Privacy Leakage Resilient Data Management System for In-Vehicle Environment in the Multi-User Setting

Woori Bae[1], Yongho Choi[2], and Taek-Young Youn[1]*

[1] Dankook University, Republic of Korea
{dnfl0117,taekyoung}@dankook.ac.kr
[2] Yoon&Yang,Republic of Korea
yhchoi@hwawoo.com

Abstract

With the development of automobiles, the driving environment has changed and drivers can enjoy various services. However, security threats are also increasing accordingly. Information used for various services in a vehicle should be treated more importantly from the perspective of privacy leakage because it contains information on various activities of an individual compared to existing in-vehicle storage data. When the same vehicle is used by multiple users, vehicle's users can be changed frequently, and users can easily access each other's privacy, which can be leaked or abused by malicious users. In this paper, a user profile based privacy management system was designed to ensure that each other's privacy is not revealed even if multiple users use a one vehicle.

Keywords. In-vehicle environment, privacy protection, multi-user setting

1 Introduction

The automobile industry is evolving rapidly, and the functions of automobiles are innovating human life. The driving environment is changing due to the emergence and increase in the use of autonomous vehicles. As driving time can be used as personal time, drivers can enjoy various services and innovative technologies in the vehicle. However, security threats are also increasing due to these changes in the driving environment. In order to provide various services and technologies, various drivers and vehicle passenger's privacy is required, which is stored in memory in the vehicle. Privacy stored in the vehicle contains information on various activities of an individual rather than data stored in the existing vehicle. Because of it, one of the most worrisome threats is the leakage of the driver's privacy. Existing privacy leakage has occurred in various scenarios, and the development and research of technology about it are also being conducted. However, the problem is the risk of leakage caused by the change of vehicle authority. Therefore, this paper proposes privacy management system based on user profile as a way to prevent the risk of privacy leakage when multiple users share the same vehicle.

2 System Model

The model we propose is a multi-user model. The purpose of this model is to protect the privacy of multiple users using the same vehicle. When multiple users share the same vehicle, there is a potential threat that other users' privacy may be leaked by malicious users because the vehicle user is changed frequently and have easy access to each other's privacy. Therefore, it is necessary to ensure that other users' privacy is not exposed during changes of vehicle user and the privacy of each vehicle user is stored and used securely.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, Japan, Article No.P-4
*Corresponding author: Dankook University, Seoul, 04620, Republic of Korea, Email: yhchoi@hwawoo.com

3 Technologies

We need to ensure that other users' privacy is not exposed even if the user is changed frequently. Therefore, we designed a privacy management system based on user profile authentication, which ensures that users' privacy is stored encrypted and cannot be accessed by other users.

Profile registration is based on the vehicle user's smartphone. The vehicle user creates his/her ID and PW through the smartphone app and uses it to register his/her profile in the vehicle. The privacy of each profile user can be encrypted and stored based on various keys, such as PW, one-time key, public and secret key pairs, etc. The user's profile authentication system is done through the in-vehicle module. Instead of entering their ID and PW to use their profile each time, they authenticate through a smartphone app. The process for a user to authenticate and access their profile in the car is as following steps:

1. The user enters the vehicle, starts it, and selects his profile.
2. The in-vehicle module sends an authentication request to the smartphone app registered to the selected profile.
3. The user authenticates with smartphone app.
4. User's privacy stored in the vehicle is decoded to provide the service.
5. The user finish driving.
6. The user's privacy is again encrypted and stored in the vehicle.

4 Analysis

Our proposed technology is expected to prevent leakage of privacy by blocking access to each other's privacy and encrypting and storing users' privacy safely when multiple users share the same vehicle. It encrypts and stores users' privacy and efficiently blocks access to each other's privacy based on user profile authentication. In addition, the user's own authentication made it easy to access privacy, so that his or her own information could be accessed efficiently

5 Conclusion

This study proposed a user profile-based privacy management system to prevent privacy leakage in a multi-user model in a vehicle in response to changes in the driving environment due to the development of the automobile industry.

Acknowledgement: This work was supported by National R&D Program through the National Research Foundation of Korea (NRF) funded by Ministry of Science and ICT (NRF2021R1F1A105611513, 100%).

References

[1] Sunghyun Yoon. "Public Law Perspectives on Personal Information Protection in the Era of Automated Vehicle". Korean Journal of Law and Society 0.53 (2016): 1-40.

[2] Woori Bae, Yongho Choi, Taek-Young Youn. "Personal Information Leakage Prevention Technology in In-car payment Services". 2023.08.