Multilevel Security at SGI

Casey Schaufler

Engineering Manager

Trust Technologist

casey@sgi.com

The Trusted Irix Product

An all platform product

- Desktop Graphic Systems
  - Compartmented Mode Workstation
- 512 Processor SuperComputers
  - Multilevel Secure Server

History of Trusted Irix

We’ve been at this a while

- Began Development 1989
- 4.0.1 Shipped 1991
- 4.0.5epl EPL Entry 2/1995
- 6.5se Shipped 4/1998
- 6.5.13 Common Criteria Evaluation 5/2002
- 6.5.x Ships Quarterly

Trust Technology Features

You can do that

- Limit the privilege a program uses
- Document system misuse
- Finely specify user access
- Strongly separate users
- Have confidence in the facilities

Capabilities

Implementation of least privilege

- Trix and Irix
- P1003.1e/2c interfaces and behavior
- Permissions to violate specific system policies
- Set on program files
- Inherited from parent processes

Security Audit Trail

Big Brother never had it so good

- Trix and Irix
- Tracks every access control decision
- Selection by user and event
- Fundamental analysis tools
- Real time processing capable

Access Control Lists

When group lists aren’t good enough

- Trix and Irix
- P1003.1e/2c interfaces and behavior
- Permission bits for arbitrary user sets
- Directory default ACLs

Mandatory Access Control

Strong separation of users

- Trix
- P1003.1e/2c interfaces and behavior
- Separation by compartments or projects
- Hierarchical discrimination
- TSIG session management protocols
- Integrity protection

Evaluations

NIAP Common Criteria Program

- National Information Assurance Program
- US version of the Common Criteria Scheme
- CAPP
  - Controlled Access Protection Profile
  - Replaces NSA C2
- LSPP
  - Labeled Security Protection Profile
  - Replaces NSA B1

Standard Interfaces

De Facto Security Interface Standards

- Supported by all system vendors
- POSIX P1003.1e/2c (P1003.6)
  - Programming APIs
  - MAC, ACLs, Capabilities
- Trusted Systems Interoperability Group
  - Programming APIs
  - Security attributes over the network
  - Network security protocols

Capabilities Feature

Limit privilege availability

- Users have capability profiles
- Programs marked with the capabilities
  - They will always have
  - They may inherit
  - They may never have
- About 40 distinct capabilities
- On Trix this is the only privilege scheme
- On Irix there is also a Superuser

Audit Trail Feature

Monitor access control decisions

- Select by user, MAC label, event type
- Simple token based record format
  - Records made up of about 20 unique data types
- Track administrative database changes
  - covici(1) revision control tool
- Advanced audit trail management
  - log rotation, reuse, and retry options
  - files, directories, and devices

Access Control List Feature

Extending file permission bits

- Read, write, and execute bits
- Specified by users or groups
- Up to 25 entries
  - That is too many to manage
- Most specific matched entry decides
- Works correctly with traditional mode bit manipulations

Mandatory Access Control Feature

Sensitivity and integrity controls

Sensitivity - protects data from users

- 256 Levels (e.g. Secret, TS)
- 65,536 Categories (Compartments)

Integrity - protects users from data

- 256 Grades
- 65,536 Divisions

Special labels isolate system data

Compartmented Mode Workstation

Defense Analyst's Desktop System

- Multilevel Window System
- Cut & Paste up, not down
- Windows at multiple MAC labels
- OpenGL Support

Distributed Development

All of SGI works on the trusted systems

- Architecture - Mountain View, CA
- Maintenance - Melbourne, AU
- Evaluation - Columbia, MD

Evaluation Status

Walking the walk

- EAL3
- *Irix 6.5.13*
  - Controlled Access Protection Profile
- *Trix 6.5.13*
  - Labeled Security ProtectionProfile
- *Certificates Awarded May 13,2002*

