Research Statement

Li Yan
yan.li.2009@smu.edu.sg
School of Information Systems
Singapore Management University
Singapore

Information security aims at protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It is concerned with the confidentiality, integrity and availability of data. In traditional centralized systems, security is typically based on the authenticated identity of external parties and rigid local authorization policy. With the development of distributed systems, traditional authentication and authorization mechanisms fail to provide powerful and robust tools for handling security at the scale necessary. Then several technologies for securing interaction in distributed environment have been introduced into information systems.

My research strives to enhancing security in distributed environment by flexible authorization policy and access control mechanism. My focus is on enabling dynamic authorization and access control to local systems in the open distributed environment. Access control for multi-domains should especially be emphasized.

Current Research

Access Control Mechanism

Access controls usually apply after authentication has been established. It can take several forms. Discretionary access control (DAC) is based on the idea that the owner of data should determine who has access to it. Mandatory access control (MAC) confines the transfer of information to one direction in a lattice of security labels. Role-based access control (RBAC) requires that access rights be assigned to roles rather than to individual users.

With the development and boom of distributed system, the sensitive files and data protection become one of most difficult tasks for accesses from heterogeneous domains and organizations. Moreover, anonymity and many unknown or unfamiliar peers worsen security problems. Traditional access control mechanisms are not suitable to such distributed environment. However, there has been relatively little work done in controlling access to the collaboration. In addition, based on different policies defined by distinct domains, traditional access control mechanisms have trouble in precise negotiations of these policies.