Solaris Security and Trusted Extensions Architecture

Glenn Faden

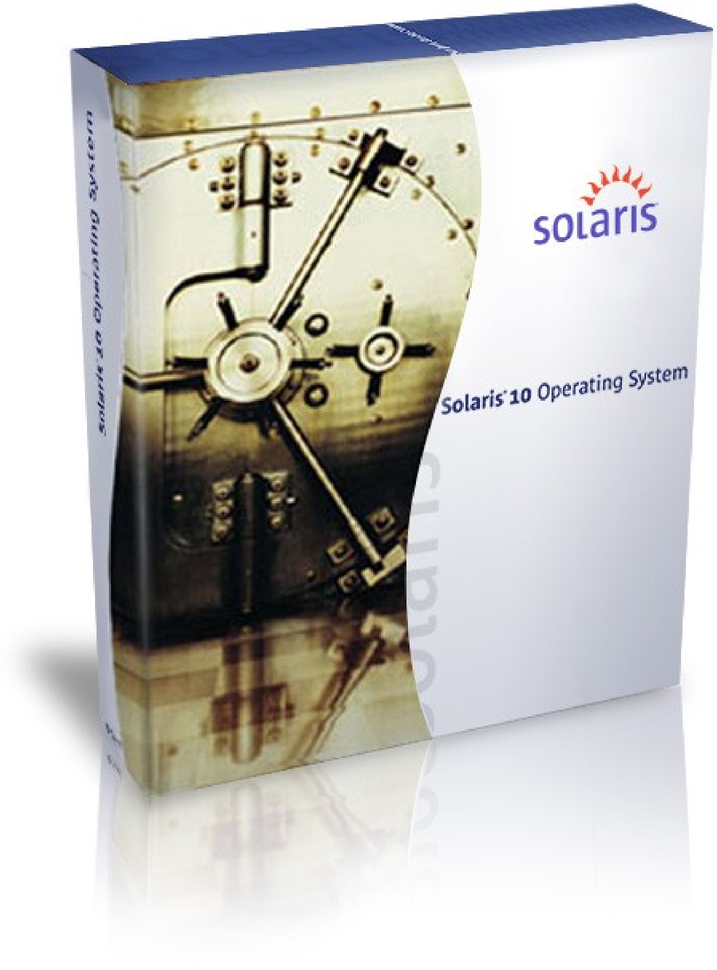
Solaris Security

Sun Microsystems, Inc.

Agenda

- Solaris 10 Security
- Trusted Extensions
- Desktop Examples
- Q & A - Anytime

Secure Foundation of Dramatic Improvements



Solaris 10 Security

Digital Certificates Everywhere

Secure Execution*

User Rights Management

Process Rights Management

Cryptographic Framework

IPFilter

Kerberos Single Sign On

Secure By Default*

* Coming in future update

Network Protection

- IP Filter firewall
  - > Sun supported stateful firewall
  - > Allows selective access to ports based on IP addr.
  - > Compatible/manageable like open source IPF
- TCP Wrappers
  - > Limit access to TCP/UDP service by domain name
- Limiting Networking Services
  - > Reduced Networking MetaCluster – Ultra small Solaris
  - > Generic Limited Networking Service Profile
    - > Will be enhanced in Solaris 10 update to include better 'out-of-the-box' security, full function desktop and no exposed network svcs

Remote Access and Auditing

- Solaris Secure Shell
  - > Standards-based encrypted remote access
- Kerberos Single Sign On
  - > Standards-based enterprise single sign on
  - > Optional encryption of NFSv3 and NFSv4 file shares
- IPSec/IKE
  - > Transparently encrypted communications
- Auditing of activities
  - > Audit records for all activities track users and roles
  - > Output in XML format for parsing and analyzing
  - > Centralized auditing and per-container audits

Cryptographic Framework

- Extensible cryptographic interfaces.
  - A common kernel and user-land framework for providing and using cryptographic functionality.
  - A common interface for cryptographic functions whether completed in hardware or software.
  - Extensible framework for vendors to provide custom functionality.
- By default, supports major algorithms.
  - Encryption: AES, RC4, DES, 3DES, RSA
  - Hashing: MD5, SHA-1
  - MAC: DES MAC, MD5 HMAC, SHA-1 HMAC
  - Optimized for both SPARC, Intel and AMD

Encrypted File Systems

- Loopback-based*
  - One physical file on disk, contents encrypted
  - Mounted as file system via loopback
  - **No** application modification required
  - Works with NFS & local file sharing
  - Early update of Solaris 10
- ZFS Module for Encryption*
  - ZFS offers modular structure for enhancements
  - Would encrypt a full ZFS file system on disk
  - No application modification required
  - All other aspects of management preserved

* Future feature releases

File Integrity and Secure Execution

- BART – Basic Audit and Reporting Tool
  - > Checksums compared periodically against known good list of files that customer generates
  - > Can be used with Sun-supplied Fingerprint Database
- Solaris Secure Execution
  - > Almost all applications are signed in Solaris 10
  - > Sys-admins can manually verify them today
  - > Future update will verify integrity at load time
    - > Customers can sign their own files, or 3rd party
    - > Can customize EXACTLY which apps can be run on whole system, preventing ANY unauthorized app from running
  - > Coming in future Solaris Update*

Network Service Hardening & Minimization

- Enhanced Limited Networking Profile
  - > Turns off many services or sets them to 'local only'
  - > Uses Solaris Service Manager for per-service config
  - > Full desktop, Web, Email, NFSv4 browsing with only Secure Shell listening to the network
  - > Install time choice presented to users
    - > OS upgrades preserve existing configuration
  - > Coming in Solaris 10 11/06*
- Reduced Networking Install
  - > Absolutely minimized Solaris install w/No networking!
  - > Basic building block for a secured system
  - > Available in Solaris today

Process and User Rights Management

Principle of Least Privilege

- In traditional UNIX, root is an all-or-nothing proposition
  - Any privileged program can compromise the whole system
- Only a small subset is usually needed
  - Bind to reserved port
  - Change scheduling priority
- So, we divide root's powers into discrete privileges

Solaris Privilege Overview

- Kernel always checks for privilege, not uid 0
- Individual privileges can be switched on and off
  - > Run with a limited subset of root's powers
  - > Can make processes less privileged than normal
- Backward compatible with superuser model
- Extensible
  - > Number of privileges and mapping of privilege names is private to the kernel
- Integrated with User Rights Mgmgt.(RBAC) and Service Management Framework (SMF)

Solaris 10 Privileges

“contract_event”	Request reliable delivery of events
“contract_observer”	Observe contract events for other users
"cpc_cpu”	Access to per-CPU perf counters
"dtrace_kernel"	DTrace kernel tracing
"dtrace_proc"	DTrace process-level tracing
"dtrace_user"	DTrace user-level tracing
"file_chown"	Change file's owner/group IDs
"file_chown_self"	Give away (chown) files
"file_dac_execute"	Override file's execute perms
"file_dac_read"	Override file's read perms
"file_dac_search"	Override dir's search perms
"file_dac_write"	Override (non-root) file's write perms
"file_link_any"	Create hard links to diff uid files
"file_owner"	Non-owner can do misc owner ops
"file_setid"	Set uid/gid (non-root) to diff id
"ipc_dac_read"	Override read on IPC, Shared Mem perms
"ipc_dac_write"	Override write on IPC, Shared Mem perms
"ipc_owner"	Override set perms/owner on IPC
"net_icmpaccess"	Send/Receive ICMP packets
"net_privaddr"	Bind to privilege port (<1023+extras)
"net_rawaccess”	Raw access to IP
"proc_audit”	Generate audit records
"proc_chroot”	Change root (chroot)
"proc_clock_highres"	Allow use of hi-res timers
"proc_exec"	Allow use of execve()
"proc_fork"	Allow use of fork*() calls
"proc_info"	Examine /proc of other processes

"proc_lock_memory"	Lock pages in physical memory
"proc_owner"	See/modify other process states
"proc_priocntl"	Increase priority/sched class
"proc_session"	Signal/trace other session process
"proc_setid"	Set process UID
"proc_taskid"	Assign new task ID
“proc_zone”	Signal/trace processes in other zones
“sys_acct”	Manage accounting system (acct)
“sys_admin	System admin tasks (node/domain name)
"sys_audit"	Control audit system
"sys_config"	Manage swap
"sys_devices"	Override device restricts (exclusive)
"sys_ipc_config"	Increase IPC queue
"sys_linkdir"	Link/unlink directories
"sys_mount"	Filesystem admin (mount,quota)
"sys_net_config"	Config net interfaces,routes,stack
"sys_nfs"	Bind NFS ports and use syscalls
"sys_res_config"	Admin processor sets, res pools
"sys_resource"	Modify res limits (rlimit)
"sys_suser_compat"	3rd party modules use of suser
"sys_time"	Change system time

