



Authentication Scheme for Secure Data Collection in Connected Car Environment

Dae-Hyun Kim and Jin Kwak*

ISAA Lab, Department of Computer Engineering, Ajou University, Yeongton-gu, Suwon, Gyeonggi-do 44374, Korea

Connected cars, unlike existing vehicles, exhibit the concept of internet of things, and their functions are becoming increasingly more advanced. By combining mechanical, electrical, and communication technologies, connected cars can provide a safe driving service using traffic and road conditions and car-to-car communication. The various forms of communication on connected cars generate an enormous amount of data including data from the real-time exchange of information, media content, and connection of mobile devices. Data generated in the connected car can be used to understand the exact cause of accident and to investigate crimes. For these reasons, a private organization called "I Am The Calvary" studying connected car security mentioned at DEF CON 2013 that "forensic information should be stored as a measure of precaution of future accident" as one of the five commandments for vehicle's cyber security. This commandment necessitated storage space for the vehicle's interior data and the data collection generated from infotainment and telematics. However, a large amount of data for digital forensics can lower the efficiency of an investigation. This paper proposes an authentication method for the connected car and its data storage server that generates, acquires, and stores data related to digital forensics via the vehicle's immobilizer, along with the processing procedures.

Keywords: Digital Forensic, Connected Car, In-Vehicle Communication, C-ITS, Infotainment.

1. INTRODUCTION

A vehicle that combines mechanical, electrical, and communication technologies for communication to various connected media is called a connected car.¹ A connected car can generate and communicate real-time data in various ways.² Unlike existing vehicles, this makes it possible for a connected car to provide safety and convenience. As explained, a connected car can enjoy many different application services through real-time exchange of information, use of media contents, and connection to mobile devices; there are targets to turn the vehicle itself into a single connected device equipped with all connectivities, platforms, and solutions to generate, transmit, and receive various types of data.^{3,4}

As a result, connected car can be useful for analyzing the exact cause of a car accident or investigating the suspect of a crime.⁴ However, the connected car data communication is over several networks and communications, unlike the personal computer (PC) environment. Collecting and analyzing all data using digital forensic techniques can reduce the efficiency because an enormous amount of data is shared.⁶

This paper proposes an authentication method for the connected car and for storing its data traffic for investigation.

This paper is organized as follows: Section 2 analyzes related studies, Section 3 explains why the digital forensics of

connected car is necessary, and Section 4 proposes an authentication technique for the storage for collecting all data traffic in the connected car. Lastly, Section 5 closes the paper with a conclusion.

2. RELATED WORKS

2.1. Connected Car

A connected car is a vehicle with technology that is connected to a network at all times. It aims to provide a safe, convenient driving experience by communicating to other cars, infrastructure, and mobile devices in real time, and unlike existing vehicles, its core technology is software, not hardware. Various information from outside can be easily shared and its efficiency can be maximized, not only because when a software command is transferred to the power train of the vehicle, the vehicle needs to convert it into a mechanical one, but also because a software update can improve the vehicle's performance and functions with the network always in connection.^{5,6} As such, many different sensors are equipped on the connected car to collect various data regarding vehicle's condition up to several gigabytes per every hour including engine rpm, oil temperature, and tire pressure. In 2022, the number of connected cars is projected to reach 1.8 billion worldwide, and therefore, the amount of related data is expected to increase exponentially.⁷

*Author to whom correspondence should be addressed.

2.2. Immobilizer

An immobilizer system is a device that uses transponder key method to forbid ignition of the car except for an allowed smart key set before the vehicle's release. Located on the grip of a key, a transponder is an anti-theft system that starts the ignition of the car by entering the matching password on the vehicle's engine ECU.⁸ At the ON-signal of the ignition key switch, the engine ECU requests the unique number of the smart key's transponder, which then transmits the unique number to the engine ECU. If the information on the key matches, the engine ECU requests the passcode a second time and verifies whether the data sent from the smart key's transponder matches what is currently stored in the engine ECU in order to start the car.⁹

3. DIGITAL FORENSIC NEEDS OF CONNECTED CAR

Significant advancement in technologies, processes, and tools for digital forensics has been attained in order to collect digital evidence as forensic evidence. Recently, digital forensics involves not only computers and smartphones but also game consoles, mobile device, wearable device, and smart TVs.¹⁰ As vehicles have become digitalized in recent years, they communicate via diversified environments and networks, moving forward to establish a form of a connected device. Connected cars generate and use various data including call history, text history, location and driving route, website search, mobile device information, and so forth.

