Benchmarking Intrusion Detection Systems

Description

Modern intrusion detection systems (IDSes) for virtualized environments are deployed in the virtualization layer with components inside the virtual machine monitor (VMM) and the trusted host virtual machine (VM). Such IDSes can monitor at the same time the network and host activities of all guest VMs running on top of a VMM being isolated from malicious users of these VMs.

The task of this work is to analyze state-of-the-art intrusion detection techniques applied in VMM-based IDSes, as well as the challenges that apply to their benchmarking.

In addition to studying and summarizing the research literature, it is a mandatory part of this seminar to gather and share hands-on experience with the available tooling infrastructure. The provided references [1] are to be considered a starting point and it is expected to extend the literature search and present a coherent view on the current state of the art in this area.

References


Contacts

Dušan Okanović (okanovic@informatik.uni-stuttgart.de)
Reliable Software Systems (RSS) Group
Institute for Software Technology (ISTE)
University of Stuttgart