



ICONI



KOREAN SOCIETY FOR INTERNET INFORMATION

The 11th International Conference on Internet

(ICONI 2019)

Dec. 15-18, 2019, Lotte Hotels & Resorts Hanoi, Vietnam

<http://www.iconi.org>

Proceedings of ICONI 2019

| Organized by |

Korean Society for Internet Information (KSII)

| Sponsored by |

Korea Electronics Technology Institute (KETI)

Contents



6-3	Deep Learning-based Bladder Cancer Image Analysis Hyunjong Kim, Dongik Oh (Soonchunhyang Univ., ROK)	148-150
6-4	Study on open IoT service platform for Interaction Device of IoT Service Jiyong Lim, Sanghyun Park, Hyosang Lee, Hochul Kim, Amsuk Oh (Tongmyong Univ., ROK)	151-152
6-5	Analysis of Security Threats and Countermeasures in Connected Car Commerce Service Minkyung Lee, JeongSeok Jo (Ajou Univ., ROK), Sungyoung Ryu (Soonchunhyang Univ., ROK), JIN KWAK (Ajou Univ., ROK)	153-155
6-6	Cost-Effective Surveillance System using Microphone Array HyungWoo Park (Soongsil Univ., ROK), James Mu (Kampuchea Thmey Daily, Cambodia, USA), Hyungbae Park (Univ. of Central Missouri, USA)	156-157
6-7	Comparison of Gradient Tree Boosting and SVM for prediction textile industry trend Se Hun Jeong, Min Seong Kim, Chang Soo Kim (Pukyong National Univ., ROK)	158-160
6-8	Classification of User Applications for Future Network Slicing Based on decision Tree Algorithm Prohim Tam, Sa Math, Seokhoon Kim (Soonchunhyang Univ., ROK)	161-163
6-9	The Effect of Business Models on Technology Commercialization Performance DongHyuk Jo (Soongsil Univ., ROK)	164-170
6-10	IoT Ontology on OneM2M Base Ontology accelerate dynamic chatbot services Jinsoo Kim, KangYoon Lee (Gachon Univ., ROK)	171-173
6-11	High-Speed Search Technology based on Ssdeep Younhjoo Lee, Junho Hwang, Taejin Lee (Hoseo Univ.,ROK)	174-175
6-12	Patent Application Trend on Foreign Object Detection for Wireless Power Transfer of Electric Vehicle Woochan Lee (Incheon National Univ., ROK), Moonseong Kim (Seoul Theological Univ., ROK)	176-177

Analysis of Security Threats and Countermeasures in Connected Car Commerce Service

Minkyung Lee¹, Jeong-Seok Jo², Sungyoung Ryu³ and Jin Kwak⁴

^{1,4}Department of Cyber Security, Ajou University
Suwon, Republic of Korea

²ISAA Lab., Department of Computer Engineering, Ajou University
Suwon, Republic of Korea

³Department of Accounting, Soonchunhyang University
Asan, Republic of Korea

[e-mail: mklee.isaa@gmail.com, jsjo.isaa@gmail.com, jackie@sch.ac.kr, security@ajou.ac.kr]

*Corresponding author: Jin Kwak

Abstract

Technological advances have led to the emergence of various services aimed at ensuring the convenience of the users of connected cars, such as autonomous vehicles and smart cars. The development of connected cars has transformed consumer activities in various ways. Online payment services have been introduced to vehicles, and connected car commerce services, which are new financial technology (fintech) platforms that enable drivers to make payments and use services without alighting from their cars, or bringing out their wallets, have emerged. These services have the potential to make the use of takeout services, fueling, and parking more convenient. However, new security threats are anticipated, because of the inclusion of the payment information in these vehicles. Therefore, this study aims to analyze these possible security threats and the corresponding countermeasures.

Keywords: FinTech, Connected Car Commerces, Security Threats, Countermeasure.

1. Introduction

According to BI Intelligence, a market research company, approximately 94 million connected cars will be produced worldwide in 2020[1]. The consistent increase in the number of connected cars and advances in related technologies have given rise to connected car commerce, a payment system using cars. According to Juniper Research, the connected car commerce market size is projected to reach approximately 49 billion by 2022, and the consumption per connected car commerce platform will exceed 100 billion[2]. The implication of this is that security attacks on the platform may cause severe damage.

