redhat.

SELinux

Daniel J Walsh

SELinux Lead Engineer

0 Day Exploits

- Patch Cycle
  - Someone discovers a vulnerability in software
  - Package Maintainer and OS Vendor Notified
  - Fix generated/Distributed
  - Fix installed by users
- What protects you before the fix is installed?
- What happens if the wrong people find the problem and don't report it?
- Exploits that don't have a patch built for them are called 0-Day Exploits.
- What are attackers after?
  - Spam...
  - Where is the good stuff?

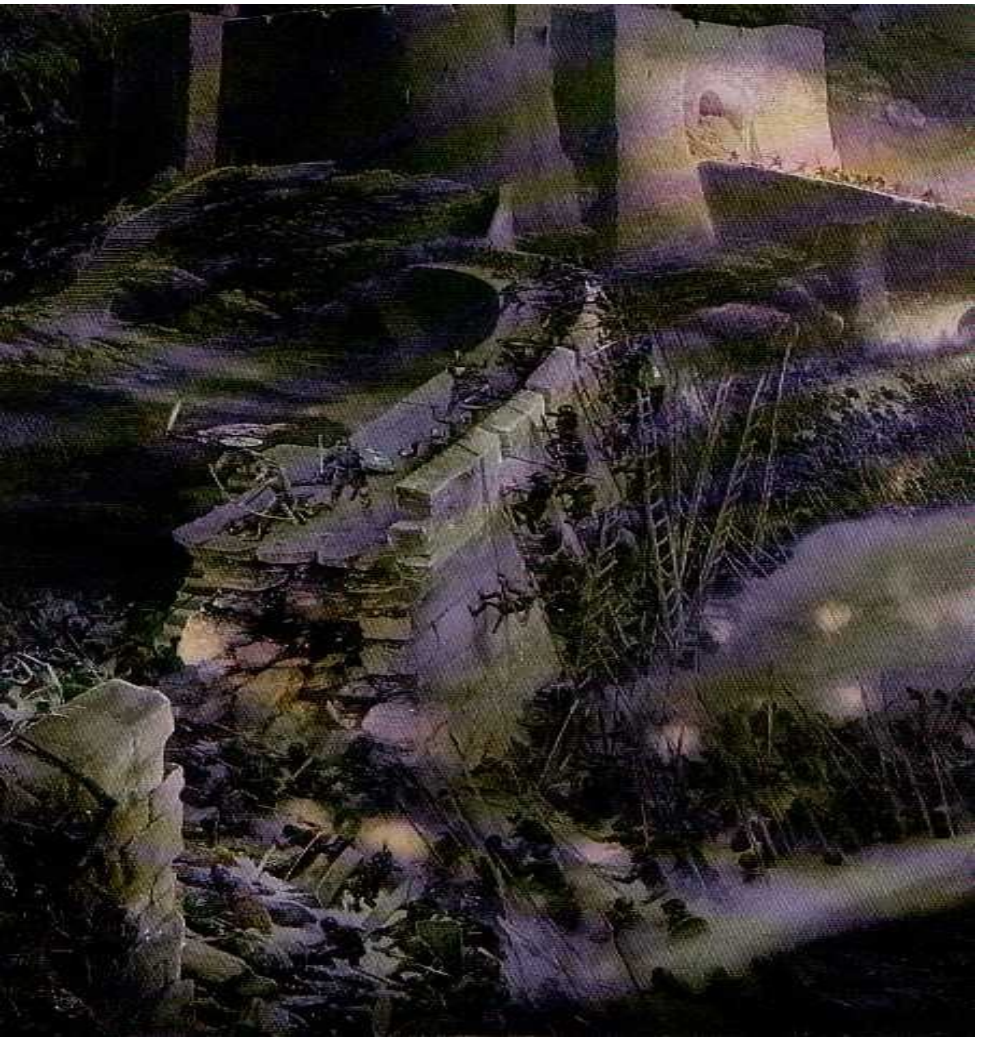
What is SELinux?

