Software Engineering Seminar (SoSe 2017)

Anomaly Detection in Application Performance Monitoring and Intrusion Detection Systems

Description

In the area of software monitoring there are at least two fields that use anomaly detection to find different kinds of problems. In the area of application performance monitoring (APM), anomaly detection is used to find performance problems while intrusion detection systems (IDS) try to detect security problems (e.g., security breaches).

After an introduction to anomaly detection approaches in both fields, the aim of the seminar paper is to elaborate on similarities and differences in the means and methods to detect anomalies and whether some approaches could be used in the other field. This might also include the implementation and evaluation of promising approaches (e.g., implementation of methods from IDS in the APM context).

The provided references are to be considered a starting point and it is expected to extend the literature.

References


Contacts

Thomas F. Düllmann (thomas.duellmann@informatik.uni-stuttgart.de)
Reliable Software Systems (RSS) Group
Institute for Software Technology (ISTE)
University of Stuttgart