Have You Driven an SELinux Lately?

An update on the Security Enhanced Linux Project

James Morris
Red Hat Asia Pacific Pte Ltd

Ottawa Linux Symposium 2008

Project Timeline

- 1980s – 1990s
  - Academic R&D
- 2000 – 2003
  - GPL release, upstream merge
- 2003 – 2005
  - Distribution integration
- 2005 – present
  - Infrastructure and usability improvements

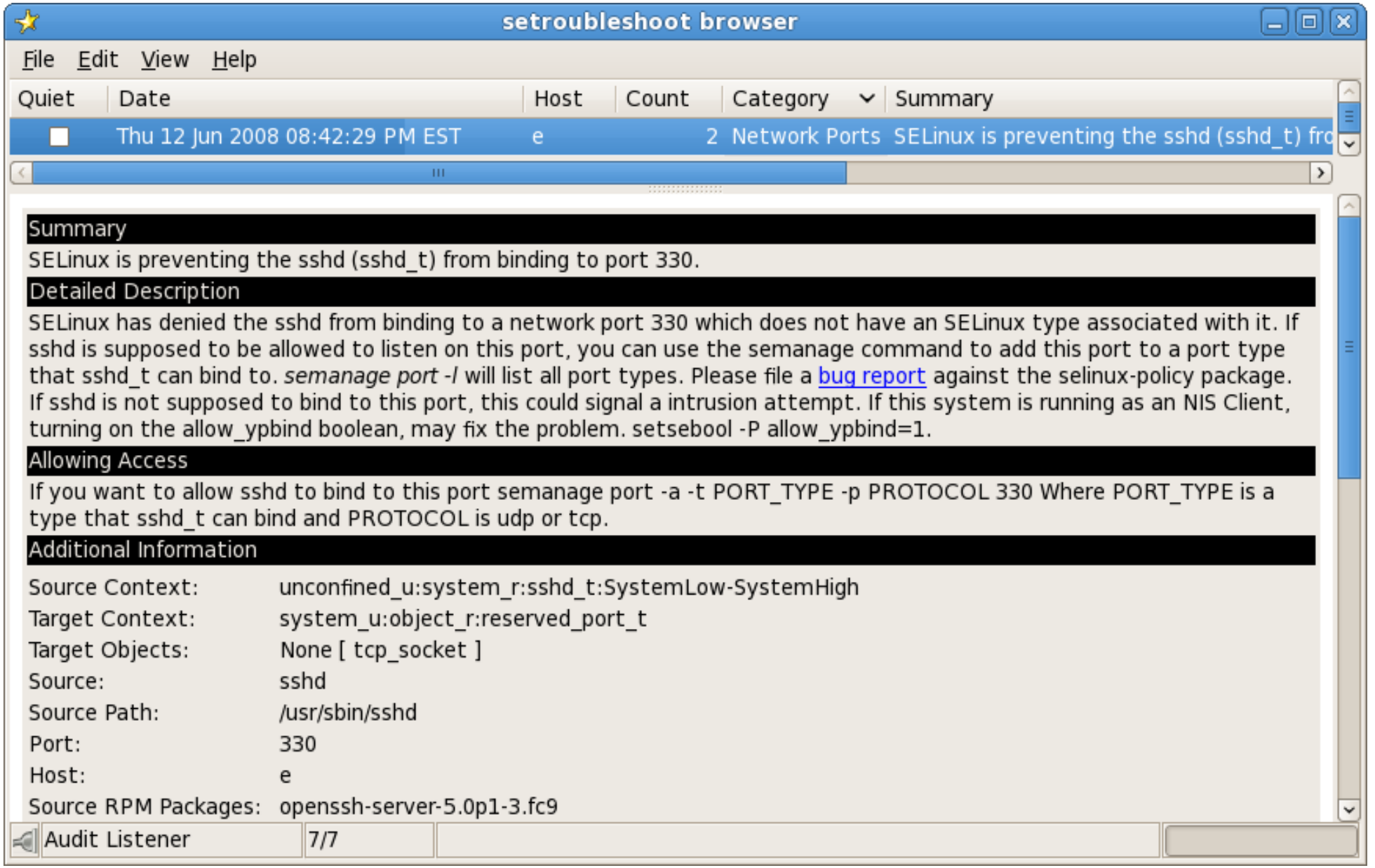
Infrastructure Work

- Loadable Policy Modules
- Reference Policy
- Policy Booleans
- Libraries
- Toolchain

User Experience

- Targeted Policy
  - Initially confined only critical applications
  - Now re-merged with hundreds of modules
    - Targeted behavior selected via the *unconfined* module
- Setroubleshoot
  - Inspired by GNOME bug buddy