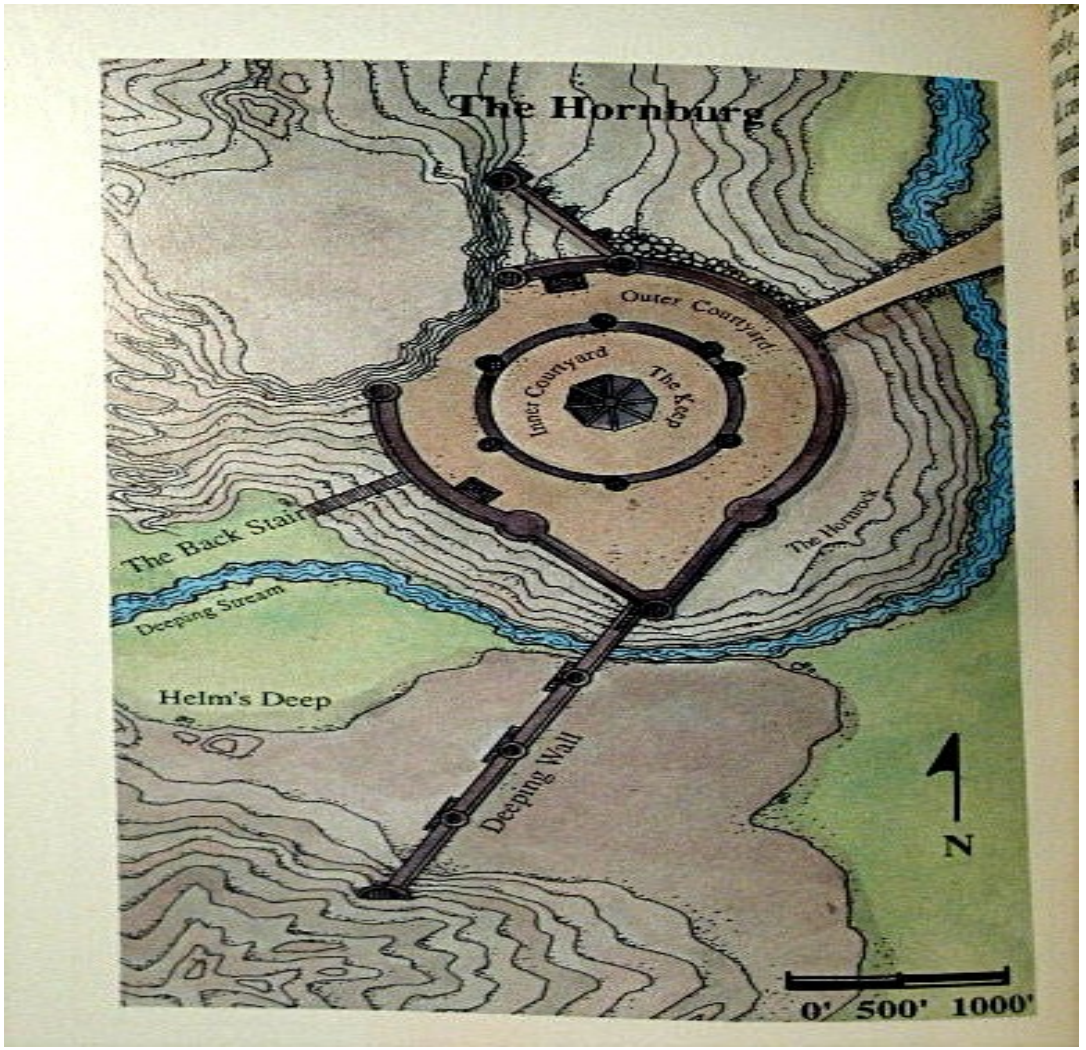
Mandatory Method (MAC)

- Current systems use DAC (Discretionary Access Control)
- User/Programs has limited privilege
- Security policy set by administrator and enforced by the System
- Incorporates program function/trustworthiness into A/C decisions.
- Root compromises confined by policy

