

Mandatory Access Control and the Principle of Least Privilege

Jarrold Millman
Neuroscience Institute
UC Berkeley

Overview

- Principles and Ideas
- Historical Development
- Understanding MAC
- MAC Implementations in Mainstream OSes

Principles and Ideas

Principle of Least Privilege

“Every program and every user of the system should operate using the least set of privileges necessary to complete the job.”

The protection of information in computer systems

Jerry H. Saltzer, Mike D. Schroeder (1975)

Inevitability of Failure

“The necessity of operating system security to overall system security is undeniable [...] If it fails to meet this responsibility, system-wide vulnerabilities will result.”

The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments

Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer,
Ruth C. Taylor, S. Jeff Turner, John F. Farrell (1998)

Access Control Security

Necessary to control access by subjects (e.g., users, processes) to objects (e.g., files, system resources)

Basic Permissions

- Own
- Transfer
- Read
- Write
- Execute

Where do the permissions reside?

- subject
- object

Complexity of Permission Management

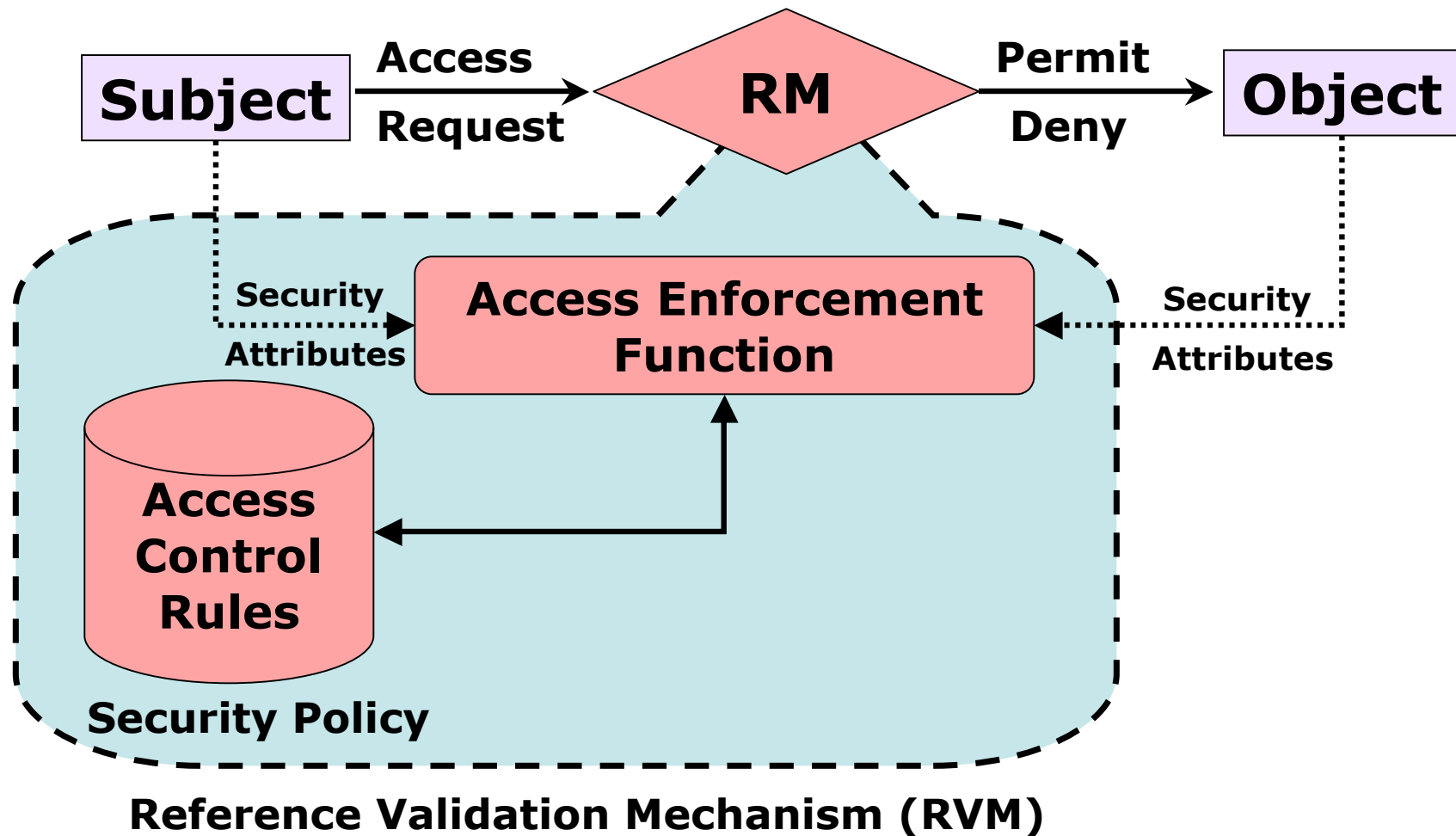
- Adding permissions
- Removing permissions
- Removing all permissions

