SQL result

Host: localhost
Database: newlspp
Generation Time: May 15, 2006 at 07:10 PM
Generated by: phpMyAdmin 2.6.4-pl1 / MySQL 4.1.12
SQL query: SELECT `tasks`.`n` as Number, `tasks`.`name` as Name, `tasks`.`description` as Description, `tasks`.`implementation` as Implementation, `tasks`.`status` as Status, `tasks`.`upstream` as Upstream, `tasks`.`percent` as Percent, `personnel`.`person` as Owner, `organizations`.`organization` as Organization FROM `organizations` JOIN `personnel` ON `organizations`.`n` = `personnel`.`org` JOIN `tasks` ON `personnel`.`n` = `tasks`.`owner` ORDER BY Number;;
Rows: 63

Number	Name	Description	Implementation	Status	Upstream	Percent	Owner	Organization
1	Audit record augmentation	Augment audit records with additional LSPP & RBACPP attributes: subj and obj labels; roles, host identity, event type, and access types where available.	Add additional SELinux fields to audit records.	Patch upstream; needs test.	Red Hat, lkml	99	Kirkland, Dustin	IBM
2	Audit of additional events	Add additional instrumentation to kernel and userspace, particularly for user data import/export; catchall for issues not covered elsewhere. May include new audit record types for: sub, obj, anomalies, responses.	Additional events have been added where necessary.	Need to identify remaining gaps.	Red Hat, lkml	90	Grubb, Steve	Red Hat
3	Audit of network events	Add hooks to IPsec implicit packet labeling. Needs to include audit by network address.	Should mostly be covered by existing AVC audit records. May need to document that network configuration changes require reboot (per @sec). DHCP should be disallowed.	Agreed that this is covered at SELinux Summit.	netdev, lkml	100	Kirkland, Dustin	IBM
4	Audit of print events	Instrument CUPS.	HP completed a new CUPS patch and discussed extensively on this list.	Patch needs to go upstream to CUPS list; depends on print patch.	CUPS mailing list	95	Anderson, Matt	HP
5	Audit of other import/export events	Audit of device allocation + audit of devices not covered by dev allocator hooks or existing AVC audit records.	Add audit hooks for device allocator and other relevant device-related events.	Consensus is this is already covered . Device allocator audit needs test.	Device allocator project; Individual dev mailing lists	99	Velarde, Debora	IBM
6	Audit of user and role modifications	Must audit tools that modify users and roles in flat file implementation. Includes passwd. Utilities upon which this depends covered in separate task.	Red Hat will be writing the user and role tools. Ensure that audit records are generated.	Needs test.	mlsutils package	100	Walsh, Dan	Red Hat
7	Audit instrumentation of trusted programs, including SELinux tools	Analyze userspace and identify those programs that require audit hooks and trusted program modification. At the moment, looks like only init and newrole need to be instrumented--others are audited by kernel.	Instrument newrole for audit, make it suid, and drop capabilities other than audit append.	No new trusted programs identified lately; identify any remaining gaps.	SELinux list, kernel community	90	Grubb, Steve	Red Hat
8	Audit-fs completion	Completion of auditfs patch.	Implementation in progress by Amy.	Patches are incorporated into development kernel. Inotify integration is still	fsdevel, lkml	85	Griffis, Amy	HP

				ongoing.				
