PURDUE UNIVERSITY

CS526: Information Security
Chris Clifton

December 4, 2003

Trusted Solaris

CERIAS Center for Education and Research in Information Assurance and Security

What is *Trusted* Solaris?

- Enhanced version of Solaris
  - Added security features
  - Common Criteria evaluation
- Key concepts
  - Trusted computing base (TCB)
    - Portion of the system that affects security
  - Mandatory and Discretionary Access Control
  - Detailed audit capabilities
  - Trust symbol displayed for valid interactions with TCB
  - Device-level authorization based on user and location

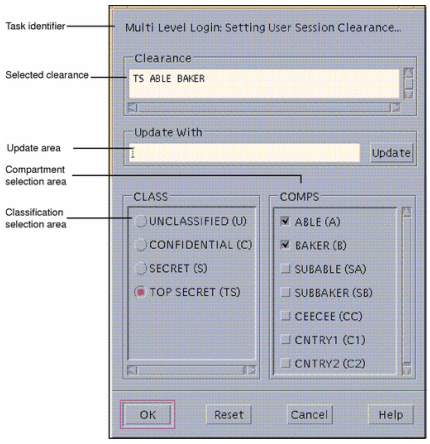
Discretionary Access Control

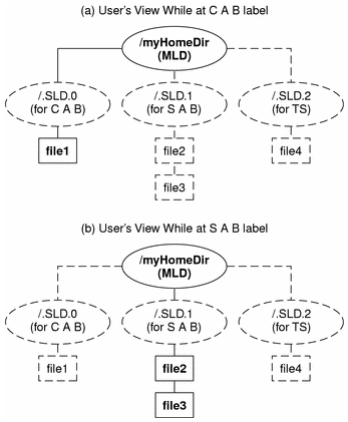
- Owner-decided
- Standard UNIX user/group/public permissions
- Access Control Lists
- Override by administrators and authorized users only
  - Not by the superuser/root

Mandatory Access Control (Bell-LaPadula style)

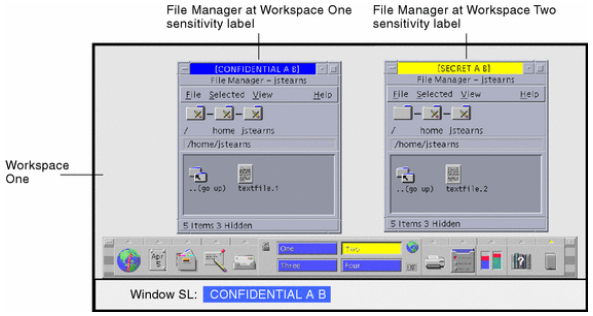
- All subjects/objects have label
  - User can have single or multi-level session
  - Objects stored in different directories (transparently) based on label
  - *Includes devices!*
- Read/write dominance enforced
- Sensitivity label displayed in window title bar
- Cut/Paste between levels causes confirmation box
  - Allowed only if user authorized
- Email enforces MAC

