Framework for Evaluating Collaborative Intrusion Detection Systems

Dennis Grunewald, Joel Chinnow, Rainer Bye, Ahmet Camtepe,
Sahin Albayrak
DAI-Labor — TU Berlin, Ernst-Reuter-Platz 7
firstname.surname@dai-labor.de

Abstract: Securing IT infrastructures of our modern lives is a challenging task because of their increasing complexity, scale and agile nature. Monolithic approaches such as using stand-alone firewalls and IDS devices for protecting the perimeter cannot cope with complex malwares and multistep attacks. Collaborative security emerges as a promising approach. But, research results in collaborative security are not mature, yet, and they require continuous evaluation and testing.

In this work, we present *CIDE*, a *Collaborative Intrusion Detection Extension* for the network security simulation platform (*NeSSi*^{2}). Built-in functionalities include dynamic group formation based on node preferences, group-internal communication, group management and an approach for handling the infection process for malware-based attacks. The CIDE simulation environment provides functionalities for easy implementation of collaborating nodes in large-scale setups. We evaluate the group communication mechanism on the one hand and provide a case study and evaluate our collaborative security evaluation platform in a signature exchange scenario on the other.