`crypt()` considered gone

Phase-Out Plan for the `CRYPT-PW` auth mechanism

Peter Koch
DENIC eG
pk@denic.de

RIPE Database Working Group
Amsterdam
2006-10-06

Auth Scheme Usage

- Multiple auth attributes work as alternatives
  - weakest scheme wins
- How many actually still use `CRYPT-PW`?
- `http://www.ripe.net/projects/dbconstat/stats-authcount.html`

Weaknesses of CRYPT-PW

`https://www.ripe.net/cgi-bin/crypt.cgi`

says

Please note that a CRYPT-PW passphrase is limited to 8 characters. Since the salt string is only 2 characters long, this method is considered vulnerable to dictionary attacks and brute force cracking. In general it's not recommended and is left for compatibility only.

Other warnings spread over DB doc

`CRYPT-PW` is just too weak!

Why bother?

- `mntner` is responsible for their data
- RIPE community is responsible for strength of the tools
- Present explicit warnings *might not be sufficient*
- News at eleven: *RIPE's database hacked by . . .*
- *Safety belt* is available (but not for routine rollback)

Proposal

- Sent to the mailing list 2006-10-04
- Discuss problem at the DB-WG meeting
- Action Plan
  - raise awareness
  - contact maintainers using CRYPT (some of those might just be migrating)
  - set date for change
  - phase out CRYPT-PW

Plane – Timeline

1. Inform (1 month)

   targetting contacts and public

2. Change SW (1 month)
   - reject any change to mntner object that adds new CRYPT-PW
   - show warning if CRYPT-PW was used during authorisation
   - show warning if object being updated still contains CRYPT-PW
   - again inform contacts and public

3. Final Phase-Out, DB SW modification
   - disable CRYPT-PW in the syntax
   - disable CRYPT-PW in authorisation
   - again inform contacts and public