
Meiko Jensen
Horst Görtz Institute for IT-Security, Ruhr University Bochum
Meiko.Jensen@ruhr-uni-bochum.de

Abstract: When SOA-based business processes are to be enhanced with security properties, the model-driven business process development approach enables an easier and more reliable security definition compared to manually crafting the security realizations afterwards. In this paper, we outline an appropriate security model definition and transformation approach, targeting the WS-SecurityPolicy and WS-BPEL specifications, in order to enable a Web-Service-based secure business process development.

A crucial part of SOA-based business process design is the ability to define security properties for the service invocations. Thus, a business process modeling tool must provide appropriate models and capabilities to specify these properties on a semantical level in order to automatically create technical realizations at the implementation layer.

In this paper, we outline a model-driven approach for adding security properties to a business process model. The approach consists of a security model definition, an appropriate model transformation, and a model-specific technical realization based on the Web Services technology (i.e. WS-BPEL and WS-SecurityPolicy).

The Security Model Approach

When it comes to the issue of specifying security properties on a process level, the conjunction of the WS-BPEL and WS-SecurityPolicy specifications is lacking completeness. Though both specifications rely on the Web Service description (WSDL), there is no possibility for specifying security properties at the process level, e.g. end-to-end encryption of particular data items within the complete business process execution. Thus, it is necessary to investigate the requirements of enabling security policy assertions to directly annotate the process document without intermediating the WSDL. This can be addressed by using the model-driven approach. The idea is to create a separate security model view for the process model, which directly annotates the communication parts of the underlying process model. Thus, the process model can be defined by a business-semantics-aware process developer, and can then be annotated with appropriate security properties by a separate security architect (cmp. Figure 1). Then, both the process model and the security model can be transformed into appropriate process and security descriptions (based on WS-BPEL and WS-SecurityPolicy), which are related in that the security description directly annotates the process description. Once these descriptions are deployed to an appropriate Web Ser-
vice execution engine, the resulting business process is ready to run, with the appropriate security properties enabled (see also [JF09]).

Future Work

A major part of the presented approach consists in specifying appropriate transformations of security model properties to WS-SecurityPolicy equivalents. Thus, for every security property considered in the security model (which by now are confidentiality, data integrity, and user authentication) it is necessary to specify an appropriate WS-SecurityPolicy fragment that properly reflects the particular security aspect. Then, these fragments must be completed with some more details (algorithms to use, data items to consider, Web Services involved etc.), and the results must be joined into WS-SecurityPolicy documents for each Web Service endpoint of the workflow.

References