Oracle Trusted Extensions & GNOME 3 Migration

August 6, 2011

Brian Cameron
Desktop Software Engineer
Solaris Desktop Group

Oracle Solaris Trusted Extensions

What is Solaris Trusted Extensions?

Integrated into Solaris

- Labeled Security for Solaris
- Mandatory Access Control based on labels

Benefits

- Isolate data based on its sensitivity
- Regulate network data flow easily
- Comply with data privacy legislation

Trusted Solaris History

- 1990, SunOS MLS 1.0
  - Conformed to TCSEC (1985 Orange Book)
- 1992, SunOS CMW 1.0
  - Compartmented-mode workstation requirements
  - Release 1.2 ITSEC certified for FB1 E3, 1995
- 1996, Trusted Solaris 2.5
  - ITSEC certified for FB1 E3, 1998
- 1999, Trusted Solaris 7
- 2000, Trusted Solaris 8
  - Common Criteria: CAPP, RBACPP, LSPP at EAL4+
  - Updates to Trusted Solaris 8 also re-certified
- 2006, Solaris 10 11/06 with Trusted Extensions
  - Common Criteria: CAPP, RBACPP, LSPP at EAL4+, 2008
  - Assurance Continuity for Solaris 10 5/08 and 5/09
  - http://www.sun.com/software/security/securitycert/
- **2011, Solaris 11 with Trusted Extensions**

What is Labeling?

- Every object has a label associated with it.
  - Files, windows, printers, devices, network packets, network interfaces, processes, etc...
- Labels have hierarchical or disjoint relationships.
- Accessing or sharing data is controlled by the objects' label relationship to each other.
  - Reading requires label dominance.
    - Reader's label ≥ objects label
  - Writing requires label equality for the subject and object.

What Gets Labeled?

Explicitly Labeled

- Users and Roles
- Zones
- Hosts and Networks
- ZFS datasets
- X11 Windows
- GNOME Workspaces

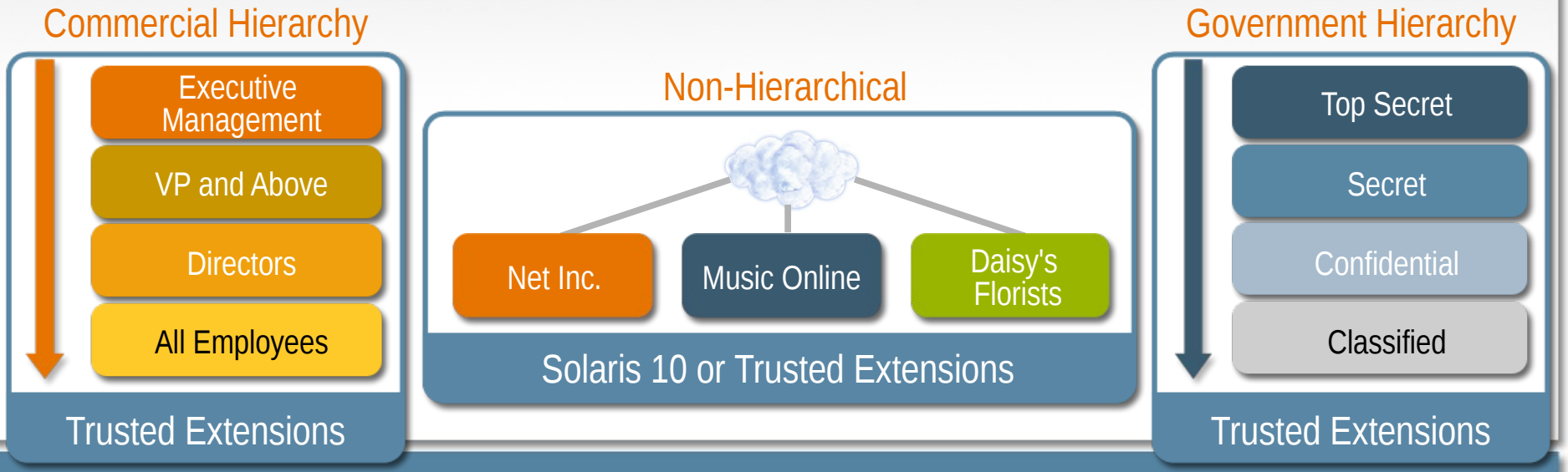
Implicitly Labeled

- Processes
- Files and directories
- Devices
- Sockets
- System V IPCs
- Pixels

- Only zones must be explicitly labeled.
- All other resources have default values.

Solaris Trusted Extensions

- All objects are labeled, based on sensitivity.
- Access governed by label hierarchical relationship.