Access Control

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)

Historical Development

Reference Monitor



Discretionary Access Control

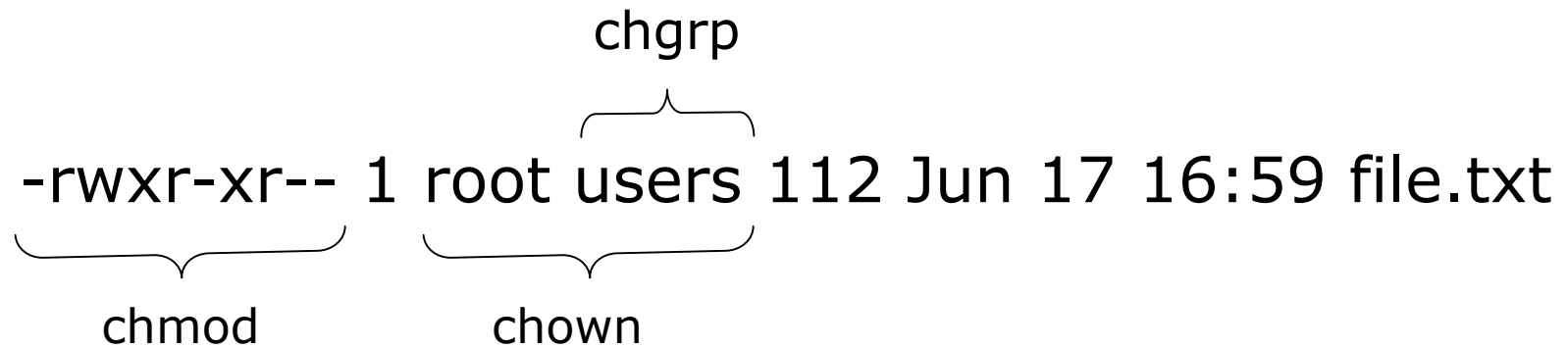
Under DAC, “resource” owners can specify which users (subjects) may or may not access those “resources” (objects).

UNIX File Access Permissions

`-rwxr-xr-- 1 root users 112 Jun 17 16:59 file.txt`

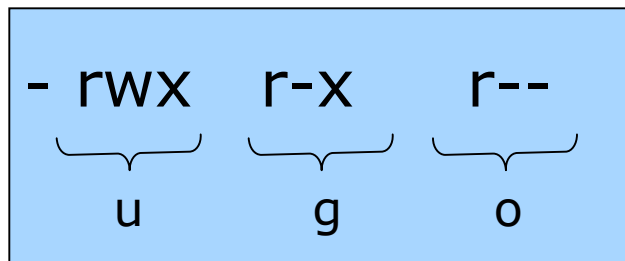
`chgrp`

`chmod` `chown`



`- rwx r-x r--`

`u g o`



Discretion Access Control

- File/directory permissions
- User/group ownership
- Access Control Lists
- Capabilities
- Procedure-oriented Access Control

