Título:

Autor:

Editorial:

Tema:

Sinopsis

Precio: $449.20

Año: 2004

Edición: 1ª

ISBN: 9780596007164

The intensive search for a more secure operating system has often left everyday, production computers far behind their experimental, research cousins. Now SELinux (Security Enhanced Linux) dramatically changes this. This best-known and most respected security-related extension to Linux embodies the key advances of the security field. Better yet, SELinux is available in widespread and popular distributions of the Linux operating system--including for Debian, Fedora, Gentoo, Red Hat Enterprise Linux, and SUSE--all of it free and open source. SELinux emerged from research by the National Security Agency and implements classic strong-security measures such as role-based access controls, mandatory access controls, and fine-grained transitions and privilege escalation following the principle of least privilege. It compensates for the inevitable buffer overflows and other weaknesses in applications by isolating them and preventing flaws in one application from spreading to others. The scenarios that cause the most cyber-damage these days--when someone gets a toe-hold on a computer through a vulnerability in a local networked application, such as a Web server, and parlays that toe-hold into pervasive control over the computer system--are prevented on a properly administered SELinux system. The key, of course, lies in the words "properly administered." A system administrator for SELinux needs a wide range of knowledge, such as the principles behind the system, how to assign different privileges to different groups of users, how to change policies to accommodate new software, and how to log and track what is going on. And this is where SELinux is invaluable. Author Bill McCarty, a security consultant who has briefed numerous government agencies, incorporates his intensive research into SELinux into this small but information-packed book.