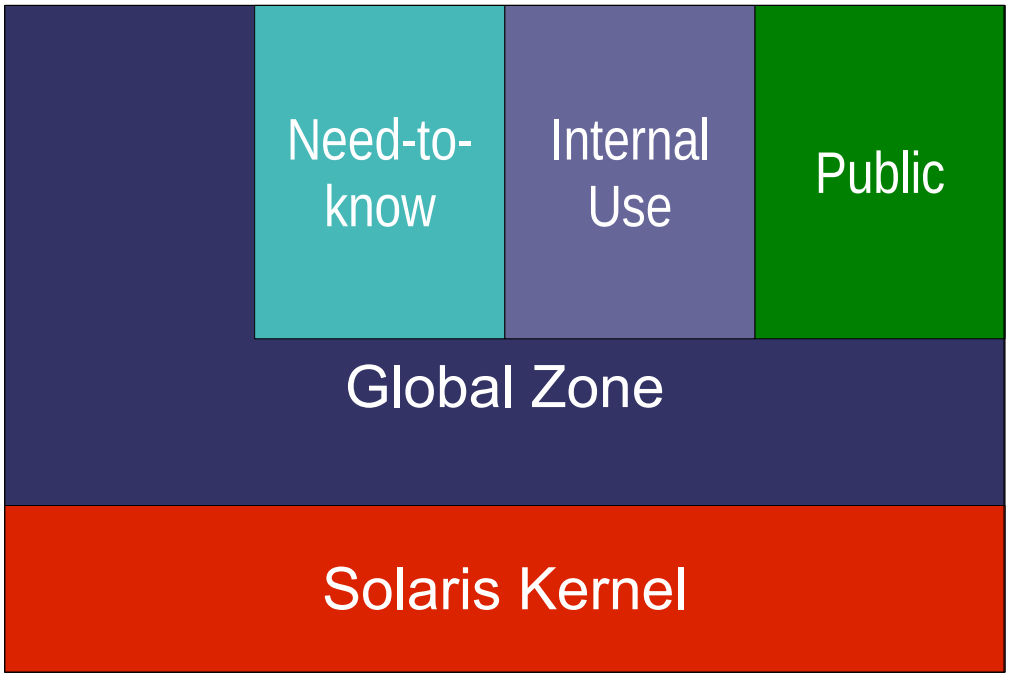


Mandatory Access Control & Security Labels

Labeled Zones in Trusted Extensions

- Each zone provides a security boundary.
  - Unique sensitivity label per zone.
  - Labels are implied by process zone ID's.
  - Processes and data are isolated by label.
- No object is writable by more than one zone.
  - Mount policy prevents writing down or reading up.
  - Network policy requires endpoint label equality (default).
- Information sharing between zones is based on label relationships.

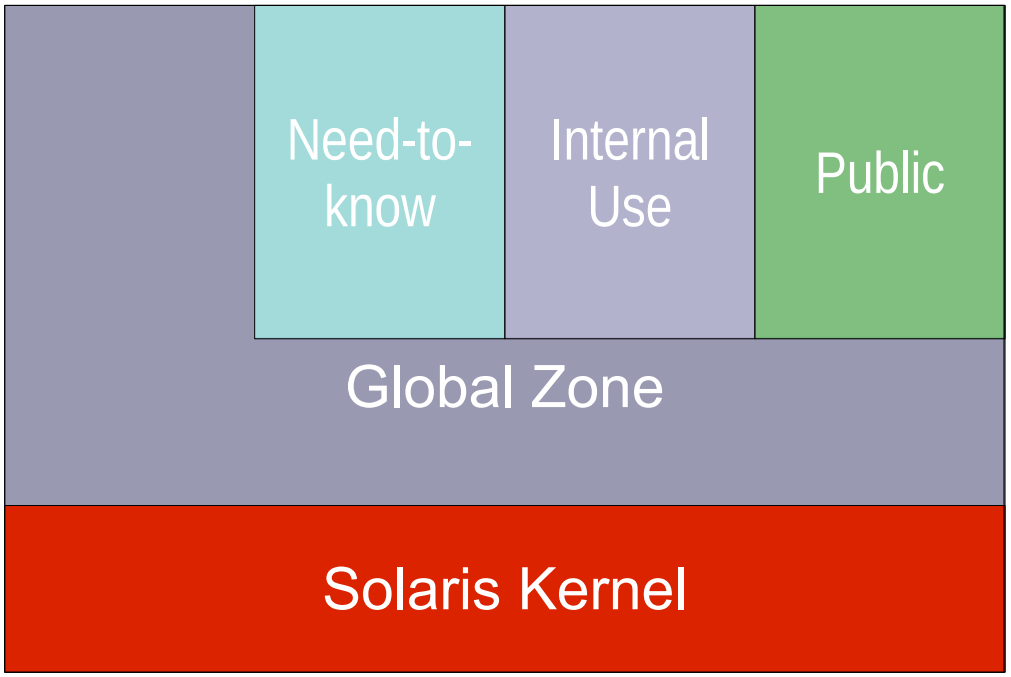
Multilevel Architecture



SPARC, x86 or x64 Hardware
Local or Sun Ray display

- Layered architecture implements:
  - Mandatory access control
  - Hierarchical labels
  - Principle of least privilege
  - Trusted path
  - Role-based access