9	Audit filtering in kernel or daemon with additional LSPP & RBACPP attributes--Selective Audit	Add kernel or daemon audit filtering to CAPP audit. Solution must filter/suppress records based on all available LSPP & RBACPP attributes: obj and subj labels, object identity, role, hostname, event type, and access type.	Red Hat, IBM, and HP have posted patches that allow filtering on various criteria.	Most all filtering should be in place.	lkml	95	Grubb, Steve	Red Hat
10	Audit browse, sort, search (ausearch) with additional LSPP & RBACPP attributes--Audit Selection	Create command line browse utility. Must include all available LSPP & RBACPP attributes: obj and subj labels, object identity, role, hostname, event type, and access type. Note there is no X-window System in certified configuration.	An ASCII version exists	ASCII ausearch w/sub and obj labels implemented; API proposed on list; binary record format being discussed.	Red Hat	95	Grubb, Steve	Red Hat
11	DAC policy and function	Existing DAC mechanisms should cover; ensure all objects are covered and ensure owner, perm bits, ACLs are appropriate.	Should already be covered.	Needs to be analyzed to ensure complete coverage. This is really an assurance issue.	What, if anything, is specific to the certification RPM?	99	Wilson, George	IBM
12	MLS policy and function	SELinux MLS function and base MLS policy provide foundation; ensure the MLS policy correctly deals with trusted processes, overrides, restrictions on import/export, VFS polyinstantiation; requires extensive testing.	NSA, TCS, Tresys, Red Hat, and others have posted patches.	Red Hat has incorporated MLS policy into Rawhide and ported it to reference policy. There are still kinks to work out.	SELinux mailing list, Red Hat MLS policy RPM	90	Walsh, Dan	Red Hat
13	IPsec labeled packets: Base patch	Indirect packet labeling based on mapping IPsec SAs to SELinux security contexts; AH-only with physical network security reduces/eliminates FIPS crypto cert requirements.	Trent Jaeger / IBM posted patch to netdev. They plan to continue working this item.	Requires documentation, and additional stress and interoperability testing.	netdev, lkml	99	Jaeger, Trent	PSU
14	Labeled print	MLS labels required on banner pages, headers, and footers.	There have been a couple of iterations on this. Current thinking is to use untrusted CUPS server to feed a trusted CUPS server as scaled image.	Matt is now working on the trusted server. Plans to post new patch soon.	CUPS mailing list	85	Anderson, Matt	HP
15	VFS polyinstantiation	Namespaces unshare() syscall patch and PAM exploitation of it.	NSA posted polyinstantiation patch. Red Hat been working on namespaces extensively. IBM has posted unshare syscall patch and PAM integration patches.	Namespaces module and config file need manpages.	lkml, pam-list	99	Desai, Janak	IBM
16	Device allocation	Device allocation patch posted by TCS + enhancements, and/or forced relabeling upon device insertion; requires testing. Functions: authorization, synchronization, device node context assignment, eject/close.	TCS posted framework patch. HP posted policy for it.	Needs to be packaged. Does not do mounting--consensus is that is OK.	Device allocator SF project	95	Hanson, Chad	TCS

17	Test and possibly restrict file archivers	star already maintains xattrs; zip/unzip patched to support xattrs. Need to restrict to the admin. Enhancements to other archivers exceed LSPP reqs.	IBM has added xattr support to zip/unzip, which did not make the cutoff date .	Need to test star w/MLS and ensure policy is correct.	archiver maintainers for modifications; selinux list for policy	95	Velarde, Debora	IBM
18	Disable udev & hotplug after boot (was Device labeling via udev)	Current thinking is to disable udev & hotplug after boot. (L/FDP_ETC, FDP_ITC) See also item 37--Disable DBUS after boot.	Disable hotplug after boot for the evaluated config. This involves investigation and modifications to init scripts for evaluated configuration.	Init script mods need to be incorporated. Debora documented the results and posted init scripts prototype.	Red Hat Certification RPM	95	Velarde, Debora	IBM
19	Label translation	Translation of sensitivity labels into human-readable form.	libsetrans incorporated into SELinux.	libsetrans is upstream; requires test.	SELinux list	100	Walsh, Dan	Red Hat
20	Mail	User mail required for admin mail only, probably only cron. Possible solutions: multi-level MTA, admin-only MTA, direct procmail invocation; direct delivery by cron into poly'd directories. Complete solution may be interesting but is not a requirement.	Modify cron to accept new mailer; use modified mailer to deliver cron output.	Cron has been modified to pass in a mailer; cannot use mailx as is; need to determine delivery mechanism (wrappered mailx or procmail).	No central cron maintainer; Red Hat will carry cron patch; need cron configuration for certification RPM.	25	Desai, Janak	IBM
21	Multilevel xinetd	Patch xinetd to obtain label from inbound connections and spawn child daemons with correct context. Will have to be documented as trusted program.	TCS has posted a patch. Trent also has a student working on an implementation.	Steve Grubb has some issues w/patch. Trent's student's patch execs children at the right level. Trent to post patch. Any concern about DAC attributes or MLS connection ranges?	Steve Grubb, xinetd list	65	Hanson, Chad	TCS
