UNICOS/MLS – IRIX/TRIX

Experiences with CRAY UNICOS–MLS and sgi IRIX/TRIX

Mats S Andersson

Associate Director

National Supercomputer Centre
Linköping University
Sweden

msa@nsc.liu.se

NSC

- *Offer supercomputing capacity and support to Swedish academic users*
- *Sharing supercomputer resources with Saab AB since 1983*
- *Consortia with Saab AB and Swedish Meteorological and Hydralogical Institue since 1996*

NSC history

Hardware	In operation	Security system	Shared with
CRAY-1	1983-1989		Saab AB
CRAY-XMP	1989-1993	UNICOS-MLS (1992-93)	Saab AB
CRAY-YMP	1993-1996	UNICOS-MLS	Saab AB
MasPar 1200	1994-1998		
Parsytec	1994-1998		
CRAY-C90	1996-2000	UNICOS-MLS	Saab AB, SMHI
CRAY-T3E	1997-	UNCOS/mk-MLS	Saab AB, SMHI
PC-clusters	1999-		
sgi2400	2000-2001	IRIX/TRIX	Saab AB, SMHI
sgi3800	2001-	IRIX/TRIX	Saab AB, SMHI

Reasons for enhanced security

Group	*Requirements*
Saab AB	
Military projects	*Classified data – military requirements*
Non military projects	*Classified data – Industry requirements*
SMHI	*Data integrity*
NSC	*Data integrity*

