Trust-Based Security in Pervasive Computing Environments

Lalana Kagal, Tim Finin, and Anupam Joshi
University of Maryland, Baltimore County

Traditionally, stand-alone computers and small networks rely on user authentication and access control to provide security. These physical methods use system-based controls to verify the identity of a person or process, explicitly enabling or restricting the ability to use, change, or view a computer resource.

However, these strategies are inadequate for the increased flexibility that distributed networks such as the Internet and pervasive computing environments require because such systems lack central control and their users are not all predetermined. Mobile users expect to access locally hosted resources and services anytime and anywhere, leading to serious security risks and access control problems.

We propose a solution based on trust management that involves developing a security policy, assigning credentials to entities, verifying that the credentials fulfill the policy, delegating trust to third parties, and reasoning about users' access rights. This architecture is generally applicable to distributed systems but geared toward pervasive computing environments.

PERVASIVE COMPUTING

Pervasive computing strives to simplify day-to-day life by providing mobile users with the means to carry out personal and business tasks via portable and embedded devices. These tasks range from the simple—switching on the lights in a conference room, checking e-mail, and organizing meetings—to the more complex—booking airline tickets, buying and selling stock, or managing bank accounts.

Pervasive computing systems require a security architecture based on trust rather than just user authentication and access control.

Pervasive computing environments of the near future will involve the interaction, coordination, and cooperation of numerous, casually accessible, and often invisible computing devices and services. As Figure 1 shows, these devices—whether carried on our person or located in our homes, businesses, and classrooms—will connect via wired and wireless links to one another as well as to the global networking infrastructure to provide more relevant information and integrated services.

The eBiquity Research Group (http://research.ebiquity.org) at the University of Maryland, Baltimore County, is designing pervasive computing systems composed of autonomous, intelligent, self-describing, and interacting components. SmartSpaces are instances of pervasive systems in which the domain is divided into a hierarchy of spaces with a controller managing the services in each space.

Centaurus is a framework we developed for SmartSpaces that includes a message-based transport protocol designed to perform well in low-bandwidth networks and with resource-poor devices. We use this protocol in the Smart Office scenario, in which mobile users access computers, fax machines, printers, the lights, and even such mundane appliances as the coffee maker via handheld devices connected over short-range Bluetooth wireless links.

SECURITY CHALLENGES

Adding security to such open models presents challenges at many levels. How do you decide whether a person who does not work in an office but has access to it—for example, as a consultant or member of a partner firm—can use certain services?

We encountered several problems providing security in pervasive environments. Having a central authority for a single building or even a group of rooms is infeasible because every possible access right will have to be specified for every user. Authenticating the identity certificate of a previously unknown user doesn't provide any access control information. Simple authentication and access control are only effective if the system knows in advance which users are going to access a Smart Room and what their access rights are.

Portable handheld and embedded devices have severely limited processing power, memory capacities, software support, and bandwidth characteristics. Also, hardware and software environments are becoming increasingly heterogeneous, a trend which will continue in the foreseeable future. Finally, security