Identification of Security Requirements for Vehicular Communication Systems

Roland Rieke

Fraunhofer Institute for Secure Information Technology SIT

Abstract

In vehicular communication systems vehicles and roadside units communicate in ad hoc manner to exchange information such as safety warnings and traffic information. As a cooperative approach, vehicular communication systems can be more effective in avoiding accidents and traffic congestion than current technologies where each vehicle tries to solve these problems individually. However, introducing dependence of possibly safety-critical decisions in a vehicle on information from other systems, such as other vehicles or roadside units, raises severe concerns to security issues. Security is an enabling technology in this emerging field because without security some applications within those cooperating systems would not be possible at all.

This talk addresses the security requirements elicitation step in the security engineering process for such vehicular communication systems. The method comprises the tracing down of functional dependencies over system component boundaries right onto the origin of information as a functional flow graph. Based on this graph, we systematically deduce comprehensive sets of formally defined authenticity requirements for the given security and dependability objectives. The proposed method thereby avoids premature assumptions on the security architecture's structure as well as the means by which it is realised.

CV

Roland Rieke works since 1982 as a senior researcher at the Fraunhofer Institute for Secure Information Technology SIT. 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. He is currently working on predictive security analysis for event-driven processes in the context of the Internet of things within the project ADiWa (Alliance Digital Product Flow). His recent papers furthermore comprise work on attack graph analysis and on proving security and dependability properties in parameterised systems based on self-similarity. Roland will be 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 starting in October 2010. He is member of the ERCIM working group on Security and Trust Management.

Contact

Roland Rieke
Security Modeling and Model Validation
Fraunhofer Institute for Secure Information Technology
Rheinstrasse 75
64295 Darmstadt, Germany
Phone +49 6151 869-284
eMail: roland.rieke@sit.fraunhofer.de

Literatur

[1] Andreas Fuchs and Roland Rieke. Identification of Authenticity Requirements in Systems of Systems by Functional Security Analysis. In *Workshop on Architecting Dependable Systems (WADS 2009), in Proceedings of the 2009 IEEE/IFIP Conference on Dependable Systems and Networks, Supplementary Volume*, 2009. http://sit.sit.fraunhofer.de/smv/publications/.

[2] Andreas Fuchs and Roland Rieke. Identification of Security Requirements in Systems of Systems by Functional Security Analysis. In C. Gacek A. Casimiro, R. de Lemos, editor, *Architecting Dependable Systems 7*. Springer, to appear.

[3] Alastair Ruddle, David Ward, Benjamin Weyl, Sabir Idrees, Yves Roudier, Michael Friedewald, Timo Leimbach, Andreas Fuchs, Sigrid Gürgens, Olaf Henniger, Roland Rieke, Matthias Ritscher, Henrik Broberg, Ludovic Apvrille, Renaud Pacalet, and Gabriel Pedroza. Security requirements for automotive on-board networks based on dark-side scenarios. EVITA Deliverable D2.3, EVITA project, 2009. http://evita-project.org/deliverables.html.