

Meeting Critical Security Objectives with Security-Enhanced Linux

Peter A. Loscocco, NSA
Stephen D. Smalley, NAI Labs

Abstract

Security-enhanced Linux incorporates a strong, flexible mandatory access control architecture into Linux. It provides a mechanism to enforce the separation of information based on confidentiality and integrity requirements. This allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications. Using the system's type enforcement and role-based access control abstractions, it is possible to configure the system to meet a wide range of security needs. This paper describes how Security-enhanced Linux was used to meet a number of general-purpose system security objectives.

The paper appears in the Proceedings of the 2001 Ottawa Linux Symposium