Chapter 7

Conclusions

This chapter concludes the thesis by summarizing the findings and the contributions of this thesis and presents several directions for future research.

7.1. Summary of Works

The security requirements are the types and levels of protection necessary for equipment, data, information, applications and facilities to meet a security policy. A secure Web service is defined as a computer supported business process that satisfies the security requirements in a workflow environment. In this thesis, the following aspects of security issues in Web services are addressed.

Chapter 2 discusses on the overview of Web service and security. The chapter mainly reviews the security aspects of Web services. It is seen that the security concerns are similar to other web applications in general; however Web services have specific security issues as well. The specific security challenges are mainly due to the adoption of XML in different components of Web services. The present study includes recent threats and attacks specific to XML-based Web services.

Chapter 3 discusses on the limitations of Web services security during SOAP message transmission. The main focus of this chapter is to show the limitations of WSS on the SOAP message integrity and also to show how the issue can be addressed by a protocol. From the discussion of this chapter it is clear that it is not possible to address the integrity issue, as
claimed in the standard [30], [31] within the scope of message level. A central arbitration mechanism is mandatory. In case of orchestrated Web service based workflow, BPEL process can take the responsibility of this arbitration along with coordination of constituent Web services. However, in case of a complex workflow across many business entities, where multiple BPEL processes are to be co-ordinated, different protocol may have to be used in addition.

Chapter 4 discusses about the SWOT analysis of 2-tuple digital signature. In public-key based 2-tuple digital signature, the signature and the message content are loosely bound. In one hand this signature scheme is adventitious from efficiency point of view but on the other hand it invites vulnerability from security point of view. Present digital signature standard is not resilient to signature replacement attack. This chapter proposes a solution in the protocol level with a central arbiter as an in-line Trusted Third Party (TTP) mechanism. The central arbitration mechanism is mandatory to address such issues.

Chapter 5 presents the synchronization of authorization flow with a work object flow. The synchronization is shown in this chapter in architecture level and protocol level exploiting obligation mechanism available in XACML standard. The chapter shows that a central arbiter is needed to give the solution of synchronization of authorization flow with a work object flow. The discussion is limited to synchronization of orchestrated web services with XACML only.

Chapter 6 proposes a model called Extra-Tree for organising execution traces of Web services. The advantage of this model is to retrieve the execution traces of Web services from the coarse-grained level to the fine-grained level at different time intervals. This is the first non-linear hierarchical model to organize execution traces in Web services domain, hitherto not discussed in literature.

7.2. Summary of Contributions

The main contributions of this thesis include the development of some proposed solutions, architecture and protocols, model with algorithm in connection with different security issues.

It is found from the investigation that there are some more limitations of current WSS standard on SOAP messages. Current version of WSS standard fails to address these issues.
In WSS standard, XML signatures and XML encryption with inclusive and exclusive canonicalization ensure proof of origin, content integrity and confidentiality issues of each individual part, that is, each signed message, in a SOAP envelope during exchange and storage. But it fails to ensure the collective integrity issue of all the parts as a whole, which means all the signed messages in a SOAP envelope signed by the original sender and the intermediaries during the workflow. It also fails to address the part reuse issue. WSS standard fails to ensure end-to-end security in SOAP message level on these issues. However, a solution with a special protocol exists. The protocol is based on a central arbitration mechanism. It is basically a client/server computing paradigm, where the arbiter is the server. To address these issues an in-line Trusted Third Party (TTP), called an arbiter, is mandatory. The arbiter serves as the trusted intermediate agent in between the current reviewer and the next.

The weaknesses of 2-tuple digital signature scheme pave the way for signature replacement attack, which is not discussed in the literature. It seems that no solution is possible keeping the loose binding of the message and the signature. A counter-measure is to create a digital envelope encapsulating the signature and the message. But the use of digital envelope also fails to give the solution of this attack which is secured during transmission not in storage. However, a solution with a special protocol exists. This protocol is based on a central arbitration mechanism. All the messages flowing from the originator to the next receiver are routed through the arbiter. To address these issues an in-line Trusted Third Party (TTP), called an arbiter is mandatory. The arbiter serves as the trusted intermediate agent in between the originator and the receiver.

The solution of synchronization of authorization flow with a work object flow has shown in two levels – the architecture level and the protocol level. In the conceptual architecture level, a 3-tier architecture is proposed. In the protocol level, the merging of the protocol for work object flow and the protocol for authorization flow are discussed.

Finally, an Extra-Tree model is proposed to organize execution traces of Web services. In this chapter an algorithm is proposed to retrieve execution traces in different levels of granularities. The scope of this model is limited to orchestrated Web services only.
7.3. Future Research

In this thesis, the study and analysis of security issues in service-oriented computing are done particularly on authorization of Web services, integrity of Web services, 2-tuple digital signature replacement attack and the model for execution traces of Web services.

For the limitations of WSS a solution is proposed by using an in-line TTP. The future research study will be in the direction of choreographed workflow implementations. The implementation of the protocol in both orchestrated and choreographed workflows in Web service world is the direction of future research. For the signature replacement attack issue, a solution is proposed by the use a central arbiter mechanism. The future works include the detail study on signature replacement attack and its counter-measures in both orchestrated as well as choreographed Web services. The synchronization of authorization flow with a work object flow using XACML and BPEL is shown in architecture level and protocol level. The coding level synchronization of both XACML and BPEL is the future research work. The synchronization of choreographed Web services with XACML is also another interesting area to be explored, which remains to be the future research work. In the Extra-Tree model, the organization of execution traces of Web services in a central point rather than in a distributed way will probably give the more secured auditing system and make the proposed model robust which is a future endeavour.