The problem with DAC

- Users rely on software

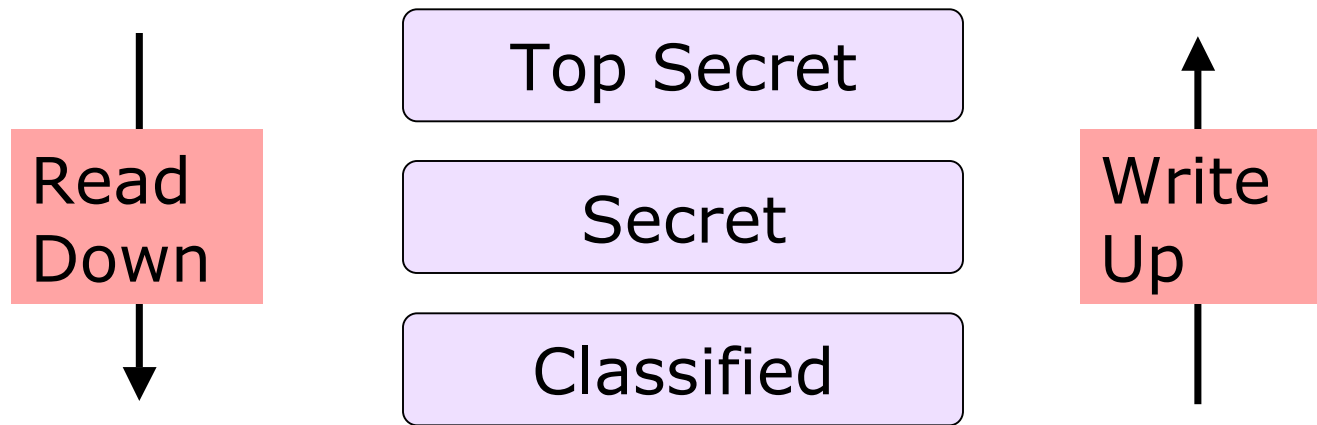
Origin of MAC



Administratively
Controlled
Organizational
Security Policy



Multi-Level Security

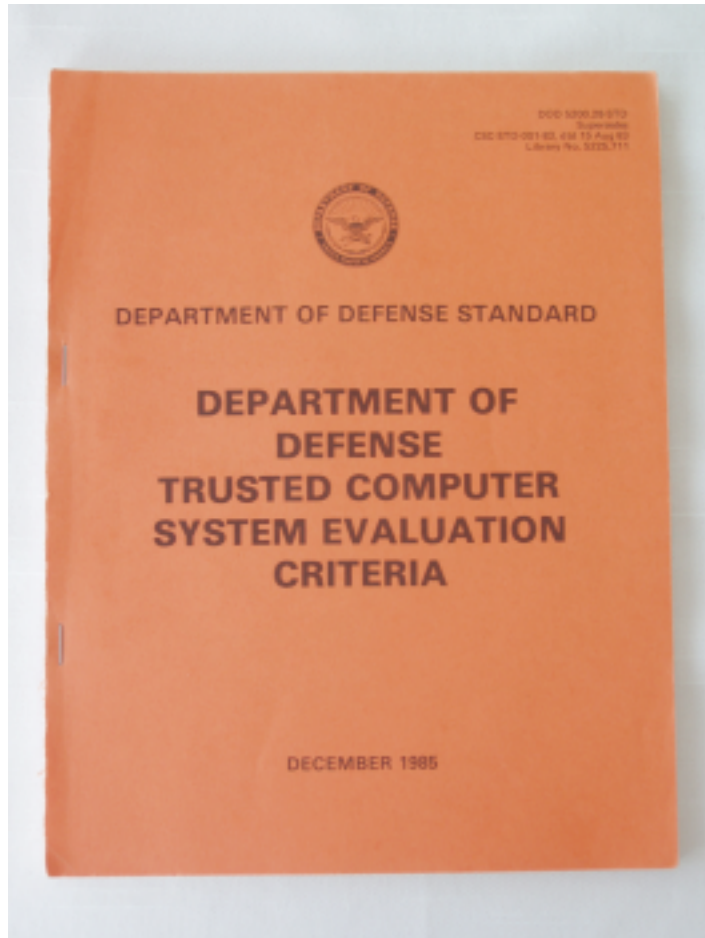


National Security Agency

- Signals Intelligence
- Information Assurance



TCSEC or the Orange Book



Objectives

- Policy
- Accountability
- Assurance
- Documentation

Research Microkernels

- LOCK
 - Type Enforcement
- Trusted Mach
 - Multilevel Security
- Distributed Trusted Mach
- Distributed Trusted OS
- Flux Advanced Security Kernel

SELinux

- Security Enhanced Linux
 - developed by NSA
 - initiated 1999
- Mandatory Access Control
 - type enforcement
 - role-based access control
 - multilevel security

SELinux History

- 2.2 Linux Kernel patch (~1999)
- 2.4 Linux Kernel patch (~2001)
- Linux Security Modules (~2002)
- 2.6 Linux Kernel mainline (~2003)

Understanding Mandatory Access Control

SELinux Architecture

- User Identity
- Role
- Type (Domain)
- Security Context
- Security Policy

User Identity/Role

- User Identity is the SELinux user account of an entity
- The Role determines which User Identities are allowed access to which Domains

Resources and Types

- Resources have a type
 - Apache executable `/usr/sbin/httpd` has type `httpd_exec_t`

