital tachograph systems

Data provided by a digital tachograph system is of no use if its trustworthiness is not guaranteed. It must accurately reflect basic data such as the activities of drivers and vehicles, including driving and rest periods, as well as the maximum speed. Such data needs to be usable in legal proceedings. Therefore, security of digital tachograph systems is crucial for preventing malicious and unlawful behaviour of system's actors and for protecting privacy sensitive data stored on the personalized cards.

We now describe the main threats to integrity, authenticity, availability and confidentiality of the data provided by smart tachographs and analyse how their integration with other in-vehicle and external systems affects these threats. Finally, as this data includes personal, localization and behavioural information, we analyse the privacy threats as well.

4.1 Data in Scope and Security Objectives

In order to support the achievement of the objectives listed in Section 1, the digital tachograph stores and process drivers' activity and personal data. In particular, the following data is in scope [ECDP12], [EC02]

- Activity data, including:
  - Driver's activity data, e.g. presence, driving and break/rest;
  - Speed information;
  - Localization/positioning data;
  - Driving distances;
- Personal data stored on the tachograph cards.

Taking into account the objectives of the smart tachographs, system actors and data in scope, it is possible to define the security objectives aiming at preventing misuse of the system and compliance with the applicable regulations, such as data protection and privacy regulation. The control objectives for the smart tachographs are focusing on protecting integrity, authenticity, availability and confidentiality of data processed, stored and transmitted by the system [FULE06], [CCPP10]

In what follows, we describe the threats against the digital tachograph data and services. Rather than providing the details on particular threat agents and their implementation, we analyze how the emerging technologies described in Section 3 and the integration of smart tachographs with other in-vehicle applications change the threat landscape. In accordance to security control objectives described in the paragraph above, the threats against data integrity, authenticity, availability and confidentiality will be analyzed. Please note that we focus on the technical rather than the procedural threats.

4.2 Threat Landscape

Even though the assets in scope are the same for *traditional* digital tachographs, the evolvement of smart tachographs and their integration with the ITS, positioning sensors and in-vehicle applications change the threat landscape. The reasons for that are twofold:

- New threats are enabled by the integration in a broader *ecosystem*; this could potentially allow the smart tachograph to be used as an attack launch pad:
- The probability of the existing threats is increased as the integration introduces a wider attack surface.

We divide the threats to digital tachograph systems into four categories: data integrity, data authenticity, availability and confidentiality. For each category we indicate the impact of the transition to 'smart' tachographs.

Threats to data integrity:

- Unauthorised modification of the vehicle's motion data exchanged between the motion sensor (MS) and the vehicle unit (VU);
- Unauthorised data modificaton while exchanged between VU and tachograph cards;
- Unauthorised data modificaton while exchanged between VU and remote stations, e.g. remote control station;
- Unauthorised modification of the data stored in the VU and the tachograoh cards;
- Unauthorised modification of data output (print, display or download);

- Unauthorised modification of hardware, firmware or software of the VU.

Impact of smart tachographs to integrity threats: The likelihood of unauthorized data modification, which includes deletion, is increased. For instance, a malware installed via one of the (remote) interfaces can cause corruption of the activity data. Further, wireless communication between the vehicle unit and the control station can be exploited to alter the data in transit. Finally, given that the number of actors involved in such online-connected system is increased, the likelihood of impersonation attacks and unauthorized access to the data is higher. Furthermore, the smart tachograph can be used as a launch pad for further attacks inside the vehicle or beyond.

Threats to data authenticity:

- Connection of rogue devices (motion sensor, smart cards, external device) to the vehicle unit;.
- Impersonation of the vehicle unit or motion sensor when sending data to a remote control station.

Impact of smart tachographs to authenticity threats: In addition to increasing the likelihood due to remote communication and the increased number of system actors, smart tachographs intoduce an additional threat to data authenticity. Given that the integration with satellite positioning system (GNSS) is foreseen ([ECIA11]) in order to track the precise vehicle position, there is a threat to exposure to a false satellite signal [ETSI10].