Compartmentalization

Helms Deep – Lord of the Rings





Developed by the NSA

Building on 10 years of NSA's OS security research

Application of NSA's Flask security architecture

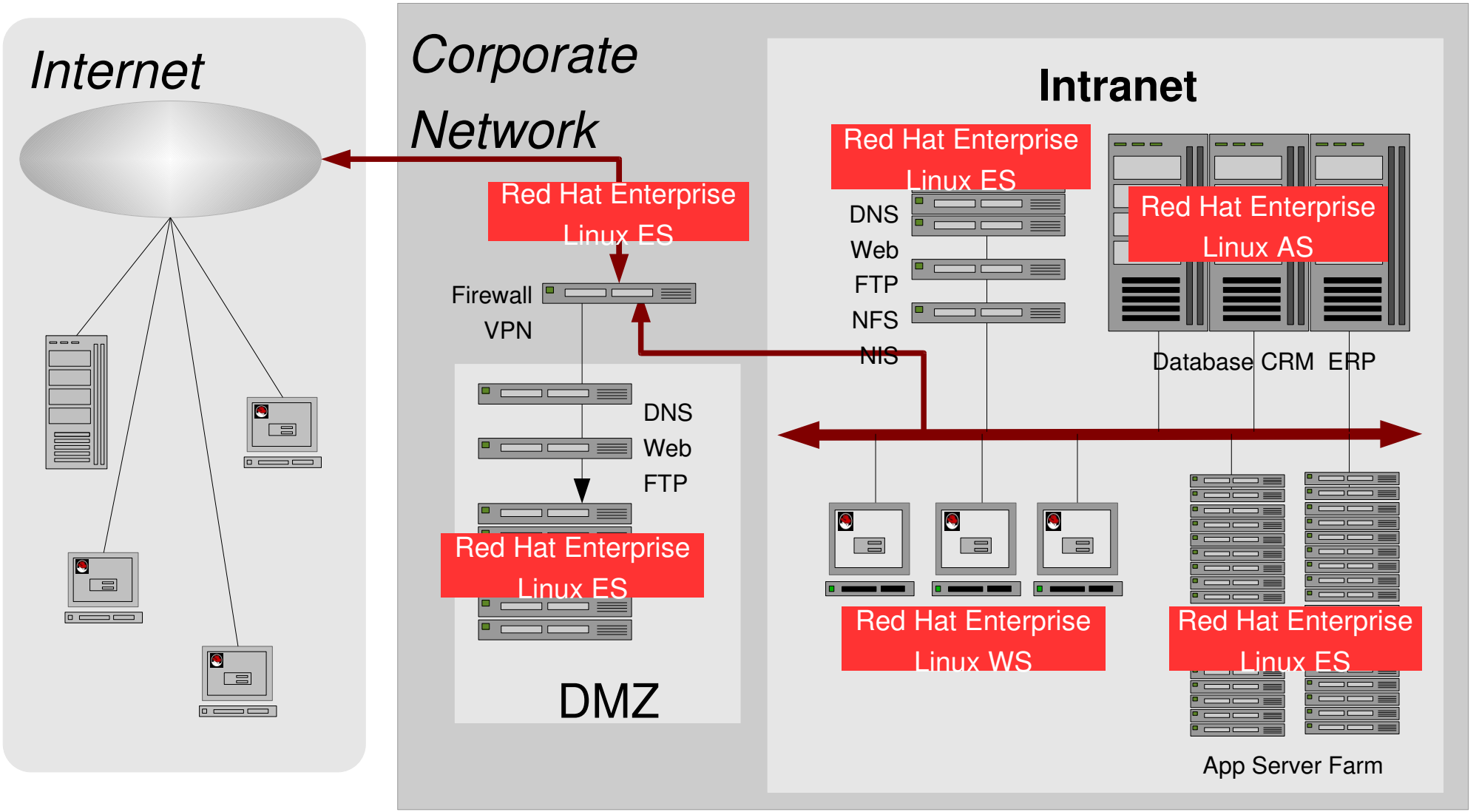
- Cleanly separates policy from enforcement using well-defined policy interfaces
- Fine-grained controls over kernel services
- Transparent to applications and users
- Removes power of root
  - Several demo machines running root as guest account

Why should you use SELinux

SELinux kernel enforces MAC policies

- Confines programs/system servers to minimum privileges
  - Reduces or eliminates harm caused by compromised applications.
- root's power decomposed: Principle of least privilege.
- Traditional operating systems depend on
  - Correctness of the Kernel
  - All the privileged applications and their configurations
- SELinux kernel depends primarily on
  - Correctness of Kernel
  - Security policy configuration.

Where should you run SELinux?



SELinux Key Components - Kernel

Patch implementing security hooks

- Uses Linux Security Module (LSM)
- Framework for security enhancements to Linux
- OTHER Linux Security Modules have been written, but SELinux is the only one in widespread use.

