Solaris Trusted Extensions

Bart Blanquart
Security Architect
Chief Technology Office

What is Solaris Trusted Extensions?

- A different *configuration* of Solaris (10+)
  - Not separate from Solaris anymore, like Trusted Solaris was
  - Up until Solaris 10 update 4 manual install
  - From S10u5: “svcadm enable labeld”
- An extension of the Solaris 10 security foundation providing access control policies based on the sensitivity/label of objects
  - A couple label-aware services which implement multilevel security

Labeling policy

- Bell-LaPadula and all that
  - “WURD”
- Trusted Extensions Label-aware services
  - Desktop
    GNOME, CDE
  - Networking
  - System management tools
    (Solaris Management Console)
  - Device Allocation

Labeling Policy

- You can write to files that are at the label you're working at
- You can read files that are at or below the label you're working at
- You can't see, read, or write files that are at labels that are outside your assigned domain.
  - For processes you can just see those that are at the label you're working at
  - On the network you can just communicate with systems or services that are at the label you're working at

It's mostly Solaris...

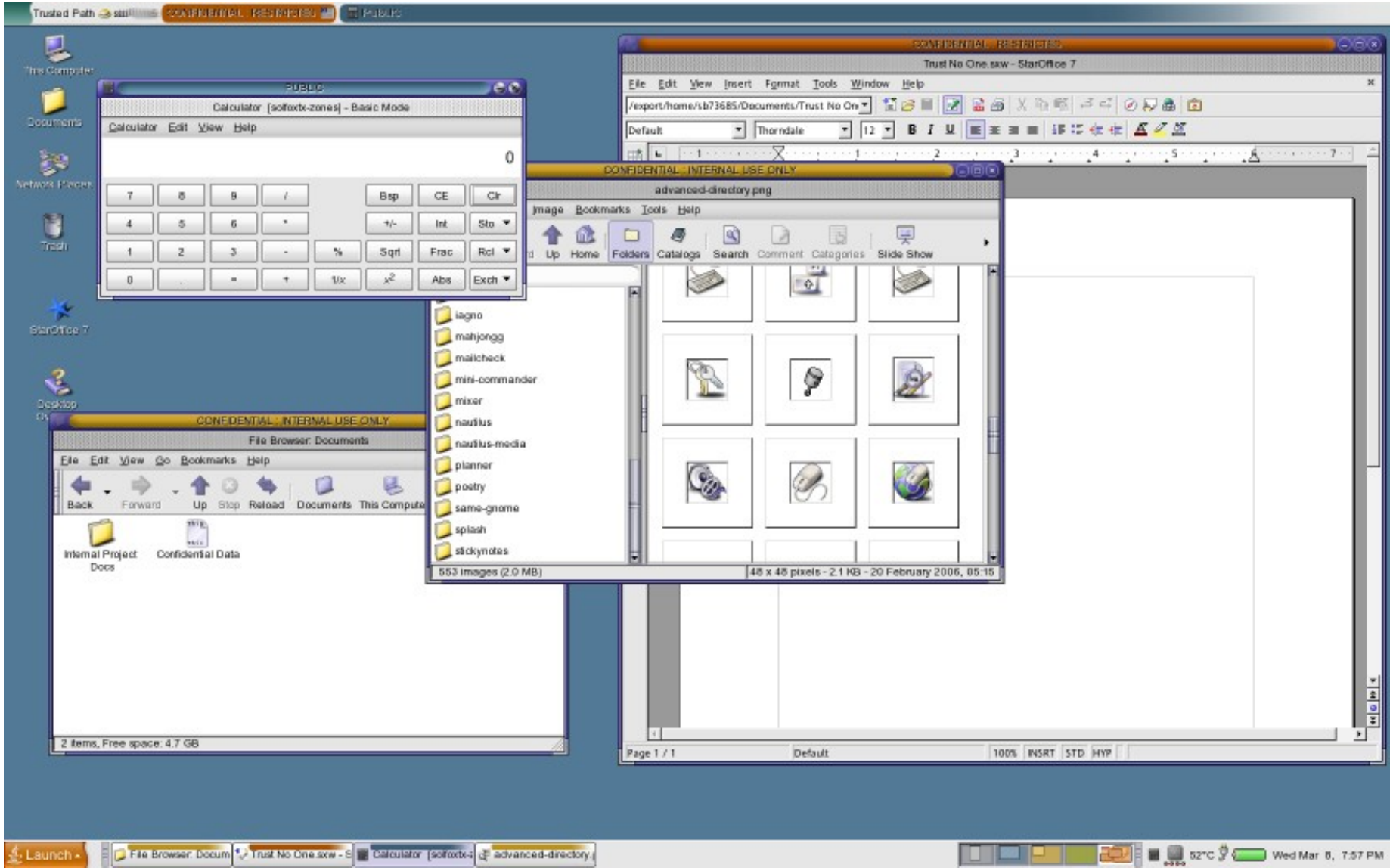
- “Regular” Solaris Privileges, RBAC, ...
- And “regular” Solaris Zones
  - But instead of being “another” system they're conceptually the same as the global zone, just at a different sensitivity level

