Abstract

Operating systems must be flexible in their support for security policies, i.e., the operating system must provide sufficient mechanisms for supporting the wide variety of real-world security policies. Systems claiming to provide this support have failed to do so in two ways: they either fail to provide sufficient control over the propagation of access rights, or they fail to provide enforcement mechanisms to support fine-grained control and dynamic security policies. In this paper we present an operating systems security architecture that solves both of these problems. The first problem is solved by ensuring that the security policy (through a consistent replica) is consulted for every security decision. The second problem is solved through mechanisms that are directly integrated into the service-providing components of the system. The architecture is described through its prototype implementation in the Flask microkernel-based OS, and the policy flexibility of the prototype is evaluated. We present initial evidence that the architecture's performance impact is modest. Moreover, our architecture is applicable to many other types of operating systems and environments.