
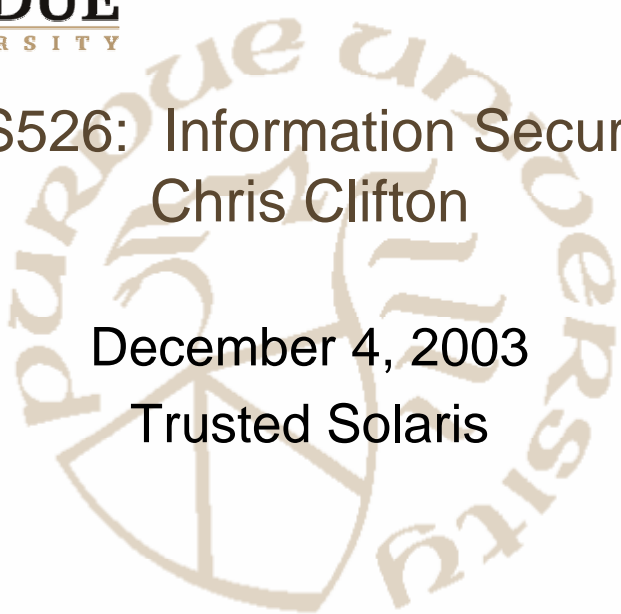



**PURDUE**  
UNIVERSITY

CS526: Information Security  
Chris Clifton

December 4, 2003  
Trusted Solaris




Center for Education and Research  
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

CS526, Fall 2003 2



## 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

CS526, Fall 2003

3




## 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

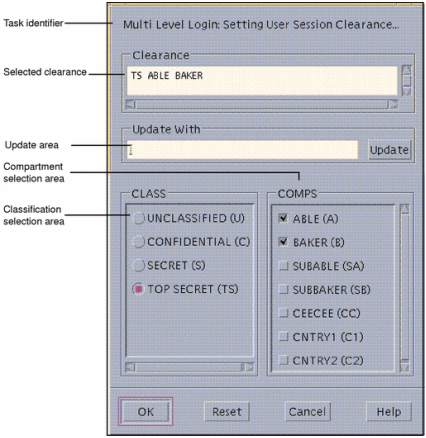
CS526, Fall 2003

4



# MAC example

---



(a) User's View While at C A B label

```


graph TD
    Root["/myHomeDir (MLD)"]
    Root --- SLD0["/SLD.0 (for C A B)"]
    Root --- SLD1["/SLD.1 (for S A B)"]
    Root --- SLD2["/SLD.2 (for TS)"]
    SLD0 --- file1["file1"]
    SLD1 --- file2["file2"]
    SLD1 --- file3["file3"]
    SLD2 --- file4["file4"]
    
```

(b) User's View While at S A B label

```

graph TD
    Root["/myHomeDir (MLD)"]
    Root --- SLD0["/SLD.0 (for C A B)"]
    Root --- SLD1["/SLD.1 (for S A B)"]
    Root --- SLD2["/SLD.2 (for TS)"]
    SLD1 --- file1["file1"]
    SLD1 --- file2["file2"]
    SLD1 --- file3["file3"]
    SLD2 --- file4["file4"]
    
```