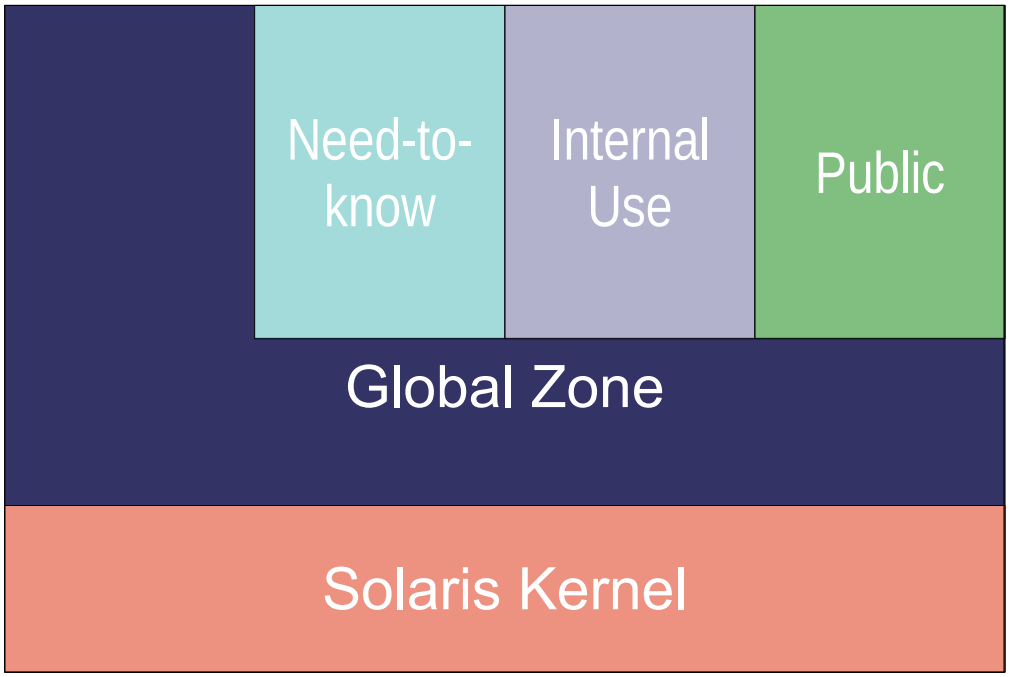
Solaris Kernel Services



SPARC, x86 or x64 Hardware
Local or Sun Ray display

- Multilevel Networking
- Filesystem mount policy
- Containment (zones)
  - Processes
  - Devices
  - Resource Pools

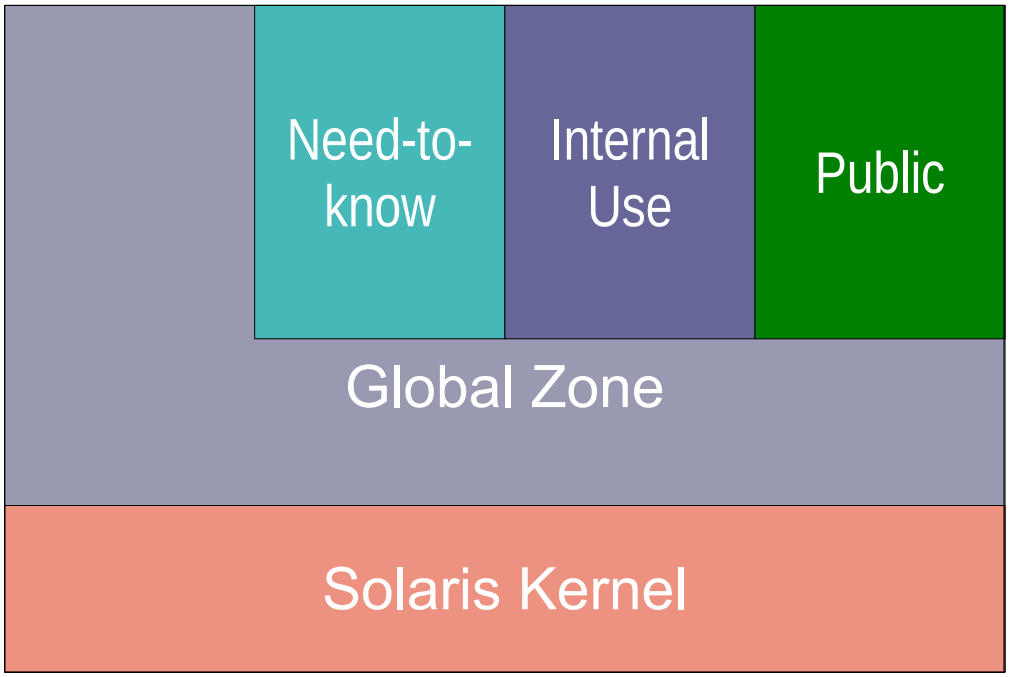
Multilevel Services



SPARC, x86 or x64 Hardware
Local or Sun Ray display

- Label Policy Administration
- Labeled Printing
- File Sharing
- Auditing
- Device Allocation
- Labeled Windows
- Single Sign-on

Single Level Applications



SPARC, x86 or x64 Hardware
Local or Sun Ray display

- Databases
- Web Servers
- Windows Remote Desktop
- Firefox
- OpenOffice
- Nautilus