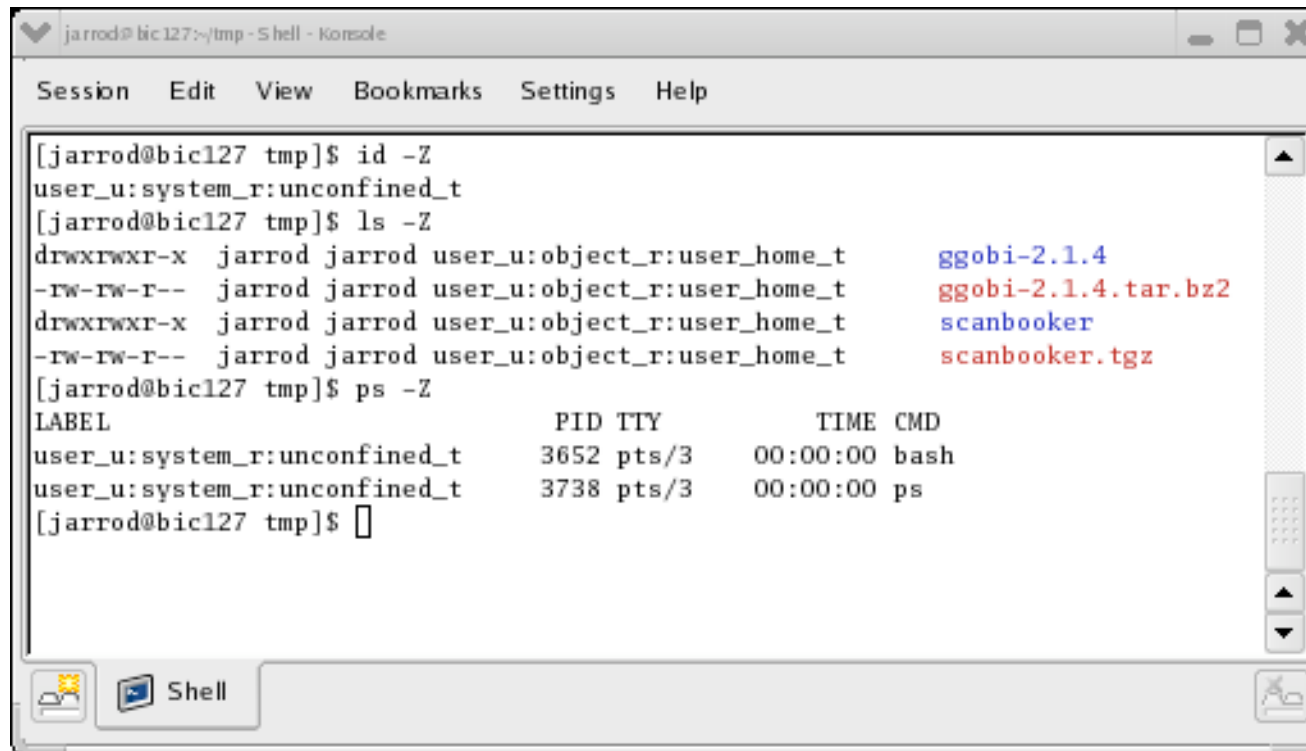
Processes and Domains

- Processes run in domains (sandboxes)
 - Apache process `httpd` runs in domain `httpd_t`
- Also called domain type, subject type, process type

Security Context

- Everything has a security context
 - `user:role:type`
 - stored in the extended attributes

Security Context Information



The image shows a terminal window titled "jarrod@bic127:~/tmp - Shell - Konsole". The terminal displays the following commands and their outputs:

```
[jarrod@bic127 tmp]$ id -Z
user_u:system_r:unconfined_t
[jarrod@bic127 tmp]$ ls -Z
drwxrwxr-x  jarrod jarrod user_u:object_r:user_home_t  ggobi-2.1.4
-rw-rw-r--  jarrod jarrod user_u:object_r:user_home_t  ggobi-2.1.4.tar.bz2
drwxrwxr-x  jarrod jarrod user_u:object_r:user_home_t  scanbooker
-rw-rw-r--  jarrod jarrod user_u:object_r:user_home_t  scanbooker.tgz
[jarrod@bic127 tmp]$ ps -Z
LABEL                                PID TTY          TIME CMD
user_u:system_r:unconfined_t        3652 pts/3        00:00:00 bash
user_u:system_r:unconfined_t        3738 pts/3        00:00:00 ps
[jarrod@bic127 tmp]$
```

The terminal window includes a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". The bottom of the window shows a "Shell" tab and a keyboard icon.

Security Policy

- Set of rules
 - Defines how each domain may access each type
 - Defines transitions and other access
- Compiled from source and loaded into Linux kernel during boot

Access Control Comparison

| | Linux | SELinux |
|------------------------------------|---|------------------|
| Subject Security Attributes | Real and effective user/group IDs | Security Context |
| Object Security Attributes | Access modes and file user/group IDs | Security Context |
| Access Control Rules | Process user/group ID and file's access modes based on file's user/group ID | Security Policy |

Type Enforcement

- Permissions allowed between subject type and object type

“Allow” Rules

- All access must be explicitly granted via an `allow` rule
 - Source type(s)
 - Target type(s)
 - Object Class(es)
 - Permissions(s)

```
allow user_t bin_t : file {read}
```

TE for passwd

```
allow passwd_t shadow_t : file
    {ioctl read write create
    getattr setattr lock
    relabelfrom relabelto append
    unlink link rename};
```

Domain Transition

- Better version of `suid`
- Solves Least Privilege problem

DT for passwd

```
allow user_t passwd_exec_t :  
    file {getattr execute};  
allow passwd_t passwd_exec_t :  
    file entrypoint;  
allow user_t passwd_t : process  
    transition;
```

