Libvmtrace: Tracing virtual machines

Benjamin Taubmann, Noelle Rakotondravony, Hans P Reiser
University of Passau
{bt,nr,hr}@sec.uni-passau.de

January 22, 2016

Virtual machine introspection can be used for several security relevant objectives such as intrusion detection, malware analysis and forensic evidence collection on virtual machines [1]. However, current implementations such as Volatility [3] are mostly static, i.e., unable to trace the execution of virtual machines at run-time. Such tracing includes for example, the monitoring of system calls or the dynamic insertion of arbitrary breakpoints.

The objective of this work is to implement a library that allows tracing the behavior of virtual machines (e.g., system calls) and their network traffic. These traces shall be gathered in a central database so that we can visualize the data for human operators. Furthermore, we are planning to apply machine learning techniques on these traces in order to perform anomaly and malware detection.

Another use case for this library is to combine both types of traces so that, for example, a memory snapshot is triggered when specific network packets are observed [2].

References

[1] T. Garfinkel and M. Rosenblum. A Virtual Machine Introspection Based Architecture for Intrusion Detection. In *Proceedings Network and Distributed Systems Security Symposium*, 2003.

[2] B. Taubmann, C. Frädrich, D. Dusold, and H. P. Reiser. Tlskex: Harnessing virtual machine introspection for decrypting tls communication. In *DFRWS EU 2016 Annual Conference*, 2016.

[3] The Volatility Foundation. Volatility framework. https://github.com/volatilityfoundation Accessed: 2016-01-19.