Threats to availability

- Tampering with a hardware or software of a motion sensor or vehicle unit.

Impact of smart tachographs to availability threats: The main availability of threat introduced by the smart tachographs is the Denial of Service (DoS) aiming at preventing the vehicle unit at responding and sending the data to the control entity. This can be achieved by various threat agents, including malware, high volume messages sent via multiple interfaces or by jamming the communication media [ETSI10].

Threats to confidentiality

- Unauthorized access to user data retrieved from the vehicle unit or smart card.

Impact of smart tachographs to confidentiality threats: Personal data in scope of the traditional tachographs is "enriched" by the positioning data. The main challenge for achieving the confidentiality, i.e. ensuring that users can only access data and functions allowed to them, is posed by the increased number of actors and communication interfaces. It can be observed that the authorities in charge of defining and operating smart tachographs will have to strike a balance between privacy and commercial "added value". The latter can come from e.g. driver or vehicle usage information resale. However, the value of such information for resale is impacted by the granularity and degree of privacy respect of the information offered. The richer the information, the higher is its value for resale.

4.3 Trends in security controls

Security controls in digital tachographs rely on symmetric and asymmetric key cryptographic techniques [CBPM12]. While symmetric systems are typically used to secure the link between

the motion sensor and the vehicle unit, asymmetric systems are protecting the communication between the vehicle unit and the tachograph cards.

Digital signatures (PKI) ensure the integrity and authenticity of data downloaded to the cards or any external media. Similarly, digital signatures of messages exchanged within the ITS are considered to be an appropriate control for protecting a communication between a vehicle and the external parties (Figure 2) against multiple integrity and authenticity related threats [ETSI10]. To foster the implementation of this control and its increased user-friendliness, the usage of mobile signatures can be considered [CBPM12]. Such mobile signatures assume the usage of the signature creation data in the SIM cards which provide a required level of security certification e.g. CC EAL4+ Security Certificate for the qualified signature. Even though the protection profile for the mobile signatures still needs to be legally endorsed, this is a promising solution given the wide usage of the SIM cards. In addition to their availability in the phones and tablets, some car manufacturers have them integrated in the on-board units [GSMA13], which could further support the implementations of mobile signatures in the ITS-integrated applications.

For a detailed analysis of the controls against the emerging threats on the ITS, we refer the reader to [ETSI10]. The next subsection discusses the privacy implications of the smart tachographs.

4.4 Privacy considerations

Given that smart tachographs are dealing with personal, behavioural and localization related data, privacy protection is of paramount importance. From the personal data protection point of view, the most relevant data in scope of the smart tachographs are [ECDP12]:

- Insertions and withdrawals of Tachograph Cards (this also indicates which driver controlled the vehicle at which point in time);
- Positioning data;
- Speed, e.g. details of over-speeding events;
- Distances;
- Time, i.e. all log entries are registered with time;
- Driver Activities: recorded in real time, as well as recorded through manual entries (Driving, Break/Rest, Available).

According to [ECDP12], the most relevant privacy threats of smart tachographs are excessive processing of personal data, i.e. processing more personal data than required for the purpose, and re-use of personal data beyond the legally defined purpose. In particular, the main concerns are:

- Permanent activity and location monitoring;
- That the remote control interface would lead to continuous remote access to the information in the equipment;
- Further processing of tachograph data via the ITS-interface.

To prevent these threats, [ECDP12] proposes two types of controls that can be applicable to smart tachographs:

- Domain separation, i.e. separate domains that process the behaviour related data, e.g. detailed positioning or card activity, and user identification information (e.g. name, address, number plate). The data of from these two domains are only aggregated on a high level, in accordance to data minimisation principle (strictly needed for the purpose).

