IDS@FutureSOC: An IDS Correlation Platform using In-Memory and Multi-Core

Background

Intrusion Detection Systems (IDS) have been widely deployed in practice for detecting malicious behavior on network communication and hosts. False-positive alerts are a popular existing problem for most of IDS approaches. The solution to address this problem is correlation and clustering of alerts. To meet the practical requirements, this process needs to be finished as fast as possible, which is a challenging task as the amount of alerts produced in large scale deployments of distributed IDS is significantly high, due to the deployment of IDS sensors in Cloud computing and open network designs (e.g., SOA). We propose the utilization of memory-optimized algorithms and In-memory databases for correlation and clustering. Different types of correlation modules can be integrated and compared on the platform prototype, which can make use of both paradigms: multi-core and In-memory.

Description

We believe that research in the area of IDS and network security as application for multi-core and In-memory based platforms can provide new paradigms for conducting security. Correlation and clustering is currently only done in a limited way using filtered data sets. Using the multi-core and In-memory platforms, it is possible to do correlation and clustering on an unfiltered data set. Thus, it might not be necessary to configure (e.g., exclude certain detection rules) the IDS sensor anymore, as the correlation and clustering can do meaningful reasoning on all alerts in a short time. Furthermore, we expect correlation and clustering services offered in the Cloud. A flexible and extensible correlation platform can provide the foundation work for a new paradigm in security.

References

- Christopher Kruegel, Fredrik Valeur, Giovanni Vigna: “Intrusion Detection and Correlation – Challenges and Solutions”, Springer, 2010, ISBN: 978-1441936240
- R. Sadoddin, A. Ghorbani: “Alert Correlation Survey: Framework and Techniques”, In: Proceedings of the International Conference on Privacy, Security and Trust (PST’06), ACM Press, Markham, Ontario, Canada, pp. 1-10 (2006).
- Roschke, S., Cheng, F., and Meinel, Ch.: “A Flexible and Efficient Alert Correlation Platform for Distributed IDS”, In: Proceedings of the 4th International Conference on Network and System Security (NSS’10), IEEE Press, Melbourne, Australia, pp. 24-31 (September 2010).

Contact

Internet-Technologies and Systems

- Prof. Dr. Christoph Meinel
- Sebastian Roschke, Feng Cheng