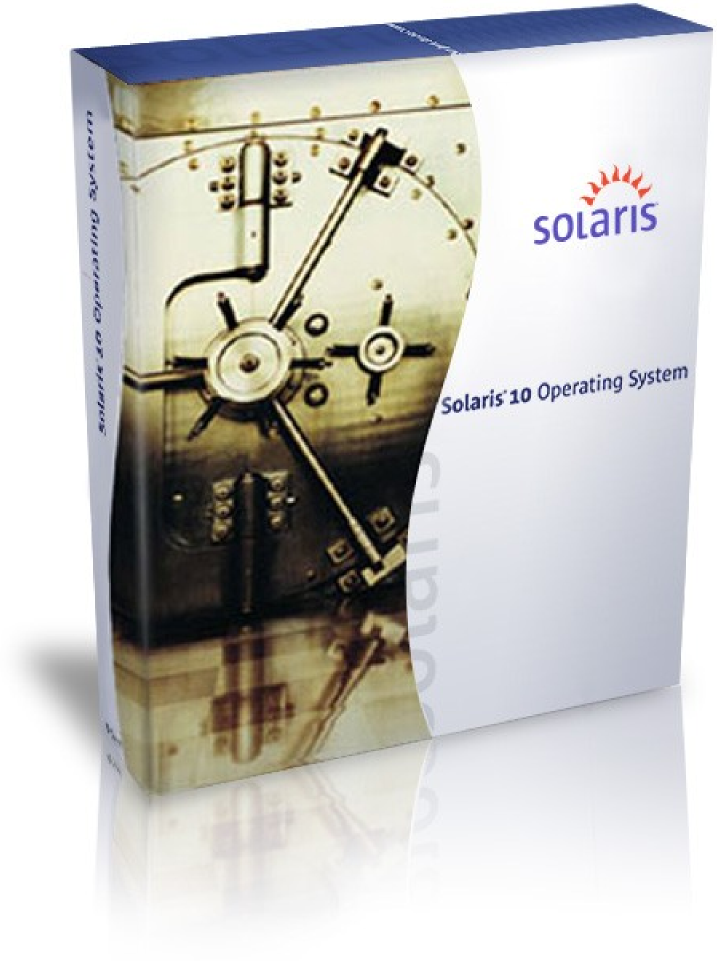
Interesting	Some interesting privileges
Basic	Non-root privileges
Removed	Not available in Zones

Daemons with Reduced Privilege

Standard Solaris 10 now uses privileges

```
$ ppriv -v `pgrep -u daemon`
333:    /usr/lib/nfs/lockd
    E: sys_nfs
    I: none
    P: sys_nfs
    L: all
170:    /usr/sbin/rpcbind
    E: net_privaddr,proc_fork,sys_nfs
    I: none
    P: net_privaddr,proc_fork,sys_nfs
    L: all
331:    /usr/lib/nfs/statd
    E: proc_fork
    I: none
    P: proc_fork
    L: all
338:    /usr/lib/nfs/nfsd
    E: sys_nfs
    I: none
    P: sys_nfs
    L: all
```

Multi-Level Labeled Security



Trusted Extensions

Adds labeled security to Solaris 10

Multi-level networking, printing

Multi-level GUI

Leverages User & Process RM

Uses Containers

Compatible with all Solaris apps

Target of CAPP, RBACPP, LSPP @ EAL 4+

Available November 2006

What is Solaris Trusted Extensions?

- A redesign of the Trusted Solaris product using a layered architecture.
- An extension of the Solaris 10 security foundation providing access control policies based on the sensitivity/label of objects
- A set of additional software packages added to a standard Solaris 10 system.
- A set of label-aware services which implement multilevel security

Goals and Benefits

- Runs all Solaris applications
  - It's still Solaris, with Containers
  - It's still Solaris, just with extended security policy
  - It's still Solaris, same kernel
  - It's still Solaris, all Solaris patches work
- Runs all infrastructure software
  - Backup, Web, middle-ware, dev tools, etc.
  - Database, file systems, devices/drivers, etc.
- Preserve and transition
  - CDE User interface, single and multi-level JDS/GNOME
  - Solaris Mgmt. Cnsle with LDAP naming service

Trusted Extensions – Available NOW

- Delivered in Solaris Express 7/06
  - No cost
  - SPARC, x86/x64
  - Next generation, Solaris Nevada, code base
  - Install located in Extra Value directory
  - www.sun.com/solarisexpress/
- Open Solaris Community and Source
  - www.opensolaris.org/os/community/security/projects/tx/
  - CDDL open source licensed
- Production release in Solaris 10 11/06

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

Security Label Hierarchy

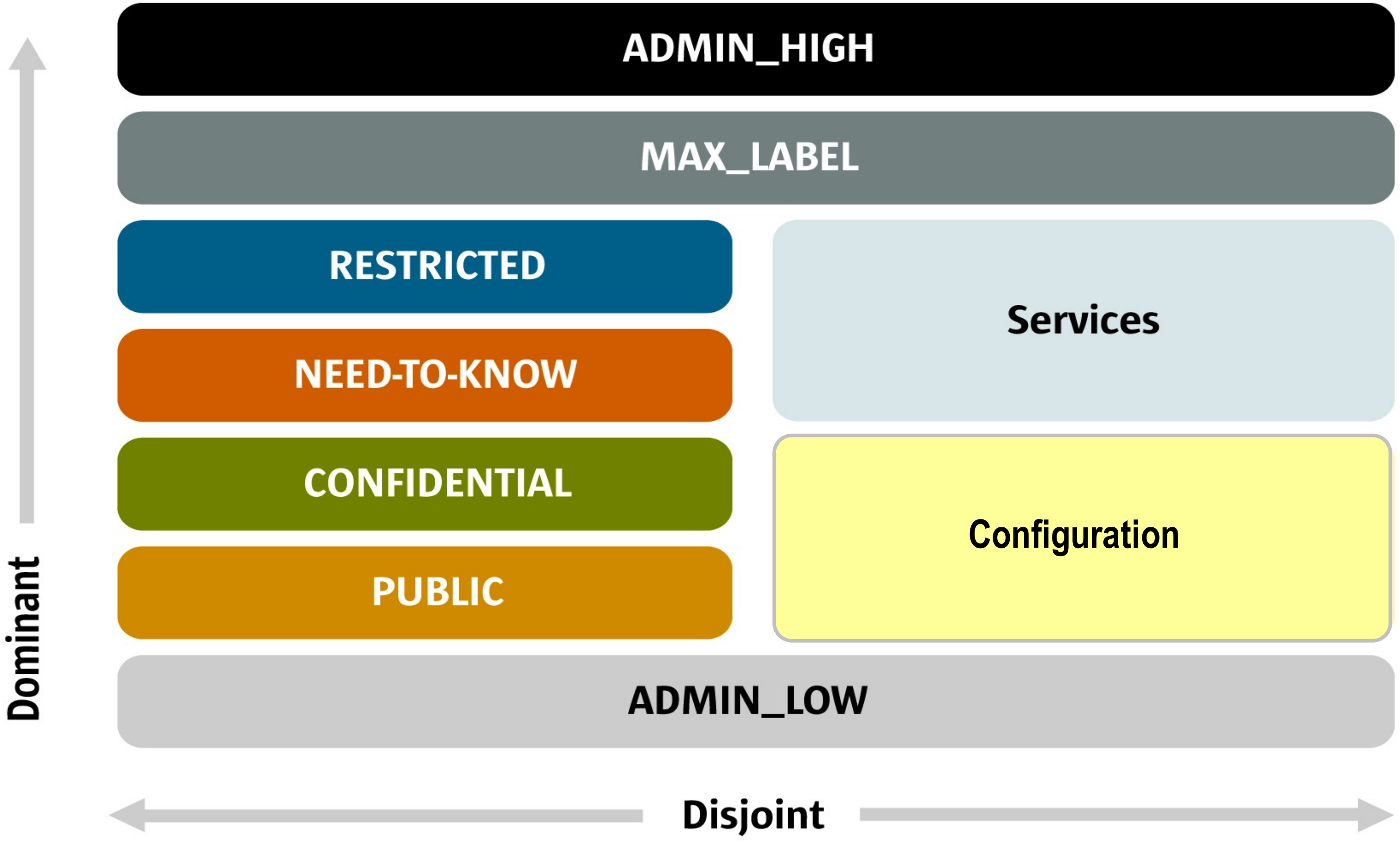


Figure 4 The Secure Network Access Platform – Example system label hierarchy relationships

What are Label-Aware Services?