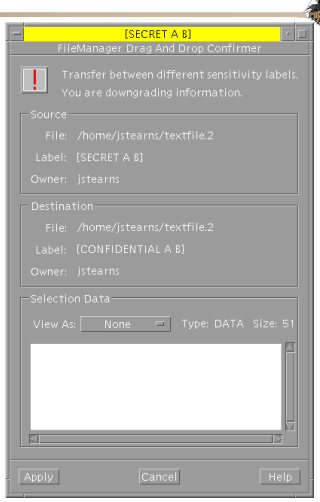
MAC example



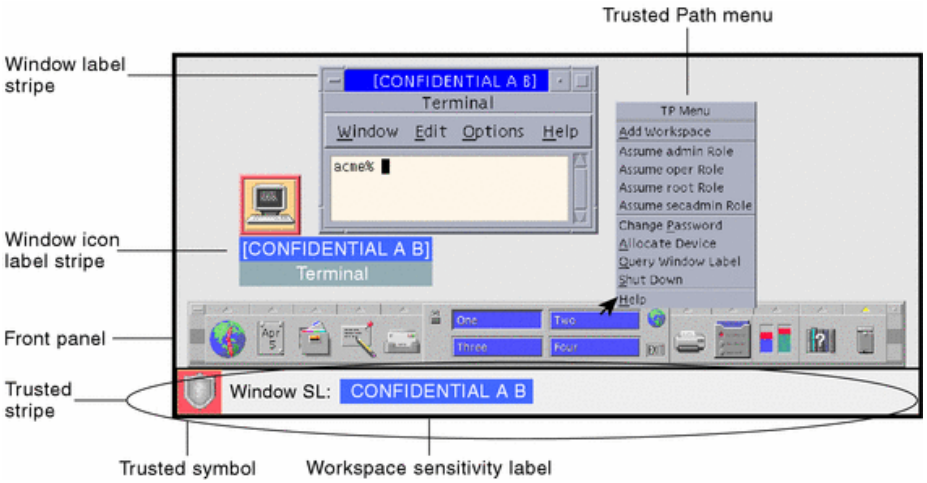


Cut/Paste Dialog





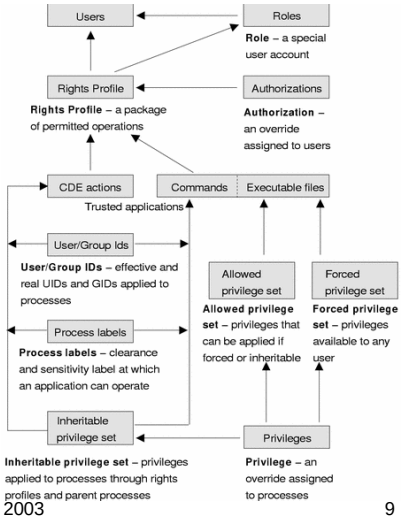
Trusted Solaris "Desktop"



Administration

- Key: Superuser not omnipotent
  - Administration based on roles
- User authorized to perform specific functions
  - *override* a specific security control
- Predefined roles
  - Root: installation
  - Security administrator: assigning labels, audit
  - System administrator: user account administration other than security
  - System operator: Backups, printers, mounts
  - Primary administrator: Tasks not enabled under others

- Trusted Application
  - Allowed to override system controls
  - In practice: SUID/SGID
- Rights Profiles
  - Specific rights given to users



Rights Profiles

- All Provides access to all executables but without privileges.
- All Actions Provides access to all actions but without privileges.
- All Authorizations Provides all authorizations (for testing).
- All Commands Provides access to all commands but without privileges.
- Audit Control For managing the audit subsystem but without the ability to read files.
- Audit Review For reading the audit trail.
- Basic Actions Provides access to the applications on the Front Panel with the necessary privileges.
- Basic Commands Provides access to basic commands necessary for all roles.
- Basic Solaris User Assigned to all users of the Solaris Management Console. Provides Read permissions and lets users add cron jobs to their crontab files. Contains the All rights profile.
- Convenient Authorizations Provides authorizations for normal users.
- Cron Management For managing cron and at jobs.

Rights Profiles

- Custom Admin Role An empty right for adding security attributes to the default Admin role.
- Custom Oper Role An empty right for adding security attributes to the default Oper role.
- Custom Root Role An empty right for adding security attributes to the default Root role.
- Custom Secadmin Role An empty right for adding security attributes to the default Secadmin role.
- Custom SSP An empty right for adding security attributes to the default SSP role for Sun EnterpriseTM 10000 administration.
- Device Management For allocating and deallocating devices, and correcting error conditions.
- Device Security For managing and configuring devices.
- Enable Login Provides the authorization for allowing yourself and other users to log in after boot.
- File System Management For managing file systems.
- File System Security For managing file system labels and other security attributes.
- Information Security For setting access control policy.

Rights Profiles

- Mail Management For configuring sendmail, modifying aliases, and checking mail queues.
- Maintenance and Repair Provides commands needed to maintain or repair a system.
- Media Backup For backing up files.
- Media Restore Restore files from backup.
- Name Service Management Grants right to control the name service daemon.
- Name Service Security Grants right to control the name service properties and table data.
- Network Management For managing the host and network configuration.
- Network Security For managing network and host security, with authorizations for modifying trusted network databases.
- Object Access Management For changing ownership and permissions on files.
- Object Label Management For changing labels of files and setting up system-wide labels.
- Object Privilege Management For changing privileges on executable files.
- Outside Accred For operating outside system accreditation range.

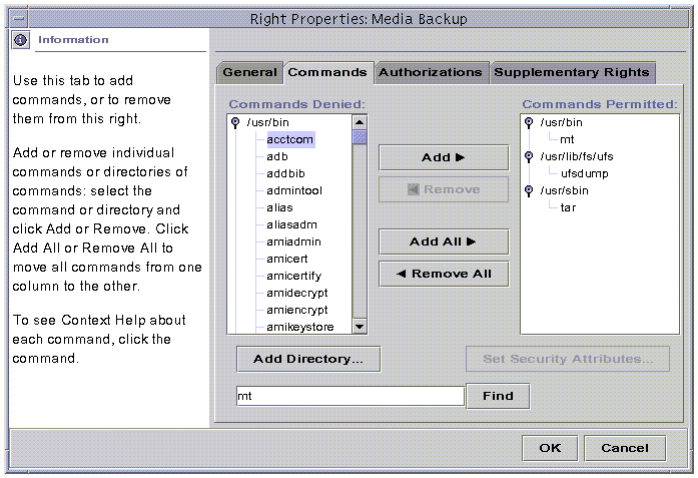
Rights Profiles

- Primary Administrator Contains subordinate rights profiles for primary administrator role.
- Privileged Shells For developers to run Bourne, Korn, and C shells with all privileges. Not intended for secure environments.
- Process Management For managing current processes, including cron and at jobs.
- Remote Administration For remote administration of headless systems.
- Rights Delegation Lets user or role assign rights assigned to that user or role to other users or roles. Lets user assign roles assigned to that user to other users.
- Rights Security For managing assignment of rights profiles, labels, and privileges, and for setting account security.
- Software Installation For adding application software to the system.

