Towards a Formalization of the Model by Jonsson and Olovsson

Billy Naumann and Matthias Werner, Technische Universität Chemnitz

There is a consensus among many researchers that the research areas of the dependability/safety research community and the one of the security research community overlap or are even basically the same (c.f. e.g., Avižienis et al. [1]). Two elements of the classic CIA-triad (confidentiality, integrity, and availability) can also be found as unique dependability attributes (but with slightly different definitions.) However, and even most researchers complain about this, both communities are split and use different terms, approaches, and models.

There exist numerous approaches to find a joint understanding and to integrate security and dependability. One that is in our opinion quite interesting is the approach by Jonsson and Olovsson [2]. In this publication, we propose a formalization of their approach on the base of automata.

We focus on the behavioral interaction of the system with its environment. Jonsson and Olovsson's concept of users, who intend to use the service as specified, non-users, who are not authorized and may attack the system, and the environment, which may induce faults into the system, is represented by constraints to the input of the automata. The traces of the automata represent the behavior of the system. We discuss interpretations of the properties reliability, availability, and confidentiality, as well as the concept of weakness/fault under our model.

[1] Avižienis, A., Laprie, J. C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. IEEE transactions on dependable and secure computing, 1(1), 11-33. https://doi.org/10.1109/TDSC.2004.2

[2] Jonsson, E., & Olovsson, T. (1992). On the integration of security and dependability in computer systems. In IASTED International Conference on Reliability, Quality Control and Risk Assessment Washington DC, USA, 1992, ISBN 0-88986-171-4 (pp. 93-97).