- Services which are trusted to protect multilevel information according to predefined policy
- Trusted Extensions Label-aware service include:
  - Labeled Desktops
  - Labeled Printing
  - Labeled Networking
  - Labeled Filesystems
  - Label Configuration and Translation
  - System Management Tools
  - Device Allocation

Extending Solaris 10 Security Features

- Process Rights Management
  - Fine-grained privileges for X windows
  - Rights management applied to desktop actions
- User Rights Management
  - Labels and clearances
  - Additional desktop policies
- Solaris Containers (Zones)
  - Unique Sensitivity Labels
  - Trusted (label-based) Networking

Trusted Extensions Privileges

file_downgrade_sl	file downgrade label
file_upgrade_sl	file upgrade label
net_bindmlp	bind to a multilevel port
net_mac_aware	required for NFS read-down
sys_trans_label	translate non-dominated labels
win_colormap	load custom pseudo-colors
win_config	set X server defaults
win_dac_read	read another user's X resources
win_dac_write	modify another user's X resources
win_devices	set keyboard and pointer policies
win_dga	write to framebuffer
win_downgrade_sl	downgrade label of X resources
win_fontpath	install custom fonts
win_mac_read	read hon-dominated X resources
win_mac_write	modify dominated X resources
win_selection	bypass trusted selection manager
win_upgrade_sl	upgrade label of X resources

The privilege limit set for zones will be configurable

Any of these privileges may be assigned to zones

Containers and Labels

Solaris Containers

Limitless partitioning – One license

1,000’s of applications on one system

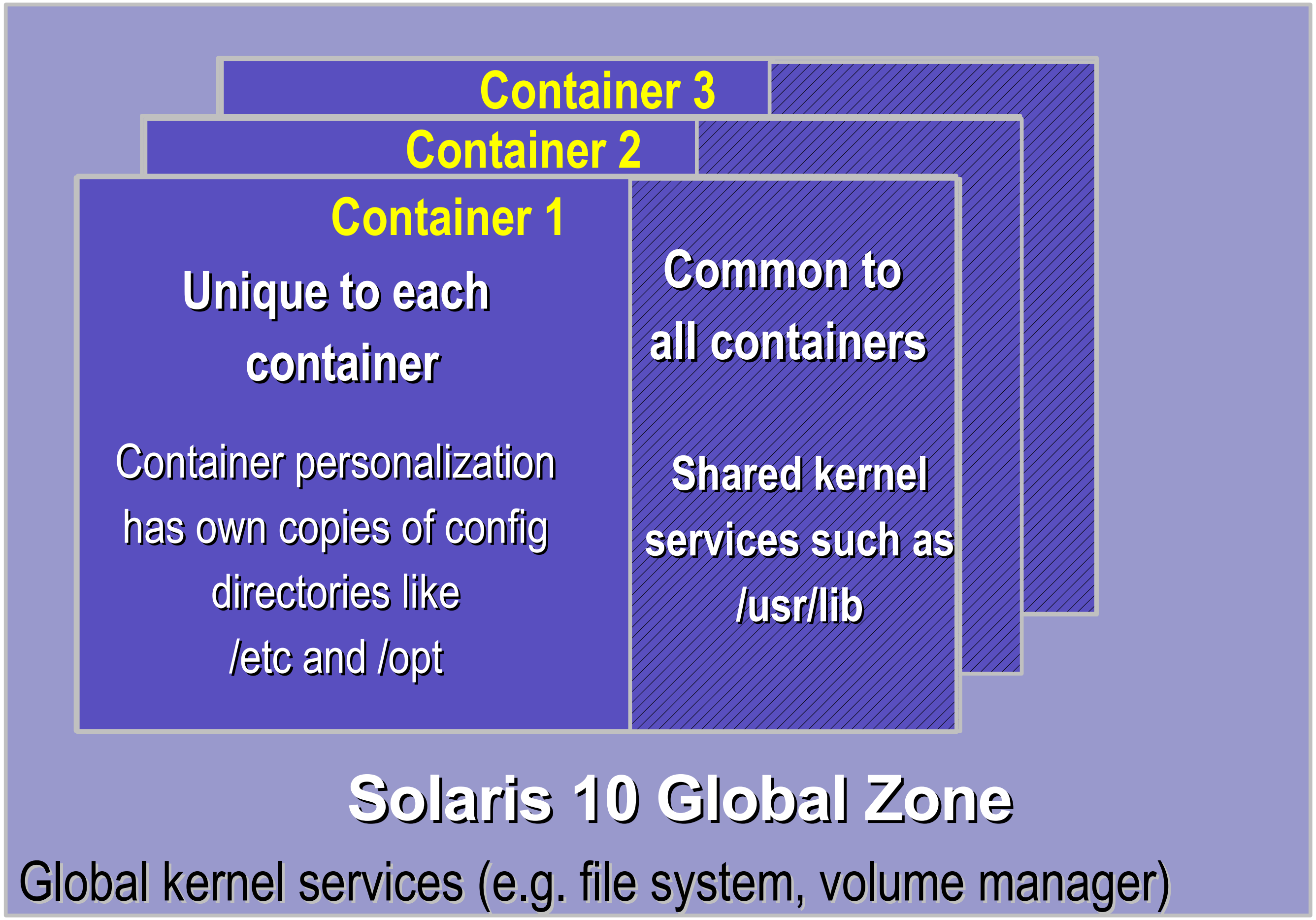
Fault & Security Isolation

Instant restart

Accelerate Consolidation

Multi-core aware

Containers


Container 3

Container 2

Container 1

Unique to each container

Container personalization has own copies of config directories like /etc and /opt

Common to all containers

Shared kernel services such as /usr/lib

Solaris 10 Global Zone

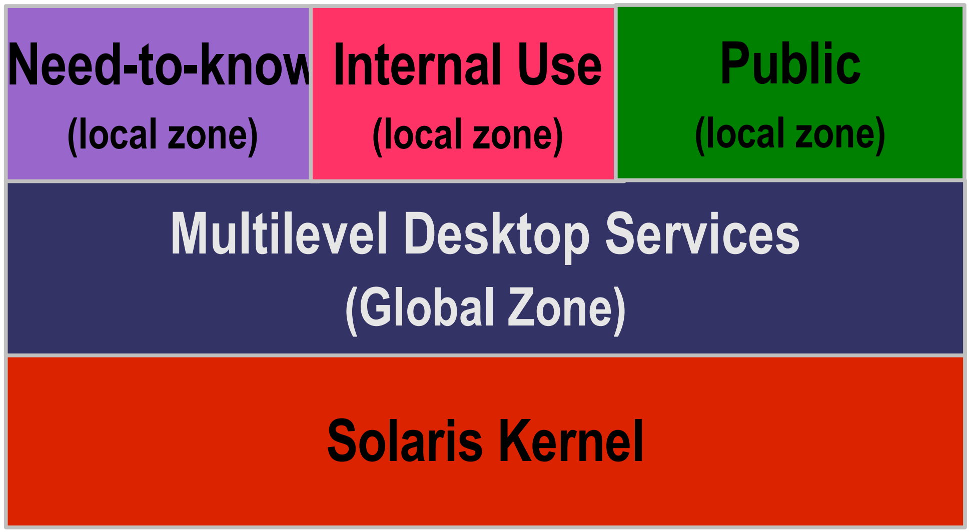
Global kernel services (e.g. file system, volume manager)

- Highly secure
- Invisible to each other
- Very efficient
- No performance penalty
- Separated file systems
- 8,000 per OS instance

Zone Concepts for Trusted Extensions

- Each zone has a label
  - Labels are implied by process zone IDs
  - Processes are isolated by label (and zone ID)
  - Files in a zone assume that zone's label
- Global zone is unique
  - Parent of all other zones
  - Exempt from all labeling policies
    - No user processes—just TCB
    - Trusted path attribute is applied implicitly
  - Provides services to other zones

Multilevel Architecture



Need-to-know
(local zone)

Internal Use
(local zone)

Public
(local zone)

Multilevel Desktop Services
(Global Zone)

