Abstract
Web Services based computing is currently an important driver for the software industry. While several standards bodies (such as W3C and OASIS) are laying the foundation for Web Services Security, several research problems must be solved to make secure Web Services a reality. This paper describes techniques for Web Services Security and some of the challenges for the future.

1. Introduction
The advance of Web services technologies promises to have far-reaching effects on the Internet and enterprise networks. Web services based on the eXtensible Markup Language (XML), Simple Object Access Protocol (SOAP), and related open standards, and deployed in Service Oriented Architectures (SOA) allow data and applications to interact without human intervention through dynamic and ad hoc connections. Web services technology can be implemented in a wide variety of architectures, can co-exist with other technologies and software design approaches, and can be adopted in an evolutionary manner without requiring major transformations to legacy applications and databases.

2. Web Services Security Stack
The open standards communities that created Web services developed a number of security standards for Web services. Figure 1 illustrates a notional reference model for Web services security standards. This reference model maps the different standards to the different functional layers of a typical Web service implementation. These layers are modeled after the OSI Reference Model but are not intended to be interpreted as strictly hierarchical.

3. Challenges
This section discusses some of the important challenges in the area of web services security.

a) Discovery
In Web services discovery, participants identify and compose Web Services Description Language (WSDL) specific services based on definitions in a UDDI registry. Due to the potentially large number of service candidates in the registry, performance rankings for algorithms used to search, match and compose services can vary from case to case.

b) End to End Quality of Service and Protection
Most Web services deployed do not provide guarantees for Quality of Service (QoS) or Quality of Protection (QoP). QoS is important in defining what the expected level of performance a particular Web service will have.

c) Availability and Protection from Denial of Service Attacks
Availability enables a Web Services Application to detect a Denial of Service (DOS) attack, to continue operation as long as possible and then to gracefully recover and resume operations after a DOS attack.