TPM 기반 위변조 방지형 디지털 운행기록 장치 설계 및 구현

Design and Implementation of TPM-based Vehicle Data Logging System for Tamper-Resistant Data Collection

박기웅
Ki-Woong Park

(300-716) 대전시 동구 대학로 62 대전대학교 해킹보안학과 시스템보안연구실
woongbak@dju.kr

요 약

디지털 운행기록장치(Digital Tachograph) 보급의 확산에 따라, 신뢰성이 보장된 방법으로 차량 데이터를 기록하는 기술이 요구되고 있다. 특히 2012년 한국에서는, 개정된 교통안전법에 따라 업무용 차량의 디지털 운행기록 장치가 의무화 되었다. 디지털 운행기록장치의 다음 단계에 있어, 네트워크 연동형 디지털 운행기록 장치가 개발되었으며, 이는 실시간 운행 정보(주행시간, 유휴시간, 브레이크 타이밍 등)의 수집 및 그에 기반한 서비스를 제공하기 위한 것이다. 본 논문에서는 위변조 방지형 디지털 운행기록 장치를 디자인하고 구현하였다. 위변조 방지형 디지털 기록을 위해 TPM의 모노토닉 카운터를 활용한 해시체인 기반 로깅 기법을 제안하였으며, 이는 디지털 운행기록장치가 장착된 차량의 운전자조차도 데이터를 위조 또는 수정할 수 없는 보안 기능을 제공한다. 본 논문에서 제안한 방법의 가능성과 연산 효율성을 테스트하기 위해, ARM 프로세서 기반 임베디드 보드에 프로토타입을 구현하였으며, 초당 995.85 로깅 트랜젝션을 처리할 수 있다.

Abstract

The ability to record the driving data in a tamper-resistant manner is a precursor to widespread deployment of digital tachograph because the driving data is potentially sensitive and must be verifiably accurate. The deployment of the digital tachograph has been mandatory for all business vehicles in Korea since 2012. As its next step, a networked digital tachograph has been developed for real-time monitoring of the driving time, breaks, as well as rest periods undertaken by a driver. In this paper, we propose a tamper-resistant logging system for the networked digital tachograph, called T-Box. To provide the tamper-resistant logging, we devised a hash-chain based logging mechanism using a monotonic counter of TPM, in which even the drivers cannot modify or falsify the driving data. To evaluate the feasibility and computation efficiency of the proposed logging mechanism, we built a prototype on an ARM-based embedded board. The evaluation results show that the proposed method can perform 995.85 logging transactions per second.

논문투고일자 : 2013. 07. 13 심사일자 : 2013. 07. 29 게재확정일자 : 2013. 08. 19

키워드: 디지털 운행기록 장치, 위변조 방지, 신뢰성 플랫폼 모듈
Keyword: digital tachograph, tamper-resistant, TPM

1. Introduction

A tachograph is a device equipped to a vehicle that records its speed and location with the driver's activity such as the driving time, breaks patterns undertaken by a driver [1]. With the widespread deployment of digital tachograph, an ability to record the driving data in a tamper-resistant manner has become a critical issue. The installation of the digital tachograph has been mandatory for all business vehicles in Korea since 2012.

As its next step, a networked digital tachograph has been developed for monitoring the legality of drivers' actions, real-time traffic status and vehicle accidents. As shown in Fig. 1, once a vehicle and a central server establish a connection, all driving data of the vehicle is recorded and transmitted to the central server. More specifically, a central server collects the logged data from vehicles, and stores it in log files. They can be exploited to evaluate the legality of drivers' actions on the vehicle with respect to a given set of drivers' rules.

However, the presence of the networked digital tachometer itself is insufficient because it is deployed on vehicles that are not operated by the central server [2, 3, 4]. The drivers may deliberately or unintentionally record incorrect monitoring data resulting in incorrect recording. Thus, the data of the digital tachometer can be tampered in various ways because the digital tachometer stores and transmits all data in a digital way [5]. For example, driver may modify or delete its logged data for false modifications by counterfeiting the data from the sensor modules of their vehicle. Some sophisticated drivers even try to disable the function of the networked digital tachograph as soon as they connect to the centralized system [6]. Therefore, tamper resistant logging mechanism should be provided for the successful deployment of the digital tachograph.