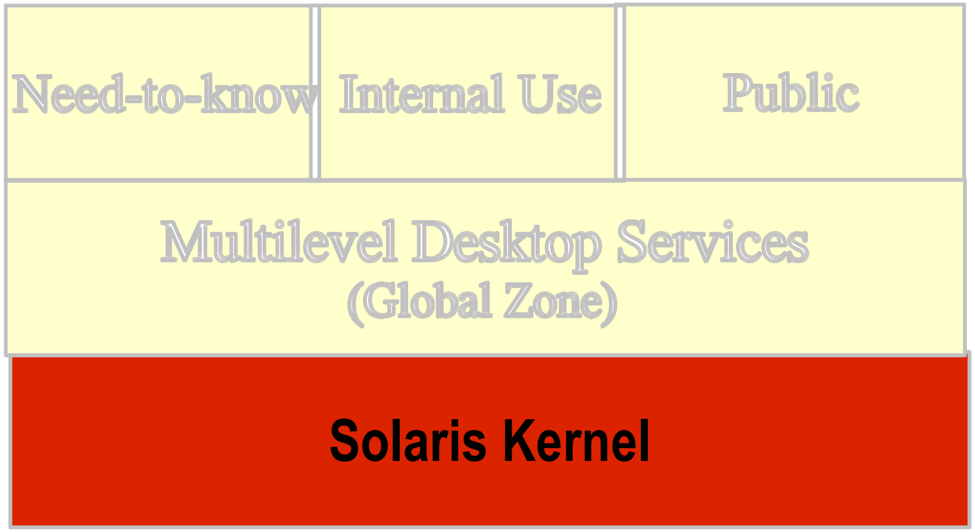
Solaris Kernel

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

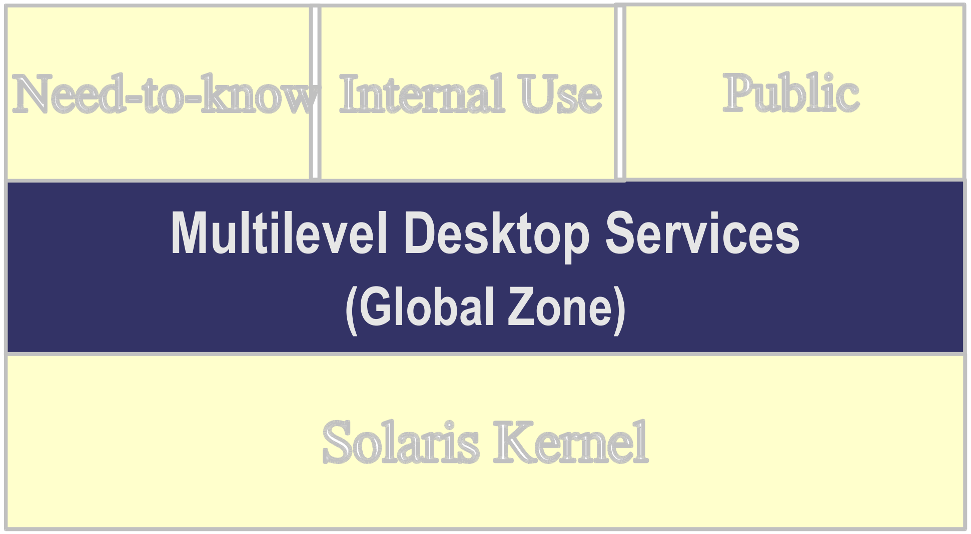


SPARC, x86 or x64 Hardware

Local or Sun Ray display

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

Multilevel Services



Need-to-know

Internal Use

Public

Multilevel Desktop Services
(Global Zone)

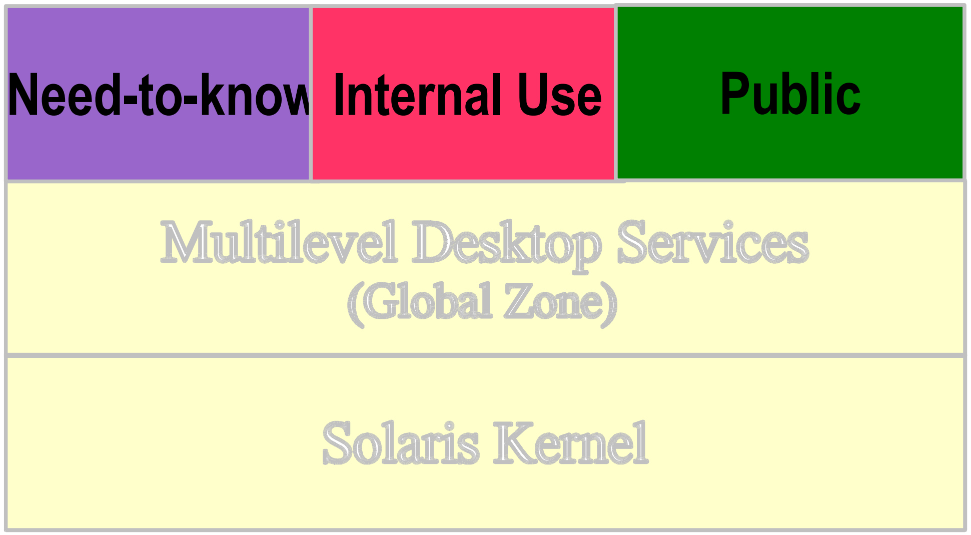
Solaris Kernel

SPARC, x86 or x64 Hardware

Local or SunRay display

- Label Policy Administration
- Name Services
- Labeled Printing
- File relabeling
- Device Allocation
- Labeled Windows
- Single Sign-on

Single-level Services



Need-to-know

Internal Use

Public

Multilevel Desktop Services
(Global Zone)

Solaris Kernel

SPARC, x86 or x64 Hardware

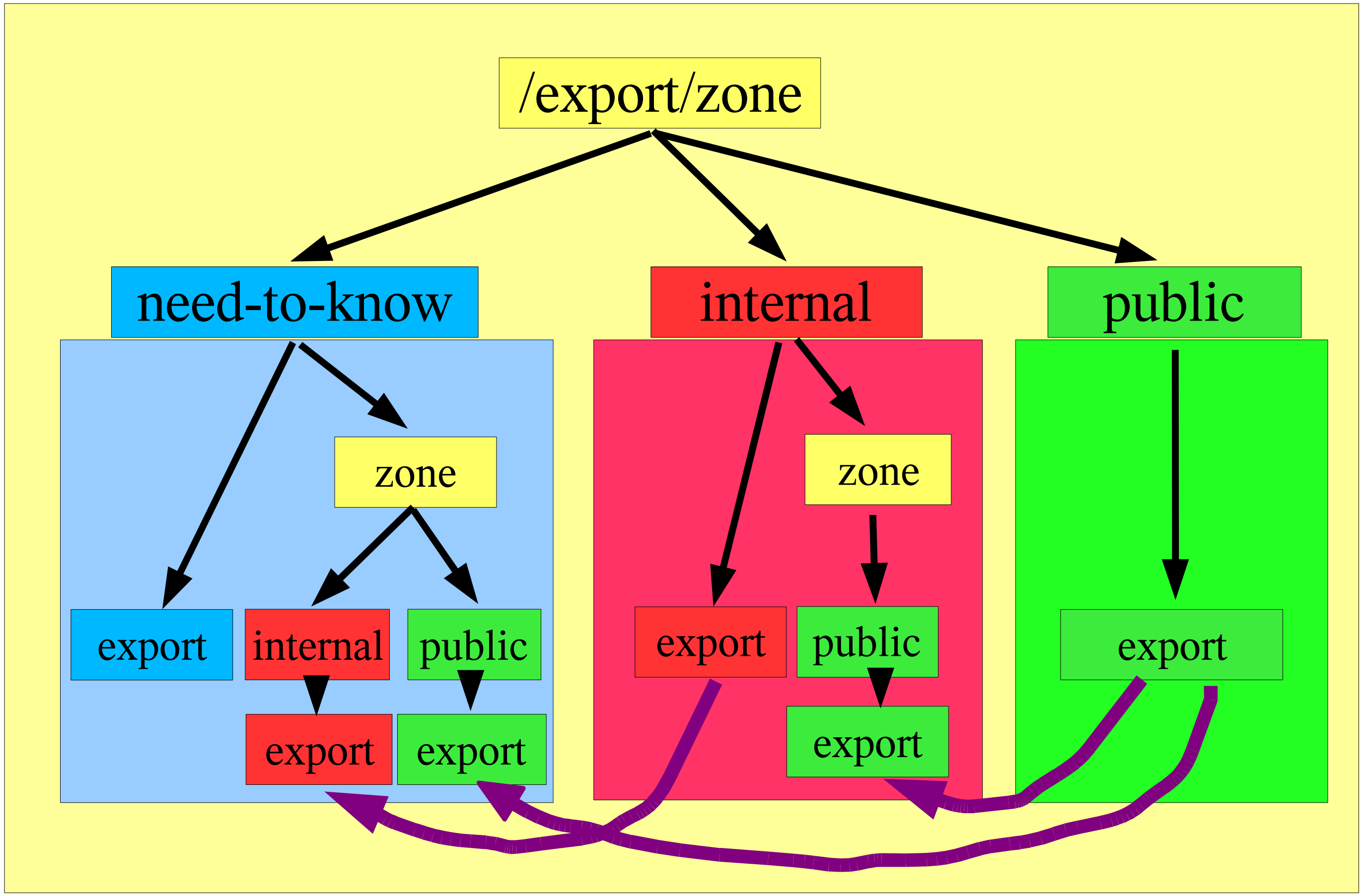
Local or Sun Ray display

- Application Launchers
- Windows XP Remote Desktop
- Mozilla
- StarOffice
- CDE or Java Desktop System

