DataTransfer PDU-based Rollback Mechanism for Securing OCPP 1.6 Against Spoofing Attacks

Dong Uk Kim*, Keon Oh Kim*, Sun-Moo Kang*, Choong Seon Hong*

*CSE Kyung Hee University 1732, Deogyeong-daero, Giheung-gu

{g9896, keonoh, extkang, cshong}@khu.ac.kr

***Abstract*—The Open Charge Point Protocol is a widely adopted communication standard that facilitates interoperability between Charge Points and Central Systems in the electric vehicle charging ecosystem. This paper explores the security implications of OCPP 1.6, with a particular focus on the risks posed by spoofed or unauthorized messages. We propose a rollback mechanism utilizing the DataTransfer PDU to mitigate these risks, allowing the Central System to trigger reversion of unauthorized changes at the CP level. The proposed solution ensures secure, efficient management of configurations and mitigates potential threats such as replay attacks, spoofed requests, and unauthorized modifications. This paper contributes to the growing body of knowledge on securing EV charging infrastructure by highlighting underexplored vulnerabilities in OCPP 1.6 and providing practical solutions to enhance the security and resilience of the protocol.**

***Keyword*—OCPP 1.6, Rollback Mechanism, Spoofing At- tacks, EV Charging Security**

Dong Uk Kim received the B.S. degree in electronic engineering with a minor in computer engineering from Korea Polytechnic University (KPU), Siheung, South Korea, in 2022, and the M.S. degree in computer engineering from Kyung Hee University, Yongin, South Korea, in 2023. He is currently pursuing the Ph.D. degree in computer engineering at Kyung Hee University, Yongin, South Korea. His major fields of study include mathematical optimization and quantum computing.

Keon Oh Kim is a Master's student in Computer Science & Engineering with research interests in machine learning, reinforcement learning, software testing, anomaly detection, and causal learning. He holds a B.Sc. in Molecular Biotechnology from the Faculty of Bioscience Engineering, Ghent University (August 2022). Professionally, he worked as a Frontend Engineer at Fama (March–November 2022) and at Krafton Thingsflow Inc. (December 2022–January 2023).

Sun-moo Kang is a Professor at Kyung Hee University, Suwon Global Campus, and Director of the Grand ICT Research Center and LINC+ Corporate Innovation Support Center. He has held this position since 2015, focusing on ICT and energy management projects. Previously, he served as an ICT Specialist for Gyeonggi Local Government (2014–2015) and held senior roles at NIANIA, KCA, NeoTelecom, and ETRI, contributing to telecommunications, digital signal processing, and protocol development. He was also a Visiting Research Fellow at L.M. Ericsson AB in Stockholm (1984–1987). His expertise includes EV charging protocols, demand response systems, IoT, AI, and blockchain for energy management and smart cities.

Choong Seon Hong [S'95, M'97, SM'11, F'24] is working as a professor with the Department of Computer Science and Engineering, Kyung Hee University. His research interests include future Internet, ad hoc networks, network management, and network security. He was an Associate Editor of the IEEE Trans. Network and Service Management, J. Communications and Networks and an Associate Technical Editor of the IEEE Commun. Mag