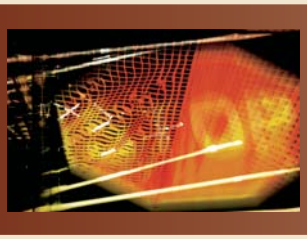
Lalana Kagal, Tim Finin, Anupam Joshi and Sol Greenspan, Security and Privacy Challenges in Open and Dynamic Environments, IEEE Computer, v39n6, pp89-91, June 2006.

Security and Privacy Challenges in Open and Dynamic Environments

Lalana Kagal, Massachusetts Institute of Technology
Tim Finin and Anupam Joshi, University of Maryland, Baltimore County
Sol Greenspan, National Science Foundation



Achieving secure open and dynamic environments requires common ontologies, behavioral norms, and trust models.

Information system security and privacy, once narrow topics primarily of interest to IS designers, have become critically important to society at large. The scope of associated challenges and applications is broadening accordingly, leading to new requirements and approaches.

Challenges arise as information systems evolve into distributed systems that are *open* in that they don't preidentify a set of known participants, and *dynamic* in that the participants change regularly, not just due to occasional failures. Such systems include peer-to-peer networks, grid computing environments, ad hoc networks, Web services, pervasive computing spaces, and multiagent systems.

In addition, as applications become more sophisticated and intelligent, they require greater degrees of decision making and independence. The long-range vision is of systems that let people, agents, services, and devices seamlessly interact as autonomously as possible while preserving appropriate security and privacy policies.

SECURITY AND PRIVACY CHALLENGES

Consider a hospital emergency facility, which contains a wide range of devices—such as defibrillators, x-ray machines, a computed tomography scanner, screens, and dialysis machines—and numerous users including doctors, nurses, specialists, and paramedics. As these people move about, agents on their personal devices detect, and are detected by, the pervasive infrastructure.

The devices must discover the services and information of interest from the infrastructure and other devices in the vicinity, negotiate for access, control information exchange, and monitor for suspicious events to be reported to the community. For example, a doctor's agent may retrieve a patient's first aid information from a paramedic's PDA.

However, not everyone should have access to all devices, services, and information available in the space. Appropriate security policies must be enforced, such as:

- specialists can only access information on a patient they're treating,
- defibrillators can only be used on patients without a do-not-resuscitate (DNR) designation, and
- paramedics can't access patient insurance data.

Privacy policies must also be considered. For example, a doctor who discovers that a patient has a drug dependency may be probited from disclosing this information to anyone including the nurses attending the patient.

An environment of this kind presents several security and privacy challenges. Agents belonging to different people and organizations have various identities as well as distinct enforcement mechanisms. This implies that agents might not be able to understand each other's security and privacy requirements or determine how to fulfill them.

Another problem is that people's identities might not be predetermined, making authentication difficult. Commonly used mechanisms such as role-based access control, access control lists, and public-key infrastructure require participants to be predetermined and can't adapt to evolving requirements.

Achieving secure open and dynamic environments requires common ontologies, behavioral norms, and trust models for communicating and cooperating applications, agents, and devices. Drawing on diverse areas within computer science as well as various social sciences, researchers must explore new languages for sharing knowledge models and data, declarative policies for information assurance and control, and trust-based approaches to security and privacy.