2022-01-0125 Published 29 Mar 2022

Mechanism to Identify Legitimate Vehicle User in Remote Keyless Entry System

Asadullah Ansari and Karthik P.C. SRM Institute of Science and Technology

Sharath D.H. Harman International India Pvt Ltd.

Mohammad Aziz Cardiff Metropolitan University

Sourik Mukherjee Harman International India Pvt Ltd.

Vivek Chidambaram Panimalar Engineering College, Chennai, India

Citation: Ansari, A., Karthik, P.C., Sharath, D.H., Aziz, M. et al., "Mechanism to Identify Legitimate Vehicle User in Remote Keyless Entry System," SAE Technical Paper 2022-01-0125, 2022, doi:10.4271/2022-01-0125.

Received: 25 Jan 2022 Revised: 25 Jan 2022 Accepted: 18 Jan 2022

Abstract

The advancements of the automotive system in all the aspects from safety to user experience brings never ending list of electronics components into the system. One of the pure critical components in providing the vehicle safety is the digital key or wireless vehicle entry systems. This component is responsible for protecting all the other components of the vehicle and the vehicle itself from thieves and illegal usage of the vehicle. The compromisations of this critical component is equivalent to a compromisations of the entire vehicle along with some legal implications on the vehicle owner. There are numerous additional systems in automotive electronics which enhances the security of the critical, digital key/wireless vehicle entry system in protecting the vehicles from attackers. However, there is no component available in the market which does user/owner authentication considering its impact and criticality on both the vehicle and its owner. Either the lost key or the stolen key in the hands of the illegitimate person who may be an attacker or a thief result in the vehicle theft or the usage of the stolen vehicle for the illegal purposes. These situations cause legal circumstances on the legitimate owner of the vehicle. Hence, in this regard there is a need of user/owner authentication in the existing digital key/wireless vehicle entry systems. The proposed system tries to address this concern by combining the user/owner biometrics with the command passing from the user in-hand device. The proposed system transmits the cryptographically secure combined bio-crypto data from the user in-hand device to the vehicle, where the cryptographic verification if followed by a user verification before proceeding on executing the user requested commands on the vehicle. Upon successful user verification, the respective command actions will be undertaken. Otherwise, the command is considered to be from an illegitimate user using the in-hand device and is discarded. This system also proposes an infrastructure support and mechanism for the user biometric enrollments through Tier-1s and Original Equipment Manufacturers (OEMs).

Introduction

Rapid technological advancements of vehicle manufacturing and the modern wireless technology opens the door for several new Intelligent Transportation applications. Over the past decade, the automotive industry has advanced the traditional ways of accessing and starting the vehicles by making use of embedded processors and wireless communications. The automotive world is no more different when compared to other domains which are susceptible to cyber attacks. The connected cars are the fancy images we all wish to pursue in future, but they equally have multiple security issues similar to thorns behind the roses. Connected cars are modifying the purpose of the vehicle by introducing multidimensional functionalities in connected car infrastructure [1]. Today's cars are not just transportation equipment, rather they do much more human needed functionalities by communication through IoT enables smart devices. The world is predicted to have over 150 million connected cars by 2020 [1] and already one-third of the existing cars are connected with the internet, this provides an open zone for the hackers to shake the automotive world through their catastrophic attacks. The famous automotive cyber news in the US in 2015 was when Jeep Cherokee forced to withdraw their 1.4 million sold vehicles when the US security experts proved that they could able to hijack and paralyze their vehicles over the internet [2] [3]. However, later they are called and patches are applied for the identified vulnerabilities. Repeated occurrences of similar incidents around the world created a fear among the automotive consumer community and it also drew a new audience's attention towards it.

which provides numerous advantages to the driver in using the vehicle. Even though there are numerous security solutions addressing the cyber attacks on the transmission medium, none of the them taken care of the user authentication in the digital key/wireless vehicle entry system. Hence, an attempt has been made to propose a system for the authentication of the user/owner of the vehicle each time when using the digital key/wireless key entry by integrating biometrics with cryptography in a novel way in this system. The biometric system is undergoing a fusion of multi-mode biometric features into verification. The future work includes the inclusion of this multi-model verification. The personalization of the biometric verification is also a promising future scope in using the biometric digital wireless key verification.

References

1. "Predicts 2015: The Internet of Things," Gartner Report, Press, Release, Jan 26, 2015, https://www.gartner.com/newsroom/id/2970017
2. Greenberg, A., "Hackers Remotely Kill a Jeep on the Highway," , 2015, https://www.wired.com/ 2015/07/hackersremotely-kill-jeep-highway/.
3. Miller, C. and Valasek, C., "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015
4. Oguma, H., Nobata, N., Nawa, K., Mizota, T., and Shinagawa, M., "Passive Keyless Entry System for Long Term Operation," , 2011, 1-3, doi:10.1109/WoWMoM.2011.5986125.
5. Schmitz, S. and Roser, C., "A New State-of-the-Art Keyless Entry System," SAE Technical Paper 980381 (1998). https://doi.org/10.4271/980381.
6. Niu, J.G., Li, C.X., Shi, X.L., and Xu, C.H., "Design and Research of Passive Entry Control System for Vehicle," *IOP Conf. Ser.: Mater. Sci. Eng.* 392 (2018): 062123.
7. https://www.maximintegrated.com/en/design/technical-documents/app-notes/1/1774.html.
8. Wang, J., Lounis, K., and Zulkernine, M., "CSKES: A Context-based Secure Keyless Entry System," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, 2019, 817-822, doi:10.1109/COMPSAC.2019.00120.
9. Glocker, T., Mantere, T., and Elmusrati, M., "A protocol for a Secure Remote Keyless Entry System Applicable in Vehicles Using Symmetric-Key Cryptography," in *2017 8th International Conference on Information and Communication Systems (ICICS)*, 2017, 310-315, doi:10.1109/IACS.2017.7921990.
10. Dadam, S.R., Zhu, D., Kumar, V., Ravi, V. and, Palukuru, V.S.S., "Onboard Cybersecurity Diagnostic System for Connected Vehicles," SAE Technical Paper 2021-01-1249, 2021, https://doi.org/10.4271/2021-01-1249
11. van de Beek, S. and Leferink, F., "Vulnerability of Remote Keyless-Entry Systems Against Pulsed Electromagnetic Interference and Possible Improvements," *IEEE Transactions on Electromagnetic Compatibility* 58, no. 4 (Aug. 2016): 1259-1265, doi:10.1109/TEMC.2016.2570303.
12. Patel, J., Das, M.L., and Nandi, S., "On the Security of Remote Key Less Entry for Vehicles," *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* 2018 (2018): 1-6, doi:10.1109/ANTS.2018.8710105.
13. Glocker, T., Mantere, T., Elmusrati, M., "A Protocol for a Secure Remote Keyless Entry System Applicable in Vehicles using Symmetric-Key Cryptography," https://arxiv.org/abs/1612.00993.

Contact Information

Asadullah Ansari
Connected Car Division
Harman International India Pvt. Ltd
Bangalore, India
+91 95355 12161
Asadullah.Ansari@harman.com

Definitions/Abbreviations

ECU - Engine Control Unit

RKE - Remote Keyless Entry

CID - Customer Identification Device.

ISSN 0148-7191