A Blend of Semantic Monitoring and Intrusion Detection Systems for the Protection of Critical Infrastructures: Research efforts within the Greek Cybercrime Center[1]

D. Kostopoulos, V. Tsoulkas, G. Leventakis, P. Drogkaris and V. Politopoulou

Center for Security Studies (KEMEA), Ministry of Public Order and Citizen Protection,
Athens, GR-10177, Greece
{tsoulkas.kemea, dimkostopoulos, george.leventakis, prokopis.drogkaris,
v.politopoulou}@gmail.com

Keywords: Semantics Monitoring, Modeling and Event Processing, Sequential Inspection Schemes.

The issues of safety and security of Critical Infrastructures (CIs) as a function of their operational continuity, within nominal operational bounds as well as their robust stability properties against perturbations generated by malicious attacks or human error, are considered globally of highest importance for today's societies. Due to the direct population impact of the CIs physical controlled processes and services, mismanagement faults or cyber attacks against their components can cause severe damage and cascaded performance degradation that can lead to major crises. Therefore, it is imperative to protect these complex and performance critical distributed systems against any threat, by:

- protecting CIs against a wide class of threat consequences,
- forbidding the threats to occur within the CIs networks and
- predicting the occurrence of a threat and quickly react by eliminating its roots.

We provide an overview of the monitoring/reasoning components of the event driven architecture. The tool is modular and provides risk analytics for rapid decision making under uncertainty. Monitored data is captured and fed into a Data Stream Management System (DSMS). This data stream is then applied to a sequential inspection scheme that translates raw data events into possible asset behaviors. These behaviors are then added into a semantics ontology through an Incremental Model Generator (IMG). The updated models are injected into the threat classification and estimation modules and the new security map of the system is displayed on the Decision Support Tool (DST) that alerts the CI supervision team of any new threats or faulty situation.

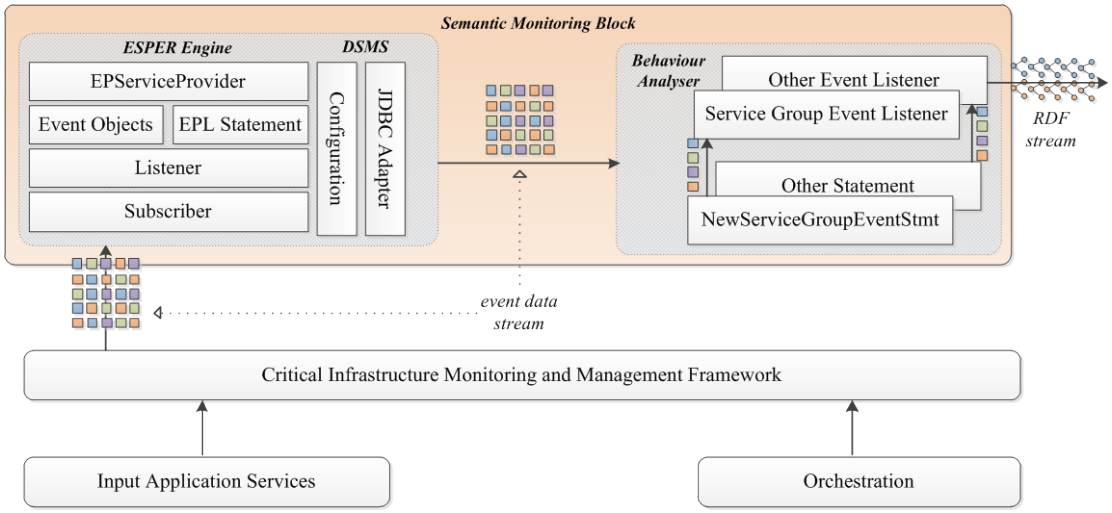

Figure 1: Semantic Monitoring Architecture Block

Figure 1 above depicts the semantic monitoring block which is comprised of the ESPER engine and the Behaviour Analyser (BA) cascaded components. The BA decides how to convert monitoring information into semantic assertions. For the data analysis part, the non-parametric cumulative sum control chart (CUSUM) was used with its associated binary decision function and stopping rule for fast sequential inspection.

[1] The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. HOME/2011/ISEC/AG/INT/4000002166.

Current and Future Research Directions:

- Combination of change detection schemes such as the Sequential Probability Ratio Test (SPRT) with Kalman filtering and Spectral analysis of monitoring data (DFT, FFT)
- New complex event processing components (currently using Esper)
- Bayesian learning likelihood estimators and Finite Markov Chains
- Other semantics reasoners (currently using Hermit)

References

1. Greek Cybercrime Center: http://www.cybercc.gr
2. D. Kostopoulos, G. Leventakis, V. Tsoulkas, and N. Nikitakos, 'An Intelligent Fault Moni-toring and Risk Management Tool for Complex Critical Infrastructures: The SERSCIS Approach in Air-Traffic Surface Control', UKSim 14th International Conference on Computer Modeling and Simulation, IEEE, pp. 205–210 (2012)
3. Esper - Complex Event Processing: http://esper.codehaus.org
4. M. Surridge, A. Chakravarthy, M. Hall-May, X. Chen, Xiaoyu, B. Nasser, and R. Nossal, "SERSCIS: Semantic Modelling of Dynamic, Multi-Stakeholder Systems" 2nd SESAR Innovations Days, Germany (2012)