Popular Configurations

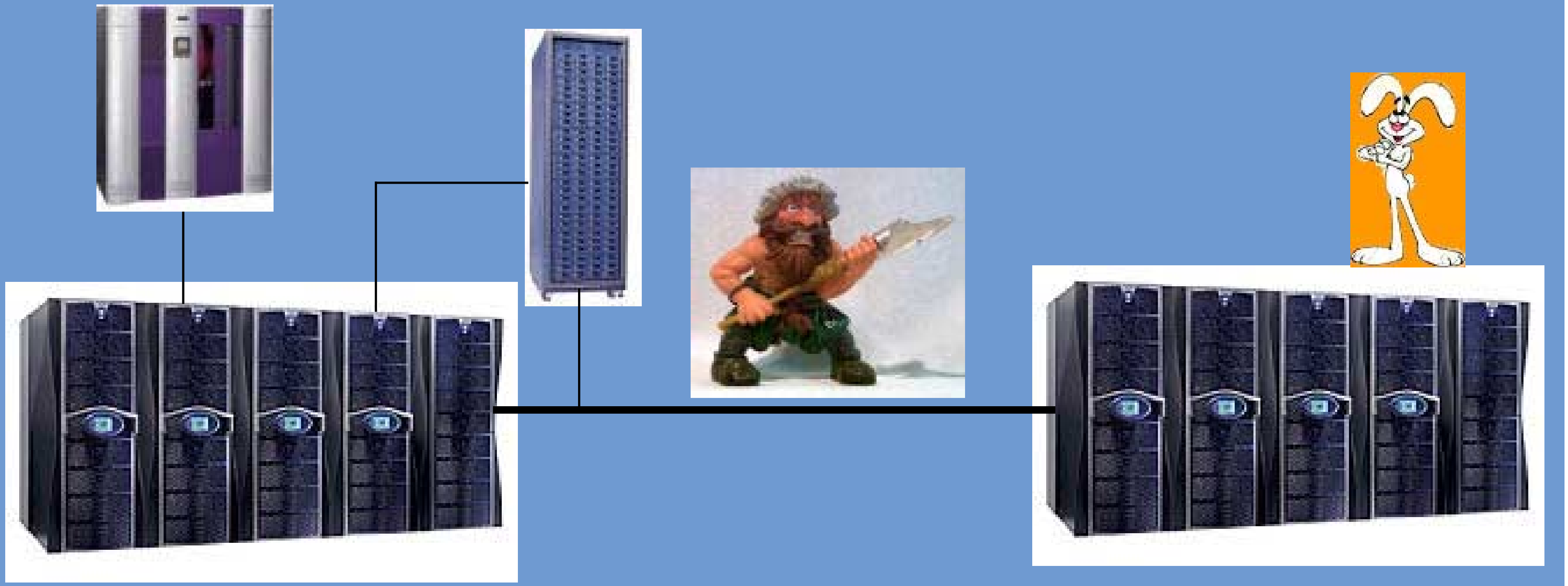
The Trix rabbit indicates which systems in each of these real deployments are running the Trusted Irix/CMW product.

Sharing A Supercomputer

A single Trix Supercomputer is shared by three diverse interests.