22	Multilevel sshd	Patch sshd to spawn child processes with correct context.	This may be possible by simply patching PAM module.	sshd needs to be tested with xinetd. Looks like we will not need this with xinetd approach. Composition with multilevel xinetd requires test. Will privilege separation cause problems?	openssh-unix-dev	0	Latten, Joy	IBM
23	Multilevel cron	TCS posted polyinstantiation-aware Vixie cron; TCS approach useful, but useful only for MLS labels and dependent on TCS polyinstantiation mechanism. Comments on redhat-lspp suggest extending cron/crontab protocol to support security context.	TCS posted the patch; IBM is working to integrate with namespaces-based polyinstantiation.	Janak is waiting to hear back from maintainers. Janak has posted an updated patch that changes the cron protocol per his writeup; needs test.	Patch should be in rawhide son. No central cron maintainer--Janak is sending to all distro cron maintainers per Stephen Smalley. Distros will have to carry the patch.	95	Desai, Janak	IBM
24	Multilevel at	Base at work on multilevel cron.	Open; IBM and TCS are likely interested in this as they have been working on cron.	This work is folded in with cron. Needs test.	Red Hat will carry patch for evaluated configuration.	95	Desai, Janak	IBM
25	Multilevel tmpwatch	Patch tmpwatch to handle polyinstantiation.	Very likely only manpage changes.	Janak has performed initial investigation; no code changes should be necessary.	tmpwatch maintainer	90	Desai, Janak	IBM
26	Multilevel slocate	Slocate needs to be removed from evaluated configuration.	Ensure removal from evaluated configuration package list.	Consensus at last discussion is to remove from package list.	Ensure this is removed by the Red Hat Certification RPM.	99	Grubb, Steve	Red Hat

27	Revocation of user and object attributes	Killall with user and context matching and wrapper script to lock account and kill all user processes. Similar approach can be taken with fuser.	George has psmisc patch to be posted. Needs to use auid and document regex caveats as well.	George will re-port killall auid patch and rewrite the user revocation script in python. Obj revocation will be procedural.	psmisc sf project, Red Hat certification RPM	75	Wilson, George	IBM
28	Useful role definitions	Define a useful set of roles in the MLS policy. The admin roles should be separated. Consider including a crypto admin role. Ensure each override is accessible through at least one role.	Red Hat added role separation to MLS policy with input from TCS. However, because the policy must be static in the evaluated config, the user admin tool will be used to assign roles to users.	Now we have sysadm and audadm. Additional flexibility exists with policy modules, including overrides. Need to document role assignment procedure.	selinux list	90	Wilson, George	IBM
29	Management of users and roles in flat file	Create command line tools to manage and audit users and roles in flat file separated from base MLS policy. Actions need to be audited, which is covered in a separate task.	Red Hat has been working on flat file user and roles implementation.	Red Hat posted user and roles in flat files documentation. Tools need to be created and instrumented with audit hooks.	Red Hat mlsutils package	100	Walsh, Dan	Red Hat
30	Self tests	Define a simple set of tests that can be run periodically by an administrator or cron job that demonstrates correct operation DAC and MAC policies, and verifies integrity of configuration files, including SELinux policy. Tests shall produce audit records.	Permission and label checks via script, binary integrity validation via rpm -V, check enforcing.	George needs to incorporate feedback from list; wrote manpage. Needs additional SELinux checks, manpage, and test. Policy integrity verification and versioning would be nice, but are not in scope.	Red Hat Certification RPM	65	Wilson, George	IBM
31	I&A	All these requirements are similar to CAPP. Augment tests to account for sensitivity labels.	Needs to be tested for certification.	This is assurance work to verify that I&A functionality.	LTP?	99	Desai, Janak	IBM
34	Ensure all named objects are covered by DAC & MAC	Objects shall include: files, named pipes (fifo), sockets, devices, shared memory, message queue, semaphores. New object: kernel keys - would need man pages, structured comments, & test cases.	Needs complete coverage for certification.	Assurance work; ensure coverage in ST.	Red Hat Certification RPM	95	Wilson, George	IBM
35	Provide minimal number of MAC levels and categories	There shall at least 16 levels of hierarchical labels and 64 compartments (L/FDP_IFF.2.7). However, we should have 256 compartments per customer requirement.	Need to meet minimum specified in LSPP. However, customers may require more.	Was marked complete. However, customer input a SELinux Symposium indicated a greater number of categories is necessary; ensure coverage in ST.	SELinux mailing list	95	Walsh, Dan	Red Hat
36	Audit record unique session/terminal ID	Events shall contain unique session identifier and/or terminal.	Could be and ID a la loginuid; don't want to add a new one; only required when available; incomplete coverage; add to audit records where available.	This work should be complete; ensure complete coverage.	lkml, linux-audit	99	Grubb, Steve	Red Hat
37	Disable DBUS after boot (was Analyze removing DBUS)	DBUS must be either documented and tested, restricted, or removed. Ideally it will be removed from the ST. See also item	Remove dbus and see what breaks; discuss with Russell.	Debora completed a report and init script mods. Mods need to be incorporated.	Red Hat Certification RPM	95	Velarde, Debora	IBM

		18--Disable udev & hotplug after boot.						
