Contribution ID: **61** Type: **Paper presentation**

Infrastructure for Capturing and Persisting Virtualization-Specific Events Triggered by In-Guest Process Executions for Behavioral-Based Analysis

Friday 5 November 2021 12:40 (20 minutes)

Nowadays, security threats become more and more harmful. Many security solutions have been implemented along the time, the most popular being the anti-viruses. They offer proper protection against computer viruses unless these malicious programs do not run at a higher privilege level than the security solution itself. This shortcoming of conventional security solutions can be reduced using virtualization-based mechanisms, which run totally separated from the main user environment, in the same time being able to monitor events and take actions if necessary. In order to improve their performance, behavioral datasets of malicious software can be used for training a model which can then be used by the security solution. There are very few publicly known and relevant datasets from which one can build such a model, so the current paper proposes an open design for an infrastructure capable of recording and storing application behavioral events in order to train a security-oriented machine learning solution. The proposed solution consists of a hypervisor that is run on an end-user system and the necessary software that controls the activation, interception and storage of virtualization events from which one can build the relevant datasets.

Authors: VARADI, Robert (Technical University of Cluj-Napoca); Mr RAT, Gabriel (Technical University of Cluj-Napoca); Dr COLEȘA, Adrian (Technical University of Cluj-Napoca)

Presenters: VARADI, Robert (Technical University of Cluj-Napoca); Mr RAT, Gabriel (Technical University of Cluj-Napoca)

Session Classification: RO-LCG 2021 ”Grid, Cloud && High Performance Computing in Science” & Cloud Computing and Network Virtualisation

Track Classification: Cloud Computing and Network Virtualisation