Sound Development of Secure Service-based Systems[*]

Martin Deubler Johannes Grünbauer[†] Jan Jürjens Guido Wimmel

Technische Universität München
Institut für Informatik
Boltzmannstrasse 3
85748 Garching, Germany

`http://www4.in.tum.de/˜(deubler|gruenbau|juerjens|wimmel)`

ABSTRACT

Service-based software systems are a useful concept recently developed to support the development of systems offering functions (the so-called *services*) which may be interrelated or may mutually depend on each other. Although appealing from a practical point of view, the development of service-based software for security-critical systems is, unfortunately, not well understood. Services may easily interact with each other in a way which may have unforeseen consequences on the various security properties provided. In this work, we propose a method for facilitating the development of security-critical service-based software systems using the computer-aided systems engineering tool AutoFocus based on the formal method Focus. We explain our method at the example of a service-based system from the automotive domain.