CIMD- Collaborative Intrusion and Malware Detection

Rainer Bye*

* Technische Universität Berlin, DAI-Labor
Ernst-Reuter Platz 7, D-10587 Berlin, Germany
rainer.bye{at}dai-labor.de

Computer networks are exposed to a variety of threats: zero-day attacks leave devices connected to the Internet susceptible to attacks because there are no appropriate signatures available during the vulnerability window. On the other hand, purely anomaly-based detection schemes capable of detecting new attacks are often of limited use due to a high false-positive rate.

Hence, intrusion detection and response can be considered a complex task. From the field of sociology we learn that teams respectively groups cope with complex tasks by their inherent cooperative character. There exist cooperative intrusion detection systems bypassing shortcomings of conventional approaches, but these are often limited to very specialized scenarios and do not take the configuration of other participating nodes into account [2, 1].

In this regard, I propose CIMD (Collaborative Intrusion and Malware Detection), a scheme for the realization of collaborative intrusion detection approaches. I argue that teams, respectively *detection groups* with a common purpose for intrusion detection and response, improve the measures against malware. By enabling participants to state their *objectives* (i.e. the aim of a detection group) and *interests* (i.e. the desired properties of the team members) an intrusion detection overlay is realized.

In our ongoing work, we contribute a taxonomy-based data model reflecting relevant properties of the participants of the overlay. We discuss each category in the taxonomy with regard to the impact on detection groups and their value for collaborative intrusion detection. Additionally, we provide a group formation algorithm taking objectives, interests, and maximum group size into account. Furthermore, we introduce the notion of *homogeneous* as well as *heterogeneous detection groups*, give concrete scenarios. The scenario for homogeneous groups is based on our previous work in [3]. Finally, we conduct a vulnerability analysis of the system.

The remaining problems include the evaluation of different ontology matching techniques for the group formation, the selection of an appropriate overlay network and common data exchange format as well as a suitable trust management approach. Eventually, we plan to carry out more detailed vulnerability analysis.

References

[1] Vinod Yegneswaran,Paul Barford, and Somesh Jha. Global intrusion detection in the DOMINO overlay system. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2004*, 2004.

[2] Katja Luther, Rainer Bye, Tansu Alpcan, Sahin Albayrak, and Achim Müller. A Cooperative AIS Framework for Intrusion Detection. In *Proceedings of the IEEE International Conference on Communications, ICC 2007*, 2007.

[3] Rainer Bye, Katja Luther, Seyit Ahmet Çamtepe, Tansu Alpcan, Şahin Albayrak, and Bülent Yener. Decentralized Detector Generation in Cooperative Intrusion Detection Systems. *Stabilization, Safety, and Security of Distributed Systems 9th International Symposium, SSS 2007 Paris, France, November 14-16, 2007 Proceedings*, Lecture Notes in Computer Science , Vol. 4838. Springer, 2008.