OWASP IoT Top 10 based Attack Dataset for Machine Learning

Nay Myat Min*, Vasaka Visoottiviseth*, Songpon Teerakanok*, Nariyoshi Yamai**

*Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom, Thailand

**Institute of Engineering, Tokyo University of Agriculture and Technology (TUAT), Tokyo, Japan

nay.min@student.mahidol.ac.th, {vasaka.vis, songpon.tee}@mahidol.edu, nyamai@cc.tuat.ac.jp

***Abstract*— Internet of Things (IoT) systems are highly susceptible to cyberattacks by nature with minimal security protections. Providing a massive attack surface for attackers, they automatically become easy targets with potentially catastrophic impacts. Researchers are currently focusing on developing various anomaly detection systems for IoT networks to deal with this situation. However, these systems require a comprehensive labeled attack dataset to classify the malicious traffic correctly. This paper presents a systematic approach to design and develop an IoT testbed to generate such an attack dataset, namely the AIoT-Sol Dataset. Our proposed dataset contains the benign traffic as well as the often-overlooked attack techniques in the existing IoT datasets. It encompasses 17 attack types from several categories: network attacks, web attacks, and web IoT message protocol attacks. We selected these attacks by referencing the Open Web Application Security Project (OWASP) IoT Top Ten. Also, we provide a mapping of possible attacks for all ten security risks.**

***Keyword*— Internet of Things, IoT, Attack Dataset, Anomaly Detection, Machine Learning, Security, OWASP IoT Top 10**

Nay Myat Min is a research student at Mahidol University, Thailand. He is an M.Sc. Degree in Cyber Security and Information Assurance candidate. He received his B.Sc. in Computer and Network Technology from Northumbria University in 2018. Since then, he has worked as a security professional in the Banking Industry. His prior work experience includes penetration testing and risk assurance. His research interests are offensive security, IoT security, and machine learning.

Vasaka Visoottiviseth is an associate professor at Mahidol University, Thailand. She received her Ph.D. degree in computer engineering from Nara Institute of Science and Technology (NAIST), Japan in 2003, M.E. and B.E. degree from Tokyo University of Agriculture and Technology (TUAT), Japan in 1999 and 1997, respectively. Her current research interests are mobile and wireless computing, Internet traffic measurement, and network security. She has been a member of IEEE since 1998.

Songpon Teerakanok received his B.E. from Prince of Songkla University, Thailand in 2013, and M.E. and D.Eng. degrees in Information Science and Engineering from Ritsumeikan University in 2016 and 2019, respectively. He was a former assistant professor at Ritsumeikan University before joining the Faculty of ICT, Mahidol University, Thailand in May 2021. His research interest covers Cryptography, Privacy, Location-based Service (LBS), and Digital Forensics.

Nariyoshi Yamai received the B.E. and M.E. degrees in electronic engineering and the Ph.D. degree in information and computer science from Osaka University in 1984, 1986, and 1993, respectively. After working at Nara National College of Technology, Osaka University, and Okayama University, he has been a Professor at the Institute of Engineering, Tokyo University of Agriculture and Technology since April 2014. His research interests include distributed systems, network architecture, and Internet. He is a member of IEEE CS, IEEE ComSoc, IEICE and IPSJ.