Attesting L-3 General Program Anomaly Detection Efficiency with SPADA

Francis Moreira*, Danilo Carastan-Santos† and Philippe Navaux‡
Department of Informatics, Federal University of Paraná
Curitiba, PR – Brazil
Email: *fbmoreira@inf.ufpr.br
Informatics Institute, Federal University of Rio Grande do Sul
Porto Alegre, RS – Brazil
Email: †danilo.csantos@inf.ufrgs.br ‡navaux@inf.ufrgs.br

***Abstract*—One of the main challenges for security systems is the detection of general vulnerability exploitation, especially when the exploit uses valid control flow. Thus, the detection of anomalous behavior provides an exciting research direction, as the research in this field tries to describe what is the standard program execution, to then detect as anomalous any behavior that does not fit that description.**

In this work, we compare two mechanisms that aim to detect general anomalies: SPADA and LAD. SPADA is an L-3 language mechanism that partitions phases and uses simple phase features to detect anomalies. LAD is a constrained L-1 language mechanism that applies complex clustering and machine learning models on specific functions to detect anomalies. In our experimental campaign with several real-world exploits, we show that SPADA's detection mechanism performs better than LAD while being much simpler and easier to implement. We therefore show experimental evidence that further attests the efficiency of L-3 attack detection mechanisms for real attacks.

Keywords*—*Computer Security, Intrusion Detection, Program Profiling.

ACKNOWLEDGMENT

The authors would like to thank CAPES and professor Israel Koren for the financial support during the PVE project nr. 117/2013 . This study was also financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001. We would also like to thank CNPq and Universidade Federal do Rio Grande do Sul (UFRGS) for the financial support.

DISCLAIMER

This abstract describes the paper "Attesting L-3 General Program Anomaly Detection Efficiency with SPADA", from the same authors, that has been published in the IEEE Symposium on Computers and Communications 2020 (ISCC '20).