Prozesskonformitäts- und Sicherheits-Compliance-Tracking zur Erkennung von Missbrauch mobiler Geldtransferdienste

Roland Rieke

Fraunhofer-Institut für Sichere Informationstechnologie

Zusammenfassung

Die fortlaufende Überwachung von Transaktionen auf Geldwäscheverdacht ist Finanzinstituten in Deutschland und anderen Ländern vorgeschrieben. *Smurfing* ist eine Form der Geldwäsche, bei der durch den Transfer vieler kleiner Geldbeträge auf unterschiedlichen Wegen (mittels Strohmännern) ein hoher Geldbetrag unauffällig transferiert wird. In diesem Vortrag wird eine neue Methode - die *prädiktive Sicherheitsanalyse* - beschrieben, mit der man Smurfing in mobilen Geldtransferdiensten erkennen kann. Die Idee ist dabei, das Wissen über das erwartete Verhalten der Prozesse und die Sicherheitsvorgaben zu nutzen, um die Sicherheit von vernetzten kooperierenden Systemen zur Laufzeit vorausschauend zu bewerten. Dies ermöglicht eine Warnung vor möglichen Gefahren und eine der Situation angepasste, proaktive Reaktion. Die prädiktive Sicherheitsanalyse bietet dazu (a) *Prozesskonformitäts-Tracking*, (b) *Sicherheits-Compliance-Tracking* und (c) die *Prädiktion von sicherheitskritischen Zuständen*. Mittels Prozesskonformitäts-Tracking können zum Beispiel Abweichungen von der vorgegebenen Verhaltensspezifikation auf Anomalien untersucht werden, die einen möglichen Missbrauch des Finanzdienstes durch Geldwäscheaktivitäten anzeigen. Die vorgestellte Methode ist auch in anderen Industrieszenarien anwendbar. Dies wurde bereits an Beispielen aus den Bereichen Logistik, kritische Infrastrukturen und dem IT-Management der Olympischen Spiele demonstriert.

CV

Dr. rer. nat. Roland Rieke works since 1982 as a senior researcher at the Fraunhofer Institute for Secure Information Technology SIT. He was deputy head of the department “Trust and Compliance” from 2007-2014. Roland obtained his PhD from Philipps-University Marburg in 2014. His thesis *Security Analysis of System Behaviour - From ’Security by Design’ to ’Security at Runtime’* was awarded the GFFT prize *Best Dissertation 2015*. His research interests are focused on the development of methods and tools for formal security models and application of these techniques for architecting secure and dependable systems. In the project EVITA (E-safety Vehicle Intrusion proTected Applications), for instance, he worked on a method for security requirements elicitation in systems of systems applied in the context of vehicular communication systems. In the project ADiWa he worked on predictive security analysis for event-driven processes in the context of the Internet of things. His recent papers furthermore comprise work on attack graph analysis and on construction principles for dependable and secure scalable systems. Roland was the research director of the project MASSIF (MAnagement of Security information and events in Service InFrastructures), a large-scale integrating project co-funded

by the European Commission 2010-2013. In the project ACCEPT, he worked on anomaly management by complex event processing technology. He was member of the strategy board of the Effects+ (European Framework for Future Internet Compliance, Trust, Security and Privacy through effective clustering) project and is member of the ERCIM working group on Security and Trust Management.

Kontakt

Dr. Roland Rieke
Fraunhofer-Institut für Sichere Informationstechnologie
Rheinstrasse 75
64295 Darmstadt, Germany
Phone +49 6151 869-284
eMail: roland.rieke@sit.fraunhofer.de
Home: http://rieke.link/

Literatur

[1] Prieto, E., Diaz, R., Romano, L., Rieke, R., Achemlal, M.: MASSIF: A Promising Solution to Enhance Olympic Games IT Security. In: International Conference on Global Security, Safety and Sustainability (ICGS3 2011) (2011)

[2] Rieke, R., Coppolino, L., Hutchison, A., Prieto, E., Gaber, C.: Security and reliability requirements for advanced security event management. In: Kotenko, I., Skormin, V. (eds.) Computer Network Security, Lecture Notes in Computer Science, vol. 7531, pp. 171–180. Springer (2012)

[3] Rieke, R., Repp, J., Zhdanova, M., Eichler, J.: Monitoring security compliance of critical processes. In: Parallel, Distributed and Network-Based Processing (PDP), 2014 22th Euromicro International Conference on. pp. 525–560. IEEE Computer Society (Feb 2014)

[4] Rieke, R., Schütte, J., Hutchison, A.: Architecting a security strategy measurement and management system. In: Proceedings of the Workshop on Model-Driven Security. pp. 2:1–2:6. MDsec '12, ACM, New York, NY, USA (2012)

[5] Rieke, R., Stoynova, Z.: Predictive security analysis for event-driven processes. In: Computer Network Security, LNCS, vol. 6258, pp. 321–328. Springer (2010)

[6] Rieke, R., Zhdanova, M., Repp, J., Giot, R., Gaber, C.: Fraud detection in mobile payment utilizing process behavior analysis. In: Availability, Reliability and Security (ARES), 2013 Eighth International Conference on. pp. 662–669. IEEE Computer Society (2013)

[7] Rieke, R., Zhdanova, M., Repp, J., Giot, R., Gaber, C.: Verhaltensanalyse zur Erkennung von Missbrauch mobiler Geldtransferdienste. In: GI Sicherheit 2014, Lecture Notes in Informatics (LNI) – Proceedings, vol. P-228, pp. 271–282. GI (2014)

[8] Zhdanova, M., Repp, J., Rieke, R., Gaber, C., Hemery, B.: No smurfs: Revealing fraud chains in mobile money transfers. In: Proceedings of 2014 International Conference on Availability, Reliability and Security, ARES 2014, pp. 11–20. IEEE Computer Society (2014)