Role-Based Access Control

- RBAC built on TE
- Extend passwd example
 - `role user_r type passwd_t;`

Multilevel Security

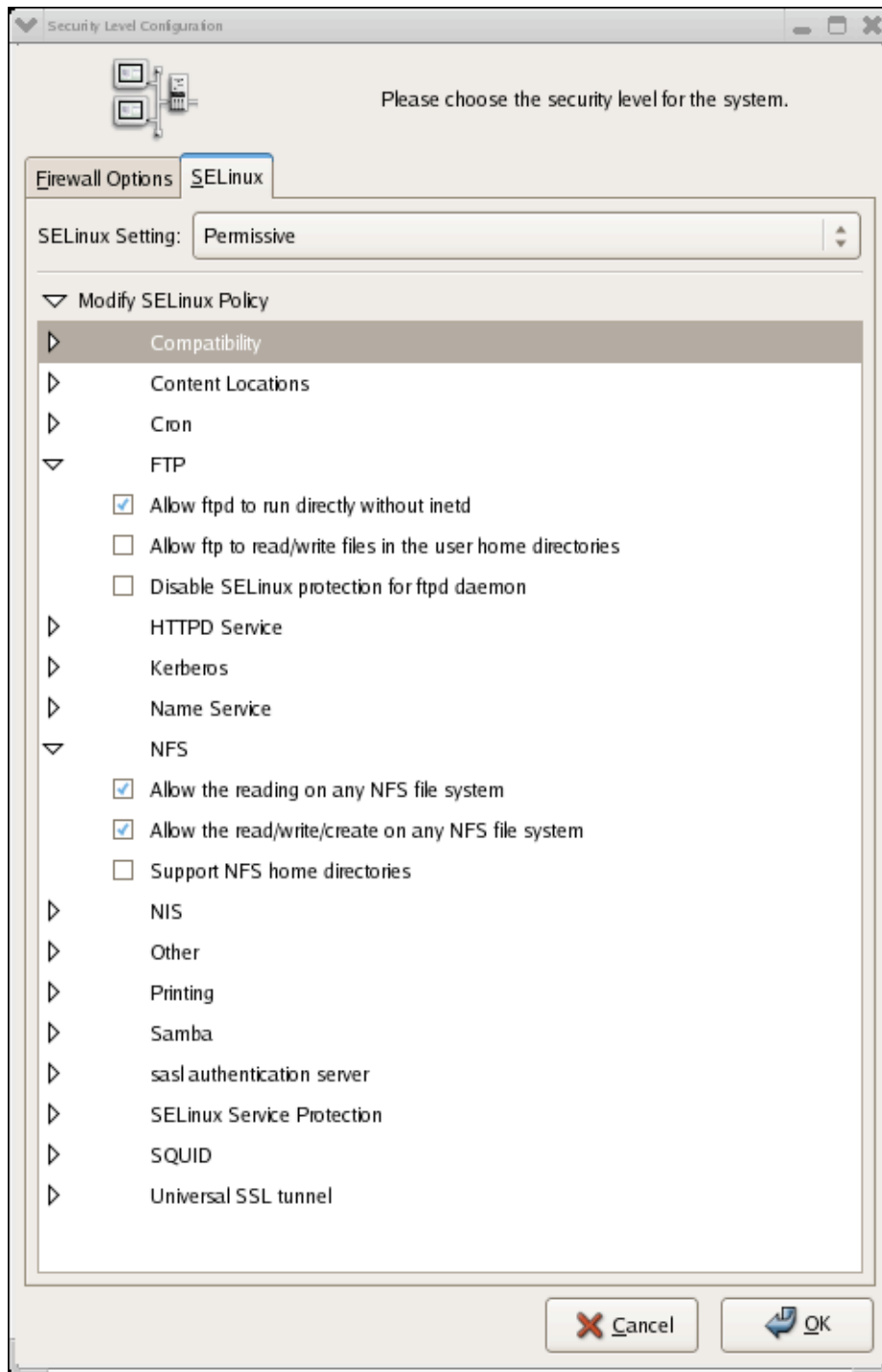
- MLS extends the security context
 - *sensitivity* (information confidentiality)
 - *categories* (user clearance level)

`user:role:type:sensitivity[:category]`
- Needed for certain classified government applications