Mostly Solaris, but...

- Enhanced X11 (& Gnome & CDE)
  - Server runs in the global zone and (helps) enforce policy
- Modified networking
  - Sends labels along (hopefully soon with Ipsec, too)
- Some bits and bobs
  - e.g. printing (can print handling instructions on banner pages, like “do not leave on train”)

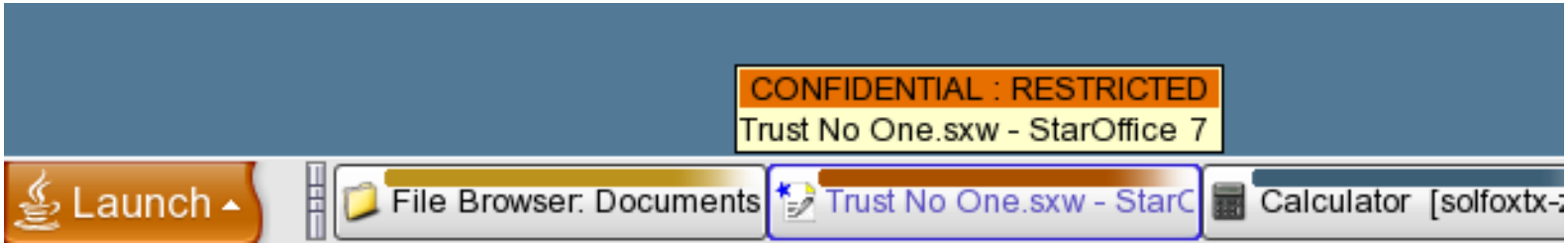
(Desktop show & tell)

Pretty pictures
(from Stephen Browne's blog)