CS526, Fall 2003 5



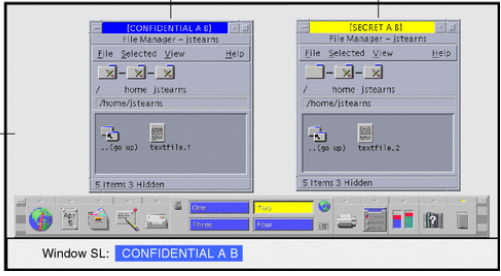
# Cut/Paste Dialog

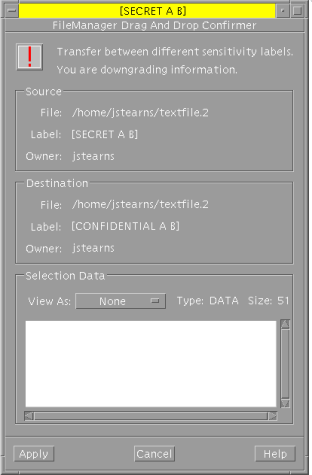
---

File Manager at Workspace One sensitivity label

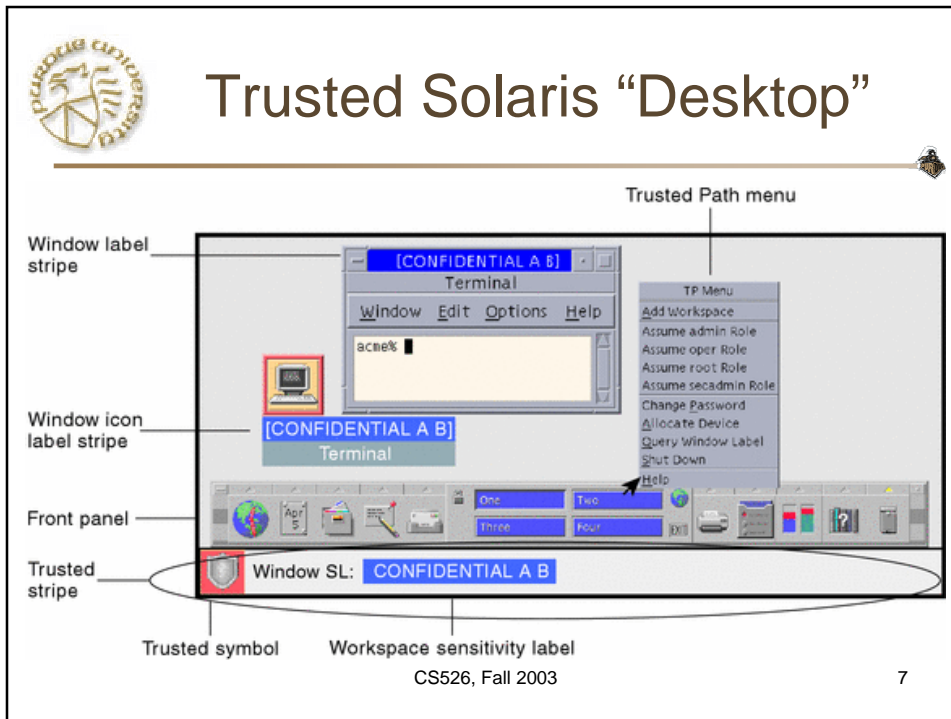
File Manager at Workspace Two sensitivity label