Therefore, in this study, possible security attacks in connected car commerce and corresponding countermeasures were proposed.

2. Related Works

2.1 Operating Principle of Connected Car Commerce

Connected car commerce refers to a payment service in which a vehicle is made a payment platform through the assignation of a digital ID linked to a payment method to it. Fig. 1 is the flowchart of the connected car commerce.

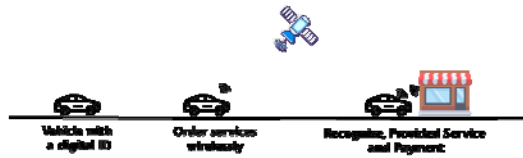


Fig. 1. Flow chart of Connected Car Commerce

A unique digital ID is assigned to the vehicle. When the user orders food, or makes a reservation for fueling using wireless communication, the vehicle's location is determined using a GPS module. The employee who receives the order can calculate the time required to provide the service, making it possible to provide efficient services. The user's arrival at the store or service point can be confirmed using a receiver that can recognize digital ID. Payment for the service can then be made from the vehicle using Bluetooth low energy (BLE) geofencing.

2.2 Popular Use Cases of Connected Car Commerce

Recent research shows a growing preference for non-contact payment methods among consumers[3]. This study analyzed the popular use cases of connected car commerce involving non-contact payment methods.

A. Parking payment

IoT-based parking stations can secure available space using OTA(Over the Air) technology, and transfer data to onboard vehicle systems[4].

B. Gas station payment

When a vehicle with a digital ID enters a gas station, the preset fuel cost is automatically paid, and an attendant pumps the corresponding amount of fuel[5].

C. Drive-through

Rather than paying fast-food staff through the window, orders can be placed, and payments made via voice commands while driving.

3. Analysis of Security Threats

3.1 Fake Store

Below is the depiction of the man in the middle attack, one of the possible security threats to connected car commerce.

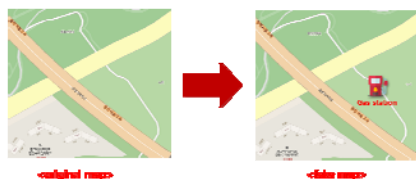


Fig. 2. Converting original map to fake map

For instance, an attacker can create a fake store, and upload a fake map containing it to the navigation system installed in a vehicle. Thus, the user passing the vicinity can be defrauded, if, led by the fake map, he places an order, and pays to the fake store using the connected car commerce platform.

3.2 Fraud

As connected car commerce uses wireless communication technologies, such as BLE geofencing, NFC, and Bluetooth, if an attacker gains control, attacks such as the man in the middle attack are possible[6].

3.3 Privacy Problem

In the process of collecting the location information of vehicles, the platform may retain payment and vehicle location information that may be exploited by platform managers.

4. Analysis of Countermeasures

4.1 Secure communication

Security measures, such as the construction of encrypted communication channels and the management of secure keys can counter the various threats caused by wireless communication. Furthermore, the introduction of wireless security systems must be considered.

4.2 Anonymous or Non-Identifiable Data

The use and storage of anonymous or non-identifiable data to ensure individuals cannot be identified is one way of solving the privacy problem.

5. Conclusions

As new security threats related to wireless communication technology continue to emerge, it is necessary to continuously examine the vulnerability of connected car commerce, a payment method that uses wireless communication, and make efforts to promptly counter these threats.

Therefore, this study analyzes the possible security threats to the connected car commerce platform and corresponding countermeasures.

References

- [1] BI Intelligence, "Automotive Industry Trends: IoT Connected Smart Cars &

- Vehicles”, Business Insider, Dec 2016.
- [2] Chase Martin, “Connected Car Commerce on The Rise”, MediaPost, Jun 2019.
 - [3] Embrain Trendmonitor, “2018 perception survey about BLE services”, 2018.
 - [4] GSMA, “Smart Parking: A Guide to Ensuring a Successful Mobile IoT Deployment”, 2017.
 - [5] GS Caltex Magazine, “Now let’s ‘Smart Pay’ with Beacon at the Gas Station”, May 2018.
 - [6] FSI, “Wireless communications Technology Security Threats and Security Considerations in Simplified Payment”, Aug 2016.