# Information Security Issues and Challenges

**James B. D. Joshi**
*University of Pittsburgh, USA*

**Saubhagya R. Joshi**
*University of Pittsburgh, USA*

**Suroop M. Chandran**
*University of Pittsburgh, USA*

## INTRODUCTION

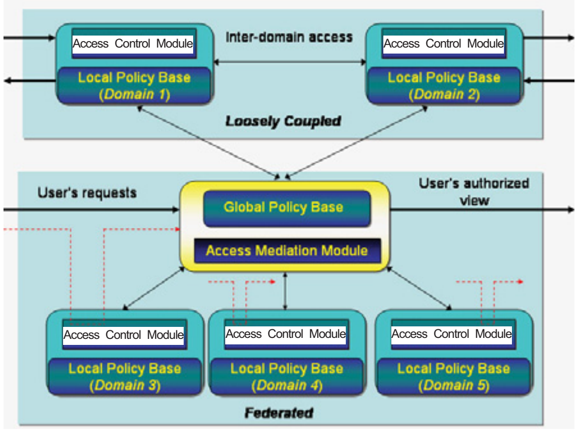
An electronic government (e-government) can be viewed as a large distributed information system consisting of interconnected heterogeneous subsystems through which government agencies, citizens, and public and private sectors interact to facilitate exchange and sharing of huge volumes of information. Such large scale information sharing and interoperation are geared towards streamlining decision-making processes through an efficient flow of information and execution of government's transactions to facilitate easy access to improved services. Key scenarios of system interactions in an e-government include: government to citizen/employee (G2C/E), government to business (G2B), and government to government (G2G), (OMB, 2004). G2C (or G2E) activities cover the interactions and information exchange between government agencies and citizens (or its employees), for instance, while filing government taxes. G2B refers to activities related to interactions between government and public and private sectors, for instance, when a government agency engages in a supplier-consumer or a buyer-seller relationship with a public/private sector business. G2G refers to activities involving interactions between two government entities. An interaction between a state office and a related federal office is an example of a G2G interaction. A critical issue related to these interactions is the need to integrate system components under disparate administrative domains with distinct policies and mechanisms. Crucial goals of an e-government infrastructure also include increasing *internal efficiency and effectiveness* (IEE) and streamlining *common lines of business* (CLoB) (OMB, 2004). For instance, if each of the federal agencies has its own payroll system, the IEE activities may involve consolidating the payroll function of multiple agencies into one system. This makes the payroll function a logical part of different agencies, thus, processing different sets of payroll information, under possibly different security policies. Similarly, if the agencies have CLoBs, the e-government infrastructure would need to remove unwarranted redundancy in service components and information processing activities.

Although emerging IT solutions provide intriguing opportunities for supporting the design and implementation of an e-government infrastructure, use of these technologies, the highly sensitive nature of information it maintains, critical transactions it processes, and the national security issues the government processes bring forth, create significant infrastructure security challenge (GAO, 2004; Joshi, et al., 2001b). The recent GAO report indicates that while interconnectivity of heterogeneous domains is a basic need for an efficient e-government system, it significantly raises the potential for unauthorized access to personal and confidential data and exposes the critical infrastructures to new vulnerabilities (GAO, 2004). A significant challenge is thus, to provide an integrated e-government infrastructure that ensures secure integration of services and information sources, fosters security assured partnerships among public and private sectors, and securely manage government resources.

## INFORMATION SYSTEMS SECURITY

Various goals of information systems security include *confidentiality*, *integrity*, *availability*, *accountability*, and *assurance* (Joshi, Aref, Ghafoor, & Spafford, 2001a). Primary mechanisms that provide the foundation for the security of information systems and infrastructures include *authentication, access control,* and *audit*. Authentication establishes the identity of an entity and is a prerequisite for access control. Access control limits the actions or operations that a legitimate entity performs. The audit process collects data about the system's activity. Once a user is authenticated, the system should enforce access control using an established technique such as a reference monitor that mediates each access by

*Figure 1. Example multidomain environment*



a user to an object. Several access-control models have been proposed to address the security needs of information systems. Traditional access control approaches fall into two broad categories: *discretionary* (DAC) and *mandatory* (MAC). DAC approach lets users grant their privileges to other users, whereas MAC approach uses a classification scheme for subjects and objects. User classification leads to several clearance levels for access control, whereas classification of objects can be established according to their sensitivity. To avoid the unauthorized flow of sensitive information, the MAC model—often known as the *multilevel model*—can enforce *no read-up* and *no write-down* rules with respect to the security levels (Joshi, et al., 2001a).

Several security technologies that are becoming indispensable for large distributed and networked heterogeneous systems, like an e-government, include *firewalls, intrusion detection systems, encryption techniques, public key infrastructure (PKI) technologies,* and *trust management techniques*. For an e-government infrastructure, designing and implementing various security mechanisms in an integrated manner poses a daunting challenge.

## SECURE INTEGRATION IN E-GOVERMENT SYSTEMS

An e-government system is essentially a multi-domain environment containing a number of independent security domains employing their own security policies, mechanisms, data models, and different architectures and computing platforms. A multidomain environment can be characterized as either *loosely coupled* or *tightly coupled* (Joshi, Bhatti, Bertino, & Ghafoor, 2004). Figure 1 depicts the two forms of multidomain interactions from an access control perspective. In a *loosely coupled* environment (e.g., domains 1 and 2), systems dynamically form transient partnerships. On the other hand, in a *tightly coupled* or federated multidomain environment (e.g., domains 3, 4, and 5), the domains form more or less a permanent partnership and their security policies are integrated to form a mediation layer or a metapolicy that mediates all accesses. Typically, a complex multi-domain environment, such as that formed by all the five domains in Figure 1, may contain several component multidomain environments that are either *loosely coupled* or *tightly coupled.* For instance, given a particular state in the USA, all state agencies can be either federated or loosely coupled with each other, depending on requirements. A *State Office* may be loosely coupled with the *Land Records Office*, but the *Land Records Office* maybe federated with the *City Electricity* department. But the components of the e-government associated with two different states may actually be acting as two loosely coupled domains. For instance, if the *Police department of Pittsburgh* wants to interact with the *Police department of New York City*, then the interaction could actually be between two independent multidomain components associated with *Pennsylvania* and *New York*, respectively.

Achieving secure integration in such a heterogeneous environment is a multifaceted problem. The key challenges include: *semantic heterogeneity, secure interoperation, risk propagation and assurance,* and *security management* (Joshi, Ghafoor, Aref, & Spafford, 2001b).

### Semantic Heterogeneity

Heterogeneity may exist in several forms (Hosmer, 1991). For example, it may be composed of diverse interacting constituent agencies with different policies, or the variations of the same set of security goals, and/or may have heterogeneous system components such as operating systems, databases, and so forth, each with different security goals and mechanisms. Integrating such heterogeneous systems within an e-government infrastructure requires powerful mechanisms to resolve semantic heterogeneity among the security attributes of the individual domains that span different layers and components. Policies can give rise to naming conflicts among similar security attributes, and structural conflicts among policy components such as user/role hierarchies and access rules.