Security-Relevant Semantic Patterns of BPEL in Cross-Organisational Business Processes

K.P.Fischer[1,3], U.Bleimann[1], W.Fuhrmann[1], S.M.Furnell[2,4]

[1] Aida Institute of Applied Informatics, University of Applied Sciences Darmstadt, Germany
[2] Network Research Group, University of Plymouth, Plymouth, United Kingdom
[3] Digamma Communications Consulting GmbH, Darmstadt, Germany
[4] School of Computer and Information Science, Edith Cowan University, Perth, Australia
e-mail: K.P.Fischer@digamma.de

Abstract

This paper presents results of the analysis of security-relevant semantics of business processes being defined by WS-BPEL (Web Services Business Process Execution Language, BPEL for short) scripts. In particular, security issues arising when such scripts defining cross-organisational business processes on top of Web services are deployed across security domain boundaries, give rise to this investigation. The analysis of security-relevant semantics of this scripting language will help to overcome these security issues making further exploitation of BPEL as a standard for defining cross-organisational business processes more acceptable. Semantic patterns being combinations of particular language features and Web services with specific access restrictions implied by security policies are defined and analysed for this purpose. Applications of the results of this analysis to distributed definition and execution of BPEL-defined business processes may be found in a previous paper of the authors.

Keywords

Cross-Organisational Business Process (CBP), Web Services Business Process Execution Language (WS-BPEL, BPEL), Semantic Analysis, Security Policy, Web Services, Service Oriented Computing

1. Introduction

Web services, and the composition or orchestration of them, play a central role in current approaches to service-oriented computing (Berardi *et al.,* 2003). Service orientation also plays an important role in Grid Computing, where the provisioning of computing resources within a huge network of collaborating computers and devices can be fostered by services (so-called Grid Services in this context) (Tuecke *et al.,* 2003). In service-oriented approaches, Web services are used for composing new services from existing services or for defining and executing processes based on existing services.

The request for fast adaptation of enhanced services and business processes to changing requirements as well as for platform-independent definition of business processes leads to the specification of standardized business process definition languages (BPDLs). While the Web Services Description Language (WSDL) (Christensen *et al.,* 2001) propagated by the World Wide Web Consortium (W3C) has been broadly accepted as a single standard for the definition of Web services, several competing approaches to standardization of BPDLs have been taken by several vendor groups and standardization organisations. However, research comparing different BPDLs has shown that these languages are comparable with respect to their semantic expressiveness (Aalst *et al.,* 2002; Shapiro, 2002, Wohed *et al.,* 2002) and are convertible to

each other (Fischer and Wenzel, 2004). Given the fundamental similarity of the different BPDLs, without loss of generality we will concentrate our research on one particular representative, namely Web Services Business Process Execution Language (WS-BPEL) (Arkin *et al.*, 2004). One reason for choosing this representative, as propagated by the Organization for the Advancement of Structured Information Standards (OASIS), is that in addition to being supported by prominent vendors like IBM, BEA, Microsoft, SAP, and Siebel, WS-BPEL is expected to emerge as the dominant standard for business process definition (Wang *et al.*, 2004). For the remainder of this paper, we will use BPEL as a short-hand for WS-BPEL.

By its nature of being a standardized platform-independent scripting language, BPEL could be used for distributed definition and execution of cross-organisational business processes (CBPs) (Lippe *et al.*, 2005). Though technically feasible, the security issues involved impede this approach from being turned into practical application. In particular, the uncertainty about the semantics of remotely defined BPEL scripts, particularly with respect to their compatibility with local security policies, gets in the way of executing them at a foreign location. Being able to assess (in an easy and preferably automatic way) that the semantics of such scripts comply to local security policies, could foster the further exploitation of standardized BPDLs by allowing remotely defined scripts being executed without jeopardizing security requirements.

In this paper we investigate semantic patterns in order to analyse the security-relevant semantics of BPEL in a generic way. Security-relevant semantics in this context considers the functional behaviour of business processes that may be expressed by the different language elements of BPEL with respect to potential security issues involved. Based on the results of this analysis, a checklist assembling semantic patterns of BPEL identified herein as being security-critical can be established as has already been set out by Fischer *et al.* (2005). Using such a checklist, local security policies can be expressed in terms of allowed and disallowed semantic patterns in remotely defined BPEL scripts. By searching scripts for particular allowed and disallowed semantic patterns, such scripts may be assessed for compatibility to local security policies prior to executing them (Fischer *et al.*, 2005). By applying the approach described in the aforementioned paper combined with the results in this paper, the distributed definition and execution of BPEL script-defined business processes could become more acceptable for adoption in practical business-to-business applications, such as supply chain management.

