Predictive Security Analysis at Runtime
– Lessons Learnt from Adaptation to Industrial Scenarios –

Roland Rieke
Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany
Philipps-Universität Marburg, Germany
roland.rieke@sit.fraunhofer.de
http://rieke.link/

Dagstuhl Seminar "Unleashing Operational Process Mining", Nov. 2013

The Internet today provides the environment for novel applications and processes which may evolve way beyond pre-planned scope and purpose. Security analysis is growing in complexity with the increase in functionality, connectivity, and dynamics of current electronic business processes. Technical processes within critical infrastructures also have to cope with these developments. To tackle the complexity of the security analysis, the application of models is becoming standard practice. However, model-based support for security analysis is not only needed in pre-operational phases but also during process execution, in order to provide situational security awareness at runtime.

This talk presents an approach called Predictive Security Analysis at Runtime (PSA@R) to support model-based evaluation of the security status of process instances. In particular, challenges with respect to the assessment whether instances of processes violate security policies or might violate them in the near future are addressed. The approach is based on operational formal models derived from process specifications and security compliance models derived from high-level security and safety goals. Events from process instances executed by the observed system are filtered for their relevance to the analysis and then mapped to the model of the originating process instance. PSA@R addresses *fault detection* and *fault prediction* by analysis of process specifications and compliance checks at runtime. The applicability of the approach is exemplified utilising processes from several industrial scenarios. Lessons learnt from the adaptation of the method to the scenarios are addressed. In particular, event model abstraction, process instance identification, semi-automatic model mining, and cross process instance reasoning is discussed. Furthermore, the need for a method to derive measurement requirements from security and dependability goals is motivated and a meta model aiming at an integrated security strategy management is presented. This meta model supports an integration of functionalities of all parts of the security monitoring and decision support process, namely: (i) detecting threatening events; (ii) putting them in context of the current system state; (iii) explaining their potential impact with respect to some security- or compliance model; and (iv) taking appropriate actions. This talk is based on [2, 4, 3, 1].

Acknowledgment. The presented work was developed in context of the project MASSIF (ID 257475) being co-funded by the European Commission within the Seventh Framework Programme and the project ACCEPT (ID 01BY1206D) being funded by the German Federal Ministry of Education and Research.

References

[1] Jörn Eichler and Roland Rieke. Model-based Situational Security Analysis. In *Proceedings of the 6th International Workshop on Models@run.time at the ACM/IEEE 14th International Conference on Model Driven Engineering Languages and Systems (MODELS 2011)*, volume 794 of *CEUR Workshop Proceedings*, pages 25–36. RWTH Aachen, 2011.

[2] Roland Rieke, Jürgen Repp, Maria Zhdanova, and Jörn Eichler. Monitoring security compliance of critical processes. In *Parallel, Distributed and Network-Based Processing (PDP), 2014 22th Euromicro International Conference on*. IEEE Computer Society, 2014.

[3] Roland Rieke, Julian Schütte, and Andrew Hutchison. Architecting a security strategy measurement and management system. In *Proceedings of the Workshop on Model-Driven Security*, MDsec '12, pages 2:1–2:6, New York, NY, USA, 2012. ACM.

[4] Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot, and Chrystel Gaber. Fraud detection in mobile payment utilizing process behavior analysis. In *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pages 662–669. IEEE Computer Society, 2013.