Have It Your Way: Generating Customized Log Data Sets with a Model-driven Simulation Testbed

Max Landauer
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
max.landauer@ait.ac.at

Florian Skopik
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
florian.skopik@ait.ac.at

Markus Wurzenberger
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
markus.wurzenberger@ait.ac.at

Wolfgang Hotwagner
Center for Digital Safety & Security
Austrian Institute of Technology
Vienna, Austria
wolfgang.hotwagner@ait.ac.at

Andreas Rauber
Institute of Information Systems Engineering
Vienna University of Technology
Vienna, Austria
rauber@ifs.tuwien.ac.at

***Abstract*—Evaluations of intrusion detection systems (IDS) require log data sets collected in realistic system environments. Existing testbeds therefore offer user simulations and attack scenarios that target specific use-cases. However, not only does the preparation of such testbeds require domain knowledge and time-consuming work, but also maintenance and modifications for other use-cases involve high manual efforts and repeated execution of tasks. We therefore propose to generate testbeds for IDS evaluation using strategies from model-driven engineering. In particular, our approach models system infrastructure, simulated normal behavior, and attack scenarios as testbed-independent modules. A transformation engine then automatically generates arbitrary numbers of testbeds, each with a particular set of characteristics and capable of running in parallel. Our approach greatly improves configurability and flexibility of testbeds and allows to reuse components across multiple scenarios. We use our proof-of-concept implementation to generate a labeled data set for IDS evaluation that is published with this paper.**

This paper has been recommended by the QRS 2020 Program Committee to the IEEE Transactions on Reliability for possible publication. To avoid duplication, only the abstract of the paper is included in the Proceedings

978-1-7281-8913-0/20/$31.00 ©2020 IEEE
DOI 10.1109/QRS51102.2020.00019