Summary of Changes - version 6

- BNF per RFC 2234; updated examples to reflect new BNF
- Added back multiple list of attributes; removed collections
- updated/expanded set of permissions and their descriptions
- Clarification of interactions of precedences and evaluations
- added access decision algorithm so nothing intuited from examples
- Added strength of authentication option into ACI syntax based on ldap bind
- Incorporated authmeth id format into subject component of ldapaci (removed kerberos format)
- ipAddress format expanded to include domain names and wildcards

Summary of Changes - version 6 (continued)

- added ability to control access to ACI; removed policy owner
- defined ldapACISubEntry to allow specification of any access control mechanism anywhere in the tree
- addressed how alias de-referencing and referrals work with respect to access control
- Versioning ldapACI: concluded that a different attribute would be used in subsequent RFCs on ldap access control
- updated the security considerations sections
- updated/expanded description of the access control model
- removed terminology section

New Comments on Draft

- discloseOnError: change from server basis to a permission? Specify as permission on entry
- Delete permission: clarify it works on leaf entry (per X.500); done already in email
- Search permission: revisit/update permissions b, r, s:: browse meant for traversal permission; if specify base level DN, it overrides specification of browse; use returnDN to allow read of entry; browse only applies to search; move t in search operation to main search section - further discussion needed for use of s, r, b, t; mention matchedDN in operations other than search (e.g. name resolution)
- Rename permission: rename perm or combination of w, o, i, e perms? Keep all and do per Chadwick's email
- Should ldapACI attribute be split into subtreeACI and entryACI attributes? Accepted Chadwick's email and remove partial inheritance text; add text on scoping of subtree at entry X and another subtreeACI beneath entry X
- Clarify use of "[all]" and "[entry]" wrt subtree scope; done already in emai
- Authentication level: clarify how it works with deny; should additional explicit choices be specified, e.g. X509? Handle on mailing list; any=authenticated via any mechanism except anonymous, need to add none to list (look at X.500 definition), what is behavior if no authentication level is specified (look at X.500 definition)
- Use of filters in ACI? – look at adding…filter behaves as specified in ldap filter spec
- Dependency on ldapSubEntry specification? - Chadwick's email to use separate entry and subtree aci (and gets rid of scope)
- Specificity precedence: ipaddr/authzID/this/role/group/subtree/public; default deny at very bottom
- Misc clarifications (e.g. add, import, export perms; empty grant list; subject definitions)
- Update control/extended operation to reflect correct conventions + other misc updates
- sync perm descriptions in sec 4 with uses in sec 5

More Comments

(from Pittsburgh aci meeting, 1 Aug)

- equality matching rule for ldapACI – see Steven Legg's component matching work
- syntax for ldapACI – bugs?
- negate syntax for disallowing attributes in ldapACI – don't do ; push to later
- specification of default ACI per object class – push to later?
- ipv6 addresses as ip addresses
- sec 5.6: clarify what happens when new rdn value = old rdn value
- clarify in bnf what perms are for attrs and for entries
- permission extensibility for extended operations – use combination of perms from existing set
- make sure examples cover all aspects of ldapACI
- revisit (update or delete) operational semantics section
- getEffectiveRights: address what if not sufficient rights on ldapACI? (get rights based on the bind authzID) - need proxy permission? – permission for entries to be proxied