39	Restrict kernel keyring access	There needs to be a way to restrict the use of the kernel keyring to the authorized administrator.	The restrictions should be defined in the MLS policy, and DAC, too, if possible.	Ensure restriction in SELinux policy.	Red Hat Certification RPM	90	Walsh, Dan	Red Hat
41	Audit of SELinux booleans	Changing policy booleans is auditable event.	SELinux needs to generate audit records when policy booleans are changed.	Needs test.	SELinux list	99	Grubb, Steve	Red Hat
42	Audit of service discontinuity and fs relabeling (was Audit of service discontinuity)	Service discontinuity and fs relabeling are auditable events.	Ensure service discontinuities an fs relabels are audited--bootup, shutdown, SELinux enable, SELinux disable.	This item needs an owner. Discontinuity should already be covered; need fs relabel record. Need runlevel records.	SELinux list, linux-audit	85	Grubb, Steve	Red Hat
43	Audit record subject labels for userspace records	When user space message is relayed, add a subject message to same event.	The kernel needs to add the subject label for audit records generated in userspace because the caller cannot be trusted.	Needs to get upstream. Tim produced an updated patch; Steve reworked to use Darrel's i/f.	SELinux list, linux-audit	99	Chavez, Timothy	IBM
44	Fail to secure state	When role data base is offline, corrupt, or inaccessible, the system shall preserve a secure state.	SELinux denies everything by default. So, if the SS, DB, or policy is unavailable, the system should come to a stop.	Should already be covered by SELinux. Does policy load failure generate an audit record?	SELinux list	90	Walsh, Dan	Red Hat
45	Maintenance mode for secure recovery	RBACPP stipulates that after a failure or service discontinuity, the machine shall enter a maintenance mode whereby the machine can be restored to a secure state. Maybe config param for rc.sysinit.	rc.sysinit change. Need to boot into single user mode for maintenance after SELinux or audit failure.	Dan Walsh volunteered to push this item. Init already panics when policy load fails. A configurable option to drop into single user mode would be nice. Also want something similar for audit.	Red Hat certification RPM	50	Walsh, Dan	Red Hat
47	Utility to list SELinux roles	User shall have the ability to see list of authorized Roles. This does not appear to be a strict requirement looking at RBACPP FIA_ATD.1.	This is not required by would be nice to have. Is there already a way to do this? If not, need a utility for a user to list roles that he/she can take on.	Nice to have. Determine if this should be removed from requirements list.	SELinux list, Red Hat certification RPM	100	Walsh, Dan	Red Hat
49	MLS enablement of userspace	All utilities that display contexts shall be updated to display levels and categories. They shall display the translated name.	Ensure all userspace utilities display levels and categories correctly. This should already be done. Unclear that they should always display xlated names.	Should already be covered requires test.	SELinux list, Red Hat certification RPM	99	Walsh, Dan	Red Hat
50	Utility to compute closure of sub access to objs	Given a file, the Admin shall be able to determine who can access it. Request from military customers.	apol does this graphically for SELinux, but relies on library to do work. Write command-line utility. Requires analysis of DAC permissions and SELinux policy.	Reid volunteered to take this item. Nice to have. But there is customer demand.	Red Hat certification RPM	10	Wightman, Reid	USAF CDS Lab
51	IPsec labeled packets: Userspace ipsec-tools patches	These are the userspace ipsec-tools patches that accompany the kernel base patch. Includes	Joy Latten and Trent Jaeger modified ipsec-tools to handle syntax modifications	Dan Walsh pushed to rawhide. Joy has forward ported and posted the patch.	ipsec-tools	90	Latten, Joy	IBM

		Venkat's MLS patch for racoon.	required by kernel base patch. Venkat produced a patch to handle MLS negotiations.	Maintainer is presently swamped. Dan is pushing from Red Hat side. Still requires incorporation of Venkat's MLS enhancements.				