- Distributed processing, i.e. processing the row data locally in the vehicle unit, and transferring the only the digested and minimized data to the central system. This principle was implemented in [BRTP+10] to achieve location privacy of electronic road tolling system.

Obviously it is possible to also consider using Privacy Enhancing Technologies (PETs) such as protocols that rely on anonymous credentials or pseudonyms, or blind signatures.

5 Conclusion

The integration of digital tachographs with emerging technologies, such as ITS, holds a potential to deliver benefits in terms of increased transport efficiency, improved driver experience and lower operational costs. On the other hand, the new functionalities and communication interfaces open new possibilities for malicious users to tamper with the tachograph data and gain unlawful competitive advantage. Furthermore, care should be taken that attacks against the tachograph and its supporting infrastructure cannot be used as mount point for other attacks.

In this article, we analysed how emerging technologies change the security threat landscape of the digital tachograph. Even though the same asset data is in scope compared to the traditional tachographs, online-connected and integrated smart tachographs provide new possibilities for the attacks and increase the likelihood of the existing ones. Furthermore, due to integration with other in-vehicle applications, a smart tachograph system deals with privacy sensitive data, which needs to be taken into account in the overall design of the system.

References

[ANDER 01] Ross J. Anderson, Security Engineering: A Guide to Building Dependable Distributed, Systems, John Wiley & Sons, Inc., 2001

[BRTP+10] Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens. PrETP: privacy-preserving electronic toll pricing. In *Proceedings of the 19th USENIX conference on Security* (USENIX Security›10). USENIX Association, Berkeley, CA, USA, 5-5.

[CBPM12] Mehmet Colak, James Bishop, Jean Pierre, Nordvik, Vincent Mahieu, Jan Loeschner. Cryptographic security mechanisms of the next generation digital tachograph system and future considerations, Eurpean Commission, Joint Research Center, Report EUR 25663 EN, 2012.

[CCPP10] Common Criteria Protection Profile, Digital Tachograph – Vehicle Unit (VU PP), Bundesamt für Sicherheit in der Informationstechnik, Bonn, July 2010.

[CJNM+11] Mehmet Colak, James Bishop, Jean Pierre Nordvik, Vincent Mahieu, Jan Loeschner: Cryptographic security mechanisms of the next generation digital tachograph system and future considerations, ISBN: 978-92-79-27990-4, 2011.

[EC02] Commission Regulation (EC) No 1360/2002 of 13 June 2002. Council Regulation (EEC) No 3821/85 on recording equipment in road transport, Annex 1 B, Requirements for Construction, Testing, Installation and Inspection.

[EC144-11] European Commission Roadmap to a Single European Transport Area – Towards a competitive and resource efficient transport system, COM(2011) 144 final, Brussels 2011.

[EC451-11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Council Regulation (EEC) No 3821/85 on recording equipment in road trans-

port and amending Regulation (EC) No 561/2006 of the European Parliament and the Council, COM(2011) 451, Brussels 2011.

[ECDP12] European Commission, DG Mobility and Transport, ITS Action Plan, ITS & Personal Data Protection, Final Report, Amsterdam, October 4th, 2012.

[ECIA11] European Commission, Impact assessment on measures enhancing the effectiveness and efficiency of the tachograph system, Revision of Council Regulation (EEC) No 3821/85, Brussels, 2011.

[ETSI10] ETSI TR 102 893 V1.1.1 Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA), Sophia Antipolis, France, 2010.

[FULE06] Igor Furgel and Kerstin Lemke, A Review of the Digital Tachograph System, Embedded Security in Cars, ISBN: 978-3-540-28384-3, Springer Berlin Heidelberg, 2006.

[GSMA13] GSMA mAutomotive, Turbo-Charged In-Car Connectivity, White Paper, 2013.

[ITAP10] ITS Action Plan, Action Area 4: Integration of the vehicle into the transport infrastructure, European Commission, DG MOVE and Rapp Trans, Brussels, 2010.