Operating Systems

RHEL 4

- Type Enforcement
- Role-Based Access Control (RBAC)
- Targeted Policy



Security Level

redhat-config-securitylevel

- disabled
- permissive
- targetted
- strict

seaudit

The screenshot displays the seaudit application window. The title bar indicates the log file is `/var/log/messages` and the policy file is `/etc/selinux/targeted/policy/policy.20`. The menu bar includes File, View, Search, Report, and Help. Below the menu are three buttons: Query policy, Modify view, and Toggle Monitor. The main area shows a table of audit events with columns for Hostname, Message, Date, Source Type, Target Type, Object Class, Permission, Executable, Command, and Other. A detailed view window titled "View Entire Message" is open, showing the following text:

```
Mar 28 00:35:43 bic127 kernel: avc: denied {} for pid=3176 comm=nxagent
name="libXcompext.so.2.1.0" dev=hda7 ino=2931237 scontext=user_u:system_r:unconfined_t
tcontext=system_u:object_r:lib_t tclass=file
```

The status bar at the bottom provides summary information: Policy Version: v.20 (binary, MLS), Log Messages: 4/4, Dates: Mar 27 23:54:43 - Mar 28 00:35:43, and Monitor status: ON.

| Hostname | Message | Date | Source Type | Target Type | Object Class | Permission | Executable | Command | Other |
|----------|---------|-----------------|-------------|-------------|--------------|------------|------------|-----------|--|
| bic127 | Load | Mar 27 23:54:43 | | | | | | | users=3 roles=6 types=1481 booleans=152 classes=58 |
| bic127 | Denied | Mar 27 23:54:43 | pam_conso | file_t | dir | | | pam_consc | dev=hda1 |
| bic127 | Denied | Mar 27 23:54:44 | bluetooth_t | bluetooth_t | capabilit | | | sdpd | capability=10 |
| bic127 | Denied | Mar 28 00:35:43 | unconfined_ | lib_t | file | | | nxagent | dev=hda7 |

apol

The screenshot displays the SELinux Policy Analysis tool (apol) interface. The main window shows a list of types on the left, search options in the middle, and search results on the right. A 'Policy Summary' dialog box is open in the foreground, displaying the following statistics:

| Policy Summary Statistics | |
|-----------------------------------|--------|
| Policy Version: | v.20 |
| Policy Type: | binary |
| MLS Status: | MLS |
| Number of Classes and Permissions | |
| Object Classes: | 58 |
| Common Perms: | 3 |
| Permissions: | 209 |
| Number of Types and Attributes: | |
| Types: | 1346 |
| Attributes: | 100 |
| Number of Type Enforcement Rules: | |
| allow: | 56957 |
| neverallow: | 0 |
| clone (pre v.11): | 0 |
| type_transition.: | 1123 |
| type_change: | 14 |
| type_member: | 0 |
| auditallow: | 23 |
| auditdeny: | 0 |
| dontaudit: | 3846 |
| Number of Roles: | |
| Roles: | 6 |
| Number of RBAC Rules: | |
| allow: | 5 |
| role_transition: | 0 |
| Number of Users: | |
| users: | 3 |
| Number of Initial SIDs: | |
| SIDs: | 0 |
| Number of Booleans: | |
| Bools: | 152 |

The status bar at the bottom of the main window displays the following summary: Classes: 58 Perms: 209 Types: 1346 Attribs: 100 TE rules: 61963 Roles: 6 Users: 3 v.20 (binary, MLS)

RHEL 5

- Multilevel Security (MLS)
- SELinux Troubleshooter

IBM Hardware & RHEL 5 Security Certifications

- Common Criteria EAL 4+
- LSPP
- RBACPP
- CAPP

Solaris Trusted Extensions

- MLS

Windows Vista

- Mandatory Integrity Control
 - Internet Explorer 7 running in Protected Mode

Mac OS X Leopard

- Based on TrustedBSD