

Reference Policy Year In Review

Chris PeBenito

SELinux Symposium '07

- All modules from Example Policy ported
- New permission set macros
 - `manage_file_perms`
 - `read_fifo_file_perms`
- New policy patterns
 - `create_Ink_files_pattern`
 - `relabel_chr_files_pattern`
- Configurable sensitivities and categories

Version 20070417

- Local Booleans and Tunables
 - single use moved to the respective module
 - only required Booleans/Tunables included
- Merge sbin_t into bin_t
- Three new modules
 - consolekit
 - fail2ban
 - zabbix

Version 20070629

- Unified labeled networking interfaces
 - labeled networking mechanism abstracted out
 - allow both Netlabel and IPSEC simultaneously
- Merge restorecon into setfiles
- Four new modules
 - amtu
 - apcupsd
 - rpcbind
 - rwho

Version 20070928

- Integrate components from LSPP effort
 - final MLS constraints
 - full set of MLS permission interfaces
- Userspace object classes for databases
- Unknown permissions handling
- Four new modules
 - application
 - awstats
 - bitlbee
 - brctl

Version 20071214

- Merge strict and targeted policies
 - unconfined module makes policy targeted-like
 - new unconfined_r role
 - mix of confined and unconfined users
 - incremental tightening of the policy
- Merge shlib_t into lib_t
- Two new modules
 - exim
 - postfixpolicyd

Version 20080402

- Basic security enhanced X server support
- 64-bit capabilities support
- One new module
 - **wireshark**

Version 20080702

- SE-Postgresql support
- Move roles to individual modules
 - configurable role selection
 - secadm and auditadm available to non MLS
- Policy capabilities support
- Six new modules
 - kerneloops
 - kismet
 - podsleuth
 - prelude
 - qemu
 - virt

Current and Future Work

- Role and user based separation experiment
 - type sets derived from role
 - enlarge the policy
 - duplication of rules
 - complicate policy interfaces
 - use role or SELinux user for separations
- More complete X server support
- FCGlob

QUESTIONS?