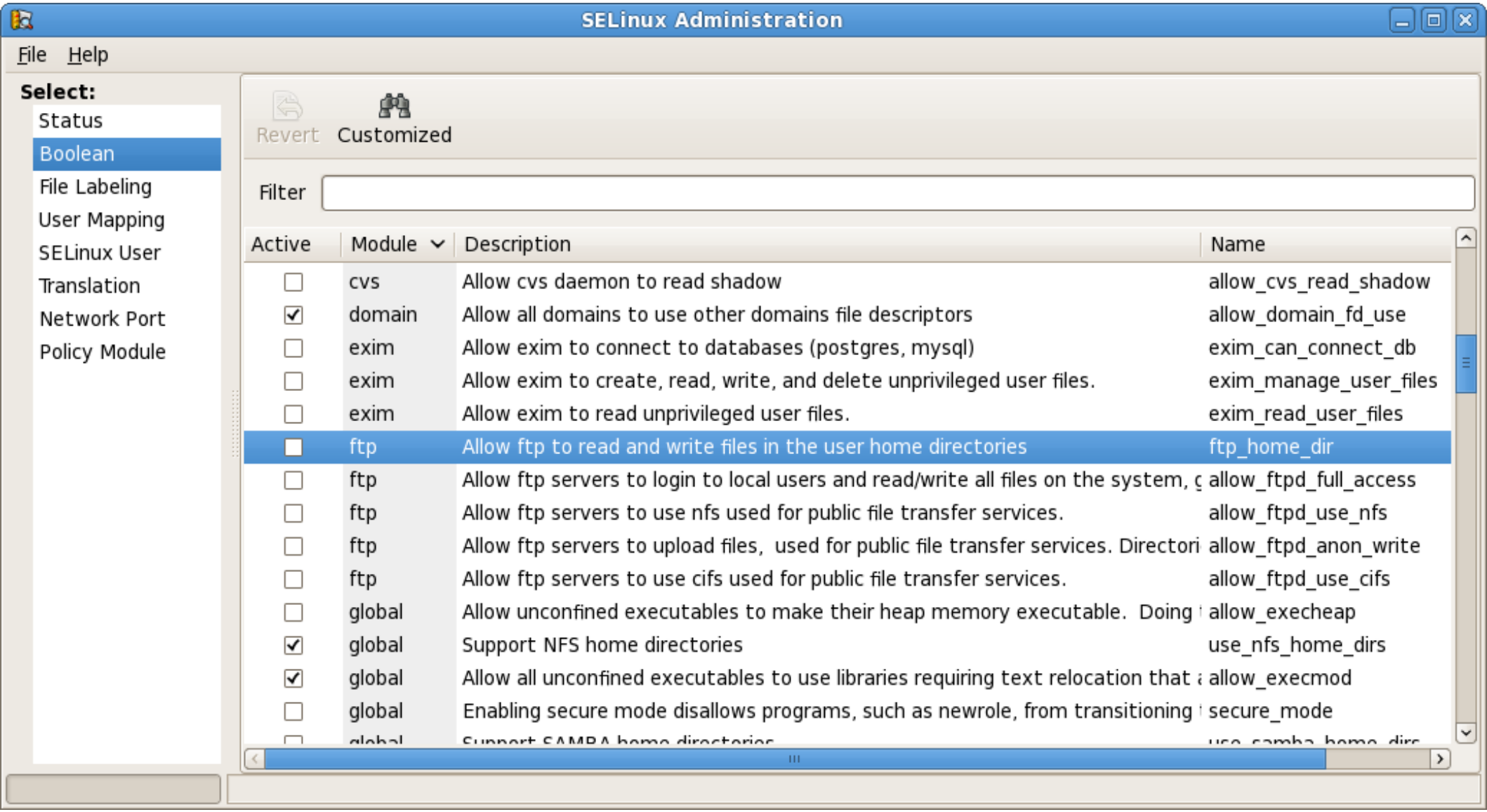
setroubleshoot



System Administration

- audit2why
- semanage
- restorecond
- system-config-selinux

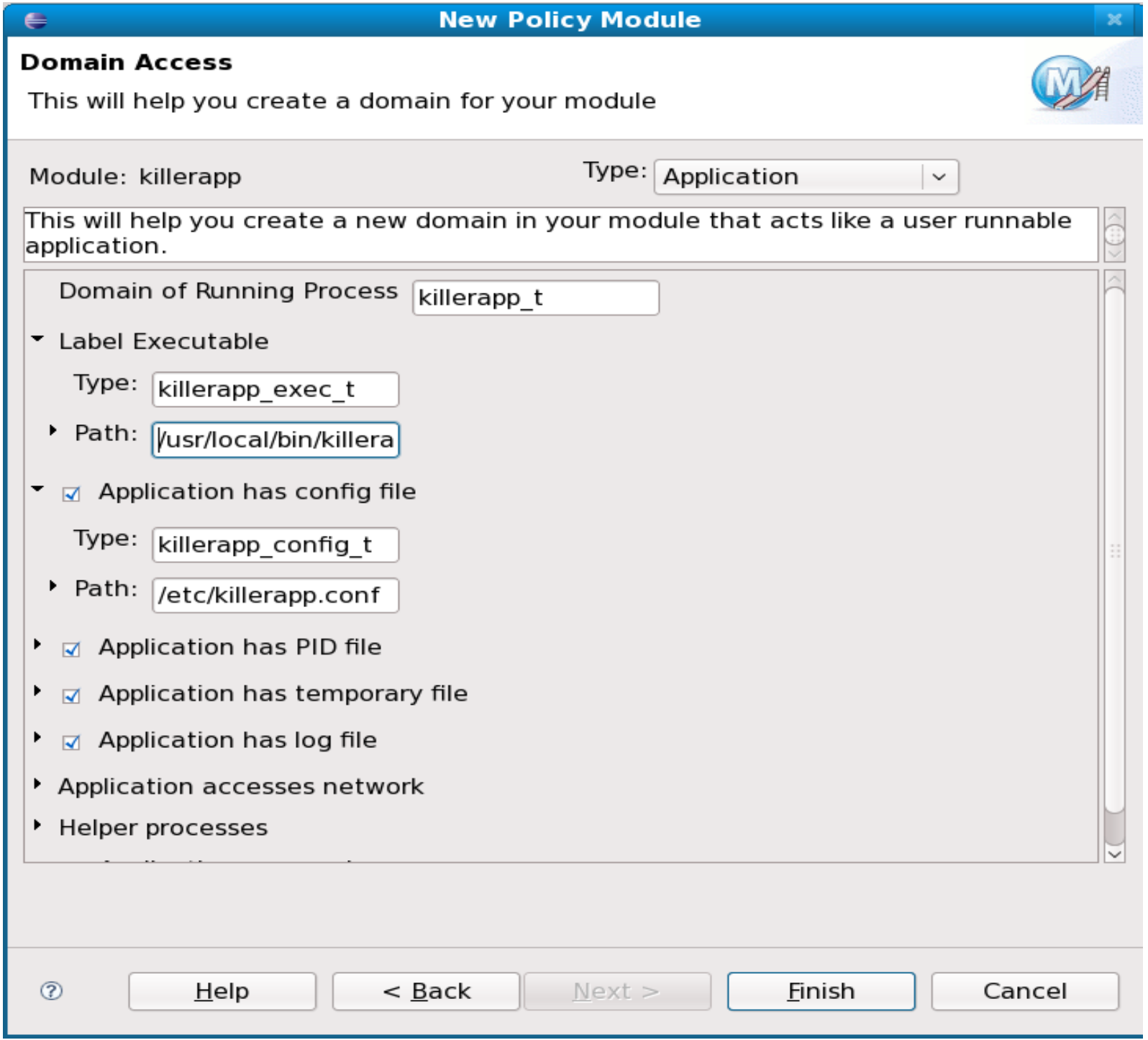
system-config-selinux



Policy Development

- Command line tools for quick fixes
- SLIDE
- SEEdit

SLIDE


New Policy Module
Domain Access
This will help you create a domain for your module
Module: killerapp
Type: Application
This will help you create a new domain in your module that acts like a user runnable application.
Domain of Running Process
killerapp_t
Label Executable
Type:
killerapp_exec_t
Path:
/usr/local/bin/killera
Application has config file
Type:
killerapp_config_t
Path:
/etc/killerapp.conf
Application has PID file
Application has temporary file
Application has log file
Application accesses network
Helper processes
Help
< Back
Next >
Finish
Cancel

Core Enhancements

- Performance and scalability improvements
- Integrated with kernel memory protection
- Netfilter-based network controls
- Labeled Networking
- Better MLS

Security Evaluation

- RHEL5 Common Criteria certifications
  - LSPP, RBACPP, CAPP at EAL4+
  - IBM, HP and SGI hardware
  - Community effort
  - Led to improved audit and other features
- Other Accreditation
  - US Coast Guard Intelligence case study

Threat Mitigation