SELinux Key Components - Policy

Strict

- A system where everything is denied by default.
  - You must specify allow rules to grant privileges
- SELinux designed to be a strict policy.
  - The policy rules only have allows, no denies.
  - Minimal privilege's for every daemon
  - separate user domains for programs like GPG,X, ssh, etc
- Difficult to enforce in general purpose Operating system.

SELinux Key Components - Policy

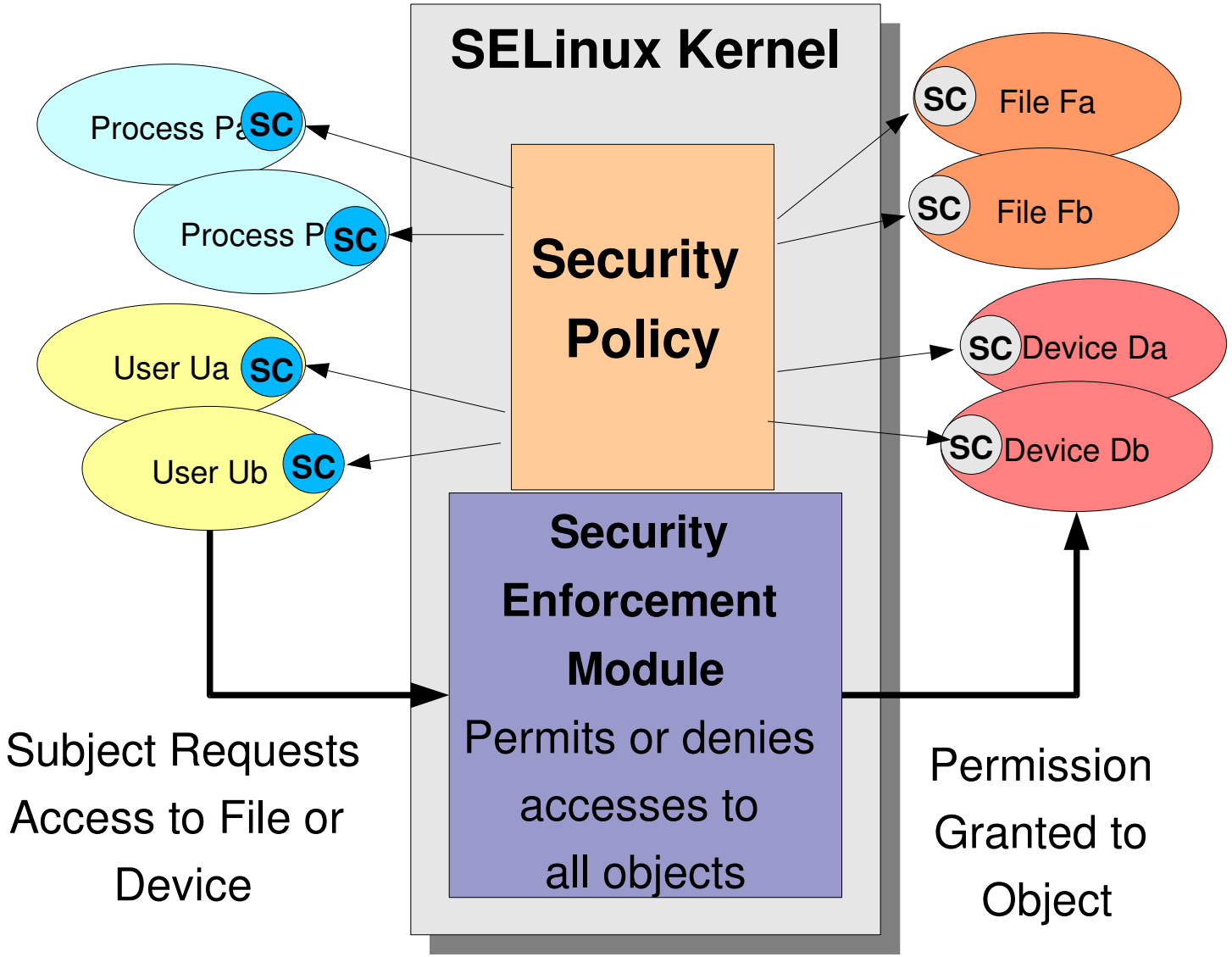
Targeted

- System where everything is allowed. use deny rules.
- Protects systems Doors and Windows
- By default processes run in unconfined_t.
  - unconfined processes have the same access they would have without SELinux running.
- Daemons with defined policy transition to locked down domains.
- httpd started from unconfined_t transitions to httpd_t which has limited access.