2. Remote Definition of Cross-Organisational Business Processes

With the advent of Web services and business processes being specified in a standardized and platform-independent manner, BPDLs were considered an instrument for the definition of cross-organisational business processes (CBPs) (Lippe *et al.*, 2005), thereby supporting the concept of virtual enterprises (Coetzee and Eloff, 2003). An aspect of CBPs that has not yet been addressed explicitly in research is the distributed definition of a business process at one site and the deployment and execution of this process at another site (*e.g.*, being located in different organisations).

Figure 1 illustrates an exemplary scenario for distributed definition and execution of a BPEL script in two different domains, A and B. The two domains are considered to belong to two different organisations. Each of the systems depicted in Figure 1 is capable of running BPEL-defined processes. Since a business process defined by a BPEL script offers services to its environment, it can itself be considered a Web service. Therefore, in this example one of the Web

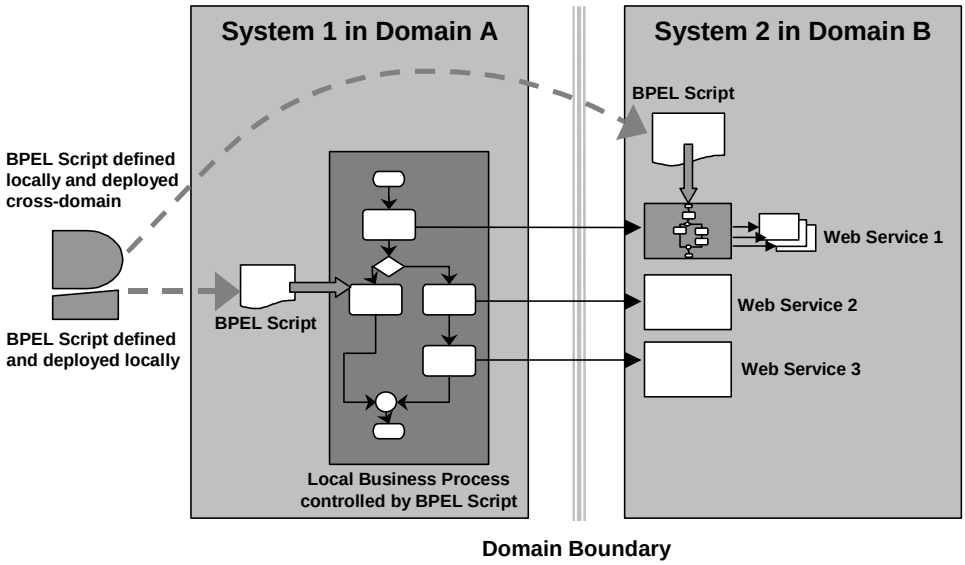

Figure 1: Distributed Definition and Execution of Business Processes using BPEL

services used by the business process in system 1 is realized as a business process controlled by a BPEL script. For this scenario it is assumed, that this BPEL script is defined in domain A and deployed across the domain boundary for execution in system 2 of domain B. Given both systems are based on a BPEL-enabled platform, this scenario would be technically feasible. However, security issues involved in this cross-domain approach of defining and running a business process may prevent this scenario from being applied in a real-world cross-organisational environment.

2.1 Security Issues of Remotely-Defined Cross-Organisational Business Processes

Since security already is an important issue in distributed applications in general, this topic is also of significant importance for CBPs and, in particular, for the application of BPDLs. Security of Web services is well studied and several approaches for access control to Web services exist (*e.g.*, Abendroth and Jensen, 2003; Dimmock *et al.*, 2004). Role-based access control (RBAC) (Ferraiolo *et al.*, 2001; Peng and Chen, 2004) is the widely used concept for dealing with security aspects in this field. However, novel security aspects not covered in the aforementioned approaches arise from the distributed definition and execution of CBPs. The following questions have to be answered in this context:

- Are the semantics of a remotely defined business process compatible with the security policy effective at the node where it is to be executed?
- Which classification, with respect to access control, is required for the Web service offered by the remotely defined business process in order to be compliant with the security policy in the domain where it will be executed?