Security models

- ***Between organisations***

  Compartments – Categories

  No communication between compartments/categories

  Horizontal

- ***Within organisations***

  Sensitivity/Integrity levels

  Controlled communication between levels

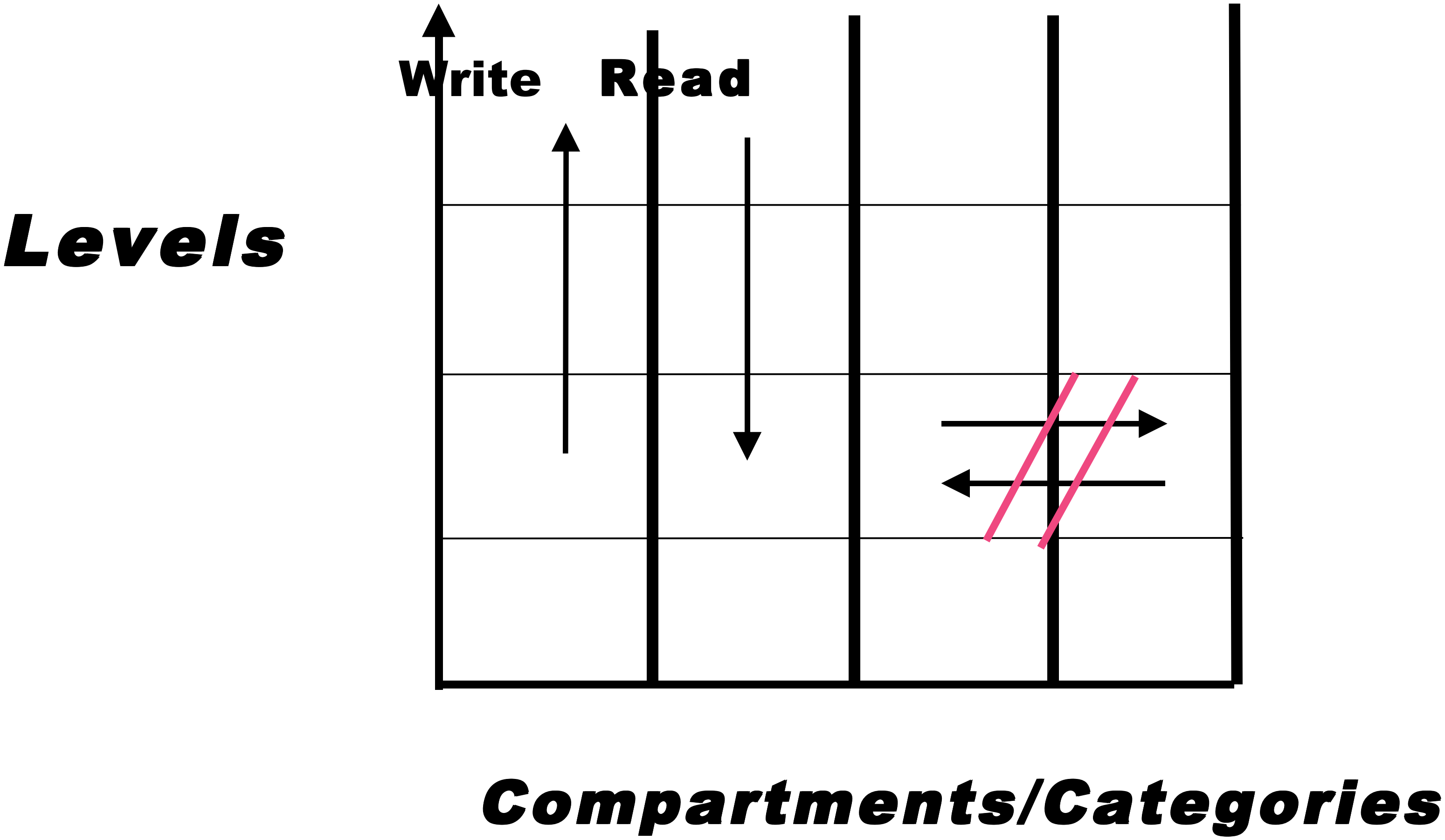
  Hierarchical – Vertical

Security models

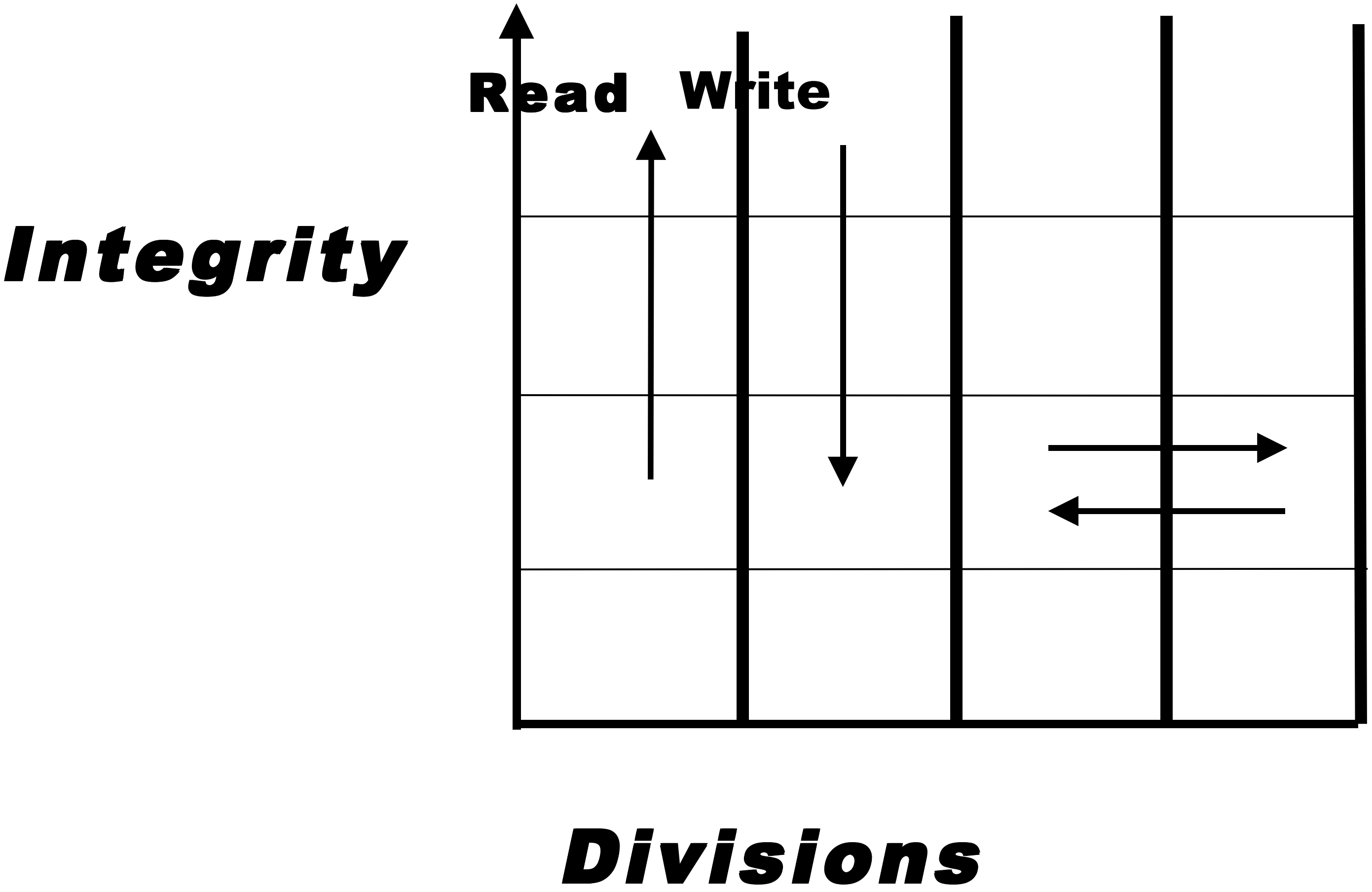
- *Sensitivity Who should see this*
  - *Writing up*
  - *Reading down*