52	IPsec labeled packets: Packet context getsockopt() patch	Patch that adds a socket-level getsockopt() to obtain packets' SELinux contexts.	Patch exists to get TCP connection peer security context. This is insufficient for UDP. Patch rework will be required to add a peek option.	Needs test and exploitation by xinetd and network audit.	netdev, lkml	99	Zhang, Catherine	IBM
53	IPsec labeled packets: Analyzers	Tcpdump and ethereal need to understand IPsec labels. This is not an LSPP/RBACPP requirement.	Augment tcpdump and ethereal for filtering on labels.	James Antill has taken this item. Nice to have.	Tcpdump and ethereal maintainers	10	Antill, James	Red Hat
54	Audit of auditd signals	Collect loginuid and context info for senders of signals to auditd. SIGUSER1, SIGHUP, and SIGTERM are only ones used.	Al Viro implemented this item.	Needs test and upstreaming.	linux-audit	95	Grubb, Steve	Red Hat
55	Shell prompt security decorations	Add new configuration options for the bash prompt so that level or other security attributes can be seen on the prompt. Not strictly required by LSPP. However, this helps the user keep the terminals straight as to what level each one runs.	TBD	James Antill has taken this item. Needs analysis.	GNU bash maintainer	10	Antill, James	Red Hat
56	LTP Tests (was Test)	Write new LTP tests or incorporate existing unit and functional tests.	Ideally, respective task owners would contribute unit and functional tests as complete LTP testcases. Share as much as possible.	Please write more LTP tests.	LTP	10	Wilson, Kris	IBM
57	PF_KEY SPD query reliability	The PF_KEY protocol does not return all the entries from SPD queries when the number of entries is large.	TCS is working on a solution wherein netlink is used to query the SPD, and PF_KEY to perform all other SPD management tasks.	TCS would like help with this item. Red Hat bugzilla 181617 tracks this issue. TCS is working with netdev & ipsec-tools communities to come to consensus on a design to remedy the problem.	netdev	15	Hanson, Chad	TCS
58	Audit data API	An API is required to provide a way for audit consumers to access audit records.	Should be a simple API that is easily wrappered by python.	Steve is implementing this.	linux-audit	60	Grubb, Steve	Red Hat
59	Audit of child processes	Need to audit child processes so that autrace can produce output useful to polgen and other audit data consumers.	Create audit records for child processes.	Steve Grubb is implementing this feature.	linux-audit	5	Grubb, Steve	Red Hat
60	Label translation daemon	Need a daemon intermediary for label translation because applying BLP rules to prevent reading the translation file will make it unavailable to most users.	A label translation daemon has already been written by TCS.	Needs test. This has been incorporated as a replacement for libsetrans.	libsetrans patch	95	Hanson, Chad	TCS

61	Audit failure action inquiry	Require a way for applications, such as CUPS, to determine whether to continue running or die when audit is unavailable.	Configuration option in auditd.conf and inquiry function in libaudit.	Design looks good. Lisa will start coding something up.	linux-audit	25	Smith, Lisa	HP
62	Audit of POSIX message queues	Need audit coverage for syscall i/f as in addition to the fs i/f.	Add audit hooks to POSIX message queue syscalls.	George will post initial patch soon.	linux-audit	65	Wilson, George	IBM
63	Analyze/instrument new kernel features	Need to check TIPC, OCFS, configfs, and mutexes for DAC & MAC coverage.	Depends on outcome of analysis.	Needs analysis. This item needs an owner.	selinux-list, others?	0	Grubb, Steve	Red Hat
64	Audit performance	Functional enhancements to the audit subsystem have resulted in an unacceptable performance degradation. Performance must be significantly improved before the changes are upstreamable.	Perhaps suppress audit data collection if record will not be emitted at syscall exit.	Amy posted a patch based on Al Viro's writeup. Needs test.	redhat-audit	100	Grubb, Steve	Red Hat
65	Audit netlink deadlock / ENOBUFS	Audit deadlocks processing a large number of syscall rules; also happens on -mm. Some change is now filling the buffer.	Queue up the packets under the mutex; still need to determine root cause.	Now we need to fix the ENOBUFS problem. Al's patch to queue skb's verified. Need to fix upstream.	linux-audit, lkml	100	Wilson, George	IBM
66	Audit watch misc bugs	First attempt to add a watch fails; subsequent adds succeed. Also, watches seem to match by len.	Incorporate missing patch.	This is fixed. Patch was missing from test kernel.	linux-audit, lkml	100	Griffis, Amy	HP
67	CIPSO	Paul Moore is working on a CIPSO implementation for Linux.	Learn from past issues and create something this is both compatible with other implementations & acceptable upstream.	Paul has posted patches and gotten good feedback.	lkml	55	Moore, Paul	HP
68	IPsec labeled packets: xfrm MLS support	Need to handle MLS in the xfrm protocol.	Augment the base IPsec labeling patch to make it aware of MLS attributes. Also augment SELinux MLS policy.	Venkat has a patch. Needs to be reviewed, commented on, submitted to netdev, and upstreamed.	netdev	70	Yekkirala, Venkat	TCS
69	IPsec labeled packets: Unix domain sockets	Need to extend inet IPsec labeling to Unix domain sockets.	Catherine wrote patches to apply IPsec labeling to Unix domain sockets.	Need to ensure the patches actually made it into the kernel.	netdev	90	Wilson, George	IBM