While the second question again arises in the context of access control, albeit from a different point of view than the aspect addressed by usual access control approaches, the first question addresses a new view of access control and beyond, that had not needed to be considered in the context of Web services as it is not relevant with their basic incarnation. Since obeying the restrictions implied by security policies is always important when developing distributed applications, this aspect is not considered an issue particularly associated with business processes,

when developing them locally. However, this aspect will gain predominant importance that is particular to business processes, when remotely defined script-based business processes are to be executed.

Security aspects in Web services concern questions like: What kind of privileges are required for invoking a particular Web service? In the cross-organisational deployment scenario of Figure 1, the view to security is taken from an opposite direction, aiming at questions like: What functionality is allowed to be provided by a remotely defined business process with respect to the security policy effective in the domain of execution? The answer to this question may in most cases depend on the intended use of the Web service provided by this business process. To keep it simple, without loss of generality we assume, that:

a) the domain where the BPEL script is specified and from where it is sent cross-domain to the system where it will be executed, is identical with the domain invoking the new Web service provided by the business process, for instance domain A in the scenario of Figure 1;
b) with respect to access control and potential other security aspects relevant in the relation between both domains, all potential external invokers of this new Web service (*i.e.*, invokers residing outside the domain running it, *e.g.*, invokers in domain A) are provided the same set of privileges.

Given these preconditions, the answer to the above question concerning the allowable functionality of the business process is related to the set of privileges owned by the invokers of it as a Web service. In terms of RBAC (Ferraiolo *et al.*, 2001), due to precondition b) all external invokers are associated with the same role. Hence, the answer is related to this role, this means in the above scenario, it depends on the role associated with invokers in domain A with respect to domain B. At this point, it becomes obvious that both security issues identified above are closely related. They may be considered to be complementary to each other, since the first issue is taking the view from inside to outside, while the second one is taking the view from outside to inside.

In this paper, the inside-out view of the first issue will be considered. For this purpose, the results of a detailed analysis of the security-relevant semantics of BPEL that need special attention in the security assessment of business processes are presented.

2.2 Related Work

While access control related aspects are predominant with Web services, they are, of course, also an issue with BPDLs. In related work, Koshutanski and Massacci (2003) address access control issues of business processes defined by BPEL scripts, in particular the problem of providing the required evidence of possessing the proper access privileges at the right time to the right place during execution of a business process.

Peng and Chen (2004) propose an extension to conventional RBAC models called WS-RBAC, in order to incorporate Web services and business processes on top of them. In their approach, Web services are subject to access control in place of common system resources in conventional approaches. Business processes and enterprises are elements in their WS-RBAC model making it suitable for application to CBPs.

In other related work, Mendling *et al.* (2004) investigate access control requirements of BPEL script-defined business processes. By extracting RBAC models from BPEL scripts, and converting BPEL language constructs in a format suitable for a particular RBAC software component, they provide an automated link of access control enforcement into business processes defined by the BPEL scripts.

Though the papers mentioned in this section do not specifically address distributed definition and execution of BPEL scripts, their approaches also are applicable to the second security aspect arising in this context as listed in section 2.1. However, none of the related work deals with the first security aspect in the list above, being the concern of the results presented herein as well as of the approaches introduced in a previous paper of the authors (Fischer *et al.* 2005).

3. Analysis of Security-Relevant Semantic Patterns of BPEL

While a detailed description of BPEL can be found in its specification (Arkin *et al.,* 2004), a comprehensive analysis of its semantics was conducted by Wohed *et al.* (2002) based on a previous version of the BPEL specification. An overview of the language and a comprehensive example is given by Leymann and Roller (2004). The nature of BPEL accommodates the analysis of security-relevant semantics by offering only little or no means for defining data processing or computational tasks as part of the language itself. For these purposes, BPEL scripts have to invoke Web services, or must import constructs from other XML standards such as XPath (Berglund *et al.,* 2005). In addition, security aspects such as authentication, provision of secure communication channels, and non-repudiation are not considered in this context, since the language does not provide any means related to these security aspects. These aspects usually are catered for by the platform running BPEL scripts. Thus, the analysis can be concentrated on the business or workflow logic, that may be expressed in BPEL, in order to identify security-relevant semantics.

