

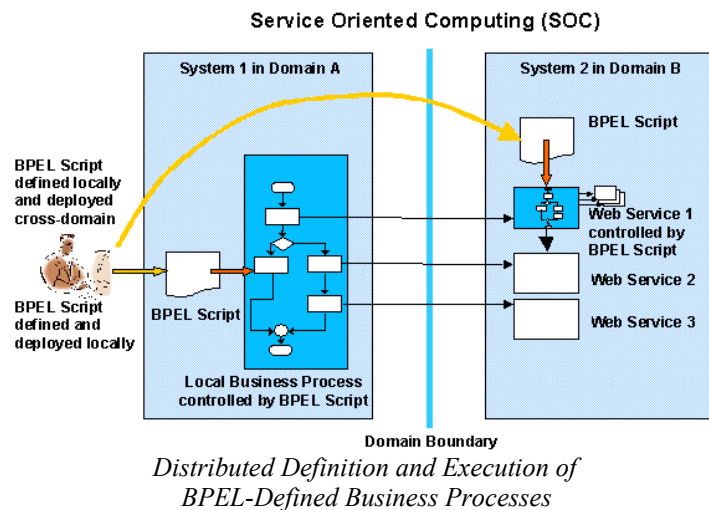
# Security Policy Enforcement for Collaborative Business Processes in Service Oriented Architecture

Dr. Klaus-Peter Fischer-Hellmann

Digamma Communications Consulting GmbH

Business processes involving several partners in different organisations impose demanding requirements on procedures for specification, execution, and maintenance in particular with respect to cross-organisational coordination. Web services provide the basis for service-oriented architecture (SOA) on which so-called collaborative business processes (CBPs) may be defined for the purpose of cross-organisational cooperation. Web Services Business Process Execution Language (WS-BPEL, usually abbreviated BPEL) has evolved to become the de facto standard for business process definition.

The fact that a broadly accepted standard is available principally allows to specify business processes in a platform-independent manner. In particular, using a platform-independent approach makes it possible to specify a business process at one location and have it executed at other locations (spread across domains possibly residing in different organisations; see figure beside). Though technically feasible, this approach has significant security implications, particularly on the side supposed to execute such a remotely defined business process (domain B in figure beside).



Novel methods developed to cope with security issues arising when business processes are specified and executed in such a distributed manner will be presented. Among others, a new approach has been devised for specifying security policies of a domain such that the assessment of business processes for compliance with these policies is greatly facilitated. An analysis of the security-relevant semantics of BPEL as a specification language conducted in this context came up with the identification of so-called security-relevant semantic patterns of business processes and Web services invoked. Based on these results, methods to specify security policy-implied restrictions in terms of such semantic patterns and to assess the compliance of BPEL scripts with these policies have been developed. The required checks (mainly involving information flow analysis) to assess compliance of a BPEL-defined business process with security policies specified in terms of such semantic patterns have been identified. This approach is particularly suited for assessment of remotely defined BPEL scripts since it allows for pre-execution enforcement of local security policies. Therefore, BPEL scripts violating restrictions imposed by security policies can be identified beforehand and do not have to be executed in order to detect their non-compliance. Hence, the approach presented helps to mitigate to a great extent or even to remove security implications involved in distributed definition and execution of business processes.

Once developed, the methods have proven to be comparatively easy to apply as they are based on common technologies in the field of Web service definition and business process specification (BPEL, WSDL, XML). The feasibility of automatic compliance assessment based on these methods has been shown by a prototypic implementation of the essential functionality required for such a compliance assessment procedure.