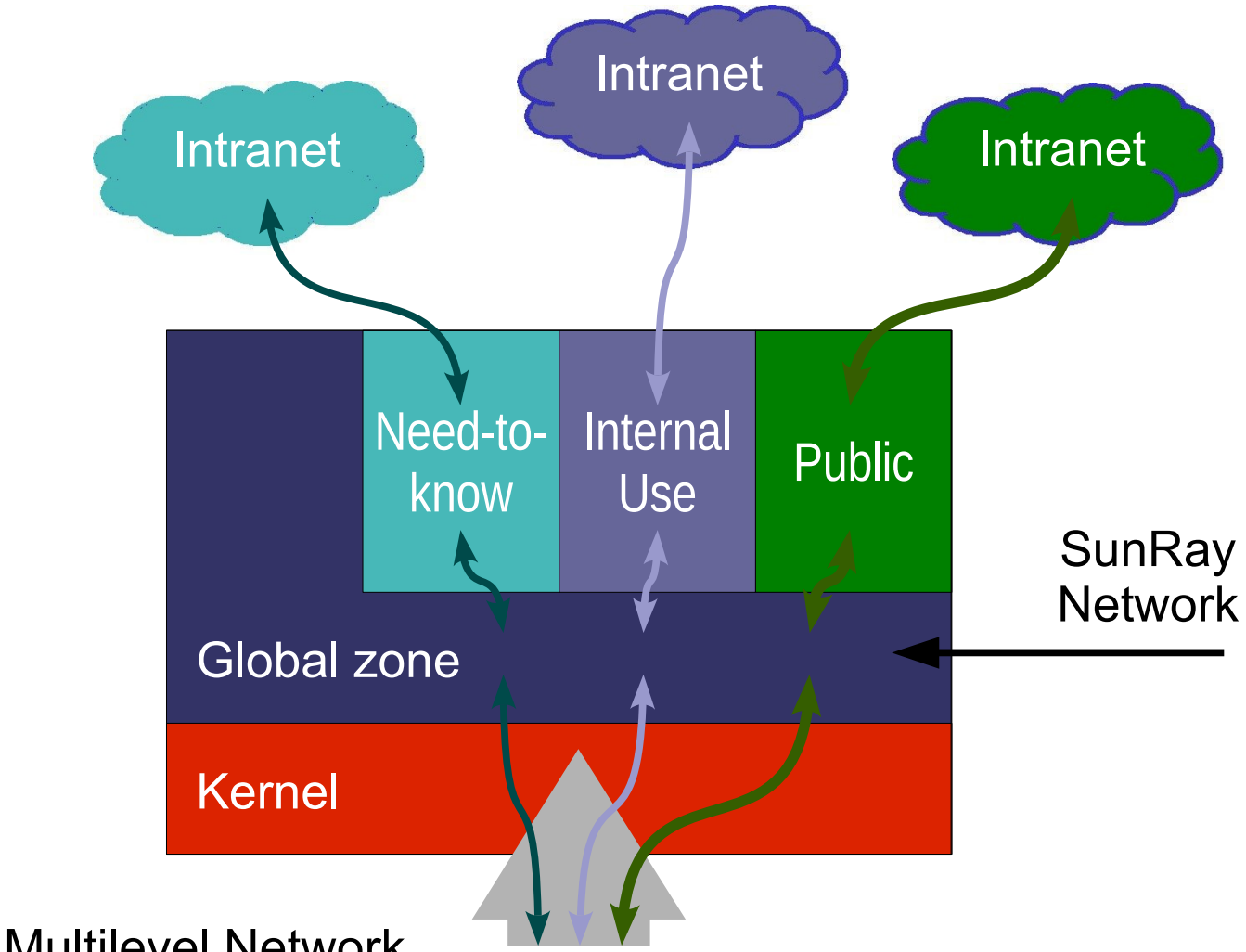
Robustness of Global Zone Policies

- Access restricted to authorized roles.
  - Roles must be assumed by authorized users.
  - Roles must be cleared to highest label.
  - Role assumption must be done via Trusted Path.
    - Mutual trust established via CIPSO protocol.
    - IPSec can be used to enhance trust and privacy.
    - No remote access by default.
- Access to labeled zones requires use of privilege.
  - Labeled zone mount points not traversable.
  - Labeled zone processes not accessible.

Robustness of Labeled Zone Policies

- Label and privilege limits configured in global zone.
- No privilege escalation beyond zone's limit set.
- No MAC policy overrides in labeled zones.
- No escape from labeled zones.
- No user access to global zone.

Labeled Networking



Single and Multilevel Ports

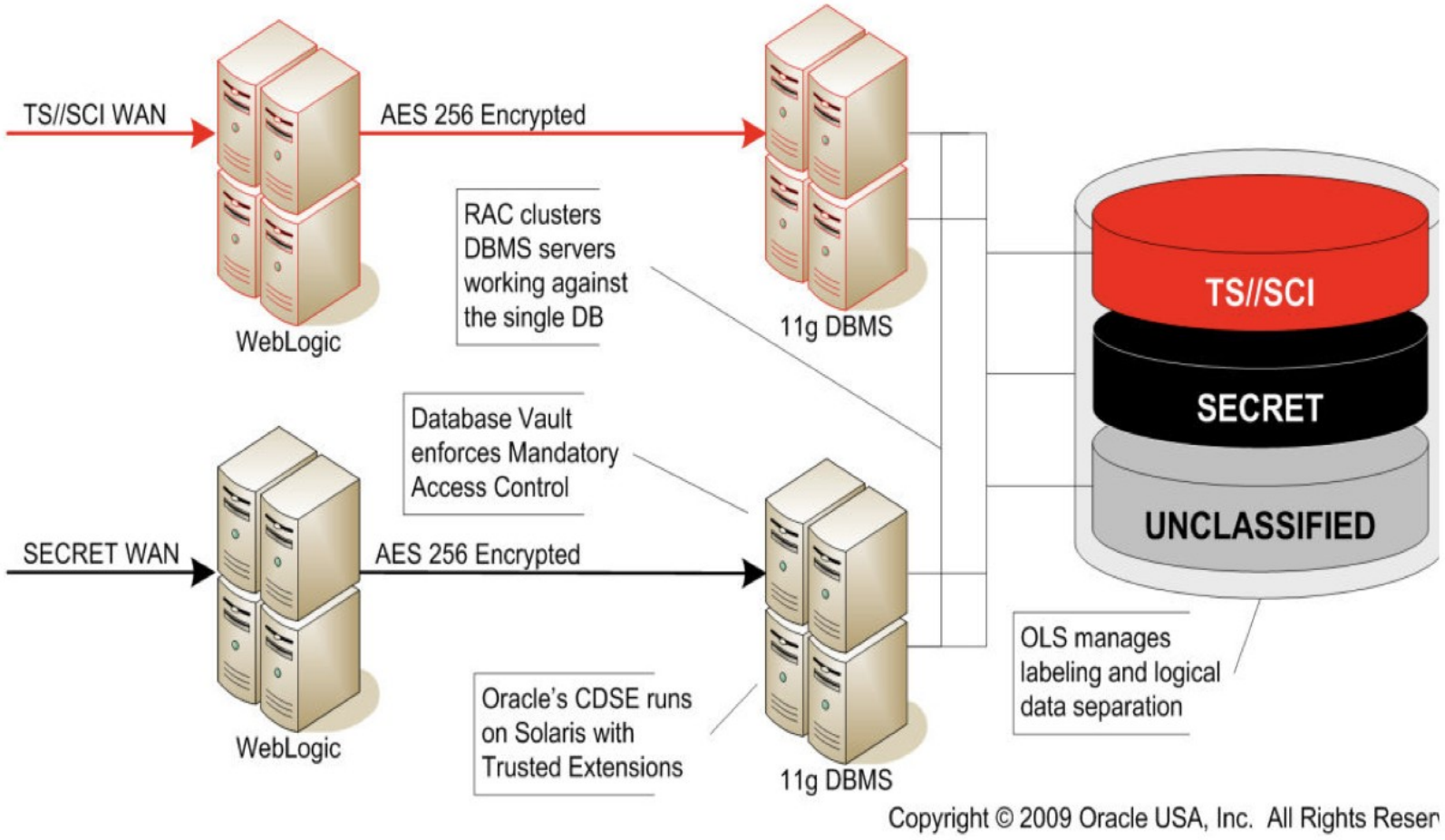
- Kernel maintains cache of labels and endpoints.
  - Implicit labels based on IP address or Network.
  - Explicit labels based on CIPSO label in packet.
- Packets are routed to hosts and zones by label matching rules.
  - Generally label equality required between endpoints.
  - Multilevel ports accept labels within range or set.
  - For NFS operations, read-down is supported.
    - Sockets are marked with special socket attribute.
    - Unique binding of port, label, and IP address.