3.1 Adjusting the Scope of Analysis

For the sake of general applicability, we aim at analysing security relevance independent from the application contexts of particular BPEL script-defined business processes. Therefore, we relate language constructs with typical restrictions implied by security policies. Analysing security relevance in this way entails the opportunity that, once the security-relevant features of BPEL are identified, no thorough analysis of each and every particular aspect of the semantics will be required during the assessment of BPEL scripts for compliance to security policies. Instead, a direct search independent from application contexts looking only for the features identified to be capable of violating the security policy will be sufficient for this purpose.

To allow as much functionality as possible in a business process within the limits imposed by security policies, it is anticipated that the restrictions derived from such policies shall be as weak as possible, but at the same time as strict as required to avoid any violation of security policies. Since the strategy aims at avoidance of compromising security policies, following Dobson (1994) access control and information flow control are the mechanisms of choice. Access control to the Web service offered by a business process under consideration is the concern of a complementary security issue not addressed in this paper as stated above. Hence, the analysis addressed herein aims at examining whether information or resources accessed and the flow of information from inside to outside the domain and vice versa are consistent with the limitations of the security policy.

Possible violations of the policy are:

- making information or use of resources available outside the domain beyond the restrictions imposed by the policy (*e.g.*, reading restricted information from a database and sending it to an external partner);
- bringing information from outside into an internal data storage that is not allowed to be written to from external sources; and
- using functionality or resources that are not allowed to be used (*e.g.*, altering data in a data base or exercising a system control function).

In BPEL, two types of processes may be modelled: executable and abstract processes. Since abstract processes are not executable by their definition, they are not in the scope of our analysis. Executable processes specify workflow logic in terms of activities. The activities expressing the semantics of a business process may be either primitive or structured. The prevalent semantics expressed in BPEL is the exchange of messages with one or several external partners, that can be thought of as invoking Web services provided by partners or being invoked as a Web service by partners. In a definition part, BPEL scripts define the potential links to external partners by references to WSDL definitions of the Web services involved. Thus, analysing these definitions in a first step yields the set of Web services that may be invoked or are offered by a business process under consideration.

3.2 Classification of Web Service Access Restrictions

Since the language constructs are not security-relevant as such, they have to be examined in the context of access to information or resources. Hence, the language constructs will be investigated in conjunction with different types of Web services because in BPEL scripts access to information or resources may only be gained via Web services. Given a particular set of restrictions implied by a security policy, that is associated to a particular set of privileges (*i.e.*, a particular role), Web services may be distinguished with respect to access allowance or restrictions to their input and output parameters. In Table 1, six different cases are defined.

Invoking Web services belonging to the cases of Table 1 in combination with the activities defined in BPEL will be investigated as semantic patterns to determine their relevance with respect to security policies, in particular access control and information flow control. Of course, a particular Web service may belong to more than one of the cases 3 through 6 simultaneously. For the ease of discussion, we analyse no combined cases, since for a Web service belonging to more than one of these cases, the results related to each of the cases it belongs to may be applied simultaneously in this situation.

As can be easily seen, Web services with unrestricted access permission (case 1) as well as Web services with total access restriction (case 2) do not pose any particular challenge for analysis. In these cases, any further distinction between combinations with different features of BPEL is not relevant. The reason for this is that their allowed or forbidden use in a BPEL script may already be detected by examining the definition part. No Web service with total access restriction (case 2) must occur in the definition part, or at least, if such a Web service should occur in the definition part, it must not be used in any communication performed in the business process. Conversely, Web services with unrestricted access permission (case 1) may be invoked freely throughout a business process, irrespective of particular combinations with BPEL

Cases	Description
1	WS with unrestricted access to all parts of resources or information offered
2	WS with completely restricted access, *i.e.*, Web services that are not allowed to be invoked
3	WS with restricted visibility of read values access: some information made accessible are not allowed to be carried outside domain B, *i.e.*, parameters returned by WS are only allowed to be used within domain B, but not in outbound messages to targets outside domain B
4	WS with restricted write access: some of the input parameters of the Web service are not allowed to be used at all
5	WS with restricted set of values allowed in write access: some of the input parameters of the WS may only be used with particular values, while others may be used without restrictions
6	WS with values in write access restricted to specific sources: for some of the input parameters of the WS only values from particular sources may be used, for instance, only values returned by a particular WS

Table 1: Classification of Access Restrictions to Web Services

activities. The only aspect relevant with Web services of case 1 is the information flow from and to parameters of such a Web service prior and succeeding its invocation, respectively. This has to be considered during information flow analysis from and to restricted parameters of Web services in cases 3 through 6.

