IoTivity Packet Parser for Encrypted Messages in Internet of Things

hyeonah Jung, Hyungjoon Koo, and Jaehoon (Paul) Jeong

Department of Computer Science and Engineering
Sungkyunkwan University, Suwon, Republic of Korea
hyeonah214, kevin.koo, pauljeong}@skku.edu

Abstract*—The Internet of Things (IoT) market has been ever-growing because both the demand of smart lives and the number of mobile users keep increasing. On the other hand, IoT device manufacturers tend to employ proprietary operating systems and network protocols, which may lead device interoperability issues. The Open Connectivity Foundation (OCF) has established a standard protocol for seamless IoT communication. IoTivity is one of reference implementations that conforms to the OCF specification. IoTivity utilizes both Datagram Transport Layer Security (DTLS) and Constrained Application Protocol (CoAP) to support a lightweight and secure communication. Although a packet analysis tool like Wireshark offers a feature to decrypt messages over TLS or DTLS by feeding a session key that a Web browser records, it cannot be directly applied to IoTivity because it lacks such a key-tracing functionality. In this paper, we present an IoTivity Packet Parser (IPP) for encrypted CoAP messages tailored to IoTivity. To this end, we modify IoTivity source code to extract required keys, and leverage them to parse each field automatically for further protocol analysis in a handy manner.

***Keyword*—IoTivity, IoT, DTLS, CoAP, Packet Parser**

Hyeonah Jung is a Ph.D student in the Department of Computer Science and Engineering, College of Computing and Informatics, Sungkyunkwan Univer-sity, South Korea, since fall 2021. Her Ph.D advisor is Professor Jaehoon (Paul) Jeong. She got a BS degree from Mokpo National Maritime University. Her research interests is Internet of Things (IoT), Cloud Computing and Internet Protocols Standardization

Hyungjoon Koo is an assistant professor in the Department of Computer Science and Engineering, College of Computing at Sungkyunkwan University (SKKU). Before joining SKKU, he was a post-doctoral researcher at SSLab in Georgia Institute of Technology. He earned his Ph.D. in Computer Science from Stony Brook University in 2019, and received the M.Sc. degree in Information Security from Korea University in 2010. He is leading the SecAI (Security with AI) Lab. His research interests lie in software security, network security, binary analysis and protection, and security leveraging artificial intelligence.

Jaehoon (Paul) Jeong is an associate professor in the Department of Computer Science and En-gineering at Sungkyunkwan University in Korea. He received his Ph.D. degree in the Department of Computer Science and Engineering at the University of Minnesota in 2009. He received his B.S. degree in the Department of Information Engineering a Sungkyunkwan University and his M.S. degree from the School of Computer Science and Engineering at Seoul National University in Korea in 1999 and 2001, respectively. His research areas are Internet of Things, Software-Defined Networking, Network Functions Virtualization, security, and vehicular networks. Dr. Jeong is a member of ACM, IEEE and the IEEE Computer Society.