Therefore, such extensive data from the connected car can highlight the exact cause of a car accident and be used as evidence in an investigation of a crime. Furthermore, connected cars enabled with various forms of communications, can obtain evidence for both physical and cyber crimes, whereas existing vehicles can only acquire evidence for physical crime.¹¹ If a car accident occurs, its cause used to be clarified by using surveillance cameras or dashboard cameras, but data in a connected car can also go through analysis for a more extensive investigation. Therefore, a digital forensic model is necessary to properly use the connected car data for crime investigations.

4. PROPOSED SCHEME

A connected car that generates, transmits, and receives a variety of data through communications to connected vehicles, surrounding infrastructure, and mobile devices must be able to collect and extract the data to efficiently secure any evidence or mark related to accidents. However, there is no unified system between the manufacturers and the after-market,¹⁵ with no sufficient storage space within the vehicle.

This paper proposes an authentication protocol between the connected car and the vehicle's data storage that saves and stores a large amount of in-vehicle, infotainment, and telematics data in real time.

4.1. Data Storage Authentication Scheme for Data Acquisition of Connected Car

4.1.1. Security Threats

The proposed system is operated in the vehicle's cloud environment. An attacker can illegitimately access the vehicle's data storage, disguised as a normal user. Therefore, without proper user authentication, the data for digital forensic investigation is under the risk of being forged.

- Illegitimate Impersonation

The attacker may attempt to receive authentication on the data storage by impersonating a normal user, if a normal authentication does occur, the attacker can access the data storage.

- Replay Attack

The attacker may attempt to receive authentication while disguised as a normal user by intercepting the user credentials and later transmitting the normal, valid values to the data storage, and if the validity of the credentials is properly verified, the attacker can access the data storage.

- Spoofing Attack on Credentials

The attacker can be authenticated as a normal user by spoofing the credentials used during the authentication process between the normal user and the data storage.

4.1.2. Proposed Protocol

This section proposes an authentication protocol between data storage and connected car using the immobilization system used for preventing car theft. The proposed system verifies the smart key's unique number and the secret code stored in the engine ECU; at engine ignition, these are used as credentials for registration followed by authentication of data storage.

- Registrations Procedure

The authentication procedure through the smart key and the connected car immobilizer occurs in a safe channel. Figure 1 illustrates the registration procedure of the proposed protocol. The registration procedure is as follows.

Step 1. The connected car requests UIN, the unique number stored in engine ECU of vehicle and the secret code P to the smart key.

Step 2. The smart key responds by transmitting the smart key UIN and P .

Step 3. UIN' and P' that are transmitted from the connected car are compared to the existing UIN and P stored in engine ECU. If the UIN pair and the P pair do not match, it is impossible to get registration to the data storage server.

Step 4. If the UIN pair and the P pair match, the engine starts.

Step 5. A random number N is generated by pseudo-random number generator.

Step 6. The UIN stored in engine ECU and the random number P are concatenated and then hashed using the hash function.

Step 7. Using the public key on the vehicle data storage server, VIN, the vehicle identification number, gets encrypted with $h(\text{UIN}||P||N)$ to be transmitted to the vehicle data storage server.

Step 8. After verifying VIN, the identification number of the connected car, at the data storage server, $h(\text{UIN}||P||N)$ gets stored in the database.

Step 9. On the data storage server, VIN, the identification number of the connected car, and the secret x of the data storage server are concatenated, and the based value and the UIN verification value are XOR-operated to create the credential Eq. (1).

$$S = h(\text{VIN}||x) \oplus h(h(\text{UIN}||P||N)) \quad (1)$$

Step 10. Using the public key of the connected car, SID, the identifier of the data storage, and S get encrypted and sent to the connected car.

Step 11. The user verifies the identifier sent from his/her vehicle and stores the S value.