As a remedy to the problem, we propose a tamper-resistant vehicle data collection system for the networked digital tachograph, called T-Box, which is protected against forgery and false modifications by drivers. The central server collects the logged data by vehicles, and stores it in tamper-resistant log files. To provide the tamper-resistant logging, T-Box has a logging mechanism in which even the drivers cannot modify or falsify the logged data. To achieve it, T-Box exploits the trusted platform module (TPM) [7, 8].

By means of the forgery-resistive logging mechanism, T-Box can (1) record all driving data of the vehicle with regard to the driver' s actions; (2) take action when a remarkable event is detected, such as accurately recording the event in a secure storage region of T-Box; and (3) transmit the logged data to the central server.

This study is an extension of our previous work [9], in which we focused on the protocol design of a tamper-resistant logging mechanism for networked digital tachograph. Our objective in this study, however, is to integrate the overall components in a real embedded computing

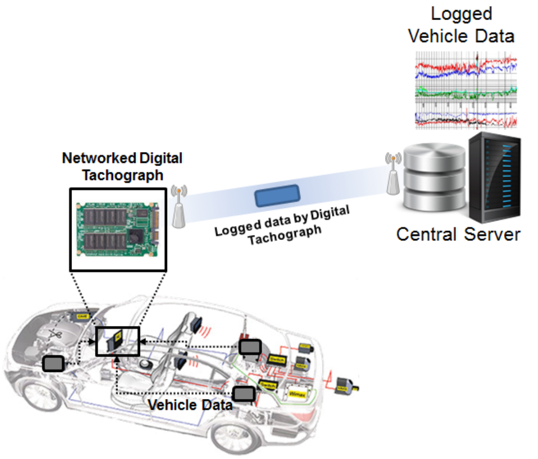

Fig. 1 A networked digital tachograph: all driving data of a vehicle is recorded and transmitted to the central server

platform and evaluate feasibility and computation efficiency of the proposed logging mechanism.

The remainder of the paper is organized as follows: In Section 2, we present the overall system design and components of the proposed billing system. In Section 3, we illustrate the tamper-resistant logging procedure based on T-Box. In Section 4, we evaluate the performance of the proposed system. Finally, in Section 5, we present our conclusions.

2. Design of Tamper-Resistant Vehicle Data Collection System

In this section, we present an overview of the vehicle data collection system. We first introduce the important components of the proposed system and then describe the overall logging procedure.

2.1 The Proposed T-Box Infrastructure

Fig. 2 shows the overall architecture and operation of vehicle data collection system on the basis of T-Box. The three major components of the architecture are listed as follows:

- **T-Box:** It is deployed into the driver`s vehicle. It has a tamper-resistant vehicle data collection mechanism, which enables it to record all driving data of the vehicle with regard to the driver' s actions in a secure storage region of T-Box and transmit the logged data to the central server.
- **Central Server:** It collects the logged data from the T-Box of vehicles, and stores it in tamper-resistant log files. In addition, the central server provides a verification mechanism against forgery and false modifications by drivers.
- **Vehicle Equipped with T-Box:** We assume that a driver starts their vehicle in such an environment; each driver makes a drive check-in request to the central server with a mutual authentication. When the driver ends driving, the vehicle makes a drive check-out request to the central server with a verification process for vehicle data.

2.2 Overall Billing Process of T-Box

After a mutual authentication phase between the T-Box in a vehicle and the central server, the central server can collect the logged data from vehicles, and stores it in tamper-resistant log files. The mutual authentication involves the generation of a hash chain by each log entity. The hash chain element of each entity is integrated into each logging transaction on a chain-by-chain basis; it enables the central server to verify the correctness of the transmitted log data.