- *Integrity Can you trust this*
  - *Reading up*
  - *Writing down*

Levels – Compartments



Integrity – Divisions



DAC – MAC

- Discretionary acces control – C1 / C2
    - Standard UNIX
    - User driven

- Mandatory access control – B1
    - Sysadm/secadm driven

Evaluated systems

- *UNICOS 8*
  - *Evaluated 1995-03-09*
  - *B1 Labeled Security Protection Profile*
- *IRIX/TRIX*
  - *Evaluation in progress (SAIC)*
  - *Common Criteria B1 Labeled Security Protection Profile*

MLS – TRIX solution

- *Dynamic allocation of CPU and primary memory resources*
- *Static allocation of file space (file-systems)*
- *Static allocation of network resources (interfaces-network addresses)*

- *Much more work to configure*
- *More work to maintain*

Alternative solution

- *Hardware split of system*
- *No MLS/TRIX to configure and maintain*
- *Less dynamic – more hardware to get same throughput*
- *Needs hands on every time you move the border*

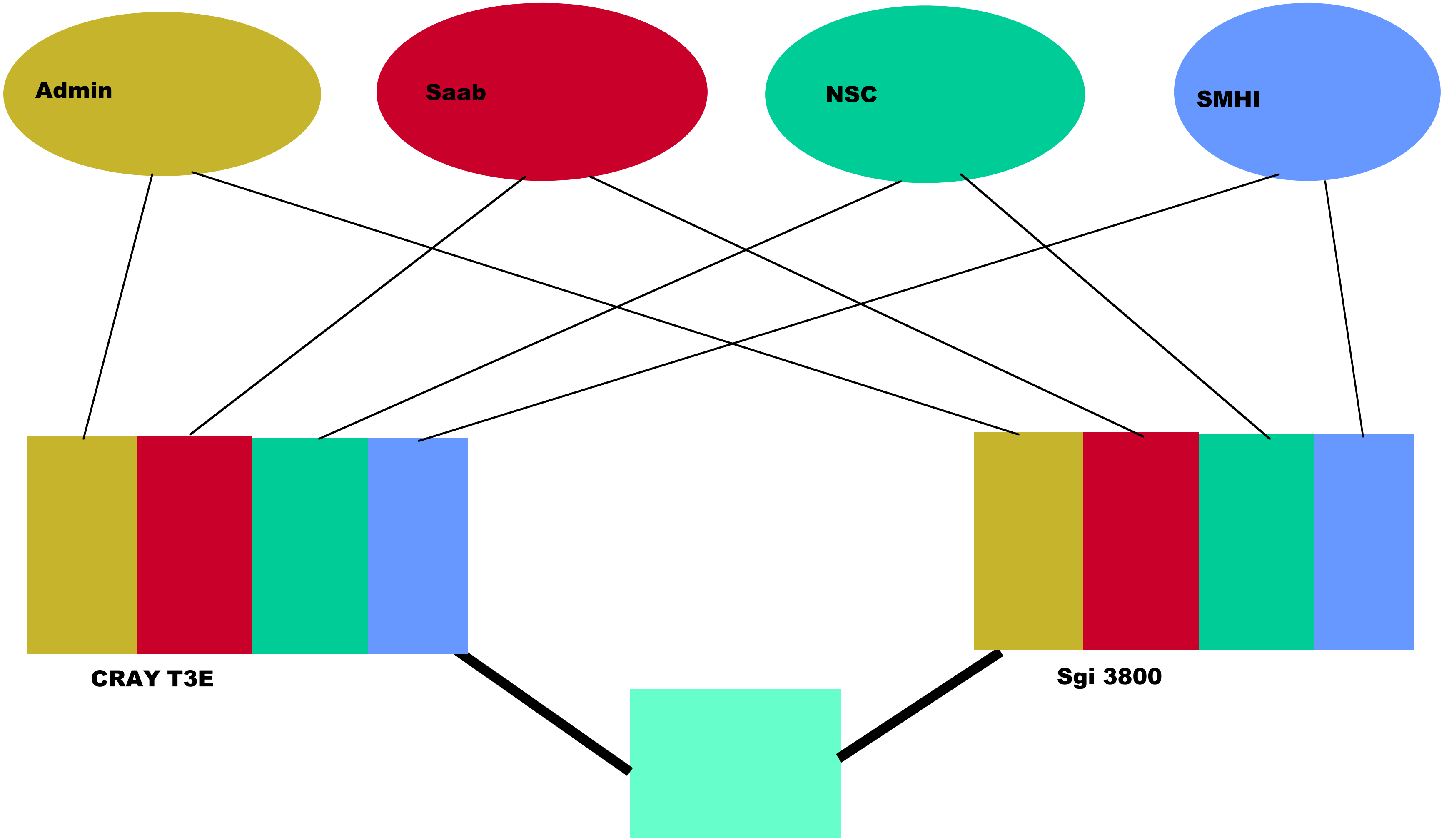
Labeled objects

- *Users*
- *Processes*
- *Files/file systems*
- *Network interfaces / addresses*

What to configure

- *User accounts*
    - *Label*
        - *Capability – what is a user alloved to do*
        - *Clearance – what compartments/categories can the user join*
- *File systems*
    - *Label*
    - *Multi-level filesystems (/tmp, /spool .....)*
- *Network interfaces/addresses*
    - *Label*

Ideal network configuration



Admin

Saab

NSC

SMHI

CRAY T3E

Sgi 3800

Stk9

User view

- *User should see as little as possible of the security system*
    - *Normal view within their own compartment/category*
    - *Do not see other other groups processes*
    - *Can see other groups batch-jobs*
- *Some tools may be missing*

Sysadm view

- *More work*
- *Much more work in*
  - *Account administration*
  - *Network administration*

Be very careful!
Easy to make the system very secure!

Auditing – Monitoring

- ***Without auditing no security***
- ***Select the level of auditing carefully***

- ***Tools will not always work the way you are used to***
- ***Remote monitoring can be very difficult***

Batch – HSM

- *Batch system*
  - *NQE – LSF*
    - *”Common” queues for all users*
    - *Batch administrator can see jobs but not the data*

- *HSM*
  - *DMF*
    - *Security information on tape ?*
    - *Few TRIX/DMF installations*

Prepartions

- *Select security model very carefully*
- *Much harder to change when in operation*

- *Be sure the support/consultant understand your environment and your requirements*

- *Doublecheck !*

Test suite

- ***Setup a test procedure to verity the configuration***
- ***Produce a test protocol***

- ***Should be rerun after upgrades***

Upgrade

- *Upgrade procedures takes more time – often less tested*
- *Check ”protection” of optional/third party software*
- *Verify security setup after upgrade*
- *Verify functionality after upgrade*

Summary

- *Describe your environment and your requirements*
- *Select security model to use*
- *Doublecheck support/consultants view*
- *Allocate much more time for system confiration and testing*
- *Allocate more time to do sysadm jobs*
- *Lack of training*
- *Sparse documentation*

- *Lack of MLS/TRIXified tools*