Security Analysis of Samsung Knox

Munkhzorig Dorjmyagmar, MinChang Kim, Hyoungshick Kim

Department of Computer Science and Engineering, Sungkyunkwan University, Korea[**]School Electronics and Telecommunications, Hanoi University of Science and Technology, Hanoi, Vietnam

fmnkhzrg, mckim, hyoungg@skku.edu

Abstract— A Trusted Execution Environment (TEE) has become popular in the mobile industry. Hardware-based security will be employed by default for every mobile device within a few years. In this paper, we explore several potential security issues of the **Samsung Knox p**latform that is one of the advanced hardware based mobile security platforms for Android devices. We describe several attack scenarios to show how the Knox platform can be compromised. We particularly performed experiments for Man in the Middle Attacks with an untrusted certificate. To mitigate such security risks, we also recommend several countermeasures based on fundamental security principles. For example, security-sensitive resources in Knox should be strictly isolated from processes in an insecure operating system.

Keyword— TrustZone, Samsung Knox, Trusted Computing.

Phuong T.K Dinh received the B.E in Radio and Communication from University of Transport and Communications, Vietnam in 2001 and M.E in Information Processing and Communications from Hanoi University of Science and Technology, Vietnam in 2006. She is currently a PhD student in Hanoi University of Science and Technology, Vietnam. From March 2016 to January 2017, she is a research student in Kyushu Institute of Technology. Her research interests include algorithms in TI-ADC as well as FFT/IFFT for wireless communication.

Munkhzorig Dorjmyagmar was born in Ulaanbaatar, Mongolia, in 1982. He received his Bachelor degree in Information Technology from Uttar Pradesh Technical University, Lucknow, India, in 2007. He is currently pursuing his M.S. degree in Electrical and Computer Engineering at Sungkyunkwan University, Suwon, Korea. He has been working in the Technology and Research Institute of Mongolia since 2008. His research interests are security engineering, mobile platform security and social network analysis.

MinChang Kim received his M.S. degree in business administration from Sungkyunkwan University, Seoul, Korea, in 2009. He is currently pursuing a Ph.D. degree in Electrical and Computer Engineering at Sungkwyunkwan University, Suwon, Korea. Since 2006, he has been working in the Software Content Research Laboratory of Electronics and Telecommunications Research Institute. His research interests are security engineering, mobile security, IoT Security, and artificial neural network

Hyoungshick Kim Hyoungshick Kim is an assistant professor in the Department of Computer Science and Engineering, College of Information and Communication Engineering, Sungkyunkwan University. He received a BS degree from the department of Information Engineering at Sungkyunkwan University, a MS degree from the Department of Computer Science at KAIST and a Ph.D. degree from the Computer Laboratory at University of Cambridge in 1999, 2001 and 2012, respectively. After completing his PhD, he worked as a post-doctoral fellow in the Department of Electrical and Computer Engineering at the University of British Columbia. He previously worked for Samsung Electronics as a senior engineer from 2004 to 2008. He also served as a member of DLNA and Coral standardization for DRM interoperability in home networks. His current research interest is focused on software security and usable security.