The distinction between cases 3 through 6 requires detailed knowledge of the semantics of a Web service. Since such detailed knowledge of external Web services may not be available in domain B, in general, external Web services tend to fall into cases 1 or 2. Conversely, the semantics of internal Web services can be assumed to be well-known within domain B, such that the differentiation between cases 3 through 6 will be possible.

3.3 Analysis of Security-Relevant Semantic Patterns

The results of the analysis of semantic patterns involving Web services of cases 3 through 6 are depicted in Tables 2 and 3. While Table 2 presents the results for semantic patterns formed by combination with primitive activities, Table 3 indicates the results for structured activities.

Tables 2 and 3 each comprise five columns. The second column contains a short description of the semantics of the respective BPEL activity in the first column. In columns three through five, the implications for security assessment is indicated, when the respective BPEL activity is combined with a Web service of cases 3 through 6. Since the entries for the cases 5 and 6 only differ slightly, the indications for these cases are combined in the fifth column.

Entry "**–**" indicates, that the respective semantic pattern is not relevant in scope of access control and information flow. As shown in Tables 2 and 3, some activities require special attention with respect to information flow. As indicated by entry **IFA(v)**, analysis of information flow is required, if a Web service belonging to case 3 is used in one of the activities **`invoke`** (with respect to the inbound parameters, *i.e.*, the output parameters of the Web service invoked), **`receive`** or the **`on message`** part of **`pick`**. This is to determine whether visibility-restricted information returned by the Web service is kept inside the security domain and is not sent outside via one of the activities **`invoke`** (within an outbound parameter) or **`reply`**.

Primitive Activities		Case 3	Case 4	Cases 5/6
invoke	invocation of a Web service	**IFA(v)**	**w**	**IFA(w/s)**
receive	waiting for a message to arrive	**IFA(v)**	**–**	**–**
reply	sending a reply to a message received	**–**	**w**	**IFA(w/s)**
assign	assignment of values between two different locations	**(relevant in IFA only)**		
wait	waiting for a specified amount of time	**time(v)**	**–**	**–**
throw	indication of exceptions such as failures during execution	**except(v)**	**–**	**–**
empty	no operation	**–**	**–**	**–**
exit (*)	termination of a process instance	**exit(v)**	**–**	**–**

(*) Note: Construct **exit** was **terminate** in previous versions of BPEL
WS = Web service
IFA = information flow analysis, (v) with respect to visibility of values read from WS, (w) with respect to values written to WS, (s) with respect to sources of values written to WS

Table 2: Security Relevance of Semantic Patterns with Primitive Activities

For case 4, only **invoke** (with respect to the outbound parameters, *i.e.*, the input parameters of the Web service invoked) and **reply** need special attention to check that the restricted input parameters of the particular Web service will not be used at all (*i.e.*, written to as indicated by the entry **w**). Cases 5 and 6 are similar, since with **invoke** (with respect to the outbound parameters) and **reply** information flow analysis is required to determine whether the restricted use of values is obeyed. With case 5, information flow analysis related to the values written to restricted outbound parameters is required (indicated by entry **IFA(w)**), whereas with case 6, analysis is required with respect to the sources of such values (indicated by entry **IFA(s)**).

As indicated in Table 2, analysis of information flow has to embrace **assign** activities to observe the movement of information within the business process. If processing such as calculation or string manipulation is performed within a BPEL script using language constructs imported from, for instance, XPath (Berglund *et al.*, 2005), it has to be analysed that no restricted information is involved, or at least, that results from the processing is not used in a manner violating the security policies. Since allowing such kind of processing on restricted information could cause obfuscation of information flow, thereby complicating the analysis of information flow, as a matter of precaution such processing should be generally considered incompatible with security policy, independent of the further use of its results.

