Draft-*-nfsv4-security

Current Status and Next Steps

David Noveck

For NFSv4 Interim

November 21, 2023

Contents

Need for New Document
Original Motivation (Slide One of Two)

- Lack of threat analyses in all existing Security Considerations sections.
- Incorrect treatment of AUTH_SYS (as an “OPTIONAL means of authentication”).
  - “OPTIONAL” gives impression that clients might use this without negative consequences.
  - Actually, does no authentication.
  - While allowing this, to be used,
    - We need to make clear the security consequences, to encourage its use only where it can be properly secured.

Need for New Document
Original Motivation (Slide Two of Two)

- Need to include connection-based security , e.g. RPC using TLS, in addition to auth-flavor-based ones.
  - Provides a means of encryption, which is generally available :
    - So, it can be used with AUTH_SYS.
    - Does not require per-fs configuration.
  - Provides peer authentication, needed to make AUTH_SYS security viable.
    - Avoids trusting an unauthenticated client.

Need for New Document
Further Issues Discovered as Work Proceeded

- Under-specification of acl/dacl attributes
  - Original motivation was to allow support of UNIX ACLs.
  - As the existing specs are written, no meaningful constraints on server implementations.
  - Creates a client interoperability nightmare.
- Pervasive misuse of SHOULD
- Many problems regarding mode semantics.

Recent Changes in -07

- Reorganization of authorization-related attributes.
- Description of Owner, Owner_Group, Mode as **REQUIRED**
- Explicit discussion of currently underspecified attributes
- Proposed changes (Consensus item #61) to address acl and dacl attributes.

Further Steps
Right now

- Need to go forward with adoption call for -07
  - Previous Adoption call for -06 no longer relevant
- Will require Working Group discussion of document.
  - For this purpose, discussion of the document should focus on Section 1.
    - Only ten pages of document to read, rather than more than one hundred in full document

Further Steps
After Adoption Call

- Would like to organize discussion around the consensus items listed in Appendix B.
- Would like to focus first on those that have most leverage:
  - For example, item #61 first.
  - Should also focus on getting consensus on Security Considerations.
- Would like to get document to the point we could get an early security review.