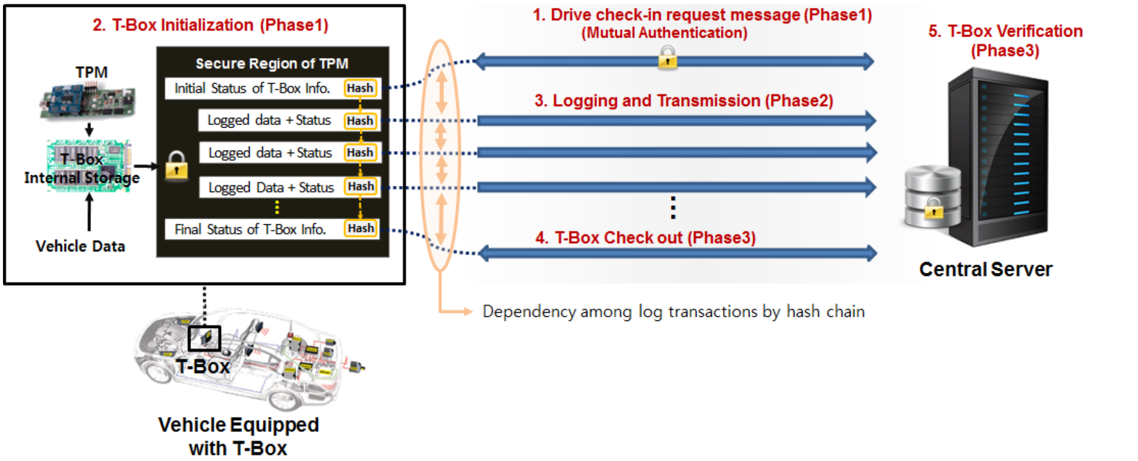
2. T-Box Initialization (Phase1)
TPM
T-Box
Internal Storage
Vehicle Data
Secure Region of TPM
Initial Status of T-Box Info.
Hash
Logged data + Status
Hash
Logged data + Status
Hash
Logged Data + Status
Hash
Final Status of T-Box Info.
Hash
1. Drive check-in request message (Phase1)
(Mutual Authentication)
3. Logging and Transmission (Phase2)
4. T-Box Check out (Phase3)
5. T-Box Verification
(Phase3)
Central Server
Dependency among log transactions by hash chain
T-Box
Vehicle Equipped
with T-Box

Fig. 2 The overall architecture and operation of the vehicle data collection system on the basis of T-Box

Fig. 2 shows the overall process of the logging transaction with our vehicle data collection system. The main steps are as follow:

- **Phase1:** The T−Box generates a drive check−in request message and sends it to the central server for a mutual authentication. T−Box is initialized and verified during the drive check−in transaction.
- **Phase2:** During drive time, T−Box records all driving data of the vehicle with regard to the driver' s actions in a secure storage region of T−Box and transmits the logged data to the central server.
- **Phase3:** Once the driver finishes their drive, the central server checks the logged data by verifying the integrity of the driving data.

One drive logging session is finished with the above transactions. Thus, the logging transactions become more objective and acceptable to drivers and the central server due to the provision of the trusted and tamper−resistant logging mechanism of T−Box.

3. T−Box Internals

3.1 Fundamental Technologies of T−Box

T−Box has a tamper−resistant logging mechanism in which even the drivers cannot modify or falsify the logged data. T−Box exploits the trusted platform module (TPM) [7]. The TPM is a widely deployed security chip in commercial−off−the−shelf computing systems. It is designed for the purpose of secure storage and remotely determining the trustworthiness of a software stack [10]. T−Box uses the following fundamental technologies of TPM.

- **Platform Integrity Measurement:** To ensure the trusted execution of T−Box, we utilize a TPM. One of the important features of the TPM is a set of platform configuration registers (PCRs). The PCR values can only be changed by the Extend() function, which is an internal function of the TPM. It outputs a hash result with (current software stack + current PCR value), and then replaces the current PCR value with the output of this operation. To enable the central server to check the correctness of T–Box, the TPM provides a Quote() function to return a digital signature of the current PCR values so that Quote() provides proof that the output of Quote() was generated on the correct software stack.

- **Secure Storage with the TPM:** The TPM provides a means of storing data in a secure fashion. The Seal() function encrypts the input data with a TPM key and specified PCR values. The Unseal() function decrypts the encrypted data only when the specified PCR values and the key are matched with the status of sealing [7]. T–Box uses the Seal() and Unseal() functions to protect the logged data in such a way that the data can only be decrypted by T–Box itself.
- **Data Integrity with the TPM:** The TPM has built–in support for a monotonic counter. The increments of this type of counter are in single steps, and the value of the counter is only incremented by the IncrementCounter() function. In addition, the TPM has a mechanism that creates a signature of the current tick value of the TPM. The tick data includes a signature of the current tick value and its update cycle. These functions are utilized in our verification mechanism. The verification mechanism enables the central server to determine whether the T–Box has been executed without a block or a data loss.