Filesystem MAC policies

- Labels derived from a filesystem owner's label.
- Mount policy is always enforced.
  - No reading-up
    - Read-write mounts require label equality in labeled zones.
  - Reading-down
    - Read-only mounts require dominance by client.
    - Can be restricted via zone's limit set and network label range.
  - Writing-up
    - Cannot write-up to regular files.
    - Limited write-up to label-aware services (via TCP and doors).
  - Writing-down
    - Restricted to privileged label-aware global zone services.

Trusted Extensions Configurations

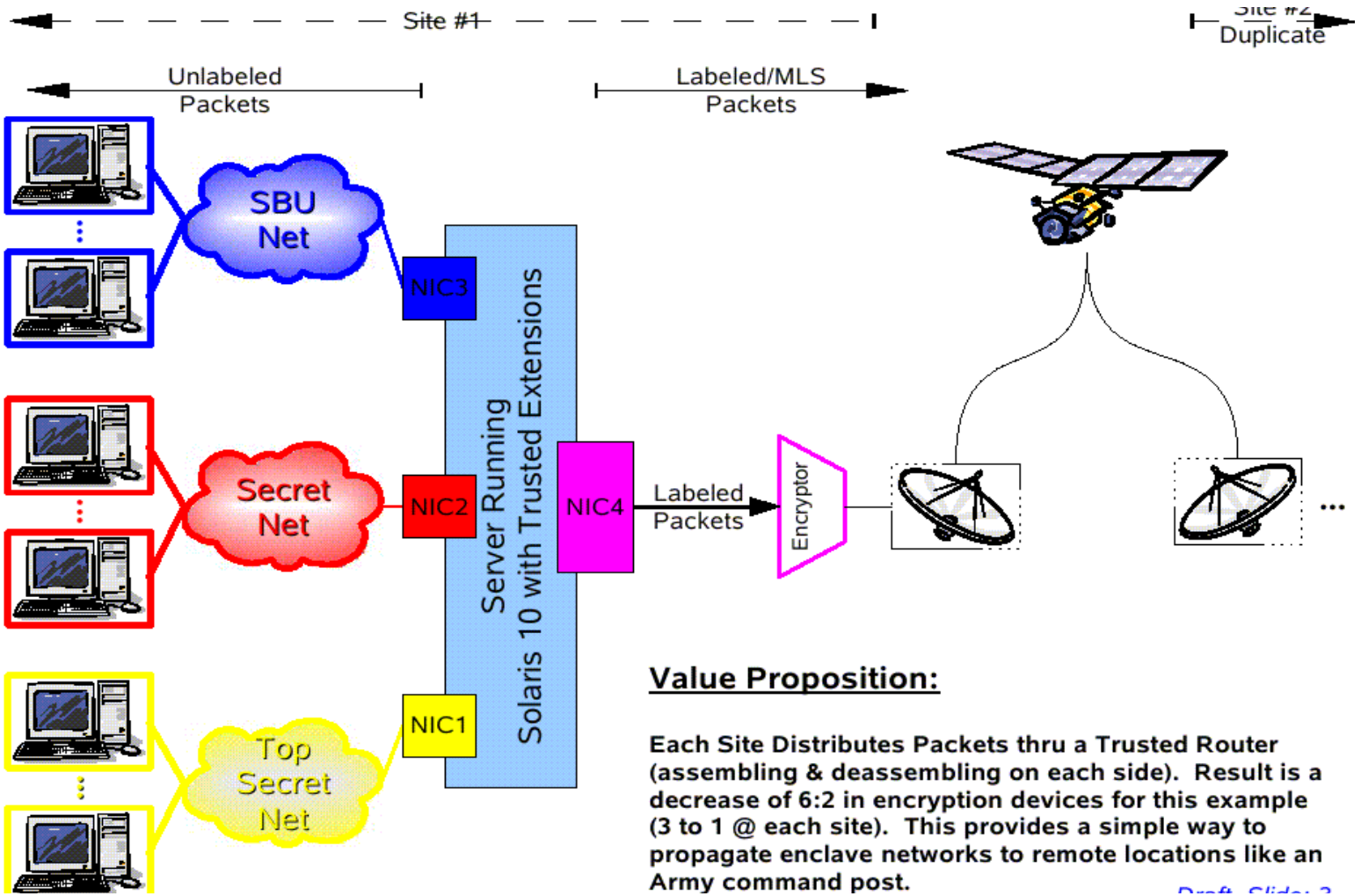
Oracle Cross-Domain Security Express



Oracle Cross-Domain Security Express

- Oracle's cross-domain solutions requires Solaris Trusted Extensions.
- DCID 6/3 PL4 Certified and Accredited.
- Labeled zones provide strong separation between clients on separate networks.
- Multilevel databases using Oracle Label Security benefit from the Common Criteria Certification of Trusted Extensions at EA4+ for LSPP and RBAC.