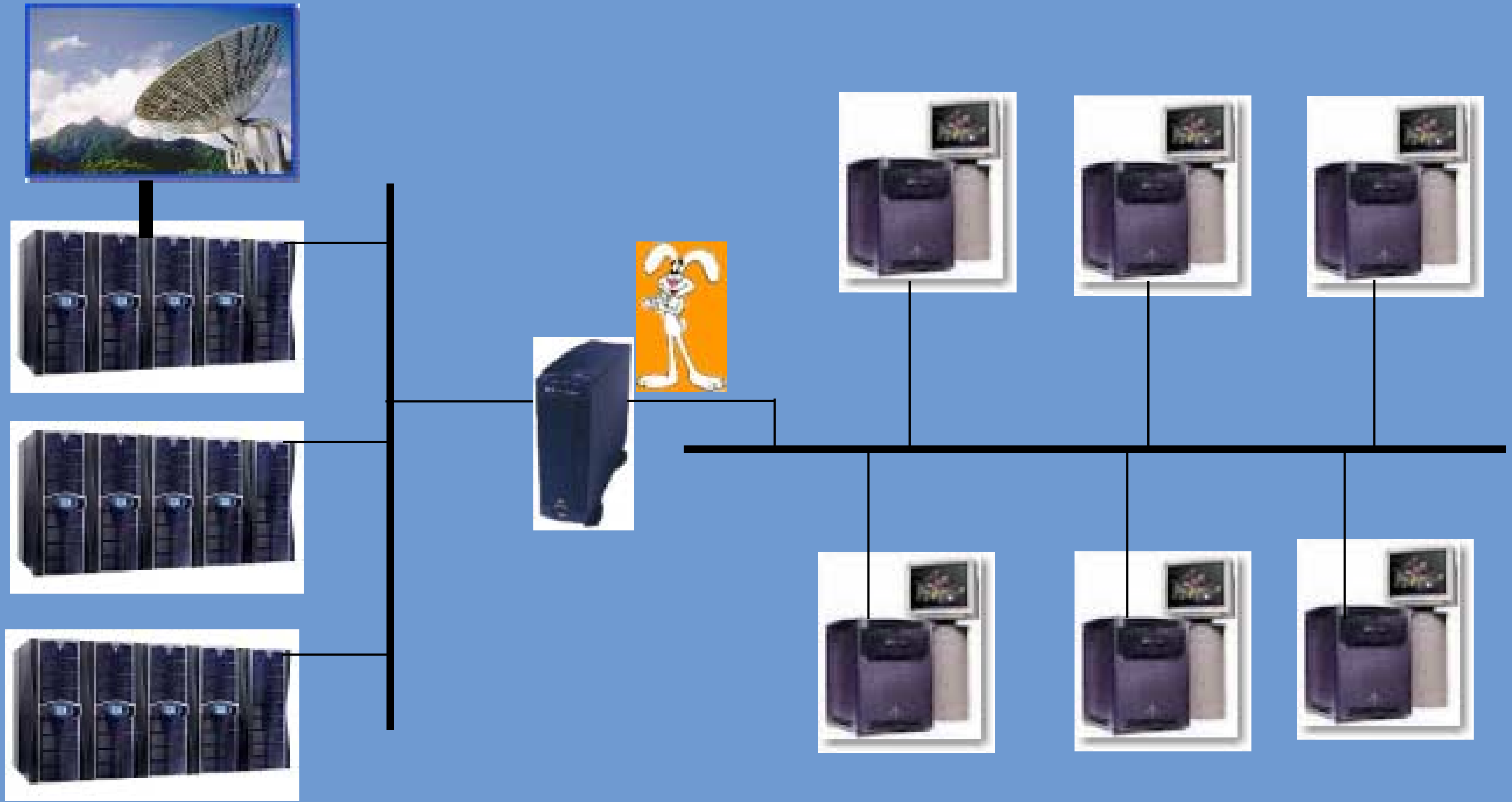
Down By The Fjord

Trix, CXFS, and a large knife switch allows a university and commercial enterprise to share computing resources.



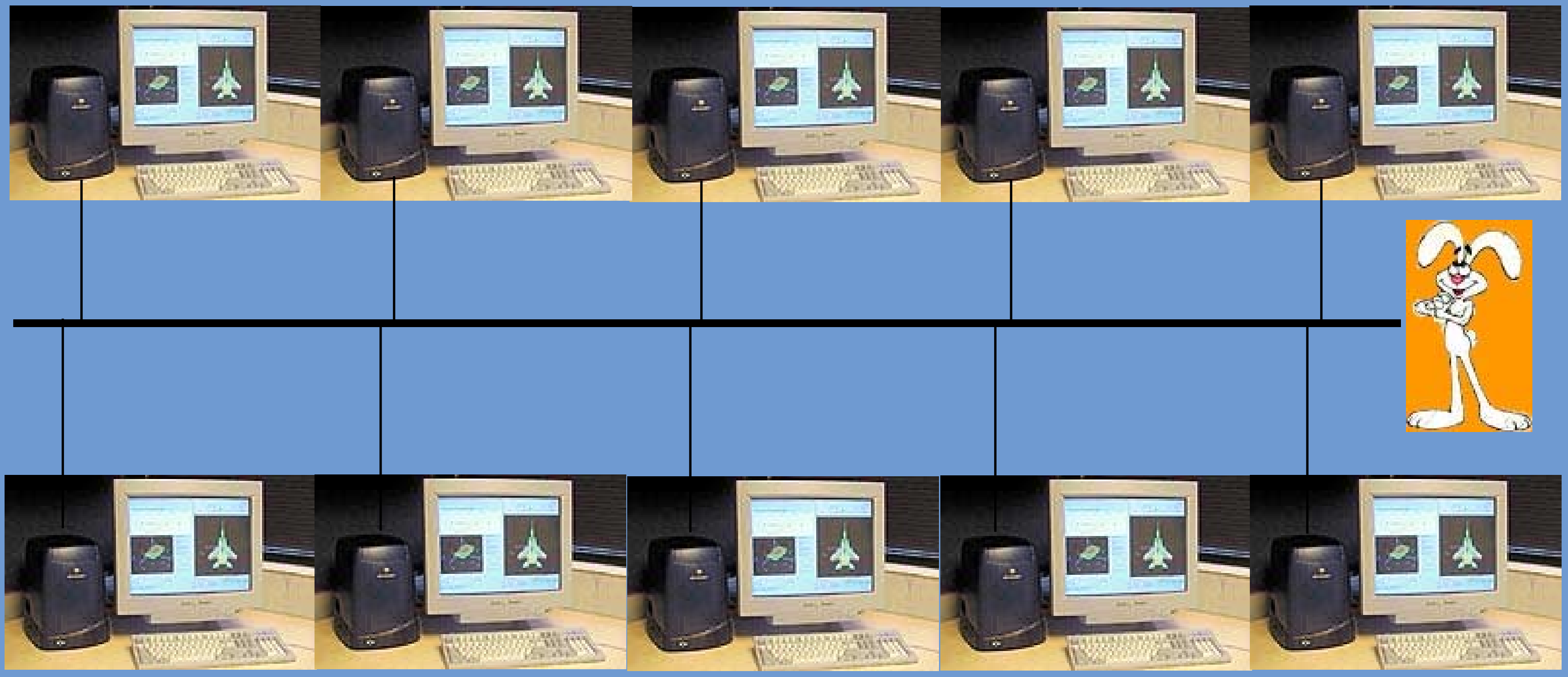
Rocky Mountain System

A guard box application on Trix allows safe downgrading of classified information.