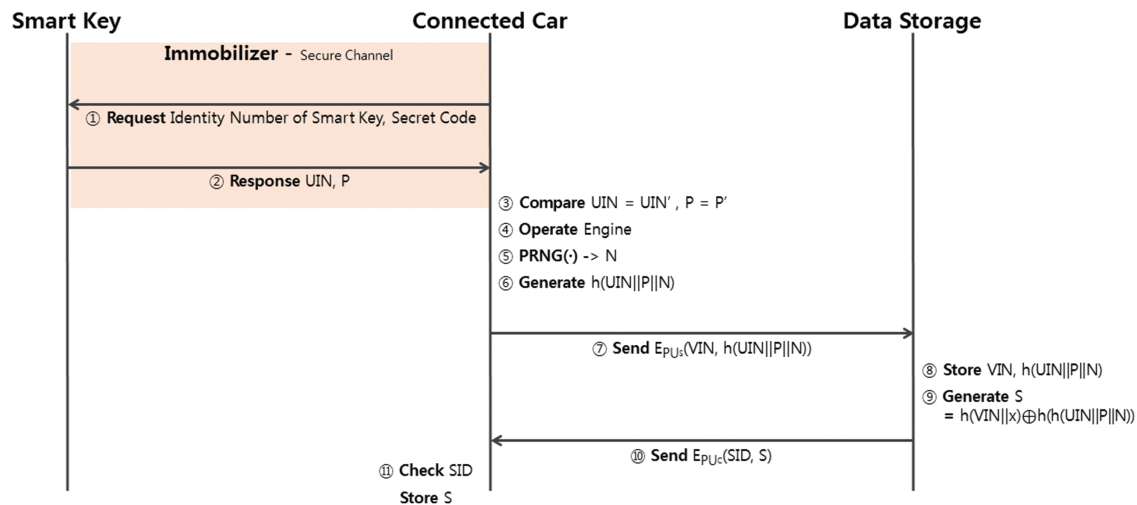


Fig. 1. Registration procedure for proposed protocol.

• Authentication Procedure

The authentication procedure begins after the authentication of the vehicle's smart key to the connected car followed by engine ignition. Figure 2 illustrates the authentication procedure for the proposed protocol. The authentication procedure is described as below.

Step 1. Engine starts after authentication completion of the engine ECU of connected car and the smart key.

Step 2. Using the public key on the vehicle data storage server, VIN (vehicle identification number), $h(UIN||P||N)$, the credential S , and the time stamp T_C are encrypted altogether and sent to the vehicle data storage server.

Step 3. The validity of the T_C is verified by comparing the difference between T'_C , the time stamp when the connected car receives the credential, and T_C , the time stamp when the connected car transmits it, to the time stamp ΔT , the transmission delay time.

Step 4. Verify the received VIN (vehicle identification number).

Step 5. Compare the verifier $h(UIN||P||N)'$ from the received VIN to the stored verifier $h(UIN||P||N)$. If they do not match, the authentication procedure fails.

Step 6. Using the public key of the connected car, SID, the data storage identifier and the time stamp T_D , are encrypted and transmitted to the connected car.

Step 7. The validity of T_D —the time stamp transmitted from the connected car—is verified by comparing the difference between T'_C , the time stamp when the credential was received from the vehicle data storage, and T_D , the time stamp when it was transmitted from the vehicle data storage, to the time stamp ΔT , the transmission delay time. After verifying SID, the identifier of the data storage, authentication completes if the authentication value S is correct.

4.1.3. Security Analysis of Proposed Protocol

The proposed protocol can prevent illegitimate impersonation, replay attack, and spoofing attack on credentials. The proposed authentication procedure employs the immobilizer system to use the unique number of smart key and the secret code that are stored in the vehicle as verification value and authentication value. This prevents illegitimate impersonation, replay attack, and spoofing attack on credentials.

