An Intelligence Defense System with SNORT Rules

Yi-Cheng Lai*, Chiao-Lin Yu*, Man-Ling Liao*, Yu-Shan Lin**, Yao-Chung Chang*** and Jiann-Liang Chen*

*Department of Electrical Engineering, National Taiwan University of Science and Technology, Taipei, Taiwan

**Department of Information Science and Management Systems, National Taitung University, Taitung, Taiwan

*** Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan

m11007505@mail.ntust.edu.tw, m10907505@mail.ntust.edu.tw, m11007502@mail.ntust.edu.tw, ysl@nttu.edu.tw, ycc@nttu.edu.tw, lchen1215@gmail.com

***Abstract*—Misconfiguration of firewall rules has always been considered a serious issue. The handwritten rule is messy and buggy under the increasingly complex firewall architecture. To avoid being attacked behind an insecure firewall. This study defines an intelligence defense system. Combined with data analysis, feature extraction, optimization, and firewall technology. Its main purpose is to replace handwritten firewall rules and provide immediate and reliable protection against diversified attacks. In the verification, 68,936,206 packets collected by Cowrie honeypot were used as the test data. The accuracy rate of classifying different attack behaviors reached 99.5%, and the packet coverage of Snort rules also achieved 98%. This thesis proposes a system that can effectively identify and defend from diverse attacks.**

***Keywords*—MITRE ATT&CK, K-means, PCRE Regular Expression, Snort Rule**

Yi-Cheng Lai was born in Taipei, Taiwan, in 1998. He received his B.S. degree in 2021. He is pursuing an M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei. His main research interests include cyber security, vulnerability research, and defense.

Chiao-Lin Yu was born in Taipei, Taiwan, in 1997. He received his M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei, Taiwan, in 2022. His main research interests include cyber security, vulnerability research, and defense.

Man-Ling Liao was born in Tainan, Taiwan, in 1998. She received her B.S. degree in 2021. She is pursuing an M.S. degree in electrical engineering from the National Taiwan University of Science and Technology, Taipei. Her main research interests include data analysis, machine learning, and cyber threat intelligence.

Yu-Shan Lin is a professor in the Department of Information Science and Management Systems, National Taitung University, Taitung, Taiwan. She received her Ph.D. degree from National Sun Yat-sen University, Kaohsiung, Taiwan. Her research interesting areas include e-Learning, Information Technology Education, and Internet Marketing. She has published about 20 journal papers, and some are highly-cited papers. Moreover, she received the Best Paper Award from IEEE ICASI 2018, IC3 2018, 2019 and TANET 2020, 2021.

Yao-Chung Chang (Member, IEEE) is a professor in the Department of Computer Science and Information Engineering, National Taitung University, Taitung, Taiwan. He received a Ph.D. degree in Computer Science and Information Engineering in Computer Science and Information Engineering from National Dong Hwa University (NDHU), Hualien, Taiwan. Also, he received the Outstanding Teaching Award from Nation Taitung University. His main research interests include Information & Network Security, Cloud & Mobile Computing, AIoT & Machine Learning.

Jiann-Liang Chen (Senior Member, IEEE) was born in Taiwan in December 1963. He received his Ph.D. in electrical engineering from the National Taiwan University, Taipei, Taiwan, in 1989. Since August 1997, he has been with the Department of Computer Science and Information Engineering, National Dong Hwa University, where he is a Professor and the Vice Dean of the Science and Engineering College. He joins the Department of Electrical Engineering, National Taiwan University of Science and Technology, as a Distinguished Professor. Also, Prof. Chen is the Dean, College of Electrical Engineering and Computer Science, National Taiwan University of Science and Technology. His current research interests include cellular mobility management, cyber security, personal communication systems, and the Internet of Things (IoT).