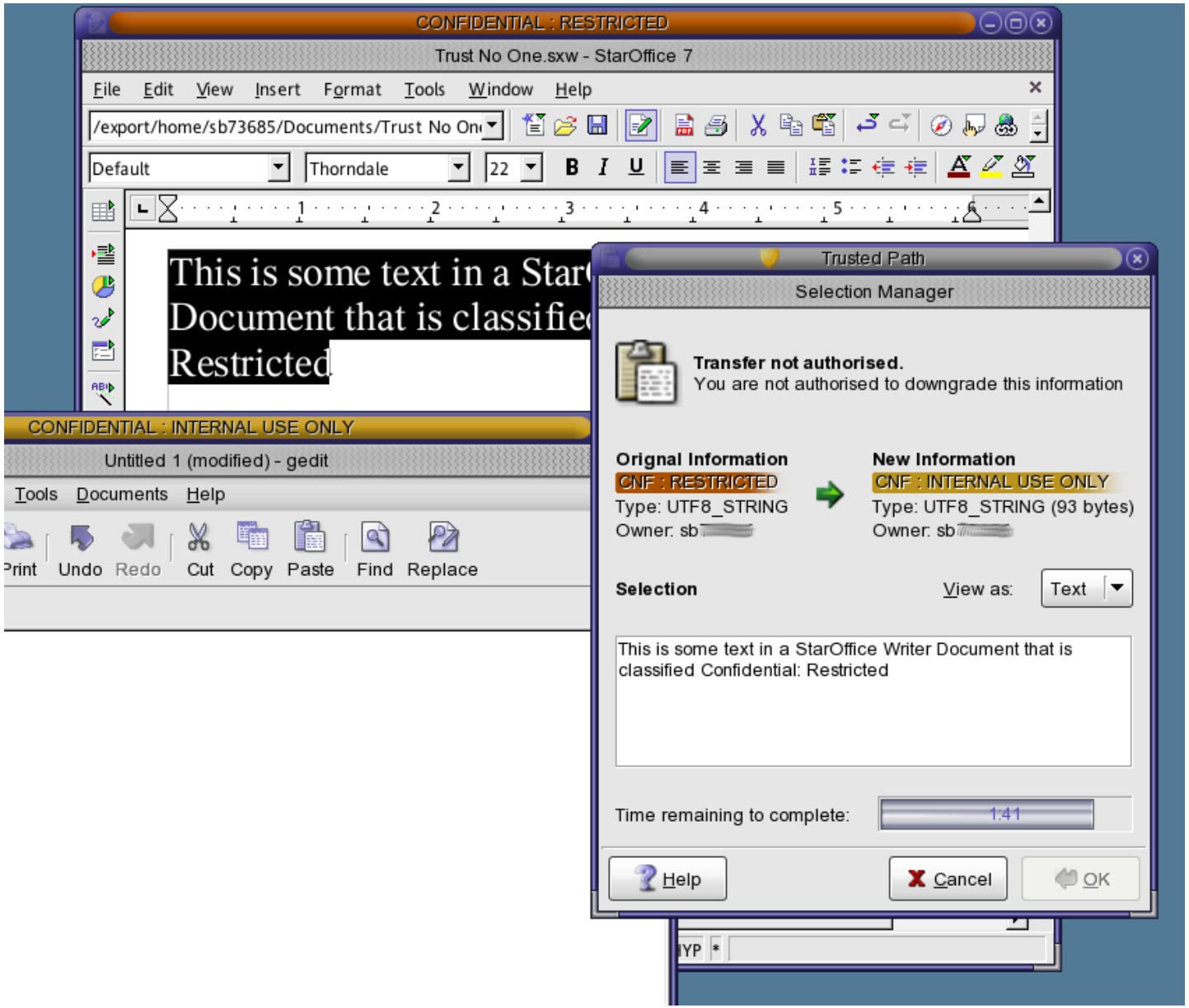


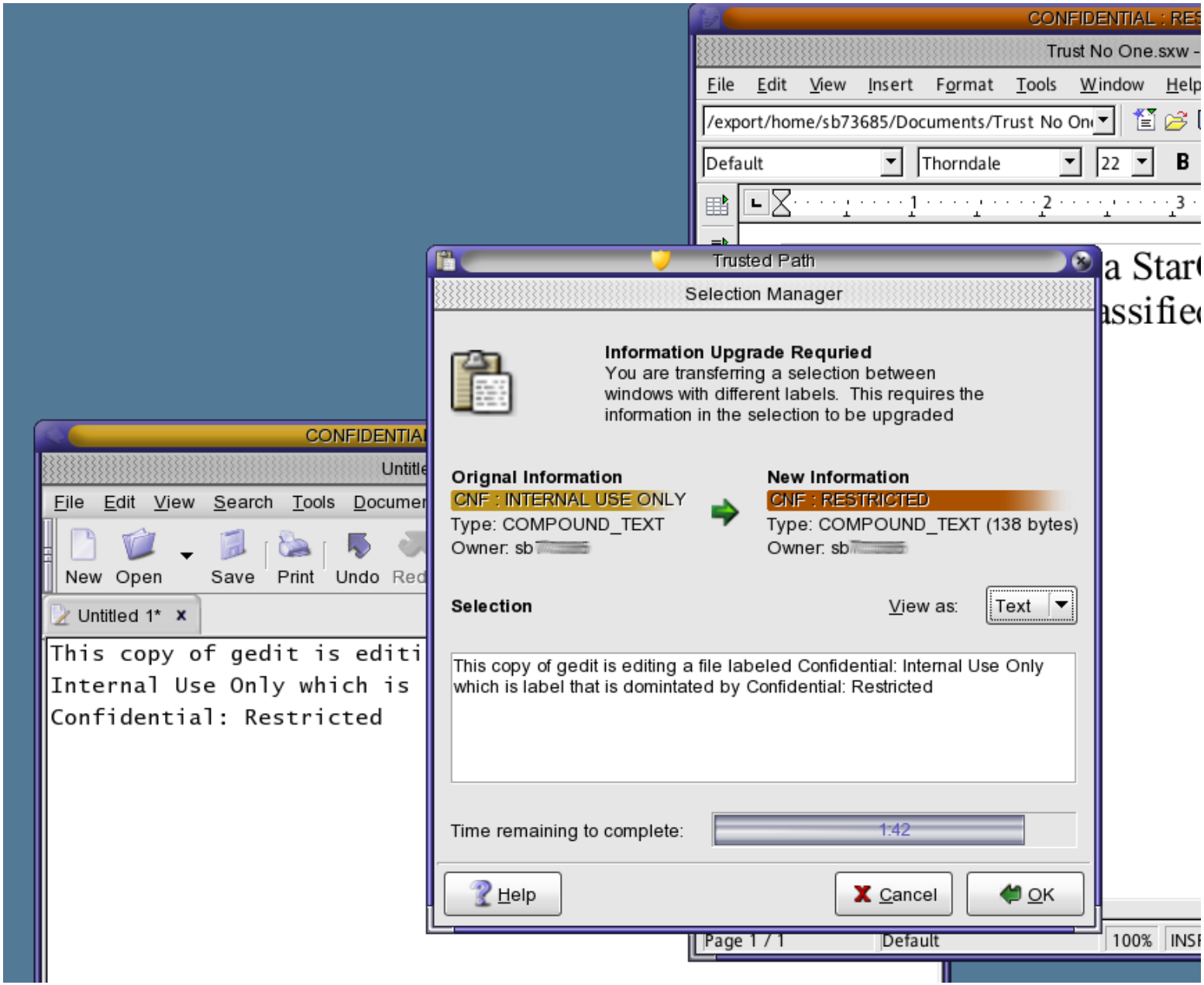

Trusted Path
sb
CONFIDENTIAL : RESTRICTED
CONFIDENTIAL : INTERNAL US


Trusted Path
sb
CONFIDENTIAL : RESTRICTED
Trusted Path

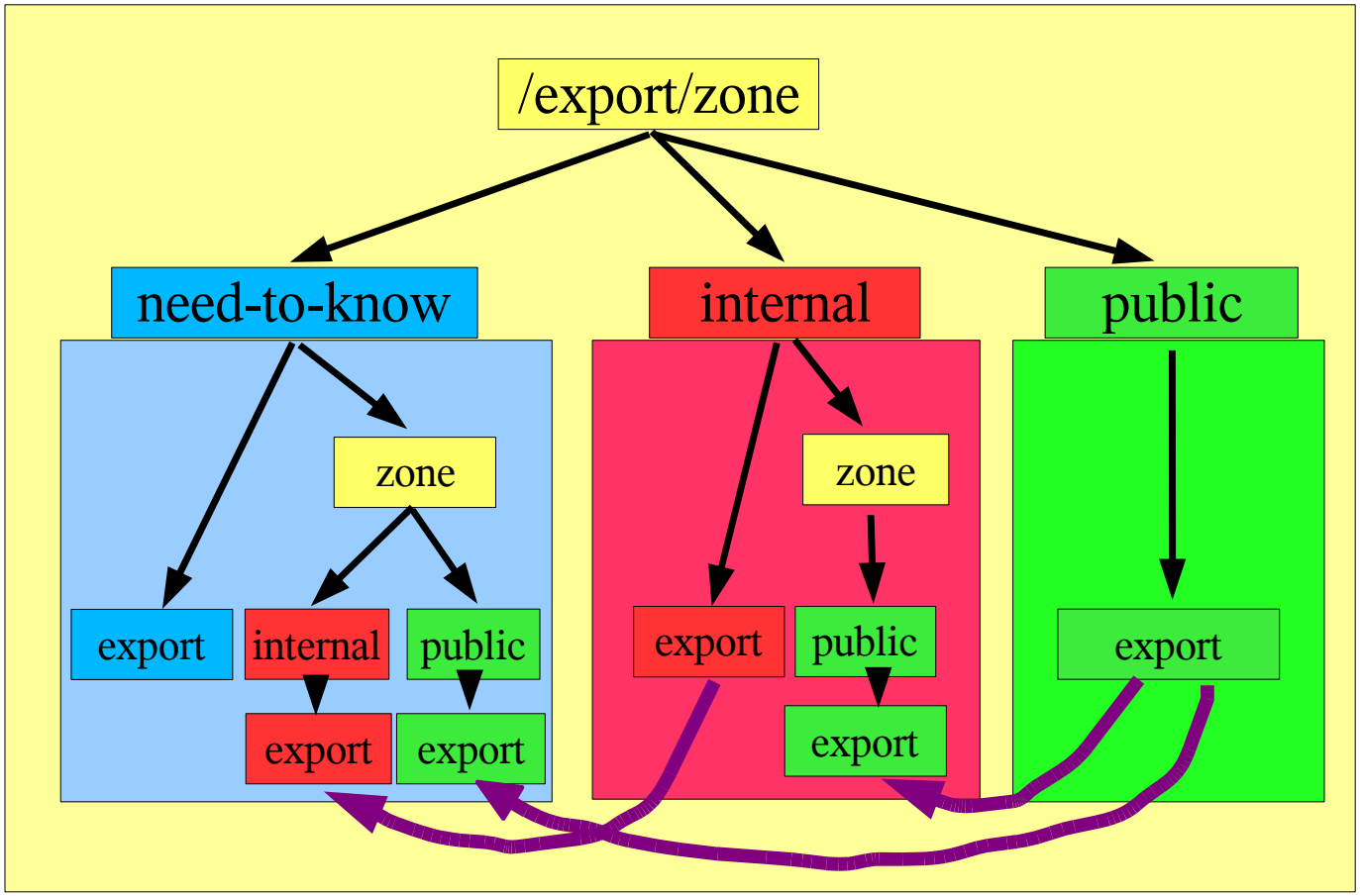

CONFIDENTIAL : RESTRICTED
Trust No One.sxw - StarOffice 7
Launch
File Browser: Documents
Trust No One.sxw - StarC
Calculator [solfoxtx-


CONFIDENTIAL : RESTRICTED
RESTRICTED
51°C
Wed Mar 8, 7:40 PM


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
This is some text in a Star
Document that is classifie
Restricted
CONFIDENTIAL : INTERNAL USE ONLY
Untitled 1 (modified) - gedit
Tools Documents Help
Print Undo Redo Cut Copy Paste Find Replace
Trusted Path
Selection Manager
Transfer not authorised.
You are not authorised to downgrade this information
Orignal Information
CNF : RESTRICTED
Type: UTF8_STRING
Owner: sb
New Information
