UNIX: Access Control

Author: Lakshmikanth Bhujang

Submitted on: March 16, 2001

Purpose of this document:

This document discusses the various concepts of UNIX security and some ways of mitigating the inherent risks/threats of native UNIX Operating system.

Audience:

This document will help for System Administrators, UNIX programmers and others who wish to understand the native UNIX security risks.

Scope of the document:

This document addresses the native UNIX security weakness w.r.t to user access to UNIX system resources and provides the comprehensive solution.

Unfortunately, Unix-based operating systems were not designed this way. Authorization decisions are made mainly for file access and are performed by the operating system itself using the 9 bits (rwx-rwx-rwx) in the file's inode entry.

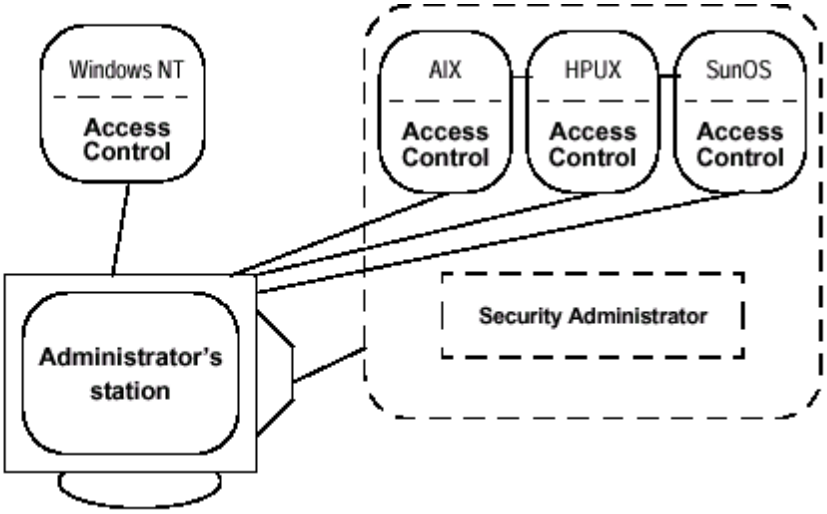
Many Operating System has built in access control mechanism using one technique or other. IBM's MVS is a well-known matured mainframe operating system includes System Authorization Facility (SAF), a set of system calls issued by operating system itself to verify a user's authorization. Access control software in an MVS environment sets a return code for the SAF call and MVS grants or denies access according to the code. The decision of what return code to set is based on the access rule and policies defined in the security database by the system administrator.

Other operating systems, like OS/2, provide similar techniques for access control. OS/2's access control module, called Security Enabling Services (SES), is based on the concept of MVS' SAF.

Unlike SAF, no exit point for event interception is provided in UNIX. Therefore further security is necessary, to perform more complex functions. This can be incorporated using some products available in the market, such as, Access Control for UNIX from Computer Associates, Unix Based Security from RSA Keon product suite, etc.. I will be discussing CA's Access Control mechanism to understand the technology.

Access Control for UNIX:

The primary function of Access control is to protect the information assets of computer centers. It checks whether users who request services from host operating system are authorized to access those services. Access control conceptually similar in structure to mainframe access control products, information centers can keep well-established security procedures, regulations and policies while integrating Unix based operating systems. CA Access control package includes the security administrator, a graphical user interface (GUI) from which you can define users, groups and access rules in access control database. We can also use it to monitor and audit events.



* Access Control for Unix-based operating systems
* Security Administraor (GUI) for all security environments

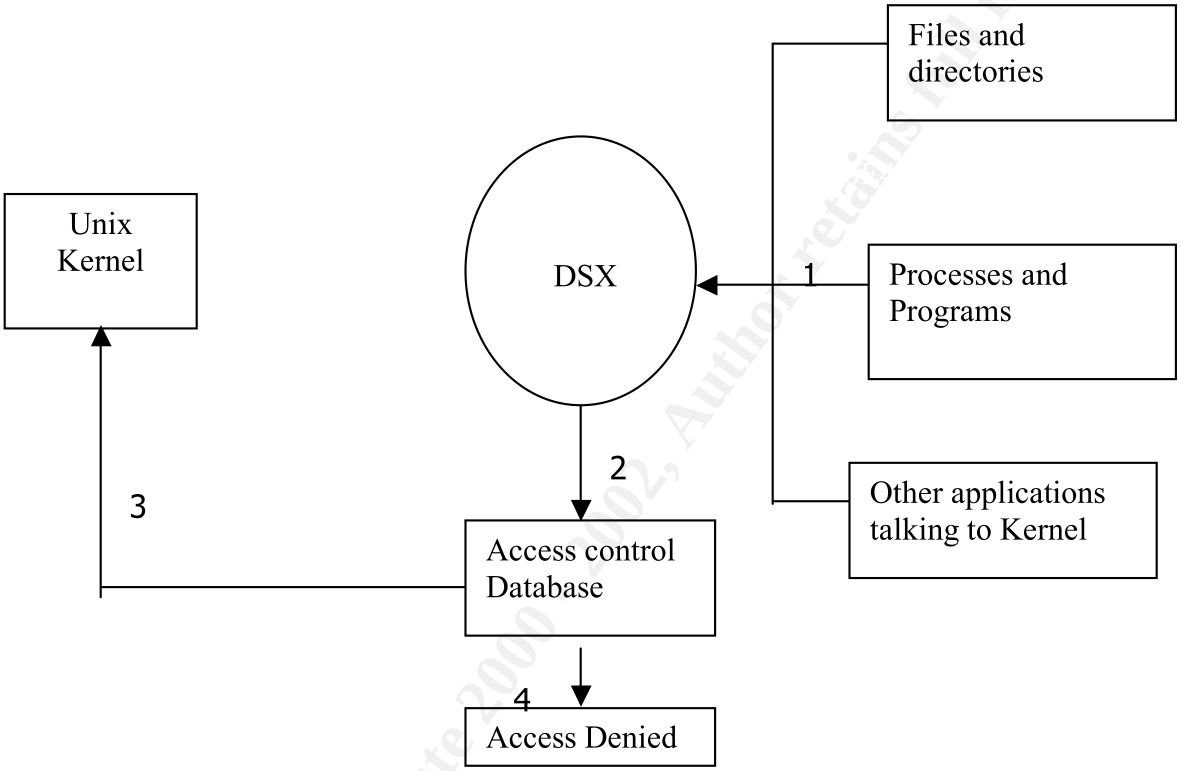
source: e-Trust Access control – Users guide