SELinux Key Components - Applications

- Most user applications and server applications unchanged
- SELinux aware applications
  - Applications used to view or manipulate security contexts
  - Programs required to set user session security context
  - Examples: login/sshd, ls, cp, ps, setfilecon, logrotate, cron ..
  - DBUS, Trusted-X

How SELinux Enforces Security Policy



Apache Example

- Apache executable unmodified
- System administrator might have three choices of policy
  - High - Apache only can display html pages in /var/www/html
  - Medium – Apache can run cgi-scripts in /var/www/cgi-bin
  - Low – Apache can display pages in users home directories
- Cracker only has access to files that Apache had access too
  - If Apache had read access to /var/www/html that is all cracker can do.
  - Cracker can cause other pages to display.

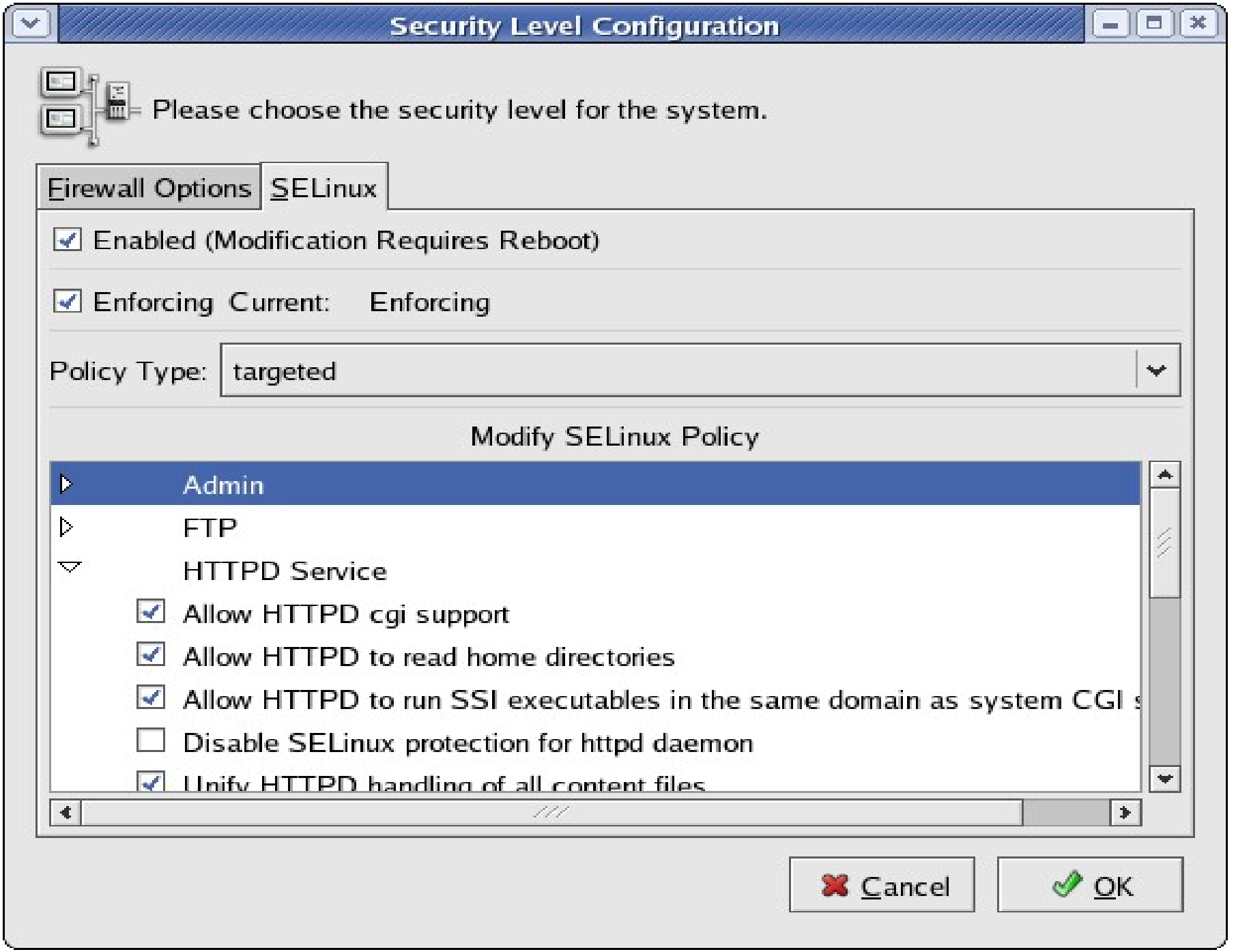
Configuring Policy

Booleans

- Turn on/off sections of policy
  - setsebool -P allow_nfs_home_dirs 1
  - /etc/selinux/targeted/booleans

File Context

- chcon -R -t httpd_sys_script_rw_t /var/www/myapp/data
- chcon -t httpd_sys_script_t /var/www/cgi-bin/myapp
- /etc/selinux/targeted/contexts/files/file_contexts.local


Security Level Configuration
Please choose the security level for the system.
Firewall Options
SELinux
Enabled (Modification Requires Reboot)
Enforcing Current: Enforcing
Policy Type:
targeted
Modify SELinux Policy
Admin
FTP
HTTPD Service
Allow HTTPD cgi support
Allow HTTPD to read home directories
Allow HTTPD to run SSI executables in the same domain as system CGI
Disable SELinux protection for httpd daemon
Cancel
OK

Configuring Policy

Apache Example

- System administrator has multiple choices of policy
  - Booleans
    - httpd_disable_trans, httpd_enable_cgi httpd_enable_homedirs httpd_tty_comm, httpd_unified
  - File Context (sys and user versions of following)
    - httpd_sys_content_t, httpd_sys_script_exec_t, httpd_sys_script_ro_t, httpd_sys_script_rw_t, httpd_sys_script_ra_t