• Illegitimate Impersonation

The user utilizes the unique number and the secret code of the smart key stored in connected car's engine ECU as the verification value $h(UIN||P||N)$ and the authentication value S . Because the attacker does not possess the secret code or the smart key,

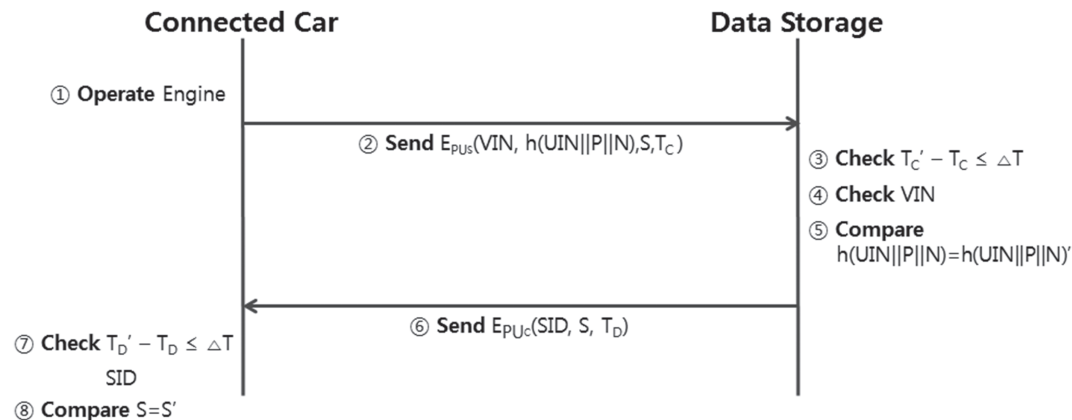


Fig. 2. Authentication procedure for proposed protocol.

it cannot figure out the vehicle's secret code. In such way, the attacker cannot attempt authentication of the data storage by impersonating a normal user.

- Replay Attack

Even though the attacker intercepts the user credential and later attempts to authenticate disguisedly as a normal user by sending a normal, valid value to the data storage, the replay attack can be prevented because the authentication value is invalid due to the valid-time check.

- Spoofing Attack on Credentials

The credentials used during the authentication process between a normal user and the data storage is generated by hash passcode, preventing the attacker's spoofing attack on credentials by detected forgery on the credentials.

5. CONCLUSIONS

As ICT technology develops, vehicle technology has been gradually developing, creating a new concept for the car, called a connected car, by combining mechanical, electrical, and communication technologies into a simple moving machine. A connected car is capable of generating data from communicating to surrounding vehicles, infrastructure, and mobile device. These data can provide safety and convenience while driving.

Communication of the connected car under various environments generates an enormous amount of data, which can be used to find the cause of an accident or when investigating a crime or a suspect to obtain forensic evidence. Because of the tremendous amount of data, however, the connected car cannot store all data, and efficiency while collecting and analyzing the data as forensic evidence can decrease.

This paper proposes an authentication technique for the connected car and the data storage onto the vehicle storage server by using the unique number and the secret code of the smart key stored in engine ECU under the vehicle's immobilization system as credentials before the connected car starts using the vehicle data storage server that can gather and extract all data in the connected car environment.

In future studies, the safe channel scheme on the connected car and the data storage need to be studied, and the data log record list and data fielders also need to be defined.

Acknowledgments: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIP) (No. NRF-2014R1A2A1A1 1050818).

References and Notes

1. D.-Y. Kwak, S.-Y. Lee, and H.-J. Yoon, *TTA Journal* 70 (2009).
2. GiorigioCalandriello, PanosPapadimitratos, J.-P. Hubaux, and A. Lioy, Efficient and robust pseudonymous authentication in VANET, *VANET'07 Proceedings of the Fourth ACM International Workshop on Vehicular Ad Hoc Networks* (2007), pp. 19–28.
3. KB Management Research Institute, Connected car development trends and future changes, KB knowledge vitamin (2016).
4. Scientific Working Group on Digital Evidence, SWGDE Best Practices for Vehicle Infotainment and Telematics Systems v2.0 (2016).
5. M.-W. Park, The future and prospects of the Connected Car, DIGIECO Report (2016).
6. KISA, Power Review, KISA Report (2015).
7. S.-G. Kim, Under the IoT/M2M technology environment, Connectors car rapid market expectations, KISTI MARKET REPORT (2014), Vol. 4.
8. HONDA, Immobilizer System.
9. TTA, Study on the digital evidence analyzed standard guidelines (2007).
10. J. Moos, G. Davies, E. Lewis, N. Williams, B. Gichohi, R. Lane, and A. Bellamy, *International Journal of Forensic Sciences* (2016).
11. D. K. Nilsson and U. E. Larson, Combining physical and digital evidence in vehicle environments, *2008 IEEE* (2008).

Received: 25 February 2017. Accepted: 1 May 2017.