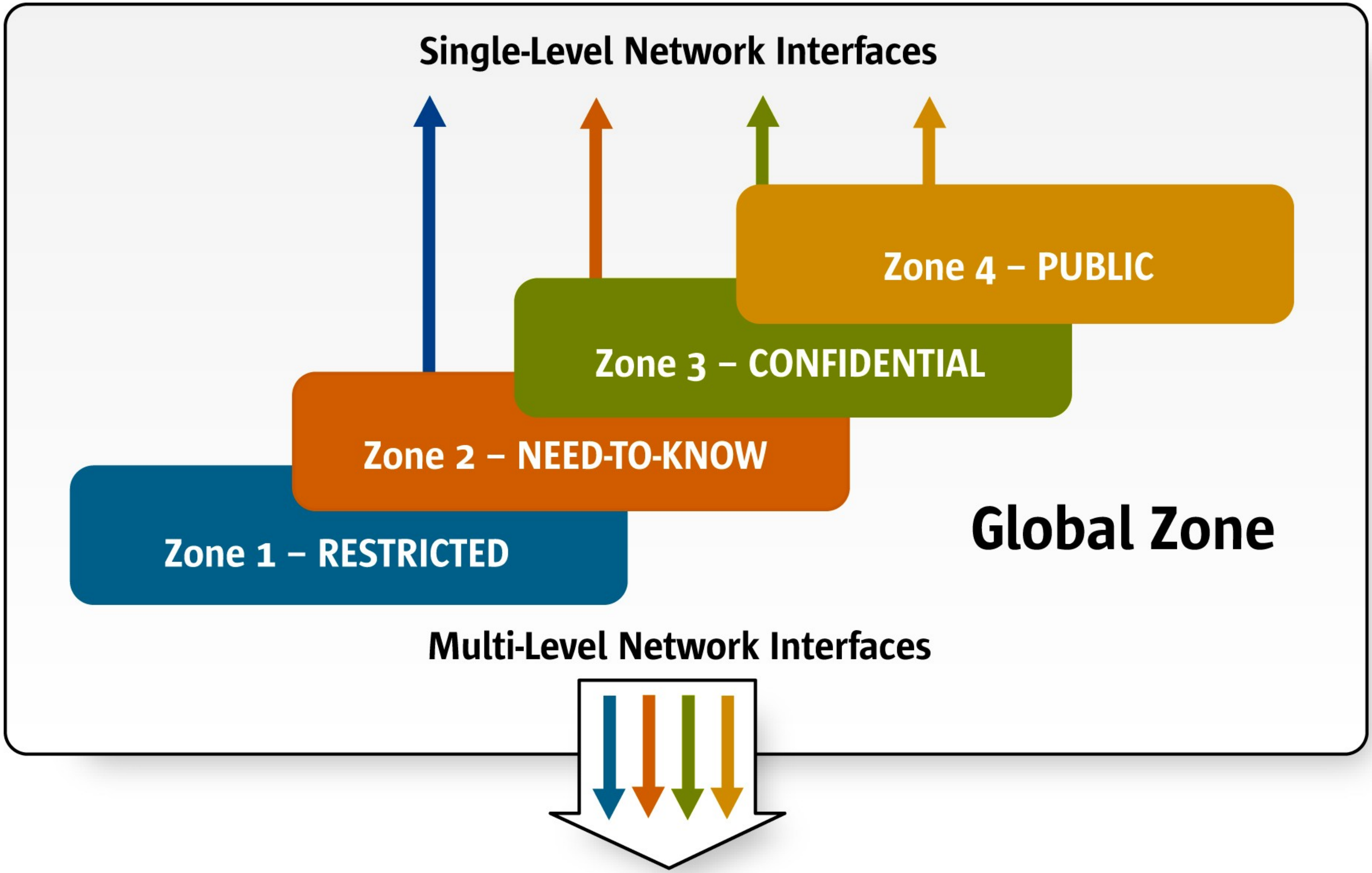
NFS Support for Zones

- NFS clients:
  - Each zone has its own automounter
  - Kernel enforces MAC policy for NFS mounts
- NFS servers:
  - Global zone administrators a share table per zone
  - Kernel enforces MAC policy for NFS requests
  - Zones don't have to be running to share data
- The global zone administrator can export filesystems from labeled zones
  - Each export must be a single-level filesystem
  - Zone's label automatically applied to each export

Reading Lower-Labeled Files



Multi-level Networking

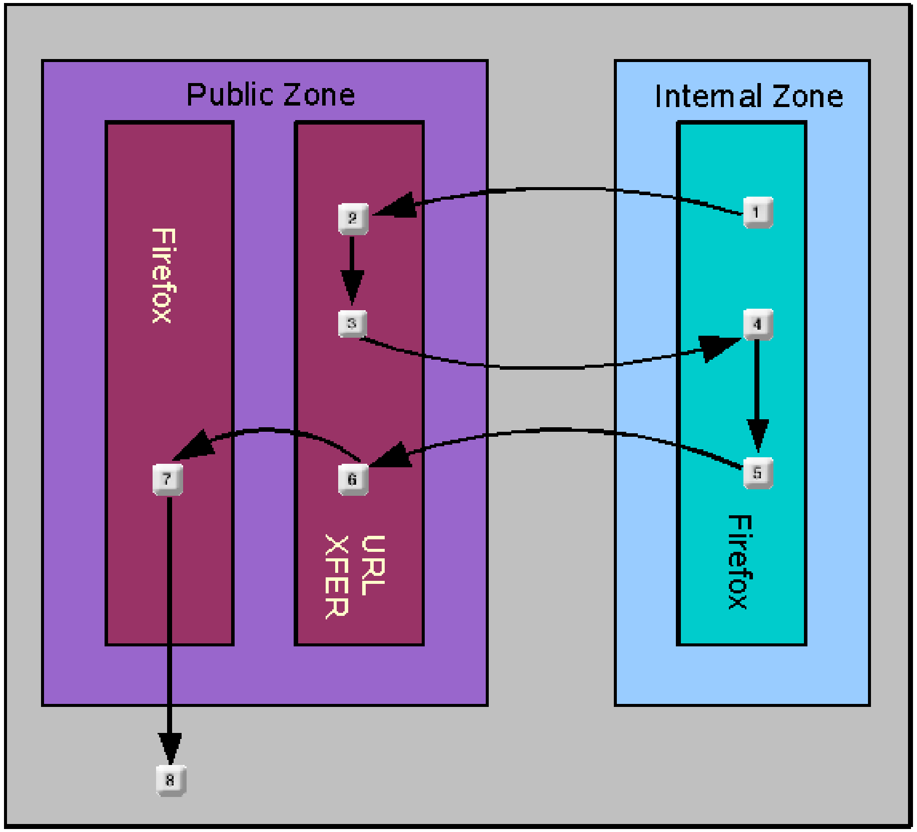


The Secure Network Access Platform – Global zones, local zones, physical network interfaces, and trusted networking relationships

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

Safe Browsing via URL Forwarding



Robustness & Certification

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

Common Criteria Certifications

- Targets include : SPARC, x86/x64 based systems, full networking, LDAP naming service, full GUI
- Solaris 10 3/05:
  - CAPP, RBACPP @ EAL 4+
  - Expected to complete by December 2006
- Solaris 10 11/06:
  - CAPP, RBACPP, LSPP @ EAL 4+
  - Officially “In evaluation” as of June 2006
  - Expected to complete by Summer 2007
- US-based upcoming requirements
  - Basic, Single-Level Medium, Multilevel Medium

Trusted and Solaris 10 Comparisons

FEATURE	TSol 8	Sol 9	Sol 10	Trust Ex.
CC Evaluation	**CA**	**CA,RB**	**CA,RB***	**LS***
RBAC	X	X	X	X
Removable Media Control	X	X	X	X
Smartcard Support	X	X	X	X
Process Rights Mgmt (a.k.a. Privileges)	X		X	X
Virtualization (containers)/MAC	X		X	X
Hardened Platform	X		X	X
Labeled Window System	X			X
Labeled Networking	X			X
Virtual Private Networking		X	X	X
Single Signon		X	X	X
Cryptography Support		X	X	X
Integrated Packet Filtering			X	X
Integrated Security Stack			X	X