CNF : INTERNAL USE ONLY
Type: UTF8_STRING (93 bytes)
Owner: sb
Selection
View as:
Text
This is some text in a StarOffice Writer Document that is classified Confidential: Restricted
Time remaining to complete:
1:41
Help
Cancel
OK


CONFIDENTIAL : RES
Trust No One.sxw -
File Edit View Insert Format Tools Window Help
/export/home/sb73685/Documents/Trust No On
Default
Thorndale
22
Trusted Path
Selection Manager
Information Upgrade Requried
You are transferring a selection between windows with different labels. This requires the information in the selection to be upgraded
Orignal Information
CNF : INTERNAL USE ONLY
Type: COMPOUND_TEXT
Owner: sb
New Information
CNF : RESTRICTED
Type: COMPOUND_TEXT (138 bytes)
Owner: sb
Selection
View as:
Text
This copy of gedit is editing a file labeled Confidential: Internal Use Only which is label that is domintated by Confidential: Restricted
Time remaining to complete:
1:42
Help
Cancel
OK
CONFIDENTIA
File Edit View Search Tools Documen
New Open Save Print Undo Red
Untitled 1*
This copy of gedit is editi
Internal Use Only which is
Confidential: Restricted
Page 1 / 1
Default
100%

File access on the desktop



loopback mounts

Trusted Networking

- 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
  - *ip:port-ip:port* becomes *ip:port-ip:port+label*
  - Generally label equality required between endpoints
  - Multilevel ports accept labels within range or set
  - For NFS operations, read-down is supported
    - NFS server knows about labels and keeps track of them

System management & Device Allocation

- System management
  - Not terribly interesting: Solaris Management Console just knows about clearances
- Device allocation
  - Not terribly interesting, either: comes with a GUI, can be configured to only allow device allocation at specific labels.

