LSS 2014: linux-integrity subsystem status

Mimi Zohar, David Safford

Linux Integrity Subsystem

- Recent performance improvements, bug fixes and other changes
- Status
- Package manager support for including and installing file signatures
- Yet more measurement/appraisal gaps

Linux Integrity Subsystem: performance improvements, bug fixes

Changes all over, some only “temporary” fixes

- Performance improvements
  - Remove unnecessary i_mutex locking from ima_rdwr_violation_check()
  - Defer template lookup until needed
- Bug fixes
  - Prevent userspace from writing 'security.evm' HMAC values
  - Prevent replacing a new file's 'security.ima' signature with a hash
- “Temporary” fixes
  - Files opened with O_DIRECT flag
  - Version of kernel_read() without permission checking

Linux Integrity Subsystem: other changes

New features upstreamed this past year

- Support for larger hash digests (D. Kasatkin, Samsung)
- Extensible template support (R. Sassu, Politecnico di Torino, Italy)
- Inclusion of file signatures in ima-sig measurement list provides file provenance.
- Keys added to the builtin, trusted IMA-keyring must be signed
  - by any key on the system keyring (default),
  - only with builtin keys (D. Kasatkin),
  - or with a specific UEFI/shim DB key (D. Kasatkin)
- Inclusion of new security xattrs in EVM HMAC
  without breaking existing labeled systems (D. Kasatkin)
- Asynchronous hash support for use with HW acceleration (D. Kasatkin)
- Support for measuring/appraising firmware

Linux Integrity Subsystem: Status

- Who is using the linux-integrity subsystem features, and how?
- Distros: configured in RHEL 7, Ubuntu 14.04,
  and expected in SLES 12, Tizen 3.0
- Looking to distros to include & install file signatures
- Current patch sets
  - Support for loading IMA keys without an initramfs (D. Kasatkin)
  - Better identification of new files (D. Kasatkin)
  - Fix measurement violation race (R. Sassu)
- Next
  - Lock “immutable” files
  - Close measurement gaps
  - Container support for IMA?
  - Directory support

Linux Integrity Subsystem: dpkg/debhelper package manager

- Including file signatures
  - Control.tar.gz in the .deb packages contain a md5sums file

    example from git package:

    923ee6071dff9168b6d3eda5f931e1d0 etc/bash_completion.d/git

  - include larger digest sums file in package (eg. sha256sums)
  - append file signatures

    cat ./sha256sums | evmctl sign_hash -a sha256 –key “${PRIVKEY}” > sha256sums

b7a2e31ce4270f2119d7e4c4f188155a2a9512e62f317ea0b9a596cd78f4cd19 ../etc/bash_completion.d/git
030204d7f6182c0080406048983bc8f3f13428f67c19f42ae401f6d52e1b125461b28ebf12e3ca0e931fdfe172da5
5d3d096794340afa8458464f4d5cf5528c04022d210c5139362f9baff889d7ac8fd762eb7832e148f955b869d551
095caa17e69426e2bb4c862e14d59f917cd7dc32fbe12591fca7927da40f8c3d2123b2af5bf31b9c6ab4bb33e

- Installing file signatures
  - debhelper script: dh_installfile-sigs
  - autoscript: postinst-file-sigs

Linux Integrity Subsystem: rpm package manager (Fin Gunter)

- Configuring digest algorithm & signing key
  - /etc/rpm/macros or ~/.rpmmacros
  - %_binary_filedigest_algorithm 2
  - %_file_sign_key <private key pathname >
- Including file signatures in RPM header
  - Sign file digests stored as RPMTAG_FILEDIGESTS
  - Store file signatures as RPMTAG_FILESIGNATURES

  rpm --addsign **[--signfiles]** PACKAGE_FILE ...
- Installing file signatures
  - Store IMA plugin in /lib/rpm-plugins
  - IMA plugin defines the fsm_file_post hook to label files

Linux Integrity Subsystem: yet more measurement/appraisal gaps

kernel modules	3.7
firmware	3.17
Kexec	-
initramfs	-
eBPF/seccomp	-
Policies:	
IMA	-
SElinux	-
Smack	-
iptables/ebtables (nftables?)	-
???	-

Linux Integrity Subsystem: yet more measurement/appraisal gaps

kernel modules	3.7
firmware	3.17
Kexec	-
initramfs	-
eBPF/seccomp	-
Policies:	
IMA	-
SElinux	-
Smack	-
iptables/ebtables (nftables?)	-
???	-

The “Trusted kernel patchset for Secure Boot lockdown” does not trust loaded MAC policies. Do signed policies affect this assumption?