As special cases, use of visibility-restricted information gained from Web services of case 3 in the activities **wait** (with respect to duration), **throw** (with respect to exception thrown), **exit** (with respect to condition for termination), **switch** (with respect to definition of cases),

Structured Activities		Case 3	Case 4	Cases 5/6
sequence	definition of a fixed execution order	**–**	**–**	**–**
flow	parallel execution of activities	**–**	**–**	**–**
switch	branching between several alternate activities depending on conditions	**switch cond(v)**	**–**	**–**
while	iterative execution, *i.e.*, looping	**loop cond(v)**	**–**	**–**
pick	waiting simultaneously for several events to occur and proceeding with the first event that actually occurs (see note)	**IFA(v)**	**–**	**–**
		time(v)	**–**	**–**

Note: Typically, one of the events waited for is a timeout event, while the other events are messages to arrive
WS = Web service
IFA(v) = information flow analysis with respect to visibility of values read from WS

Table 3: Security Relevance of Semantic Patterns with Structured Activities

while (with respect to loop control), and **pick** (with respect to timeout interval) also turns out to be security-relevant as shown in Tables 2 and 3. The reason for this is, that defining any of the terms indicated in parenthesis dependent on visibility-restricted information could be exploited to circumvent restrictions implied by security policy. For instance, if the visibility-restricted information *I* is used to control the amount of loop cycles in a **while** activity, providing some externally observable behaviour such as sending a message to an external Web service from within the loop body could be used to circumvent the visibility restriction on *I*. In this way, an external observer would be able to count the numbers of such messages and to deduce the value of *I* from this observation. However, revealing *I* to an external observer would violate the security policy restricting this information from being disclosed outside the domain.

4. Conclusions and Further Work

In this paper we have presented results deduced from an analysis of security-relevant semantics of business processes defined by BPEL scripts. The security risks associated with particular constructs of BPEL in conjunction with various types of security policy-implied restrictions on the use of Web services, herein called semantic patterns, have been identified. The results of this analysis are of particular interest, when using BPEL scripts defined externally from the security domain where they are to be executed. Having determined the security-relevance of the different semantic patterns allows for specifying security policies in terms of such patterns. In a previous paper (Fischer *et al.,* 2005), we have described, how security assessment of cross-organisational business processes defined and executed in a distributed manner can be facilitated, once the security-relevant semantics of business processes have been identified in a generic way. It is anticipated that becoming able to cope with security issues arising from this way of applying standardized BPDLs such as BPEL will foster the acceptance of cross-organisational development of business processes. This may allow additional capabilities provided by these standards to be employed in practical applications.

Further work will be dedicated to formalising security policy-implied restrictions with respect to semantic patterns analysed in this paper. Such a formalism will be a precondition for making the process of security assessment of BPEL scripts machine-processable.

5. References

Aalst, W.M.P. v.d., Dumas, M., ter Hofsted, A.H.M., and Wohed, P. (2002) "Pattern Based Analysis of BPML (and WSCI)" *Technical report FIT-TR-2002-05*, Queensland University of Technology, May 2002, http://xml.coverpages.org/Aalst-BPML.pdf, last accessed 2005-11-22.

Abendroth, J. and Jensen, C.D. (2003) "Partial Outsourcing: A New Paradigm for Access Control" In *Proceedings of the 8th ACM Symposium on Access Control Models and Technologies, SACMAT'03*, pages 134–141, June 2003.

Arkin, A., Bloch, B., Curbera, F., Goland, Y., Kartha, N., Liu, C.K., Thatte, S., and Yendluri, P. (2004) "Web Services Business Process Execution Language Version 2.0", *OASIS*, December 2004, http://www.oasis-open.org/committees/download.php/10347/wsbpel-specification-draft-120204.htm, last accessed 2005-11-22.

Berardi, D., De Rosa, F., De Santis, L., and Mecella, M. (2003) "Finite State Automata as Conceptual Model for E-Services", In *Proceedings of the 7th World Conference on Integrated Design and Process Technology, IDPT-2003*, June 2003.

Berglund, A., Boag, S., Chamberlin, D., Fernández, M.F., Kay, M., Robie, J., and Siméon, J. (2005) "XML Path Language (XPath) 2.0", *World Wide Web Consortium*, November 2005, http://www.w3.org/TR/xpath20, last accessed 2005-11-22.

