

New Security Document

draft-dnoveck-nfsv4-security-02

David Noveck

Nfsv4 Working Group Interim Meeting

October 27, 2021

Talk Overview

- **Document Introduction.**
 - **What has changed (from RFCs 7530 and 8881) and why.**
- **Issues to be discussed and eventually resolved.**
 - **Dealing with Appendix B.**
 - **Need to decide about priorities.**
- **Process going forward.**
- **Expectations for progress**

Document Introduction

Overall

- Need a new document
 - To support rfc5661bis effort.
 - Needs to deal with all minor versions.
 - No time to do multiple documents.
- Problems with security in RFCs 7530 and 8881
 - Not very secure (AUTH_SYS and lack of attention to data security).
 - Need to adapt to the opportunity provided by RPC-with-TLS.
 - Lack of a threat analysis in haphazard Security Considerations sections.
 - Unsatisfactory treatment of ACLs and particularly of coordination of ACL and mode attributes.

Document Introduction

Basic Security Issues (Slide One of Three)

- Existing Security Considerations sections
 - IESG member quote: “A set of random observations, inelegantly expressed”.
 - Unfortunately, true 😞
 - No threat analysis 😞
 - Need to provide one.
- Existing Approach to Data Security
 - It is possible to provide encryption
 - *Server* can require its use.
 - But is expensive and not offloadable.
 - Specs never discuss need for it
 - Hardly ever used 😞

Document Introduction

Basic Security Issues (Slide Two of Three)

- Existing handling of AUTH_SYS.
 - “An ‘OPTIONAL’ means of authentication”
 - It does not provide authentication.
 - Since it affects security negatively, “OPTIONAL” is not right.
 - “SHOULD NOT” is correct, but everybody would have ignored it then.
 - Not clear what to about it now. Sigh!
- Proposed handling of AUTH_SYS.
 - Avoid both “SHOULD NOT” and “OPTIONAL” unless forced to choose.
 - Take advantage of facilities provided by RPC-with-TLS to mitigate the security issues.

Document Introduction

Basic Security Issues (Slide Three of Three)

- Proposed handling of AUTH_SYS (continued).
 - Tell the truth about the AUTH_SYS security issues.
 - Separate old AUTH_SYS (in the clear w/o client peer authentication) from new (encrypted, with peer mutual authentication)
- Taking advantage of RPC-with-TLS.
 - Already available as an OPTIONAL transport.
 - Server policies could OPTIONALLY enforce that.
 - Am proposing recommendations regarding such policies.
 - Includes encryption and peer authentication.
 - Expect some controversy for the working group to resolve.

Document Introduction

ACLs and Related Issues (Slide One of Three)

- Existing handling not appropriate to a standards-track document.
- Focus on providing server freedom to do some approximation of ACL support, leaving not much the client can rely on.
 - Each ACE mask bit is its own optional feature, with no way for client find out which ones are supported.
 - Handling of ACL/mode co-ordination follows this pattern
 - Multiple methods of computing mode from ACL (via an “intentional” SHOULD).
 - Many SHOULDs, have no clear motivation, making it impossible to determine whether or why recommendation would be ignored.
 - Many passages simply describe possible server behaviors, implying they are necessarily OK.

Document Introduction

ACLs and Related Issues (Slide Two of Three)

- This approach creates interoperability issues
 - Might have not mattered in the past due to limited use of the feature.
 - Lack of v4-oriented client-side APIs may have kept client/application expectations low.
 - Still, it is now an important OPTIONAL feature with an important security role.
 - Need to provide at least a pathway to interoperable implementations.
- Need to accommodate both:
 - Development of interoperable implementations.
 - Support for existing implementations.

Document Introduction

ACLs and Related Issues (Slide Three of Three)

- Current proposal
 - Establish a preferred server behavior
 - Get available information about actual behaviors
 - Describe it using SHOULD
 - Limit valid reasons to ignore recommendations.
 - When we allow variations, delimit allowable variances
- Will need to discuss on list
 - Expecting progress by -04.

Issues to Resolve

Overview

- RFCs 7530 and 8881, both saying pretty much the same thing, were adopted by consensus and published as Proposed Standards.
- Now we have to say something different about these issues and we need to be clear that there is a working group consensus for these changes.
- These issues are summarized in Appendix B, to make the process clear 😊
- But there are 49 of them 😞
 - Will discuss proposed priorities in [Slide 12](#).

Issues to Resolve

Summary of Appendix B

Issue Group	Responsibility	Statuses	Count
Overall Security Issues	Proposed text for WG discussion	NM*, BE, BC, CI	12
	Incomplete text; WG discussion would help	NE	2
	Waiting for Author	LD	5
	Total	ALL	19
ACL-related Issues	Proposed text for WG discussion	NM, BE, BC, CI	28
	WG discussion would help prepare	WI	2
	Total	ALL	30
Everything	Grand Total	ALL	49

Issues to Resolve

Establishing Priorities

- Possibilities:
 - Easiest first, most controversial first, most interesting first, ...
 - Focus first either general issues or ACL-based issues.
- My proposal:
 - Primary focus on general issues.
 - Already known as of -00, and there are only 14 to deal with 😊
 - Secondary focus in getting general understanding of ACL-based issues
 - Includes preliminary discussion about POSIX ACL choices (see next deck)
 - Hoping to also resolve #11 and #27 as part of that.
- Resolve priority choices on list (in the next week or so)

Process Going Forward

Overview

- Discussion of document
 - Focusing on identified consensus issues
- Periodic document updates
 - Approximate two-month cadence.
 - Updates will reflect results of discussion
 - When consensus is achieved on individual items, draft update will reflect that

Process Going Forward

Things to Discuss and not Discuss for Now

- Definitely:
 - Reasons for change
 - Objections to change.
 - Possible compatibility issues
 - Also, how to deal with likely lack of info.
 - Possible alternate approaches
- Possibly not:
 - Wordsmithing
 - Eventually valuable but need to focus on substance right now.

Process Going Forward

Forums for Discussion

- Working group list
 - Will have a major role but may not be adequate for some issues.
 - Some discussions make progress but never quite get to a conclusion
- Meeting like this
 - Too few to have a major impact.
- Other possible forums
 - Smaller, more focused meetings , to resolve controversies.
 - May need to make these official interim meetings.

Expectations for progress

Near-term

- -03 (2-3 weeks from now)
 - Corrections from list (for next week)
 - Filing in some missing sections
 - Adaptation to NIST 900-209 & other terminology changes
 - Thanks, Chuck!
 - Possible switch to new approach to UNIX ACLS (see next deck)
- -04 (9-11 weeks from now)
 - More missing sections
 - Results of WG discussions of Consensus items
 - Unsure how many but expect there to be some.

Expectations for progress

Getting to a Working Group Document

- Will not happen by -04.
- Probably won't happen by -05
- We need to discuss the appropriate state of completion for this to make sense.
 - Better than an artificial deadline.
 - Some requirements mentioned in draft but we need to have a sense as to how much unresolved controversy we can address after wg doc acceptance.