Chapter 1

Introduction

This thesis contributes to the subject area of Web Services Security (WSS). It is mainly focused on the study and analysis of security techniques in Service Oriented Computing (SOC).

Today information is spread over many interconnected computers, termed as network. Internet is the world’s largest network which contains almost every kind of information. With the availability of on-line resources anyone can search for many fields of knowledge deeply and thoroughly. The use of cryptography and encryption techniques also helps to address security issues in the Internet. The encryption technique [1] is a mathematical process involving the use of formulas or algorithms to protect the confidentiality, integrity and authentication of the information. It is the process of taking a message and scrambling it so that only the intended party can read it.

Services are simply a means for building distributed applications specifically how these applications are built and how services should function together harmoniously. The applications will use services by composing or putting them together. An architecture for service-based applications has three main parts: a provider, a requester and a registry. Providers publish or announce their services on registries, where requesters find and then invoke them. Services provide higher-level abstractions for organising applications for large scale open environments. Thus, they help us to implement and configure software applications in a manner that improves productivity and application quality.
Service-Oriented Computing (SOC) [2] is the latest paradigm of computing. It provides a way to create a new distributed architecture that reflects a trend towards autonomy and heterogeneity of the components. Service Oriented Computing (SOC) [2] can be viewed in terms of several different cross-cutting levels of abstractions ranging from those that concerns services within an application to those that concern service application interacting across enterprises.

Security is a major concern of Web services because of the fact that current trends in performing B2B (business-to-business) and B2C (business-to-consumer) transactions have been extended to the Web services. Web services facilitate different business processes belonging to various organizations into one single application.

This thesis aims to study the standard security issues in Web services.

1.1 Motivation

The growing trend of software architecture is to build platform-independent software component called Web services [3] that are available in the distributed environment of the Internet.

In Service Oriented Computing (SOC) [4], developers use services as fundamental elements in their application development processes. Services are platform and network independent operations that clients or other services invoke. To operate in an SOC environment, services must define their properties in a standard machine readable format. SOC offers three native capabilities – description, discovery and communication. For example, developers implement SOC native capabilities using Web Service Description Language (WSDL) for description, Universal Description Discovery Integration (UDDI) for discovery and integration and Simple Object Access Protocol (SOAP) for communication. There are four types of communications defined involving a service operation – (i) The end point resume a message, (ii) End point sends a message, (iii) End point receives a message and sends a correlated message and (iv) It sends a message and receives a correlated message. SOAP is an eXtensible Markup Language (XML) based means of passing messages that is intended to be language independent.
There are different hurdles to overcome if we look at the interoperation aspects in any system. The first is the connectivity among the applications, which protocols, such as HTTP, can readily ensure. The second is the ability of the various components to understand each other. Various enterprise policies must readily authenticate and authorize the parties involved in different interactions. A new problem arises when we want to introduce new applications and configure them to interoperate systems likely to be developed on different platforms and perhaps running on different operating systems.

Services can be implemented on a single machine, distributed on a LAN or even across several company networks. In all instances, a service must first be found and then it can be accessed. To this aim, each Service Oriented Architecture (SOA) relies on to distinct infrastructures called service discovery and service delivery. In most of the case, security is only addressed from the service delivery point of view and in some other cases it covers the discovery phase too.

This thesis represents a detailed analysis of the security requirements in Service-Oriented Computing (SOC) [5] which are still missing in the current literature. The ultimate goal of the security solutions is to provide security services such as authentication, confidentiality, availability and integrity to Web services. In order to achieve these goals, the security solution should provide complete protection spanning the entire protocol stack [6].

### 1.2 Objectives

Security is an important aspect of an information system; so far acceptability in the society is concerned. The main objectives of this proposed work is as follows:

1) To study the general security issues of Service Oriented Computing.

2) To study the special security issues of Service Oriented Computing.

3) To investigate the limitations of various security solutions and propose its counter-measures.

4) To develop the security techniques in Service Oriented Computing in different environments.

5) To provide solutions on various security protocols for evaluating better performance.
1.3 Methodology

In this thesis, the security issues and techniques of Service Oriented Computing are studied. The following steps are included as research work in this thesis:

1) A review on the literature on Service Oriented Computing (SOC) in general and security in specific was first done.

2) A study on the security mechanisms in SOAP messages was done and found the limitations of SOAP messages in Web Services Security. A solution was proposed using an in-line Trusted Third Party (TTP) to overcome these limitations.

3) A SWOT analysis on 2-tuple digital signature was then studied along with the findings of signature replacement attack. A solution was proposed to overcome this attack using an arbiter as a central server.

4) A technique was applied to synchronize the authorization flow with a work object flow using XACML and BPEL. The synchronization was done in architecture level and protocol level.

5) Finally, a model named Extra-Tree to organize execution traces of Web services was proposed.

1.4 Contributions

In this thesis, some security techniques in Web services are developed. Major parts of the works done in Web services security are focused on access control models. There are many more issues which are yet to be focused properly but important. In this thesis some such issues are addressed. In particular, there are four main contributions. These are -

1) To propose a solution on SOAP message integrity where Web Service Security (WSS) standard fails to ensure end-to-end security on SOAP messages.

2) To identify signature replacement attack and give a counter-measure.

3) To give a solution on the synchronization of authorization flow with a work object flow which has solved in architecture level and in protocol level.
4) To propose a model which organises execution traces of Web services using tree in distributed environment.

1.5 Thesis Organization

The rest of the thesis is organised as follows -

Chapter 2: Literature Survey on Web Services Security. This chapter presents an overview of Service Oriented Computing and its technologies. This chapter also provides a study on the security issues in Web services, the threats that they are facing today and the possible attacks that might be aimed at Web services.

Chapter 3: A Solution of SOAP Message Integrity. This chapter discusses on the limitations of Web Service Security in providing end-to-end integrity of a SOAP message in a document production workflow environment. A solution in BPEL process level using a special protocol is proposed.

Chapter 4: A Solution on Signature Replacement Attack. This chapter presents a signature replacement attack which is brought into the focus for the first time. The chapter proposes a solution for digital signature, resilient to signature replacement attack where a trusted central arbiter is used as an in-line TTP. The chapter proposes a solution with a BPEL process which acts as a central arbiter in the proposed special protocol.

Chapter 5: Synchronization of Authorization Flow with a Work Object Flow. This chapter presents the issue of synchronization of authorization flow with work object flow in a document production workflow environment. This chapter shows how a work object flow is synchronized with the authorization flow using a central arbiter. The outcome of this chapter is an authorization decision which may be either permit, deny, indeterminate or error occurred during evaluation.

Chapter 6: Extra-Tree: A Model to Organize Execution Traces of Web Services. This chapter presents a non-linear model, called Extra-Tree, to organize execution traces of Web services. This proposed model provides us a secured logging system which records the history of all the suspicious or malicious activities from the initiation of the Web service to
the completion of the Web service. The main focus of this chapter is to organize execution traces of Web services in a distributed environment in the form of a tree.

Chapter 7: Conclusions. Finally, this chapter presents the conclusions. Summary of the works and contributions are outlined along with the discussion of future research work.