International Conference on Network and Service Management (CNSM 2015)

Risto Vaarandi

In November 9-13 2015, senior researcher Risto Vaarandi from TUT Centre for Digital Forensics and Cyber Security participated in the 2015 International Conference on Network and Service Management (CNSM 2015), and presented the paper "LogCluster - A Data Clustering and Pattern Mining Algorithm for Event Logs". CNSM is a selective single-track conference which has been organized since 2005, and is one of the premier academic events in the field of network management. The presented paper has been co-authored by Mauno Pihelgas (PhD student at TUT), and discusses a data mining approach for knowledge discovery from event logs. The paper presents a novel clustering algorithm LogCluster which mines line patterns from textual event logs. The algorithm is able to address the shortcomings of existing clustering algorithms and mine more meaningful patterns from event logs. The discovered line patterns can be used for developing event correlation and alerting rules, writing event parsers, but also for the detection of anomalous events. In addition, the paper describes a publicly available implementation of LogCluster which has been released under the terms of GNU GPL. In the paper, several scenarios of using the LogCluster implementation are discussed, and the paper provides performance evaluation of the implementation. The paper has been published in the IFIP digital library (accessible from http://dl.ifip.org/db/conf/cnsm/cnsm2015/1570161213.pdf), and the LogCluster implementation can be downloaded from http://ristov.github.io/logcluster.