3.2 Tamper-Resistant Logging Procedure

This section elaborates how the T–Box can perform the logging procedure in collaboration with the central server. The T–Box procedure consists of three phases. Phase1 is performed for the beginning of a drive session; Phase2 is for transmitting the logged data to the central server periodically during a drive session; and Phase3 is performed for the end of the drive session. The central server can consequently determine whether the collected log data is correct or not [11]. The details of the three phases on the basis of T–Box are as follows:

- **Phase1 (T-Box Initialization):** In a drive check–in session, the T–Box initializes itself and sends a drive check–in request message to the central server for a mutual authentication [12, 13, 14, 15]. The drive check–in request message contains data on the correctness of T–Box as well as the authentication data, which is generated by Quote() and Extend() operation of the TPM. To enable the central server to check the correctness of the T–Box, the central server checks the PCR value of the T–Box.
- **Phase2 (Logging and Transmission):** Phase2 periodically occurs during the drive time. Whenever this phase occurs, the monotonic counter is increased, and the value of the counter is stored in the secure region of TPM by Seal() operation of TPM. As increasing the value of the monotonic counter, the logged data by T–Box and the current tick–stamp are appended to a log packet. Because each log packet is extended by a hash function for every log packet, each log packet is linked to the previous log packet. This linking process enables the central server to check its consistency.
- **Phase3 (T-Box Check Out and Verification):** Phase3 is executed when the corresponding drive session is ended by the driver. T–Box transmits the final log packet to the central

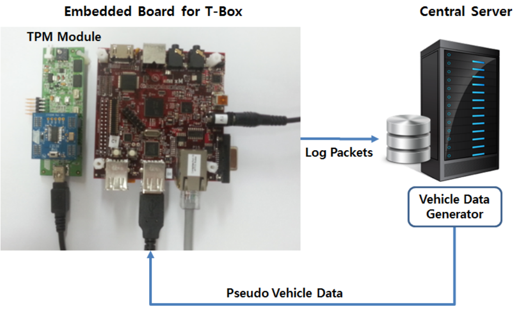

Fig. 3 The overall experimental environment to evaluate the operational efficiency of T-Box

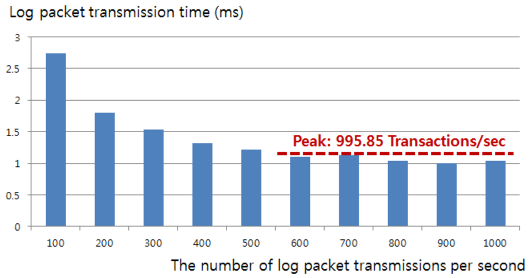

Fig. 4 Log transactions overhead with varying the number of transactions per second operational efficiency of T-Box

server. Before sending the final log packet, T–Box appends the current status itself by using the Extend() operation of TPM. The context of the final log packet enables the central server to check whether T–Box was executed correctly without a break or halt and whether the previous log packets were truly generated by T–Box. Thus, the central server can trust the vehicle data from T–Box.

4. Performance Evaluation

In this section, we present the performance results obtained with our prototype implementation of T–Box. First, we demonstrate the overall experimental environment. We then describe the operational efficiency of the tamper–resistant logging process.

4.1 Experiment Environment

Fig. 3 shows the overall experimental environment. To evaluate the operational efficiency of T–Box, we constructed T–Box enabled embedded board, which is equipped with TPM module and coupled it to a vehicle data generator. The embedded board is connected to the central server, and the embedded board receives the vehicle data from the vehicle data generator. The generator is a module that generates vehicle data to produce log packets. The T–Box module has A8 Cortex processor and a 512 MB main memory, and the central server and the generator have a Xeon E5505 processor and a 16 GB main memory.

4.2 Operational Efficiency of T–Box

Fig. 4 illustrates the time taken for each log packet. For this experiments, the total time taken is measured by varying the number of log packet transmissions per second from 100 to 1000 (x–axis); and the time taken for each log packet transmission (y–axis) is calculated by dividing the total time by the number of log packet transmissions. Through this experiment, we found that the throughput was saturated on 995.85 transactions per second as the number of packet transmissions increased. This outcome is due mainly to the cryptography operations and the communication overhead of both the client side and the server side [16].

5. Conclusion

In this paper, we propose a tamper–resistant logging system for the networked digital tachograph, called T–Box. To provide the tamper−resistant logging, we devised a TPM−based logging mechanism in which even the drivers cannot modify or falsify the logged data. By integrating the T−Box into each vehicle, we made the vehicle data collection system more objective. From our design of the T−Box system architecture and a three−stage tamper−resistant log transmission procedure, we built a prototype on an embedded system and server system. The benefits of T−Box are not limited to a networked digital tachograph. The proposed system also can be integrated into server computing platforms as a black box logging for system transaction.