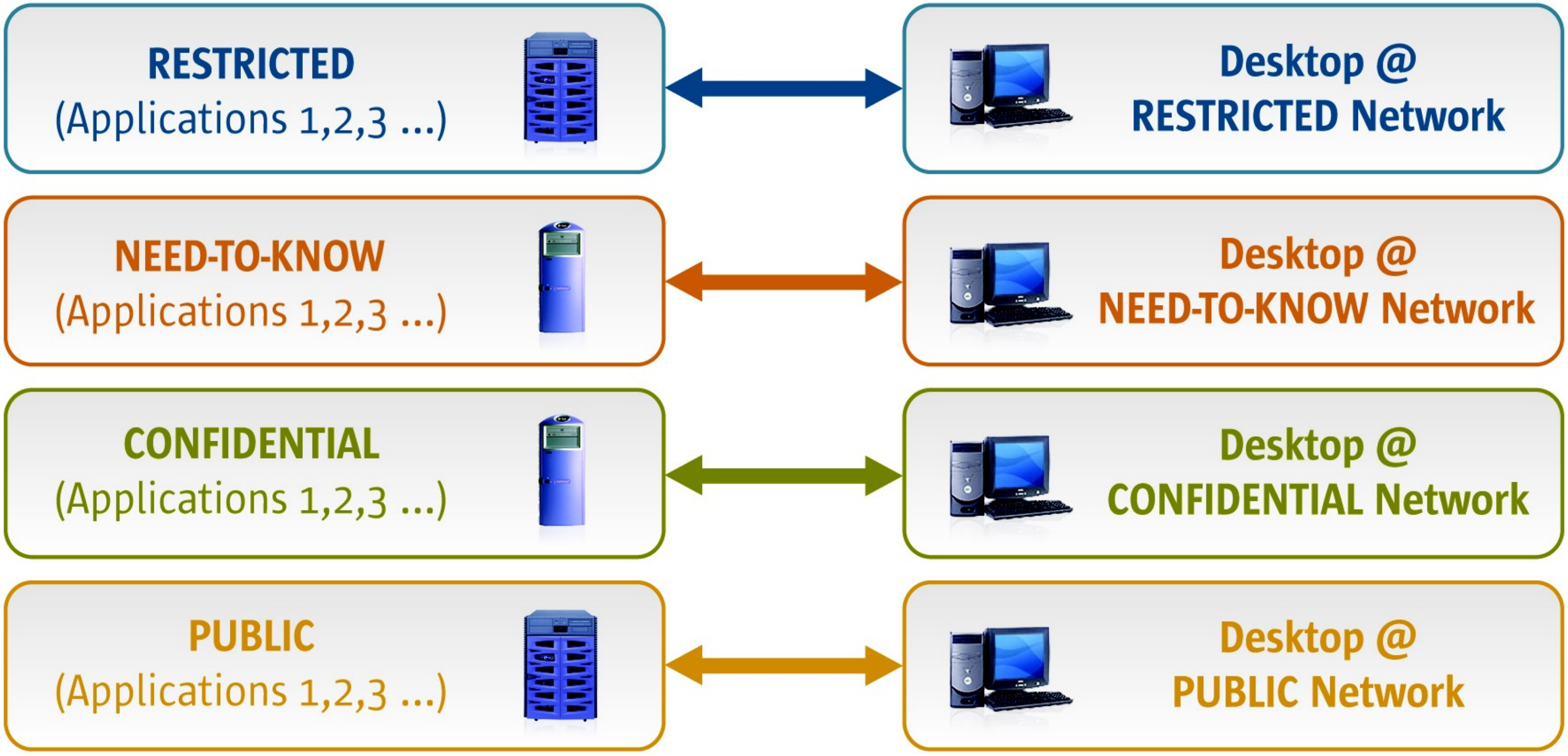
Legend **x = fully implemented**

x = partially implemented

Desktop Examples

Status Quo Example: Stove Piped Networks for Secure Communications

Multiple Desktop Access Multiple Enclaves



RESTRICTED (Applications 1,2,3 ...)

Desktop @ RESTRICTED Network

NEED-TO-KNOW (Applications 1,2,3 ...)

Desktop @ NEED-TO-KNOW Network

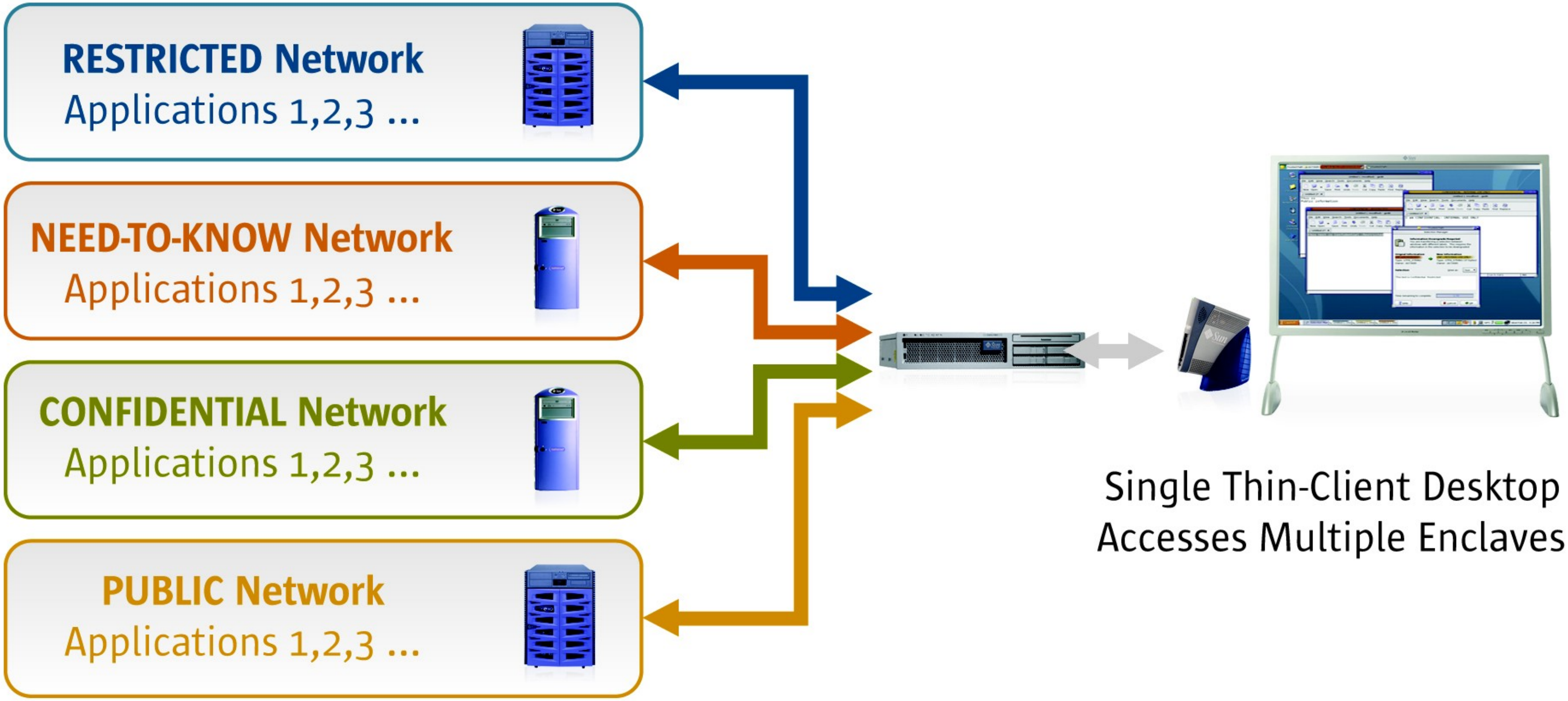
CONFIDENTIAL (Applications 1,2,3 ...)

Desktop @ CONFIDENTIAL Network

PUBLIC (Applications 1,2,3 ...)