Christensen, E., Curbera, F., Meredith, G., and Weerawarana, S. (2001). "Web Services Description Language (WSDL) 1.1", *World Wide Web Consortium*, March 2001. http://www.w3.org/TR/2001/NOTE-wsdl-20010315, last accessed 2005-09-24.

Coetzee, M. and Eloff, J.H.P. (2003), "Virtual Enterprise Access Control Requirements", In *Proceedings of the 2003 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology*, pages 285–294, 2003.

Dimmock, N., Belokosztolszki, A., Eyers, D., Bacon, J., and Moody, K. (2004) "Using Trust and Risk in Role-Based Access Control Policies", In *Proceedings of the 9th ACM Symposium on Access Control Models and Technologies, SACMAT'04*, pages 156–162, June 2004.

Dobson, J. (1994), "Messages, Communications, Information Security and Value", In *Proceedings of the 1994 workshop on New security paradigms*, pages 10–19, August 1994.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, R., and Chandramouli, R. (2001). "Proposed NIST standard for role-based access control", *ACM Transactions on Information and System Security (TISSEC)* 4(3): 224–274, 2001.

Fischer, K.P., Bleimann, U., Fuhrmann, W., and Furnell, S. (2005), "A Security Infrastructure for Cross-Domain Deployment of Script-Based Business Processes in SOC Environments", In *Proceedings of the 5th International Network Conference, INC'2005*, pages 207–216, July 2005.

Fischer, O. and Wenzel, B. (2004) "Prozessorientierte Dienstleistungsunterstützung: Workflowbasierte Komposition unternehmensübergreifender Geschäftsprozesse", University of Hamburg, http://vsis-www.informatik.uni-hamburg.de/getDoc.php/thesis/177/DA-Wenzel-Fischer-final.pdf, last accessed 2005-11-22.

Koshutanski, H. and Massacci, F.(2003) "An Access Control Framework for Business Processes for Web Services", In *Proceedings of the 2003 ACM Workshop on XML Security*. pages 15–24, October 2003.

Leymann, F. and Roller, D. (2004), "Modelling Business Process with BPEL4WS", In *Proceedings of the 1st Workshop on XML Interchange Formats for Business Process Management (XML4BPM'2004)*, pages 7–24, March 2004.

Lippe, S., Greiner, U., and Barros A. (2005). "Survey on State of the Art to Facilitate Modelling of Cross-Organisational Business Processes", In *Proceedings of the 2nd Workshop on XML Interchange Formats for Business Process Management (XML4BPM'2005)*, pages 7–22, March 2005, http://wi.wu-wien.ac.at/~mendling/XML4 BPM2005/xml4bpm-2005-proceedings.pdf, last accessed 2005-09-23.

Mendling, J., Strembeck, M., Stermsek, G., and Neumann, G. (2004) "An Approach to Extract RBAC Models from BPEL4WS Processes", In *Proceedings of the Thirteenth IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises (WET ICE 2004)*, pages 81–86, June 2004.

Peng, L. and Chen, Z. (2004) "An Access Control Model for Web Services in Business Process", In *Proceedings of IEEE/WIC/ACM International Conference on Web Intelligence (WI'04)*, pages 292–298, September 2004.

Shapiro, R. (2002) "A Comparison of XPDL, BPML, and BPEL4WS". http://xml.coverpages.org/Shapiro-XPDL. pdf, last accessed 2005-11-22

Tuecke, S., Czajkowski, K., Foster, I., Frey, J., Graham, S., Kesselman, C., Maquire, T., Sandholm, T., Snelling, D., and Vanderbilt, P. (2003) "Open Grid Services Infrastructure (OGSI) Version 1.0", *Global Grid Forum*, June 2003, http://www.ggf.org/documents/GWD-R/GFD-R.015.pdf, last accessed: 2005-09-23.

Wang, H., Huang, J.Z., Qu, Y., and Xie, J. (2004). "Web services: Problems and Future Directions", *Journal of Web Semantics*, 1(3): 309-320, April 2004.

Wohed, P., van der Aalst, W., Dumas, M., and ter Hofstede, A. (2002). "Pattern-Based Analysis of BPEL4WS", *Technical report, FIT-TR-2002-04*, Queensland University of Technology, Brisbane, 2002, http://is.tm.tue.nl /research/patterns/download/qut_bpel_rep.pdf, last accessed 2005-11-22.