Rights Profiles

- SSP Administration Tools for administering the SSP.
- SSP Installation Tools for installing the SSP.
- System Administrator Contains subordinate rights profiles for system administrator role.
- User Management For creating and modifying users but without the ability to modify self (as a security measure).
- User Security For creating and modifying users' security attributes but without the ability to modify self (as a security measure).

Defining New Rights



Authorization

- Right granted to user/role that is checked by trusted applications
  - Generally for system administration
- Examples:
  - solaris.admin.diskmgr.read - View Disks
  - solaris.admin.diskmgr.write - Manage Disks
  - solaris.admin.printer.read - View Printer Information
  - solaris.admin.printer.modify - Update Printer Information
  - solaris.admin.procmgr.admin - Manage All Processes
  - solaris.admin.procmgr.user - Manage Owned Processes

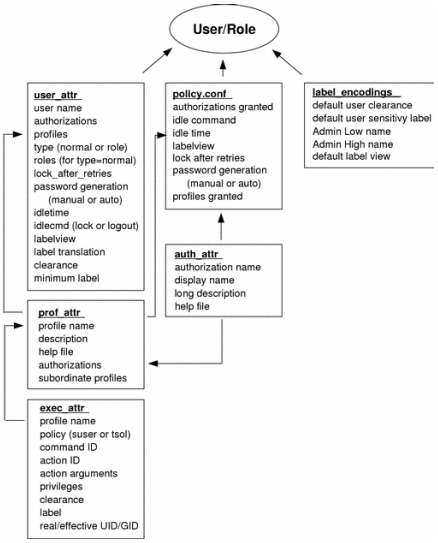
Privilege

- Right to perform an action that otherwise violates policy
- Granted to processes
  - Allowed privilege: Must be set for process to have privilege
  - Forced privilege: Effective for all users running application
  - Inheritable privilege: From user's rights profile

Types of Privileges

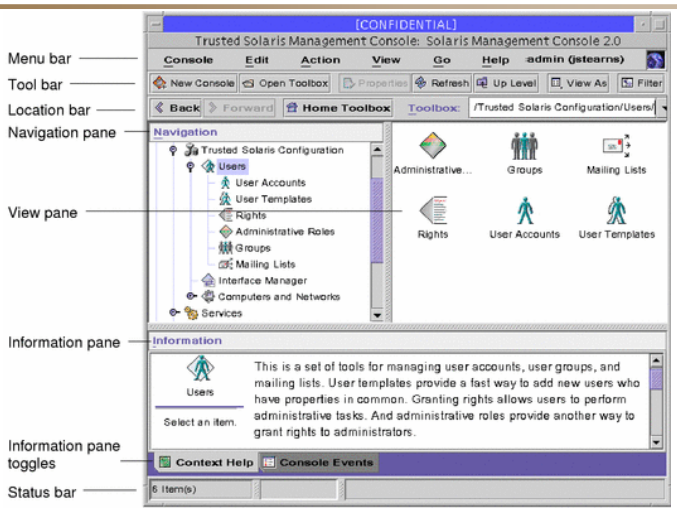
Type	*Example*
• File system security	• file_dac_chown - Lets a process change the owner user ID of a file.
• System V Interprocess Communication (IPC) security	• ipc_dac_read - Lets a process read a System V IPC message queue, semaphore set, or shared memory region whose permission bits do not allow process read permission
• Network security	• net_broadcast - Lets a process send a broadcast packet on a specified network
• Process security	• proc_mac_read - Lets a process read another process where the reading process label is dominated by the other process label
• System security	• sys_boot - Lets a process halt or reboot a Trusted Solaris computer
• Window security	• win_selection - Allows a process to request inter-window data moves without the intervention of selection arbitrator

Adding it all together



19

System Management Console



20

Etc.

- ADMIN_HIGH/ADMIN_LOW: Max/Min labels
  - ADMIN_HIGH used for audits, administrative data
  - ADMIN_LOW used for public executables
- Objects cleared when deleted
  - Files
  - Memory
  - Each device has *device_clean* script
- Includes label in TCP packets in a trusted solaris domain
  - TSIX, CIPSO, RIPSO also supported
  - Min/max/default labels defined for data to/from different hosts

Try it!

- Trusted Solaris x86 licensed to CERIAS
  - Source available to U.S. citizens
- Available for experimentation/research
  - Talk to Randy Bond or Prof. Spafford if interested