How does Access Control work?

Other than the regular security functions, such as access rule database, as audit log and administration tools, Access control intercepts the operating system events that are to be protected, in memory and no changes are made to system files and the operating system is not modified at all.

The Access control process is invoked immediately after the operating system has finished its initialization. Access control places hooks in system services that need to be protected. In this way, the control is passed to Access control before the service is performed. Access control decides whether the service should be granted to the user or not.

For example, a user may attempt to access a protected resource. This access request generates a system call to the kernel to open the resource. Access control intercepts this system call and decides whether to grant access. If permission is granted, control is passed to regular service of the system, otherwise access control denies the access, and it returns the standard "permission denied" error code to the activated program that activated the system call.



<u>**Architecture of Access Control**</u>

Process:

1. Request is generated/initiated at user level. This may include, request to kernel via programs, accessing files or directories or any other programs, which is trying to access kernel for information.

2. These requests will be sent to Access control (DSX- Dynamic Security Exchange), which will intercept the request, and sends requests for access control verification.

3. The policy rule will be checked against the request and GRANT will be given, if it meets the policy.

4. Otherwise the access will be denied.

Distinctive features of Access Control:

- Centralized Administration

  Access Control enables you to manage the administrator workstation and every other workstation on which Access control is installed-from a single point.

- Self Protection

  A self-defense mechanism prevents hackers or other users from bringing down the access control services. This also brings the mechanism of protecting Access control files and directories.

- Profile group

  It allows you to base the security rules depending on group membership.

- User Accountability

  Access Control has the unique ability to prohibit the user hiding behind super user and performing un-traceable activities. It maps each activity to a specific user who can be named and held accountable.

- Stack Overflow Protection

  This feature prevents hackers using stack over-flow exploits, which can enable them to execute arbitrary commands in order to break into systems.

- Cross-platform Protection

  Administrators can create, implement and maintain similar or identical security polices for Unix and Windows NT.

- Centralized logging

  The audit log of every workstation will be captured on single system, for central audit review and generating reports. Also, the user activity and other resource access can be obtained.

Conclusion:

Access Control provides an essential Business element — regulating access to critical business assets. In a world where business systems are all too accessible, Access Control provides policy-based control of who can access specific systems, what they can do within them, and when they are allowed access. Policies can be created, managed, and distributed on an enterprise-wide basis, or customized to meet the security requirements of specific applications. The best-of-breed solution can be deployed in individual departments, such as payroll, to the largest enterprises — and everything in between. Its hardened operating system security, complete audibility, and cross-platform access control secures everything from LANs and web servers to mainframes. Access Control's built-in baseline policies give organizations immediate results right out of the box. Open and extensible, this powerful solution supports all industry-standard platforms, databases and applications and includes published interfaces allowing it to secure any resource. Ease of use, combined with centralized user and access administration enables organizations to confidently exploit Business. As a part security solution, Access Control is providing a powerful, comprehensive solution for building, deploying, and managing security as part of the larger task of enterprise management.

References:

Matt. "Unix Security". February 21, 2001.
URL: http://www.deter.com/unix/#papers(10th March 2001)

Access control – Protecting critical resources
http://ca.com/solutions/enterprise/etrust/access_control/etrust_access.pdf

Peter Baer Galvin. "The Solaris Security FAQ". March 05, 2001
URL: http://www.unixinsider.com/common/security-faq.html (9th March, 2001)

AUSCERT, Australian Computer Emergency Response Team. "UNIX Computer Security Checklist (Version 1.1)". Last Update   19-Dec-1995.
URL:http://www.securityportal.com/research/unix_security_checklist1.1
(10th March, 2001)

Deborah Russell & G.T. Gangemi, Sr. "Computer Security Basics". July 1991
Book Name: "Computer Security- O'Reilly & Associates, Inc" (14th March 2001)

Computer Associates-Security Solution Home.
Access control – Regulating access to critical business assets
URL: http://www3.ca.com/Solutions/Overview.asp?ID=154 (12th March 2001)

Computer Associates. “What is Access control”. Version 5.0. September 1999. Book: e-Trust Access control for UNIX-User reference guide. (12th March 2001)