    - chcon -R -t httpd_sys_content_t /home/dwalsh/public_html
- http://fedora.redhat.com/docs/selinux-apache-fc3/
- man httpd_selinux

Configuring Policy

Writing Policy

- Requires selinux-policy-POLICYTYPE-sources
  - /etc/selinux/targeted/src/policy
- Tunables
- AVC messages in /var/log/messages or /var/log/audit.log

  avc: denied { read write } for pid=6775 exe=/usr/sbin/crond name=null dev=tmpfs ino=2150 scontext=root:system_r:system_crond_t tcontext=system_u:object_r:null_device_t tclass=chr_file
- audit2allow -i /var/log/messages
  - allow system_crond_t null_device_t:chr_file { read write };
- make rules

SELinux in Fedora Core

- Fedora Core 2
  - Shipped with SELinux off by default
  - Defaulted to Strict Policy
  - Targeted policy available via Rawhide
- Fedora Core 3
  - Shipped with SELinux on by default
  - Targeted Policy with 10 targets
  - Strict policy available via Rawhide, requires a relabel
- Fedora Core 4
  - About to ship with SELinux on by default
  - Targeted Policy with 70 Targets
  - Strict policy available via Rawhide, requires a relabel

SELinux in RHEL 4

- SELinux is an installation option that is on by default
- Default policy is targeted policy
  - dhcpd mailman.te mysqld named nscd ntpd portmap postgresql squid syslogd winbind
- Strict Policy provided by professional services.
- Training
- Policy writing Services

SELinux Futures

- Additional “targets” for targeted policy
- Better lock down of executable stack
- Better controls over networking
  - IPSEC/Named Networks
  - Iptables Integration
- New Policies – MLS
  - LSPP Compliance?
- Better control over user space
- Trusted X
- Compartmentalized Workstation

Q/A

- **More Information Red Hat Enterprise Linux Resource**
  - http://www.redhat.com/software/rhel/
- **SELinux Resources**
  - http://www.nsa.gov/selinux
  - http://fedora.redhat.com/projects/selinux/
- **Mailing Lists**
  - selinux@tycho.nsa.gov - NSA List
  - fedora-selinux-list@redhat.com - Fedora SELinux List