Service-oriented architecture (SOA) facilitates to dynamically organize a set of services to work seamlessly as a larger system for user applications. Compared to traditional centralized computing architecture, SOA provides more flexibility for system development because it improves systems’ interoperability and reusability. With well defined message-based interfaces, a particular service may serve multiple systems through requests/response message pairs. Because SOA usually involves intensive message communication among services distributed across various organizations, new security risks should be considered in SOA.

Authentication and authorization

The most attractive aspect of services is that they can be discovered and then integrated to any system that discovered it. However, from the security point of view, the discoverability of services makes services vulnerable to be attacked by malicious service consumers without appropriate authentication and authorization mechanisms to restrict their access to services.

Various authentication and authorization solutions for SOA have been developed, such as XACML to encode authentication and authorization information within XML messages, XKMS to specify XML key management, WS-Policies to provide basic structures and syntaces for policy specification, and XML encryption and signature to protect XML messages’ confidentiality and integrity. Basically, these solutions are motivated by the message-based interactions among services and try to adapt existing general authorization and authentication mechanisms for SOA by incorporating policies and credentials within XML messages and protecting these messages during transmission. We need to develop new mechanisms for SOA to address the following security challenges specifically for SOA:

First, more powerful authentication and authorization in SOA are needed. Current authentication and authorization in SOA rely on distributed identity management, which is difficult to be implemented in SOA because each service in SOA requires authentication and authorization, and these services may come from different administrative realms. Federal identity management, like single sign-on, has been proposed as a solution for authentication and authorization across various services, which allows users to be authenticated and authorized once, and then can access all federal services without duplicating authentication and authorization. However, a more sophisticated approach is needed to address the authentication and authorization across different federations because a common identity management authority trusted by all federations may not exist. Therefore, the federal approach across federations may require either an identity transformation approach to transferring identities among different federations and then the identity of a federation can be understood by other federations, or a proxy approach to convincing the federation that the service consumer is trusted because another federation has authenticated and authorized that consumer before.

Second, policy management is needed for authentication and authorization in SOA. Because SOA makes a group of services to work together, and the group services may have different security requirements, security mechanism implementations or security management, policy management for SOA is needed to
deal with policies written with different languages and policy contradictions among services. The SOA policy management should deal with these problems from the standpoint of the whole system instead of each service, and hence needs to rewrite polices using a unified language and syntax, and incorporate policy reconciliation mechanisms to resolve policy contradictions.

Service behavior enforcement
Besides authentication and authorization of SOA, service behavior enforcement also needs addressed. Most of the current research in service behavior enforcement is to focus on the protection of services from malicious service consumers, not on the protection of service consumers from malicious services. There are two major aspects:

First, the authentication and authorization between services and service consumers should be mutual. Before service consumers send their data to the connected services, they should authenticate the connected services to ensure that they are indeed the services intended, and have appropriate privileges to access their data.

Second, even the connected services are successfully authenticated and authorized, further protection mechanisms are required to either audit services’ behaviors, or make them impossible to reveal or damage customers’ data. These mechanisms have been widely discussed in privacy-preserving data mining and anonymous access to databases, but have not been studied in-depth in the SOA environment, where the design of such mechanism is more challenging due to the complex interactions among services.

Tradeoff between performance and security
Tradeoff between performance and security must be taken into account in SOA because security mechanisms usually have negative impact on performance and discourage developers to use them in SOA system development. Existing techniques cannot effectively support the analysis and adaptive control of the tradeoff between security and performance, or among other QoS, due to lack of comprehensive understanding of such tradeoff and its relations to service operations, and lack of effective metrics and their monitoring in general and SOA in particular.