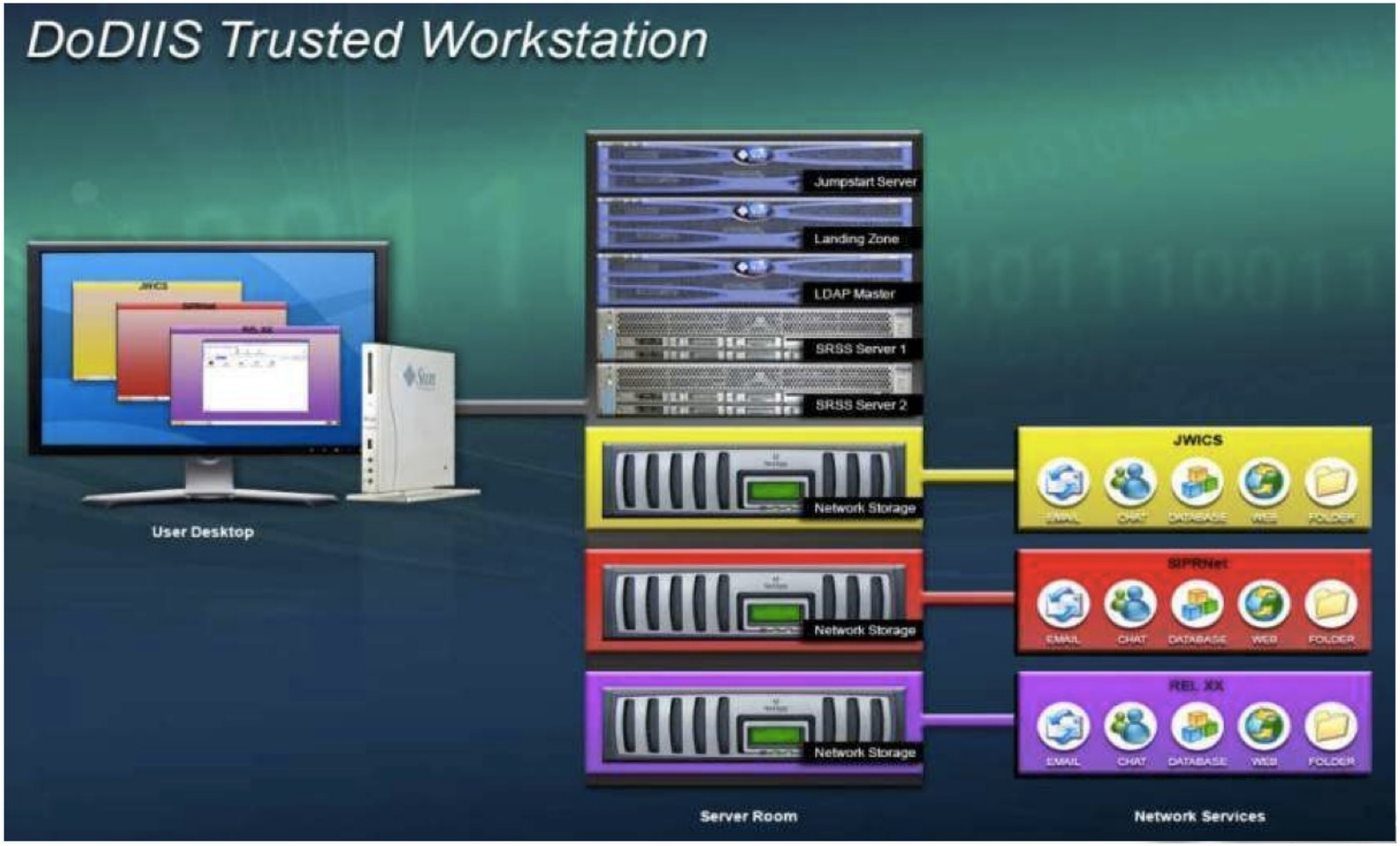
Labeled Routing



Value Proposition:

