SELinux
Targeted vs Strict policy
History and Strategy

Daniel J Walsh
SELinux Lead Engineer
dwalsh@redhat.com

redhat

Policy

Flask architecture provides **flexible** support for mandatory access control policies.

redhat

Strict Policy

- Definition
  - 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 privileges for every daemon
  - Separate user domains for programs like GPG,X, ssh, etc
  - Default policy provided by NSA
- Difficult to enforce in general purpose Operating system.
- Default/Off in Fedora Core 2
- Available in Fedora Core 3

redhat

Strict Policy Problems

- Fedora Core 2 Experience
  - Bogged down handling incredible permutations of Linux.
  - Analysis of Strict policy becoming impossible.
  - Strict Policy becoming less strict.
  - Fixing userspace problems while ignoring server space.
  - Caused hundreds of bugs to be reported.
  - #1 Question **“How do I turn off SELinux?”**
  - Don't want to become Trusted Solaris

Strict Policy Problems

- Red Hat Management
  - **”SELinux can not cause the phones to ring.”**
  - SELinux can not cause our support costs to rise.
- Available via Consulting for Red Hat Enterprise Linux 4

redhat

Targeted Policy

- Guard the Gates
- Definition
  - System where everything is allowed. use deny rules.
- Unconfined_t domain created
  - By default processes run in unconfined_t.
  - Unconfined processes run as if SELinux is disabled.
- Targeted Daemons transition to locked down domains.
  - httpd started by unconfined_t transitions to a locked down httpd_t.

Targeted Policy

- Built off same pool as Strict Policy
- Default On in Fedora Core 3
- Default On for Red Hat Enterprise Linux 4
- FC3/RHEL4 Protected Domains
  - httpd, dhcpd, mailman, mysqld, named, nscd, ntpd, portmap, postgresql, squid, syslogd, winbind, snmpd

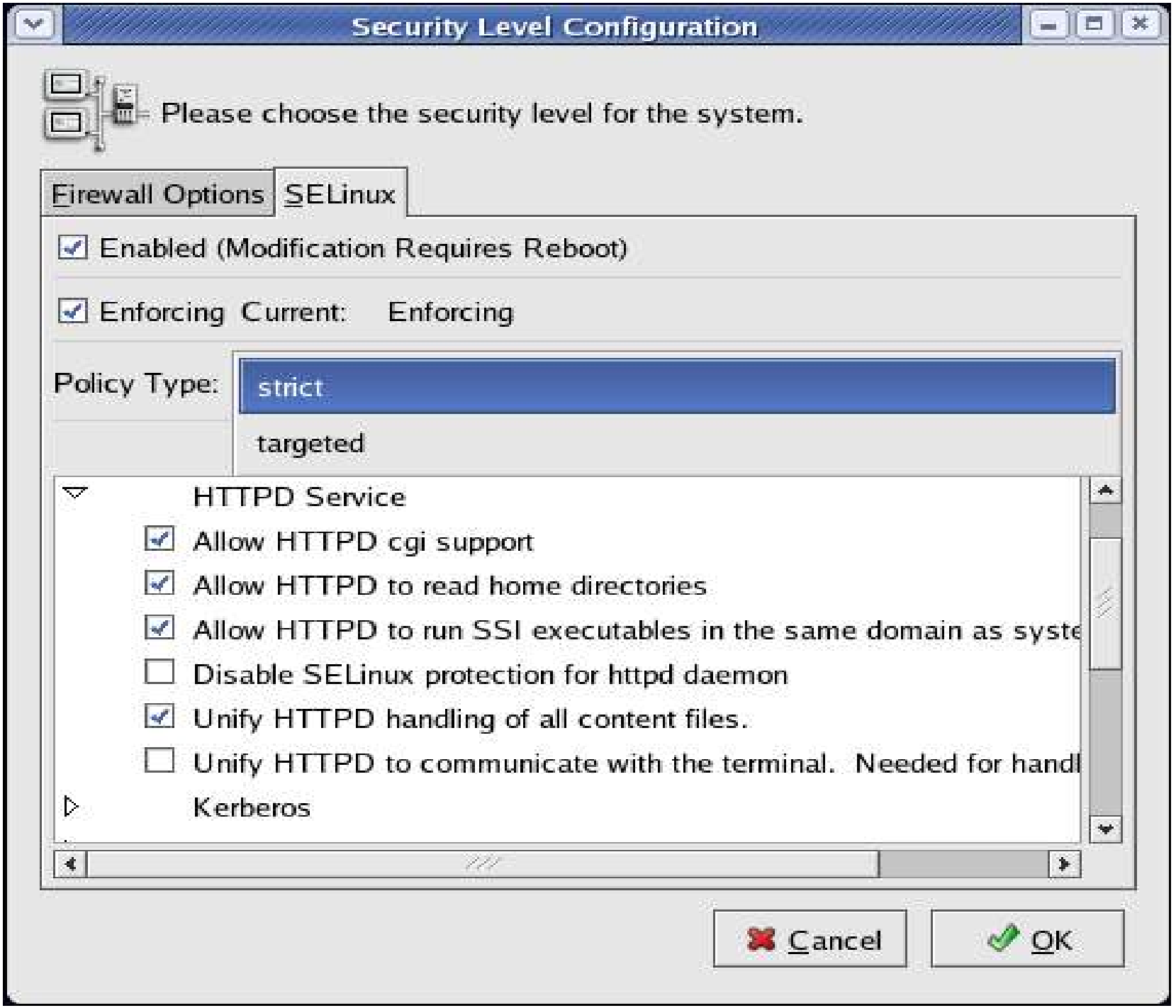
Targeted Policy Problems

- If hacker breaks into apache and get a shell account he would be running as httpd_t
  - He would only have that access (Same as strict policy).
  - However, if he figures a way to transition to another user he could get unconfined_t and have full access.
  - With strict policy he has to figure out how to become sysadm_t.
  - Since the number of policy contexts and transitions are limited in relaxed policy this could be studied.
- User space does not receive any protections from SELinux.

redhat

Changing Policy

- Policy installed in /etc/selinux/POLICYTYPE
- Edit /etc/selinux/config
  - SELINUXTYPE=targeted (strict, mls)
  - SELINUX=enforcing (disabled, permissive)
- Relabel file system
  - touch /.autorelabel
  - reboot


Security Level Configuration
Please choose the security level for the system.
Firewall Options
SELinux
Enabled (Modification Requires Reboot)
Enforcing Current: Enforcing
Policy Type:
strict
targeted
HTTPD Service
Allow HTTPD cgi support
Allow HTTPD to read home directories
Allow HTTPD to run SSI executables in the same domain as syste
Disable SELinux protection for httpd daemon
Unify HTTPD handling of all content files.
Unify HTTPD to communicate with the terminal. Needed for handl
Kerberos
Cancel
OK

redhat

Future

- MLS (Built off same policy pool?)
- Additional targets for targeted policy
  - amanda apache chkpwd cups dhcpd dictd dovecot fingerd ftpd howl i18n_input init initrc inetd innd kerberos ktalkd ldconfig login lpd mailman modutil mta mysqld named nscd ntpd portmap postgresql privoxy radius radvd rlogind rpcd rshd rsync samba slapd snmpd squid stunnel syslogd telnetd tftpd winbind ypbind ypserv zebra
- Protections for userspace
  - See Colin Walter's Talk
  - Unconfined/Unconfined_execmem split?