References

〔1〕 ISO 16844-3, Road Vehicles−Tachograph Systems – Part 3: Motion Sensor Interface, 2004-11-01

〔2〕 J. Ferreira, J. fonseca, and J. Lopes, "Wireless Vehicular Communications for Automatic Incident Detection and Recovery", Proceedings of the 10th Portuguese Conference on Automatic Control, Jul, 2012

〔3〕 Kargl, F., Papadimitratos, P., Buttyan, L., Muter, M., Schoch, E., Wiedersheim, B., Ta-Vinh Thong, Calandriello, G., Held, A., Kung, A., Hubaux, J-P, "Secure vehicular communication systems: implementation, performance, and research challenges," Communications Magazine, IEEE , vol.46, no.11, pp.110,118, November 2008

〔4〕 Schweppe, H., Roudier, Y., "Security and privacy for in-vehicle networks," Vehicular Communications, Sensing, and Computing (VCSC), 2012 IEEE 1st International Workshop on , vol., no., pp.12,17, 18-18 June 2012

〔5〕 Joint Interpretation Library (JIL): Security Evaluation and Certification of Digital Tachographs, JIL Interpretation of the Security Certification according to Commission Regulation (EC) 1360/2002, Annex 1B, Version 1.12, June 2003

〔6〕 S. Yaqoob, C. Lee, and T. Shon, "A Study on Tachograph based Security Network", International Journal of Smart Home, Vol. 7, No. 1, Jan, 2013

〔7〕 D. Schellekens, B. Wyseur, B. Preneel, "Remote Attestation on Legacy Operating Systems With Trusted Platform Modules", Electronic Notes in Theoretical Computer Science, Volume 197, Issue 1, February 2008.

〔8〕 박기웅, 박규호, "1회 읽기 가능 메모리를 통한 오프라인 방식의 모바일 전자 지불 시스템 설계 및 구현", 한국차세대컴퓨팅학회 논문지, Vol.9 No.1, pp.51-62, 2013년 2월

〔9〕 K-W. Park, "T-Box: Tamper-Resistant Vehicle Data Collection System for a Networked Digital Tachograph", International Conference on ICT for Smart Society, June, 2013

〔10〕 N. Aaraj, A. Raghunathan, and N. Jha, "Analysis and design of a hardware/software trusted platform module for embedded systems", ACM Trans. Embed. Comput. Syst. 8, 1, Article 8, Jan 2009.

〔11〕 K-W. Park, K. Park, "Design and Implementation of One-Time-Readable Memory-Based Offline Digital Payment System", The journal of Next Generation Computing, Vol.9 No.1, pp.39-50, Feb. 2013

〔12〕 B. Suh , "An Improved User Authentication Scheme Based on Random Nonce and Timestamp", The journal of Next Generation Computing, Vol.8 No.6, pp.69-76, Dec. 2012

〔13〕 M. Park, "RFID Mutual Authentication Protocol on Open Channel for Improvement of Hash Computational Load and Forward Secrecy of the Each Entity", The journal of Next Generation Computing, Vol.6 No.5, pp.20-26, Oct. 2010

〔14〕 서병문, "랜덤 넌스와 타임스탬프 기반의 개선된 사용자 인증 스킴", 한국차세대컴퓨팅학회 논문지, Vol.8 No.6, pp.69-76, 2012년 12월

〔15〕 박미옥, "각 객체의 전방향 안전성과 해쉬연산 로드를 개선한 공개 채널상의 RFID 상호인증 프로토콜", 한국차세대컴퓨팅학회 논문지, Vol.6 No.5, pp.20-26, 2010년 10월

〔16〕 Najwa Aaraj; Raghunathan, A.; Ravi, S.; Jha, N.K., "Energy and Execution Time Analysis of a Software-based Trusted Platform Module," Design, Automation & Test in Europe Conference & Exhibition, 2007. DATE '07, vol., no., pp.1,6, 16-20 April 2007

Authors

◆ 박기웅

- 2005년 연세대학교 Computer Science 학사
- 2007년 KAIST Electrical Engineering 석사
- 2012년 KAIST Electrical Engineering 박사
- 2008년 Microsoft Research Asia, Wireless and Networking Gourp, Research Intern
- 2009년 Microsoft Research Redmond, Network Research Group, Research Intern
- 2012년 국가보안기술연구소 연구원
- 2012년 ~ 현재 대전대학교 해킹보안학과 조교수
- 관심분야: 시스템 보안, 모바일-클라우드 컴퓨팅, 보안 프로토콜, 디지털 포렌식 등