Zero-Day Attack Packet Highlighting System

Jang Hyeon Jeong, Jong Beom Kim*, Seong Gon Choi

Information & Communication Engineering, Chungbuk National University, Cheongju-si Chungcheongbuk-do, Korea

*Xabyss Inc, Seongnam-si, Gyeonggi-do, Korea

wkdgus4788@chungbuk.ac.kr, jbkim@xabyss.com, choisg@chungbuk.ac.kr

Abstract— **This paper presents Zero-Day Attack Packet Highlighting System. Proposed system outputs zero-day attack packet information from flow extracted as result of regression inspection of packets stored in flow-based PCA. It also highlights raw data of the packet matched with rule. Also, we design communication protocols for sending and receiving data within proposed system. Purpose of the proposed system is to solve existing flow-based problems and provides users with raw data information of zero-day packets so that they can analyze raw data for the packets.**

Keyword— **NIDPS, PCA, Zero-Day Attack, DPI**

Jang Hyeon Jeong received B.S. degree in the College of Electrical & Computer Engineering, Chungbuk National University, Korea in 2019. He is currently a M.S. candidate in School of Electrical & Computer Engineering, Chungbuk National University. His research interests include Network Security, Smart Grid.

Jong Beom Kim received B.S. and M.S. degree in the College of Electrical & Computer Engineering, Chungbuk National University, Korea in 2017 and 2019. His research interest is network programming, He is currently researcher in Xabyss Inc. His research interest is network security.

Seung Gon Choi received B.S. degree in Electronics Engineering from Kyeongbuk National University in 1990, and M.S. and Ph.D. degree from Information Communications University, Korea in 1999 and 2004, respectively. He is currently an associate professor in College of Electrical & Computer Engineering, Chungbuk National University. His research interests include smart grid, IoT, mobile communication, high-speed network architecture and protocol.