Kerberos V set-password v2

draft-ietf-krb-wg-set-passwd-02.txt

Nicolas.Williams@sun.com

Changes from -01

- Removed some authors
  - added acknowledgements
- Removed UDP as transport, redundant framing ASCII art (referenced through [RFC3244])
- Cleaned up major version negotiation text
- I18N... To be discussed at KRB WG meeting
  - See new developments around this
- Added dry-run facility

Changes from -01 (cont.)

- Added op to get current s2k params for princ and a way to change them w/o changing pw
  - To sync salts after principal/realm renames
- Added optional password quality codes as hints for smart clients (by request from Larry)
- Added delayed-commitment to change-pw and set-pw operations (also requested by Larry)

Changes from -01 (cont.)

- Removed field indicating version of Kerberos V supported
  - the isupport stuff may still be controversial...

Extensions, set-passwd v2, I18N

- Once more, into the breach
- Not just just-send-8, but also just-use-8!
- Extensions/set-passwd v2 clients won't necessarily be representative of pre-extensions clients also used by same users
  - UTF-8 [+ SASLprep] loses local encoding info
- The KDC needs hints about what encodings will be used on pre-extensions systems
- Number of encodings can be large

Extensions, set-passwd v2, I18N (cont.)

- Dual-mode pre-extensions/extensions deployments essentially require aliasing of non-ASCII princ/realm names, salts and passwords if the such are to be usable on pre-extensions just-8 clients
  - This should be optional; w/o it only all-ASCII names/salts/passwords will interop properly
    - Like to day, but maybe even less
- Yes, this can be done w/o extensions
  - But it's harder, and extensions stops the rot

Extensions, set-passwd v2, I18N (cont.)

- One more thing: to help with per-extensions clients that use unnormalized encodings salts and passwords, where they are sent on the wire, should be display strings
  - But SASLprepped as query strings prior to string2key (), on clients
    - As storage strings, on servers

SASLprep and control characters

- Some existing Kerberos V KDCs explicitly allow ASCII control characters in passwords
- SASLprep explicitly prohibits the such in output
- Problem?
  - Discuss