The (hopefully) more interesting bits

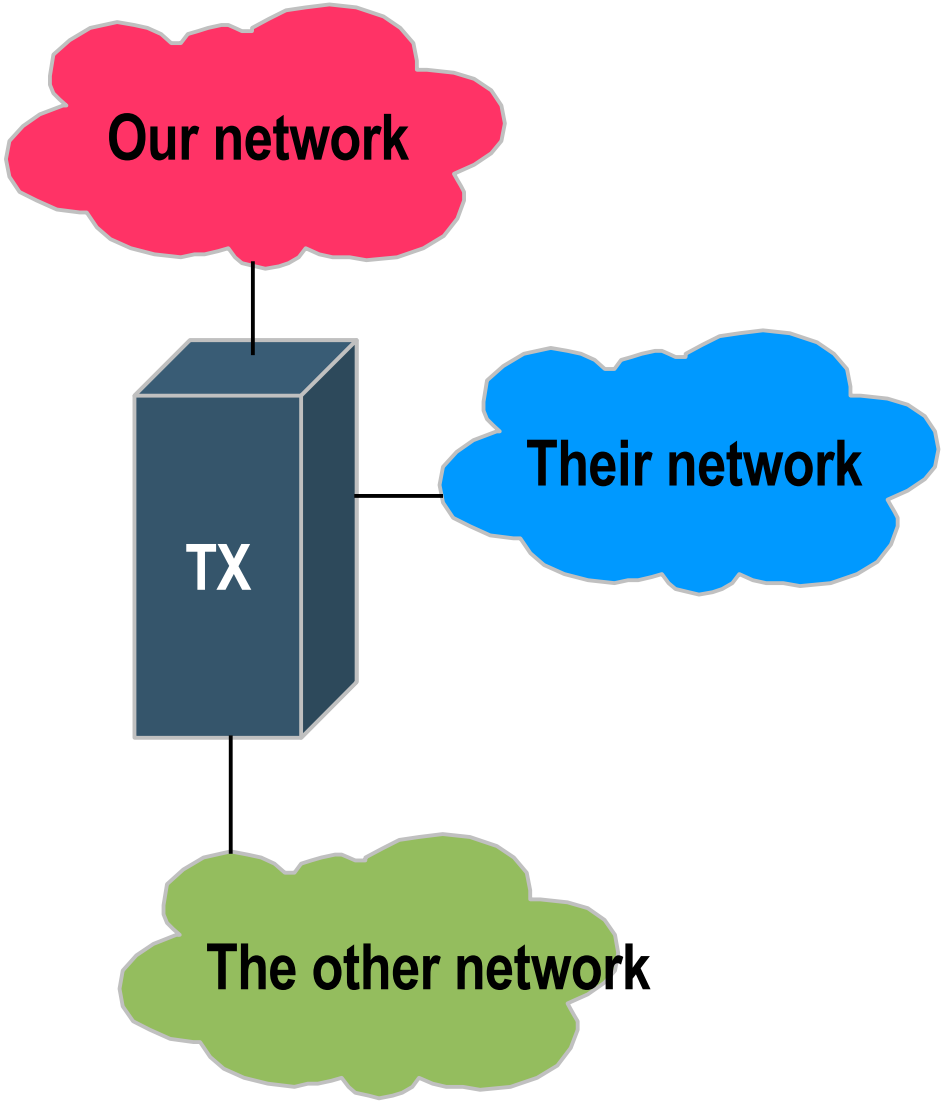
- Use it as a desktop system
  - with a strict policy for people with such needs
    - Heavily regulated sectors as well as the usual suspects
  - with a loose policy for us :)
    - Labeling to help keep track of what's what
    - avoiding unintentional disclosure (but giving the choice)
    - and avoiding unintentional mislabeling
  - or something in between
    - plug in your own policy

something in between

- Boundaries are where policy can be adjusted
  - Relabeling
    - files
      - /etc/security/tsol/relabel is a shell script...
    - copy/paste buffers
      - no equivalent (yet)
  - Multilevel services
    - Modified services (if they need to do policy enforcement)
    - Unmodified (if they're there for convenience)

TX: The Glorified KVM Switch

- Users log in on TX desktop
  - Workstation or Sun Ray
- TX considers the different networks as being disjoint
- Only local applications are vnc, RDP client or similar



Beyond the desktop

- Using TX as a controlled L7 firewall
  - differently labeled networks can't communicate
  - zones can't either, except for privileged processes
    - And then only if labeling and privilege configuration allows
    - Chain of (privileged) proxies in subsequent zones
    - Only way to get to other side is via the controlled channel

Cross-domain browsing

- Connecting multiple networks
  - “Corporate network”
  - “Partner network”
- Disallow communication between the two
  - suspenders and a belt: TX + ipfilter
- Chaining proxies

More stuff beyond the desktop

- Automatic file relabeling
  - Similar idea to chaining proxies, but now policy-enforcing components are chained
  - Documents forced to take a specified path, e.g. internal > processing > external
  - Policy checks on the way; chain broken if a check fails

Going forward...

- Labeled IPsec
  - opensolaris.org/os/project/txipsec/
- Further TX refinements
  - opensolaris.org/os/community/security/projects/tx/
- Further OpenSolaris refinements
  - RBAC, Auditing,... at opensolaris.org/os/community/security/

Bart Blanquart
bart.blanquart@sun.com