Desktop @ PUBLIC Network

Changing the Game: Single Multi-Tiered Secure Communications

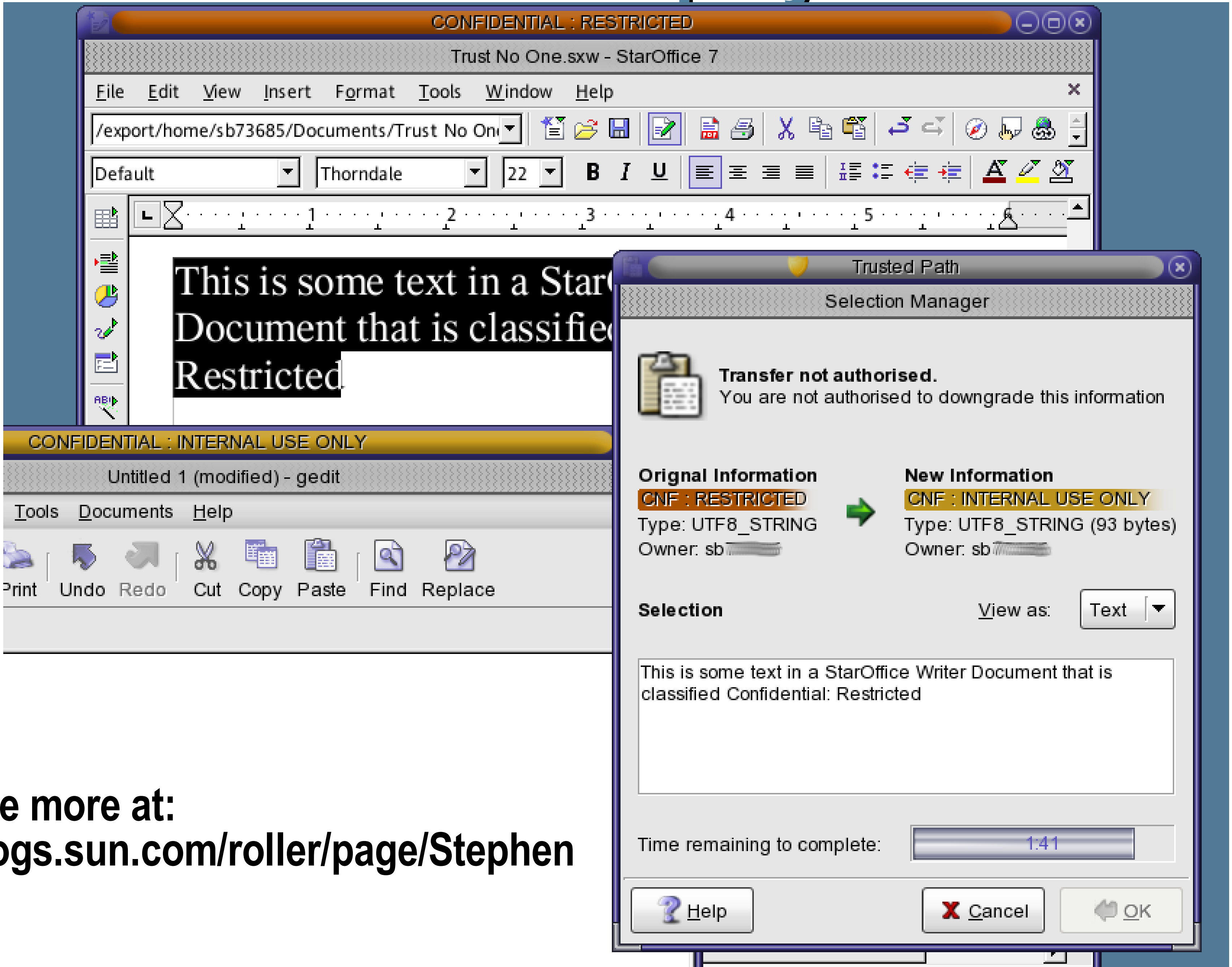


Providing a single desktop with secure access to multiple security enclaves

Multi-Level Desktop Plans

- Trusted CDE standard
  - Similar to Trusted Solaris 8
  - Included in initial Common Criteria Evaluation
- Java Desktop System (GNOME)
  - Single Level desktop
    - Full accessibility requirements
    - More modern look-and-feel to customers
  - Multi-level desktop
    - Expected to include some version in initial release
    - Is currently planed to test for Common Criteria LSPP

Trusted Java Desktop System


CONFIDENTIAL : RESTRICTED
Trust No One.sxw - StarOffice 7
File
Edit
View
Insert
Format
Tools
Window
Help
/export/home/sb73685/Documents/Trust No On
Default
Thorndale
22
CONFIDENTIAL : INTERNAL USE ONLY
Untitled 1 (modified) - gedit
Tools
Documents
Help
Print
Undo
Redo
Cut
Copy
Paste
Find
Replace
Trusted Path
Selection Manager

This is some text in a Star
Document that is classifie
Restricted

Transfer not authorised.
You are not authorised to downgrade this information

Orignal Information		**New Information**
CNF : RESTRICTED	→	CNF : INTERNAL USE ONLY
Type: UTF8_STRING		Type: UTF8_STRING (93 bytes)
Owner: sb[redacted]		Owner: sb[redacted]

Selection View as: Text

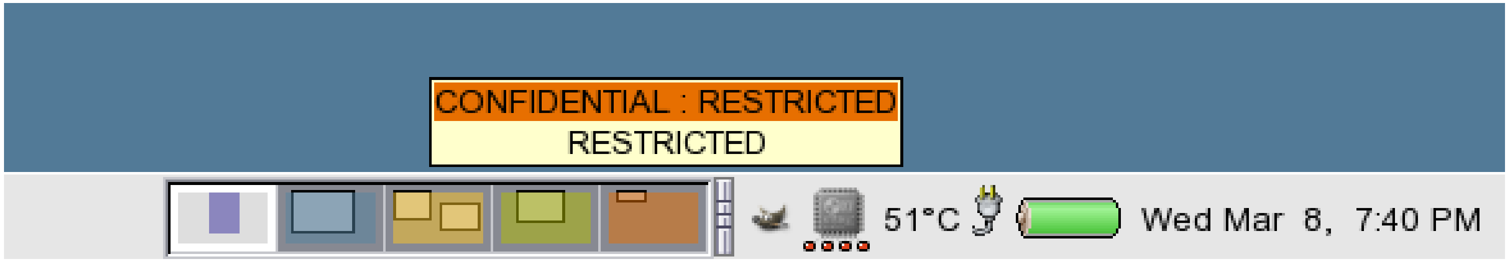
This is some text in a StarOffice Writer Document that is classified Confidential: Restricted

Time remaining to complete: 1:41

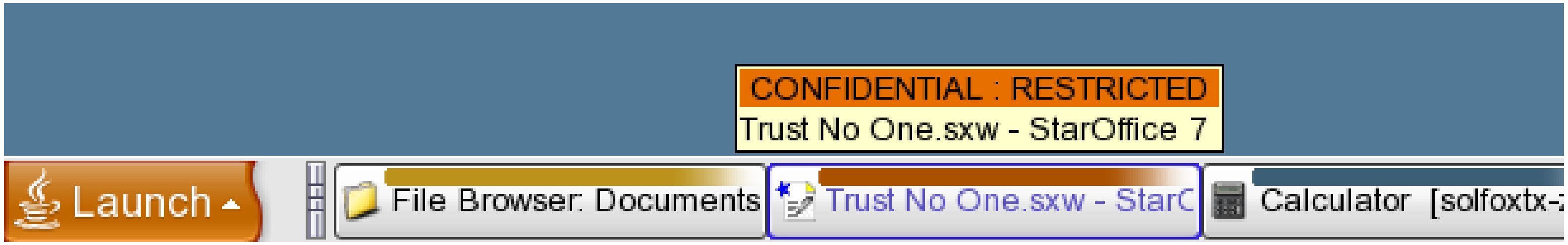
See more at: blogs.sun.com/roller/page/Stephen

Trusted Java Desktop System Details

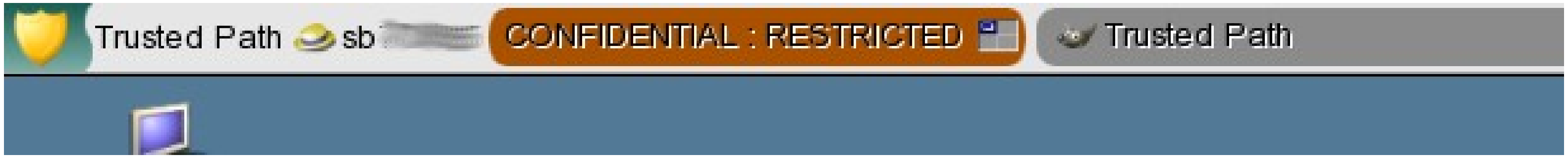
Workplace switcher



Task switcher



Trusted stripe and Trusted Path menu



Compatibility with Trusted Solaris 8

Label Compatibility

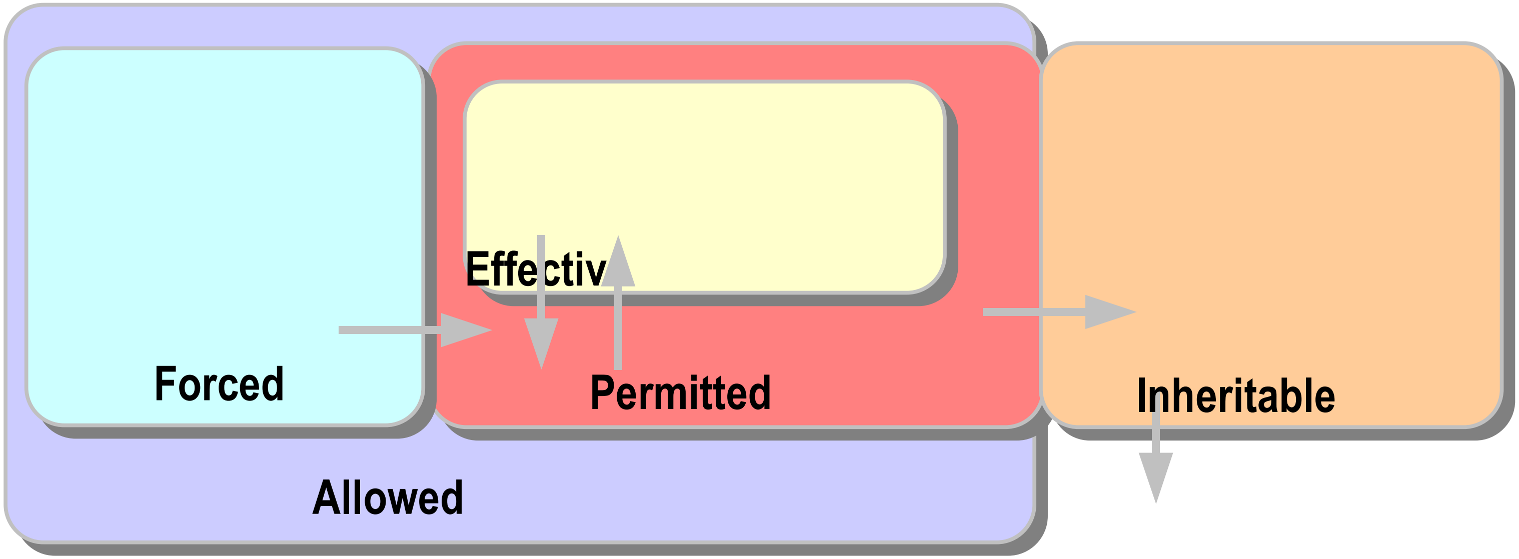
- Label encodings files are compatible between Trusted Solaris 8 and Trusted Extensions
- Use -T option of tar(1) to transfer multilevel directories from TS 8 to TS 10
  - MLDs and SLDs are converted to zone-relative paths
  - Symlinks to SLDs are are also converted
  - Files with explicit label settings may not be preserved
  - Other file attributes (e.g. Privileges and Flags are lost)

