9 Conclusions and Directions of Further Research and Development

To conclude and wrap up, this chapter summarises the achievements and limitations of the approaches presented in this book. It also considers possible directions of further research and development based on these results.

9.1 Which Contributions Have Been Achieved?

The increasing need for business-to-business applications has led to the specification of collaborative business processes (CBPs) using standardised specification languages. The de facto standard for this purpose is WS-BPEL (BPEL for short) that has been adopted as an OASIS standard in April 2007. Making full use of the fact that BPEL is a standard for specifying business processes, particularly executable ones, and, therefore, allows for definition of processes in a platform-independent way motivates the approach to specify a CBP at one location and have the different parts constituting this CBP executed on BPEL-enabled platforms of the respective partners involved in the CBP. Though technically feasible because BPEL-defined business processes are executable on any such platform, security issues involved in the execution of remotely defined business processes stand in the way of turning this approach into practical application. To mitigate or even eliminate these security issues, methods have been developed and presented in this book that allow for assessing the compliance of remotely defined business processes with local security policies prior to their execution. This assessment should preferably be performed automatically with as little as possible human intervention. At the same time, the assessment should incorporate methods for as fine-grained as possible an information flow control to avoid disadvantages of pure RBAC-based approaches that imply overly strict information flow control in order to securely avoid information leaks. Being able to have a remotely defined business process assessed for compliance with local security policies in an automatic way should allow for execution of the business process without security concerns.

In order to find methods that support compliance assessment in the manner aimed for, the security-relevant behaviour expressible in BPEL scripts has been investigated. The results of this investigation have been presented in Chapter 4. Based on an analysis and classification of security policy-induced restrictions to Web service invocation, combinations of restriction classes with BPEL activities called security-relevant semantic patterns have been analysed for their potential impact related to compliance with security policies. The derivation of these semantic patterns is depicted in Figure 24. Types of checks required for verification as to whether a BPEL
script specifies behaviour that would violate security policies have also been indicated in Chapter 4.

Figure 24: Approach to Definition of Security-Relevant Semantic Patterns

Based on the identification of security-relevant semantics of BPEL, a method for specifying security policies in such a way that the assessment of compliance with these policies is essentially facilitated has been introduced in Chapter 5. To this purpose, so-called security policy statements (SPSs) are used that indicate security policy-induced restrictions to Web services that are allowed to be invoked by a remotely defined business process. An approach to possibly reduce the complexity of an SPS is also introduced in this chapter, as well as an approach to cope with dynamic aspects of security policy-induced restrictions that by their very nature may only be checked at runtime of the process defined by a script.

The procedure of compliance assessment resulting from and enabled by these preparations have been described in Chapter 6. How a BPEL script under consideration is examined in order to assess its compliance with security policies as indicated in an SPS was described there. The novel approach to security policy enforcement enabled by the methods and procedures introduced in this book is outlined in Figure 25. After transformation of the relevant security policies into the formal representation introduced in Chapter 5, the compliance assessment reduces to searching business processes under consideration for occurrences of security-relevant semantic patterns that represent the restrictions implied by these security policies. This approach differs considerably from the approaches of related work as discussed in Chapter 3 and classified in Section 3.6 by the following aspects: