Online surveillance of critical computer systems through advanced host-based detection

TotalADS

Shariyar Murtaza, Wael Khreich, Wahab Hamou-Lhadj

Software Behaviour Analysis (SBA) Research Lab
Concordia University
Montreal, QC, Canada

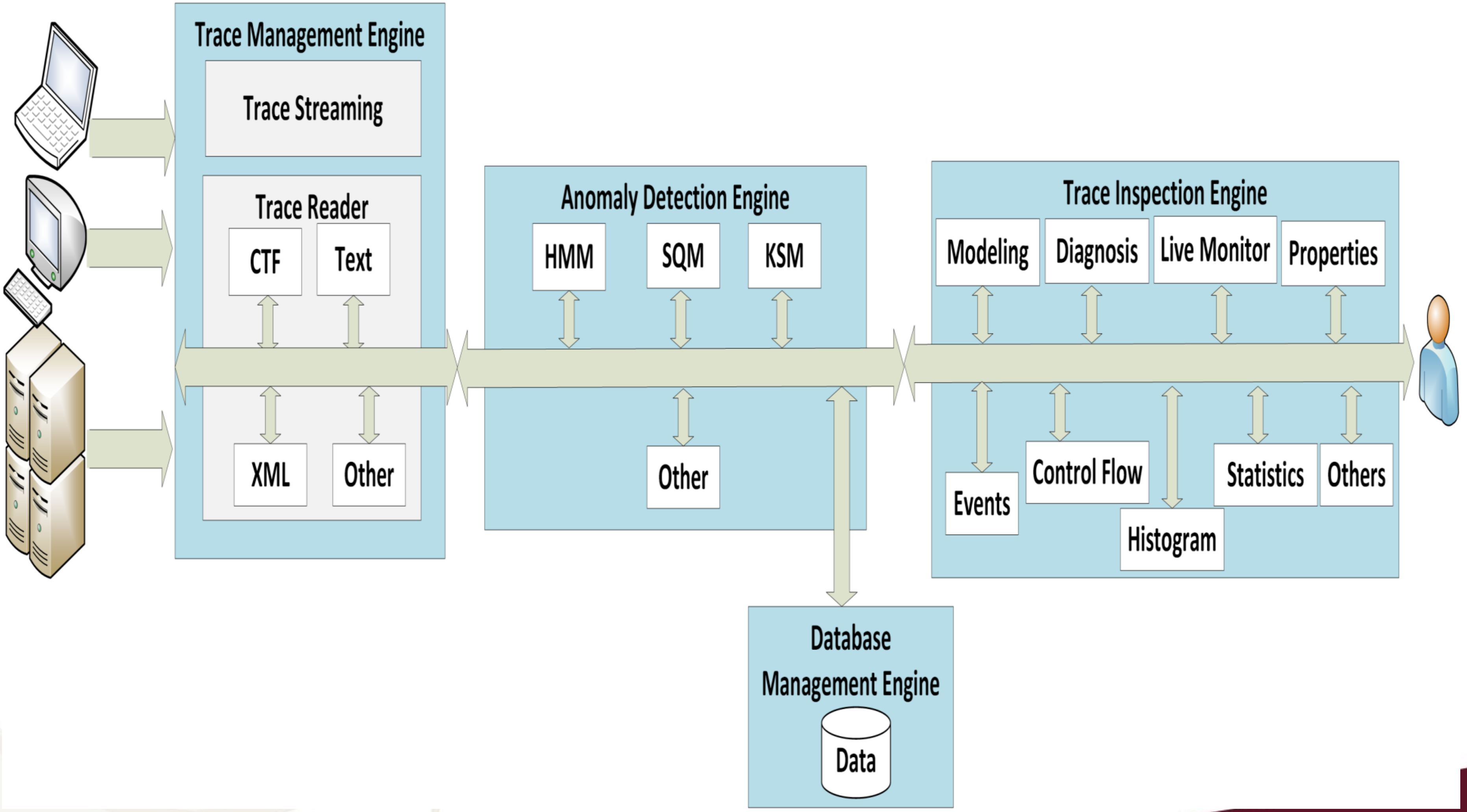
Dec 10, 2014

TotalADS: Total Anomaly Detection System

- TotalADS is a framework that integrates different anomaly detection algorithms and trace types for automated anomaly detection.

- Applications:
  - Automatic detection of zero day attacks.
  - Automatic detection of anomalies in logs and traces (e.g., performance issues, crashes, etc.).
  - Self adaptive surveillance and monitoring.

TotalADS Architecture



TotalADS Features

- Integrates existing (and newly developed) anomaly detection algorithms
- Supports traces and logs in CTF, XML, and text
- Supports live training and anomaly detection
- Supports variety of trace inspection views for forensic analysis (control flow of processes, resource usages…)
- Provides extendable interfaces to add new algorithms, trace formats, and views
- Available as an Eclipse Plugin

Demo.

Open Issues

- We need to monitor 100+ hosts, what is the best way to deploy and manage TotalADS?
- Centralized vs. local deployment
- Centralized Architecture:
  - Can LTTng extract live stream of system calls without affecting the monitored system and network performance?
  - Taking TotalADS to its limits for monitoring live streams: what would be the best solution to make anomaly detection algorithms process the data stream?

TotalADS Open Issues (Cont.)

- Local Deployment:
  - Off-line vs. online scenarios
  - Efficient ways to transfer the system call traces from several hosts to a local machine
  - Updating the internal algorithms to adapt to changes in the software

Getting attack traces

- Open issue for both centralized and local scenarios

  Generating and simulating attacks for:

  - Tuning parameters of anomaly detection algorithms
  - Evaluation of the ADS
  - Setting decision thresholds
  - Combing multiple detectors

Using additional features

- Improving system calls anomaly detection systems using additional features:
  - What events can be extracted from LTTng and used for host monitoring?
- Detecting anomalies in log files and crash traces:
  - What events can be extracted from logs or crash traces to automatically detect anomalies?
  - How can custom logs be visualized using TMF?

TotalADS won the Best People's Choice Showcase Award at the IBM Center of Advanced Studies Conference (CASCON).

TotalADS Download

- http://www.ece.concordia.ca/~abdelw/sba/totalads/
- Installation instructions
- User's guide
- Developer's guide
- Source code
- Binaries
- Documentation (papers)
- Contact: wahab.hamou-lhadj@concordia.ca