Network Interoperability

- Use Commercial IP Security Option (CIPSO) between Trusted Solaris 8 and Trusted Extensions
  - Don't use TSOL or TSIX
  - Can't pass process attributes in network packets
- CIPSO restricts compartment bits to 240 (out of 256)

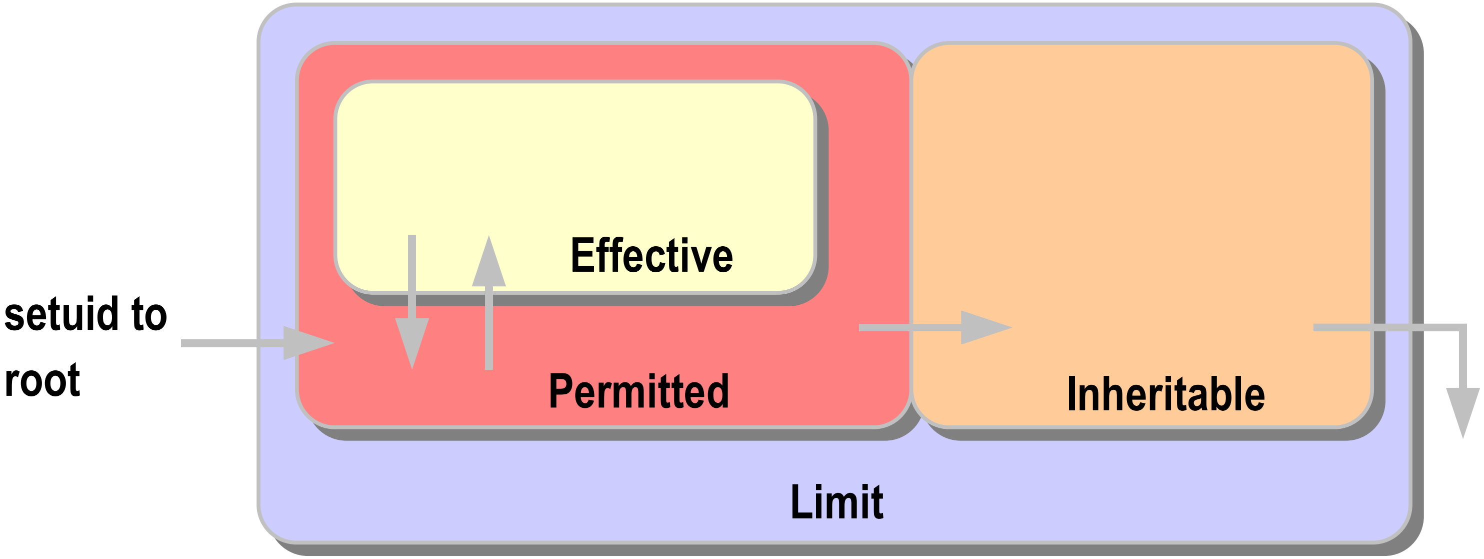
Trusted Solaris 8 Privilege Sets

- Forced and Allowed
  - > Attributes of the executable file
- Inheritable
  - > Masks privileges passed from parent process
- Effective and Permitted
  - > Effective are checked for policy overrides



Solaris 10 Privilege Sets

- E - Effective set
  - > Privileges in effect
- P - Permitted set
  - > Upper bound of E
- I - Inheritable set
  - > Privs of exec'ed program
- L - Limit set
  - > Applies to process and all descendants



Trusted Desktop Interoperability

- X TSOL protocol extensions are fully compatible
- Multilevel remote display works in either direction (using CIPSO)
- CDE Remote Login from Trusted Extensions to Trusted Solaris 8 *should* work

API Compatibility

- Most label manipulation APIs are unchanged
- Trusted networking APIs are different
  - > Trusted Extensions extends getpeerucred(2) from Solaris 10
  - > Usually unnecessary to modify network services
    - > Polyinstantiated and Multilevel ports are administratively specified
    - > Label matching is automatic for replies
- Most objects have fixed labels

Administrative Interoperability

- Trusted Solaris 8 and Trusted Extensions must be in separate administrative domains
- Name services are different
  - > Trusted Solaris 8 uses NIS+
  - > Trusted Extensions uses LDAP
- File formats are similar but not compatible
- Solaris Mgmt. Console tools are similar but not compatible

Documentation

- All Solaris 10 documentation applies!
  - Security Administrator's Guide
    - Process and user rights management
  - Containers and Resource Management
  - Service Manager, CDE and Java Desktop
- Transition Guide
  - API-by-API mapping from Trusted Solaris 8 to Solaris with Trusted Extensions
  - Available now as part of Early Access

Developer's Guide In Development

- Goal : Provide practical guide to writing a multi-level application using Trusted Extensions
- Cover general transition issues
  - File label manipulation, privileges, containers
- Application specific examples
  - Desktop - CDE and later JDS
  - Trusted Printing
  - Web Guard – moving data w/appropriate business logic
  - Multi-level middleware and app server
  - LDAP and label queries

Pricing & Open Source

- Simple – It's included in Solaris
- It's Free, just as Solaris is free
- Solaris 10 support contracts include support for Trusted Extensions
- OEM licensing model is still under discussion
- Open Source of all core Solaris changes today
  - Trusted Extensions label deamon and other utilities will be opened sourced as well

Solaris Security and Trusted Extensions Update

Mark Thacker

mark.thacker@sun.com

972-992-3178

Appendix A :
Resources, Citations and URL's

Other Resources

- Solaris 10 Home
  - http://www.sun.com/software/solaris/10/
- Solaris 10 AnswerBook
  - http://docs.sun.com/db/prod/solaris.10#hic
- Solaris 10 Security Blog Articles
  - http://blogs.sun.com/gbrunett
  - http://blogs.sun.com/casper
  - http://blogs.sun.com/arunpn
  - ... and many others in the Appendix...

References

- Desktop System Streamlines Analysis Work, SIGNAL, Henry S. Kenyon
  http://www.afcea.org/signal/articles/anmviewer.asp?a=427&z=39
- USS Mt. Whitney exercise
  http://www.jfcom.mil/newslink/storyarchive/2004/pa062104.htm
- JEDI page describing DoDIIS Trusted Workstation (DTW)
  - https://extranet.if.afrl.af.mil/jedi/
  - http://www.rl/tech/programs/afdi
- Super-Secure Systems Gain in Private Sector, Investor's Business Daily, 10/12/04; Donna Howell
  http://www.investors.com/editorial/tech01.asp?v=10/12

Related Information

- Sun Security Home Page
  - http://www.sun.com/security
- Solaris Patches & Finger Print Database
  - http://sunsolve.sun.com/
- Sun Security Coordination Team
  - http://sunsolve.sun.com/security
- Sun BluePrints for Security
  - http://www.sun.com/blueprints
    - Developing a Security Policy
    - Trust Modelling for Security Arch. Development
    - Building Secure n-Tier Environments
    - How Hackers Do It: Tricks, Tips and Techniques

Related Service Information

- Sun Consulting Security Services
  - http://www.sun.com/service/sunps/security
- Sun Education Security Services
  - http://suned.sun.com/US/catalog
- Sun Support Services
  > http://www.sun.com/service/support
- Network and Security Products
  - http://www.humanfirewall.org

Solaris Security and Trusted Extensions Update

Mark Thacker

mark.thacker@sun.com

972-992-3178