“A security framework originally published by the US National Security Agency has begun to rack up an impressive list of protections against security holes.”

- *LinuxWorld, Feb 2008*

- SELinux has mitigated several serious security threats to everyday users of Fedora & RHEL.

- Tracked @ Tresys Mitigation News

SELinux Adoption

- Widely adopted in Fedora
  - Smolt statistics show majority have SELinux **enabled.**
- RHEL adoption by military, govt, finance:
  - Factor in NYSE/Euronext adoption, handling over $140 Billion/day in trades.
- Embedded / consumer electronics:
  - Reduce risks and costs of vulnerabilities
  - Simpler systems can have tighter policy

Kiosk Mode (xguest)

- Anonymous desktop sessions
- Innovative application of several security technologies
- Useful for conferences, training, trade shows, libraries, child-proofing...

Current Work

- Wider distribution support:
  - Ubuntu, Debian, Gentoo
- Beyond kernel:
  - Virtualization (XSM)
  - Desktop (XACE)
  - Storage (LNFS)
  - Applications (Database etc.)
- Beyond Linux:
  - OpenSolaris FMAC

Challenges

- Improved usability, as always!
- Documentation
- Keep community growing

How to Participate

- Install SELinux enabled distribution
- Join mailing lists
- IRC
- Ask questions, report bugs!

by marco_ely @flickr