Integrity Measurement

Chuck Lever

<chuck.lever@oracle.com>

Purpose of This Work

- The Integrity Measurement Architecture (IMA) provides an end-to-end cryptographic file-integrity service.
- IMA metadata is transparent to data storage, generated and interpreted only by security infrastructure.
- A standard extension to NFS or a standard side-car RPC program would enable transport of per-file IMA metadata for storage on NFS servers.

draft-ietf-nfsv4-integrity-measurement

- This is a Working Group document defining NFSv4 protocol extensions for exchanging integrity measurement metadata. This document describes the format of that metadata as opaque.
- Objection: Missing description of metadata format could make broad implementation challenging.
- Progress towards publication is blocked until an adequate metadata format specification can be provided.

Legal Challenges

- There currently exists no published specification for the metadata format. There is only implementation code.
    - This makes it impossible to reference a specification of the format.
- User and Linux kernel implementation is under GPLv2.
    - Legal opinion is a format specification based on this implementation would also fall under GPLv2.
    - GPLv2 is not compatible with the IETF’s Code Components License. Without a license change, the format cannot be contributed to the IETF.

Alternatives

- Work with Linux Foundation to gain permission to relicense implementation as GPL-and-BSD, then contribute the format specification to the IETF as an Internet-Draft.

- Identify a GPL-friendly standards process, then write and publish a specification of the metadata format via that process.

- Are there others?

Technical Requirements

- Existing formats:
  - There is a file content metadata format that is signed and self-identifies the digest and signing algorithms. It uses an x.509v3 key pair.
  - There is a file attribute metadata format that is signed and portable (that is, independent of the underlying file system type, no raw inode numbers, etc).
- Further format extensibility is necessary in order to construct formats that can for instance sign Merkle trees or protect directories. Therefore IANA registries will be provisioned.

Current Legal Status

- There is plenty of Linux kernel code that is dual-licensed
- The authors of this code still actively contribute to the Linux integrity and security communities.
- A legal process has been initiated to explore re-licensing the relevant code base.

Current Editorial Status

- I’ve authored an I-D style document that:
    - Fully specifies the metadata format.
    - Provides mechanisms for extending the format via IETF standards process.
- I intend to submit this document once the legal issues have been resolved.

Current Implementation Status

- An out-of-date Linux prototype of the previously proposed NFSv4 extension exists.

- Security and performance analysis suggests that maintaining a per-file Merkle tree is necessary.

    - Each tree's root would be signed and stored as per-file IMA metadata.

    - Assessors would use fs-verity-like infrastructure to re-create each Merkle tree on first read, and then use the tree to verify portions of each file as needed.