Workspace One





CS526, Fall 2003 6

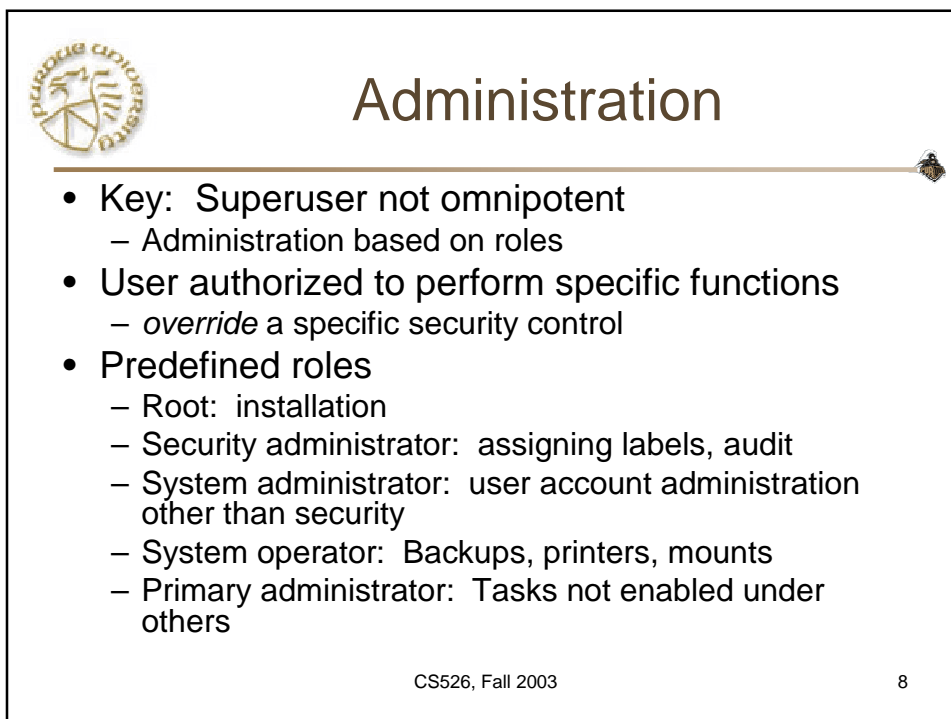


The screenshot shows a Solaris desktop environment with a terminal window titled "[CONFIDENTIAL A B] Terminal". The terminal displays the prompt "acme%". A "Trusted Path menu" is open, showing options like "Add Workspace", "Assume admin Role", "Assume oper Role", "Assume root Role", "Assume secadmin Role", "Change Password", "Allocate Device", "Query Window Label", "Shut Down", and "Help". The desktop includes a front panel with icons for "One", "Two", "Three", and "Four". A "Trusted stripe" is visible at the bottom left, containing a "Trusted symbol" (a shield) and a "Workspace sensitivity label" that reads "Window SL: CONFIDENTIAL A B".

Annotations in the image include:

- Window label stripe
- Window icon label stripe
- Front panel
- Trusted stripe
- Trusted symbol
- Workspace sensitivity label
- Trusted Path menu


CS526, Fall 2003 7



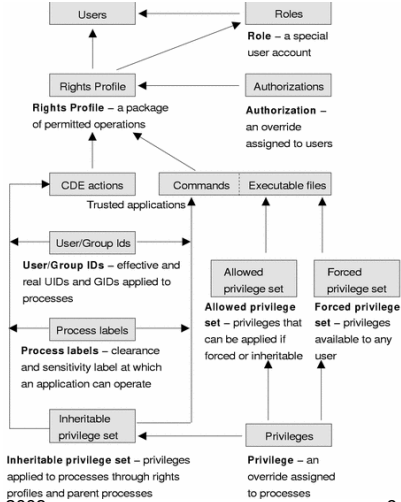
## Administration

- 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

CS526, Fall 2003 8




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



The diagram illustrates the security architecture. At the top, 'Users' and 'Roles' are linked. 'Roles' is defined as a special user account. 'Rights Profile' (a package of permitted operations) and 'Authorizations' (an override assigned to users) are linked to 'Users'. Below, 'CDE actions' (Trusted applications) and 'Commands' (Executable files) are linked to 'Rights Profile'. 'User/Group ids' (effective and real UIDs and GIDs applied to processes) and 'Process labels' (clearance and sensitivity label at which an application can operate) are linked to 'CDE actions'. 'Inheritable privilege set' (privileges applied to processes through rights profiles and parent processes) and 'Privileges' (an override assigned to processes) are linked to 'User/Group ids'. 'Allowed privilege set' (privileges that can be applied if forced or inheritable) and 'Forced privilege set' (privileges available to any user) are linked to 'Privileges'. 'Allowed privilege set' and 'Forced privilege set' are linked to 'Commands'.

CS526, Fall 2003 9



## 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.

CS526, Fall 2003 10



## 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 Enterprise™ 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.