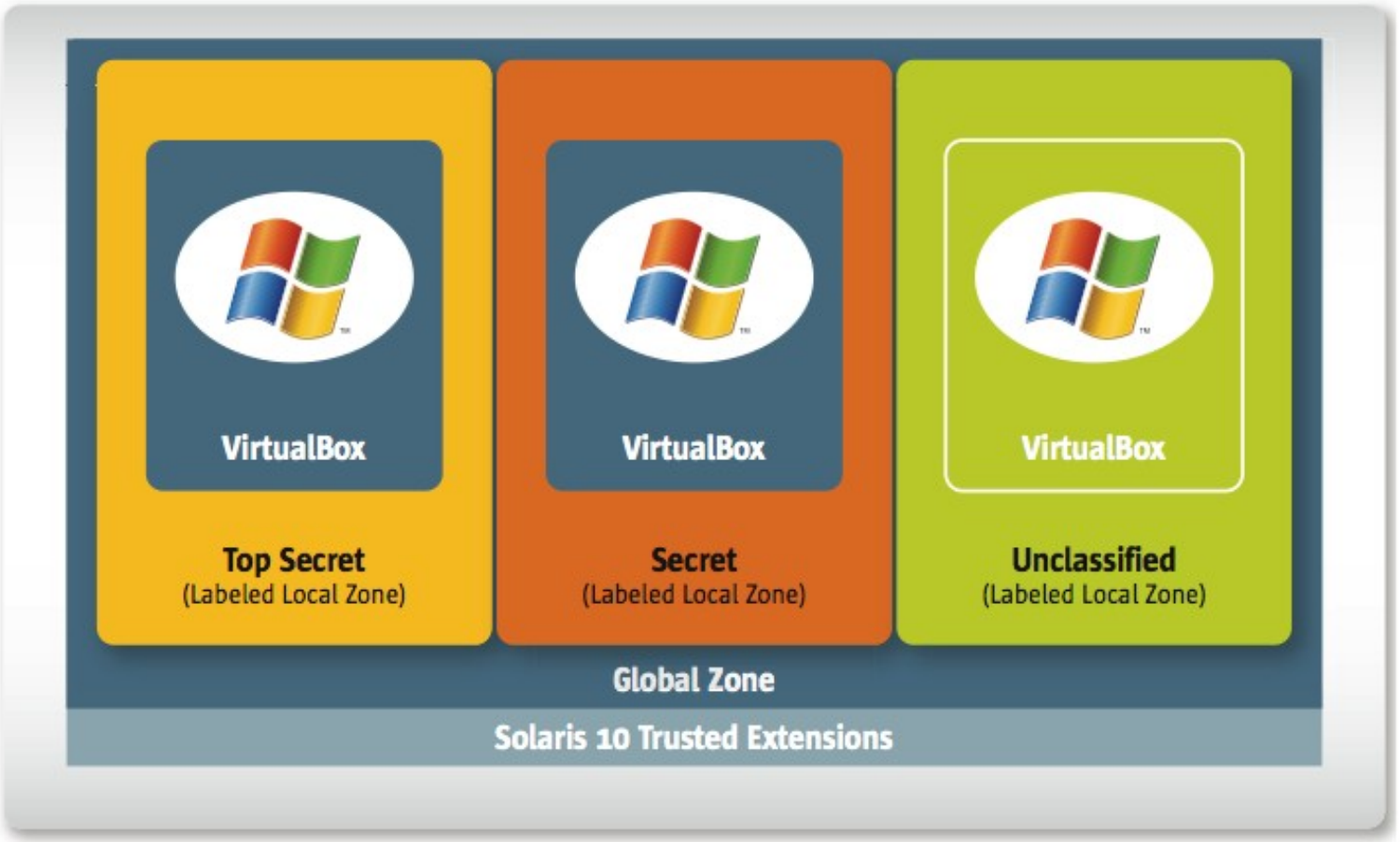
Each Site Distributes Packets thru a Trusted Router (assembling & deassembling on each side). Result is a decrease of 6:2 in encryption devices for this example (3 to 1 @ each site). This provides a simple way to propagate enclave networks to remote locations like an Army command post.

Multilevel Thin Client Solution



DTW 4.1 is included in latest UCDMO Baseline
http://www.ucdmo.gov/conference09/Durante_DTW_09012009.pdf

Labeled Virtual Machines



Trusted Extensions and GNOME

Trusted Solaris GNOME Features

- GNOME 2 has been customized via patches to support a number of unique features:
  - Some parts of GNOME run in the global zone: gnome-session, sysadmin programs, screen lock, gnome-panel, and panel applets.
    - Programs that run in the global zone are controlled by placing desktop files in a special Trusted directory, or are hardcoded to run in the zone (e.g. gnome-session and gnome-panel).
    - Some of these programs do not need to run in the global zone. Further enhancements would be needed to support the panel and applets running in different zones, for example.
  - Most applications run in the labeled zone associated with the workspace.
  - (Continued on next slide)

Trusted Solaris GNOME Features (con't)

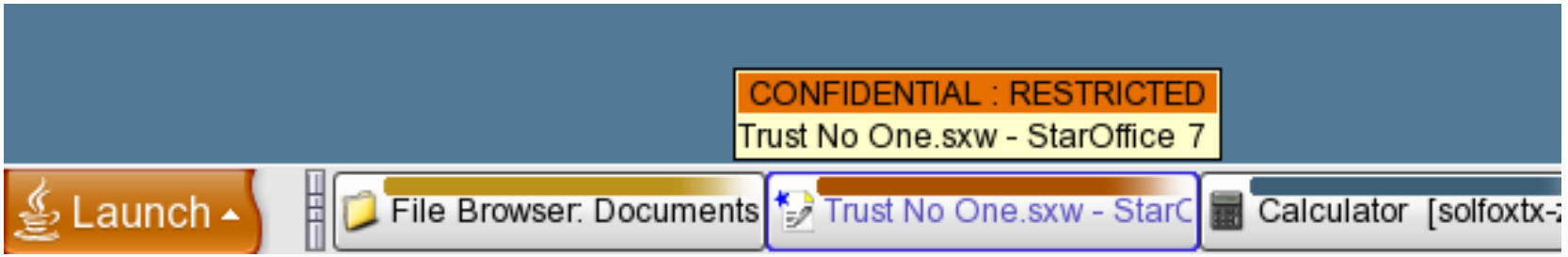
- Solaris role and zone awareness: workspaces and windows are associated with a unique role and zone; identified by unique colors and labels.
- RBAC awareness. Only programs that the user can run are shown in the menus, such as in the panel menu.
- Trusted Path features - An X11 Trusted extension is used to tighten X security.
  - Works with the Trusted Stripe to indicate when the user is in the Trusted Path when the lock screen is showing.
  - Better enforces how grabs are managed. Better grab support helps to avoid grab issues with the lock screen program, for example.
  - Copy/Paste access control. No copy/paste across boundries.
- The Trusted Stripe, see next slide.