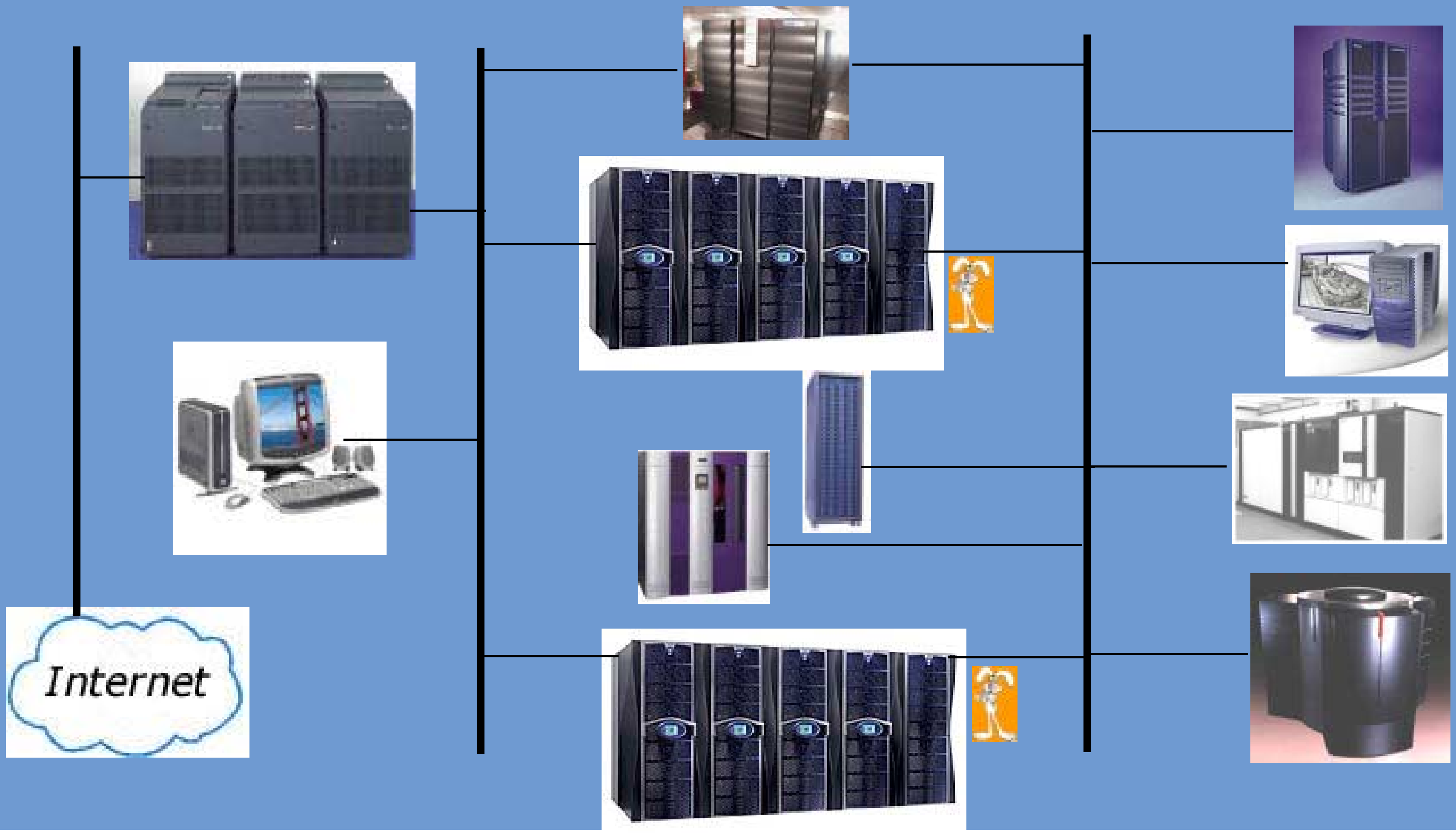
Maryland Machines

Everyone runs Trix here!



California Community

Here they have classified, unclassified, old, new, and multilevel systems.



Serious Security

SGI Provides It

- *Commitment To Compatibility*
- *Meet Or Exceed Accepted Criteria*
- *Assurance Through Evaluation*
- *Long Term Commitment*