LSS 2018: linux-integrity subsystem update

Mimi Zohar, IBM

New Features

- EVM (file metadata) new features (Matthew Garrett, Google)
  - Portable & Immutable EVM signatures
  - Runtime support for defining and including additional EVM protected security extended attributes
  - Support for larger EVM digests

    *** LSS-EU: Tying EVM into LSM policy ***
- IMA (file data)
  - Build time IMA policy, persists after loading a custom policy
  - Run time enabled IMA architecture specific policy (Nayna Jain, Eric Richter IBM)

*** LSS-EU: Using Linux as a secure boot loader for Power ***

Closed IMA-measurement, IMA-appraisal, & IMA-audit gaps

- Re-measuring, re-appraising, & re-auditing files on filesystems without i_version support (Sascha Hauer, pengutronix)
- Prevent kexec'ing unsigned kernel image (kexec_load syscall)
- Prevent loading unsigned firmware (sysfs)
- FUSE file systems
  - Unprivileged mounted FUSE filesystems
    - Measure/audit once, always fail appraisal
  - Privileged mounted FUSE filesystems
    - Default: re-measure, re-appraise, re-audit on each file access
    - Optional: builtin "fail-securely" IMA policy

Outstanding problems resolved

- Re-introduced an IMA specific lock to resolve the i_rwsem lockdep (Dmitry Kasatkin, Huawei)
- Major TPM performance improvements (Nayna Jain, IBM LTC)
- Disambiguated IMA audit records (Stefan Berger, IBM Research)

Testing!

- IMA Linux Test Program(LTP) tests updated (Petr Vorel, Suse)
- evmtest: a standalone IMA testing framework (David Jacobson, IBM summer intern)
  - Direct testing of currently running kernel image
  - Designed for integration with LTP and xfstests in mind

Current and future work

- Using the platform keyring (firwmare keys) for validating the kexec kernel image signatures (Nayna Jain, IBM LTC)
- Appended signature support (Thiago Bauermann, IBM LTC Core Kernel Team)
- evmtests: extend the testing framework with additional tests
- Key management: black lists, revocation, resetting IMA cache status
- Namespacing IMA (ima-audit, ima-measurement, ima-appraisal)
- initramfs: CPIO extended attribute support
- Directory protection support (Dmitry Kasatkin, Huawei)
- Hardening the IMA measurement list memory allocation (Igor Stoppa, Huawei)

*** LSS-EU: Kernel Hardening: protecting the protection mechanisms ***

- fs-verity integration with IMA policy (Mike Halcrow & Eric Biggers, Google)

How can you help?

- Review patches
- Participate in patch discussions
- evmtests: extend the testing framework with additional tests
- Simplify usage: sample IMA policies, updating documentation

- **Don’t introduce new IMA-measurement, IMA-appraisal, or IMA-audit gaps!**

Thank you!

- For all the automated testing
- For the “minor” bug fix patches
- For help with updating & packaging ima-evm-utils

And for coming to this talk

Questions?

Defined New LSM hooks

- security_cred_getsecid - credentials of the target execve
- security_kernel_load_data