CS526, Fall 2003

11



## 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.

CS526, Fall 2003

12



## 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.

CS526, Fall 2003

13



## Rights Profiles

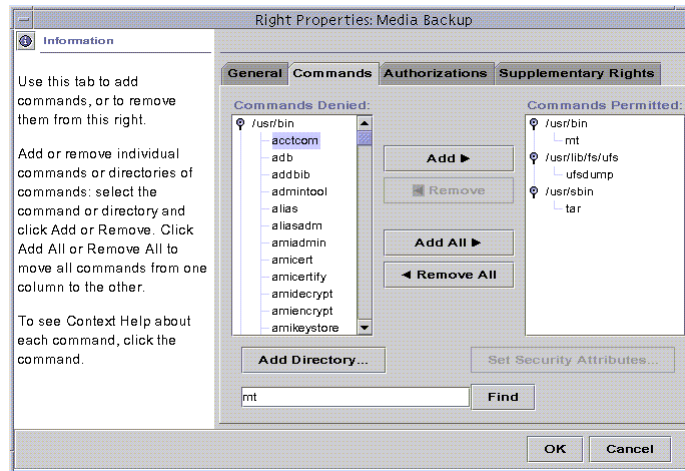
- **SSP Administration** Tools for administering the SSP.
- **SSP Installation** Tools for installing the SSP.
- **System Administrator** Contains subordinate rights profiles for system administrator role.
- **User Management** For creating and modifying users but without the ability to modify self (as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

CS526, Fall 2003

14



## Defining New Rights



CS526, Fall 2003

15



## 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

CS526, Fall 2003

16



## 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

CS526, Fall 2003

17



## Types of Privileges

### Type

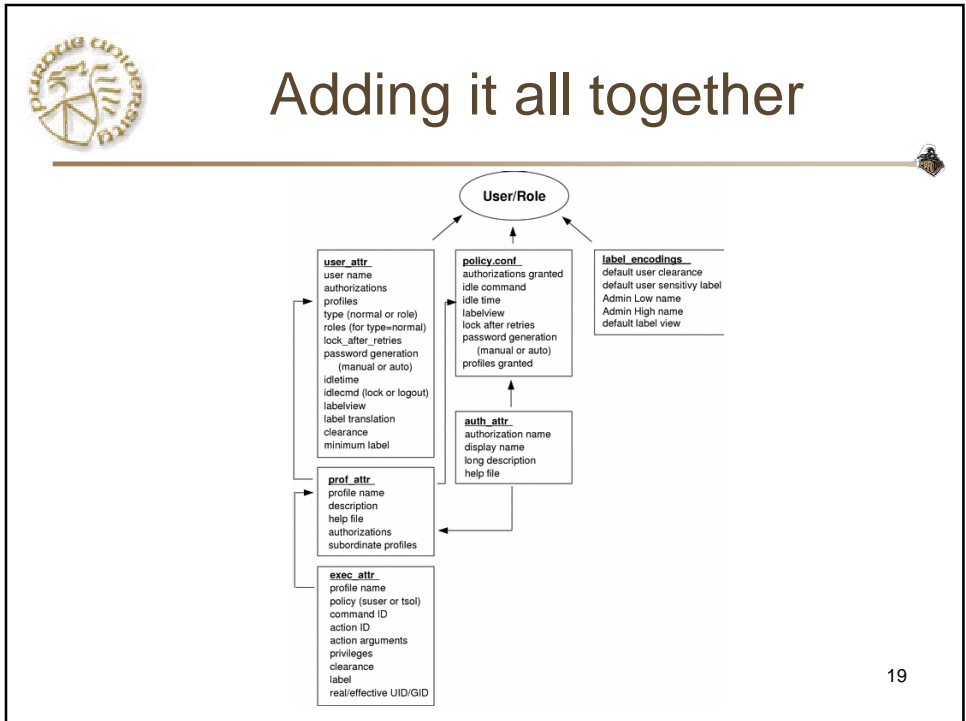
- File system security
- System V Interprocess Communication (IPC) security
- Network security
- Process security
- System security
- Window security

### Example

- `file_dac_chown` - Lets a process change the owner user ID of a file.
- `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
- `net_broadcast` - Lets a process send a broadcast packet on a specified network
- `proc_mac_read` - Lets a process read another process where the reading process label is dominated by the other process label
- `sys_boot` - Lets a process halt or reboot a Trusted Solaris computer
- `win_selection` - Allows a process to request inter-window data moves without the intervention of selection arbitrator

CS526, Fall 2003

18



**System Management Console**

Menu bar ———

Tool bar ———

Location bar ———

Navigation pane ———

View pane ———

Information pane ———

Information pane toggles ———

Status bar ———

CS526, Fall 2003

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

CS526, Fall 2003

21



## 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

CS526, Fall 2003

22