

Working Set-Based Access Control for Network File Systems

Stephen Smaldone, Vinod Ganapathy, and Liviu Iftode
Department of Computer Science
Rutgers, the State University of New Jersey

Abstract

Securing access to files is an important and growing concern in corporate environments. Employees are increasingly accessing files from untrusted devices, including personal home computers and mobile devices, such as smart phones, that are not under the control of the corporation, and may be infected with viruses, worms, and other malware. In such cases, it is crucial to protect the confidentiality and integrity of corporate data from malicious accesses. Existing tools available to network administrators are either too permissive or too restrictive in allowing file access from untrusted devices.

This paper proposes a novel scheme called Working Set-Based Access Control (WSBAC) to restrict network file system accesses from untrusted devices. The key idea is to continuously observe and extract working sets for users when they access files from trusted devices. These working sets are used to restrict file accesses when users connect from untrusted devices. This paper reports on the design and implementation of tools to automatically extract working sets, and transparently enforce WSBAC without requiring changes to the file system. Our experiments with realistic network file system traces lead us to conclude that using working sets offers a flexible yet secure way to restrict access from untrusted devices, and that the runtime overheads of WSBAC enforcement are negligible.