Solaris Commercial Extensions Products

Security Products

The Account Resource Management (ARM) and Automated Security Enhancement Tool (ASET) Security Products are members of the Solaris™ Commercial Extensions Products series. They enhance the versatility and security of UNIX® systems used for demanding technical and commercial applications. ARM and ASET provide system administrators security features previously available only on proprietary systems, thereby significantly increasing the security of UNIX systems.

Account Resource Management is a set of administrative security features that enhances account protection and usage control. By supplementing the standard UNIX login and password mechanisms, ARM provides account protection and access denial features expected by commercial customers. ARM enables solutions tailored to an organization's unique security needs.

The Automated Security Enhancement Tool allows system administrators to audit current workstation security levels and to adjust the level of security on their networks — from the most open access to the most restrictive.

These commercial security features have virtually no impact on system or network performance.

Key Features and Benefits

As the popularity of open, networked computing has grown, so has the need for securing and protecting information on the network. The need for software security is critical in commercial, government and university installations. With the ARM & ASET security products, Solaris can better address user needs for reliable, flexible software security tools.

ARM and ASET enable corporate MIS managers and network administrators to create customized security solutions that help protect their UNIX networks from security breaches. ARM is a set of administrative security features which aid system administrators in controlling user account access. All of ARM's features are network-extensible, and can be customized on a per-account basis.

ARM account protection capabilities include:

Password Aging
- Keeps passwords valid for a user-specified minimum and maximum amount of time. This helps ensure that passwords are changed periodically. NIS passwords are also aged.

Account Expiration
- Automatically locks expired accounts from the system. An account may be deleted or placed in an inactive state (i.e., it can be re-activated by the system administrator).

Auto-Logout
- Terminates inactive sessions to limit unauthorized account usage.

Auto-Lockscreen
- Automatically closes workstation window access to limit unauthorized workstation usage.

Dial-Pass
- Presents an additional level of security for modem or network access. When users attempt to log in to a protected port, the user must enter an additional password in order to get logged into the system.

Password Qualification
- Allows sites to specify their own policy on passwords including length and other parameters.

ARM also provides the following access/denial features:

Login Disabling
- De-activates an account after repeated invalid attempts, to help reduce password "cracking" and breakins. After a specified number of consecutive unsuccessful login attempts, an account is locked for a selected amount of time.

Access Hours
- Denies account access, and terminates active sessions outside of authorized work hours. Access hours can be specified on a daily basis.

ASET provides an automatic audit of security policy, allowing the system administrator to enforce workstation security at low, medium, or high levels. ASET checks and tightens file permissions, checks the contents of critical system files such as the password files, examines environment variables in user startup files, investigates system configuration files, and checks EEPROM data for system startup parameters. Where possible, ASET modifies the weaknesses it finds, and brings the system to the desired security level. If ASET cannot automatically resolve the security issue, it informs the system administrator. ASET can automatically apply the basic security parameters for "firewall machines" — systems that serve as gateway machines to public networks.

Requirements

Hardware
- Specific configurations of the SPARC® reference platform.

System Software
- Solaris 1.0 or any SunOS™ 4.1.x release

Typical Configuration
- Networked workstation or server

Distribution Media
- CD-ROM

For more information, call 1 800 227-9227 or 415 336-4252.

2550 Garcia Avenue • Mountain View • California 94043-1100

Printed in USA 9/91 91011-0 4K