Abstract

One of the most significant difficulties with developing Service-Oriented Architecture (SOA) involves meeting its security challenges. Access control is an important security mechanism for organizations to protect their resources in collaborative environments and processes. In these processes, shared resources are often used and there are complex relationships between activities and users, so the definition and administration of different security levels (tasks, users, resources, etc.) is necessary. Different access control models and mechanisms have been proposed in recent years. However, under the new collaborative paradigm based on Web services and workflow technologies, some specific access control requirements should be addressed to support the various processes. In this paper, an access control model is proposed that considers the necessary elements to represent authentication, authorization and access control aspects in SOA environment. One of the underlined issues in this model is Separation of Duty (SoD) policy, which is widely considered to be a fundamental security principle for prevention of fraud and errors in information security.
An Access Control Model for Web Services with Dynamic Separation of Duty Rules


Index Terms

Computer Science Security
Keywords
Web Service  Separation Of Duty  Access Control rule Definition  Authentication  Authorization