Trusted Java Desktop System Details

Only labeled GNOME-based interface shipped with an OS

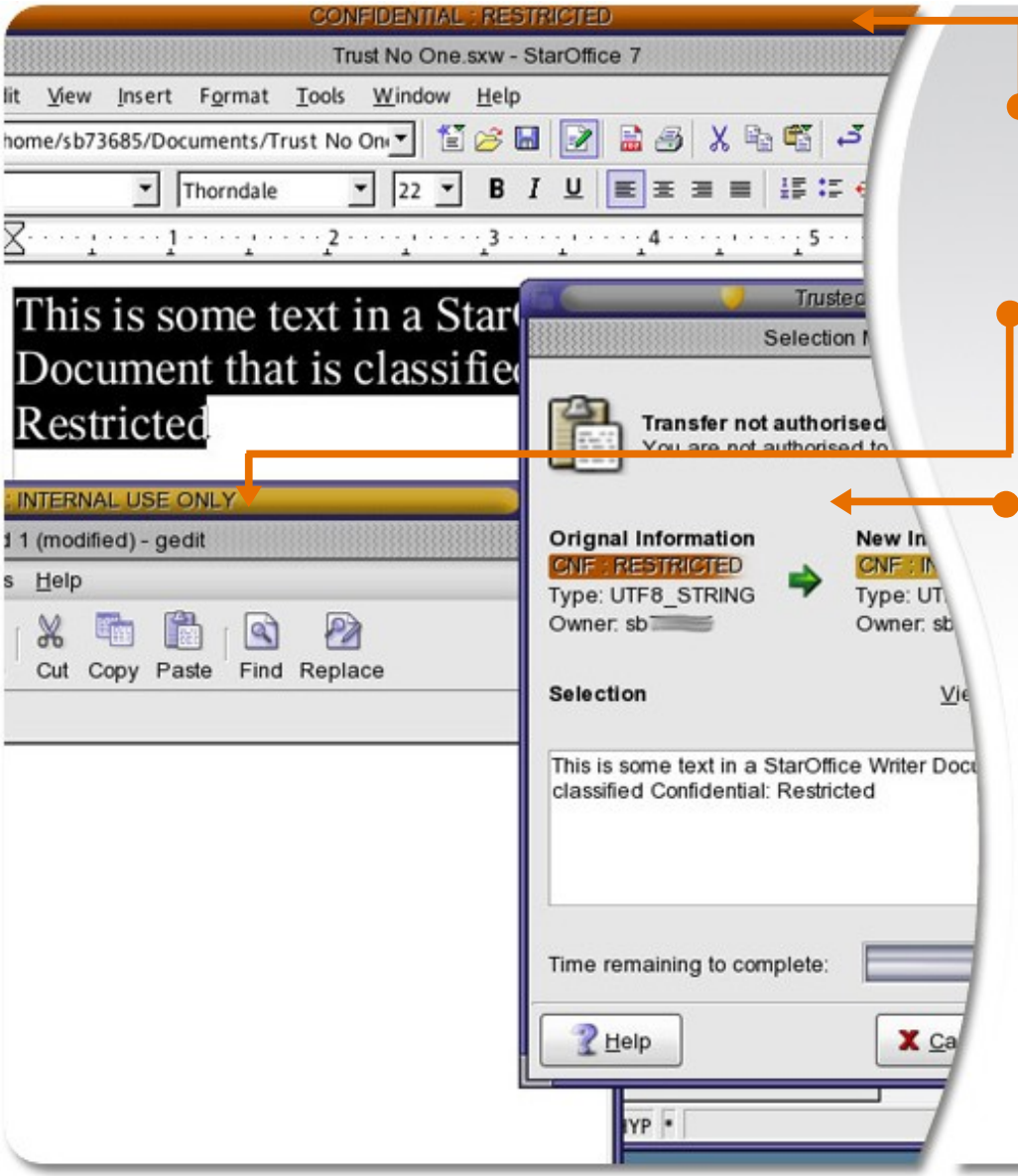
Workplace Switcher

Task Switcher



Trusted Stripe and Trusted Path Menu

Access Control Enforced Everywhere



Stripe showing 'Restricted'

Stripe showing 'Internal'

Attempts to 'drag-and-drop' data between windows fails because user is not authorized to do so.

Enforced when transferring data anywhere to anything on the system.

GNOME 3 Porting Issues

- GNOME Shell vs. GNOME 3 Fallback
  - Solaris Trusted Extensions is typically deployed on Sun Rays, which do not support OpenGL. Therefore, it makes sense to initially port Solaris Trusted Extensions to work with GNOME 3 Fallback mode.
  - There could be value in making Solaris Trusted Extensions work with GNOME Shell.
  - GNOME Shell and GNOME 3 Fallback mode use different workspace switching and window management mechanisms, which means porting Solaris Trusted Extensions to GNOME Shell would require significant rework.
  - Our work so far shows that porting Solaris Trusted Extensions code and patches to GTK3 will require a significant amount of work.
  - The GNOME panel and applets in GNOME 3 Fallback mode have been reworked, so the porting effort will be non-trivial.

GNOME 3 Porting Status

- Over the past month, GNOME Shell and GNOME 3 Fallback mode have been ported to work on Solaris.
- It works well on both standalone desktops and GNOME 3 Fallback mode works well on Sun Rays.
- 10 of the 20 patches required to make GNOME 3 Fallback mode work with Solaris Trusted Extensions have already been ported.
- Likewise, some patches to make GNOME 3 Fallback mode work well with Sun Ray have not yet been ported. For example, configuration tweaks that need to be ported from using GConf to GSettings.

Opportunities to Collaborate

- All Solaris Trusted Extensions code is free software released under GPL licensing.
- Many features of Solaris Trusted Extensions are generally useful.
  - Labeled workspaces and windows.
  - Hooks for running GNOME in environments where the desktop and applications run in different environments, such as zones.
  - More sophisticated window switching features, such as more rich libwnck signals.
- If there is interest within the GNOME community, we could collaborate to provide support for such features upstream.
  - Efforts were made by Sun in the early GNOME 2 release cycle to collaborate in this area, but there was not much interest.


Q&A