`crypt()` considered (too) harmless

A request to deprecate the CRYPT-PW auth mechanism

Peter Koch
DENIC eG
pk@denic.de

RIPE Database Working Group
Amsterdam
2005-10-14

Overview

- Current DB Auth Mechanisms
- Weaknesses
- Usage
- Proposal

Current DB Auth Mechnisms

- `http://www.ripe.net/db/support/security/`
- PGPKEY
- X.509
- MD5-PW
  - BSD based

    `http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/crypt.html`
  - `openssl passwd -1 -salt pepper “on tomatoes“`
- CRYPT-PW
  - based on Unix `crypt()`
- MAIL-FROM (phased out 2002-07-11)

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

- Christian Huitema's presentation at Paris IETF

  `http://www3.ietf.org/proceedings/05aug/slides/apparea-4/sld1.htm`

- Cost of breaking a single password maybe around EUR 50
- What does it cost to break one `mntner`'s `CRYPT-PW`?
- "cleartext" passwords are readily accessible from the DB

Present Caveats

`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

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

- 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
- Will have to invoke PDP

Why not deprecate `MD5-PW`?

- Baby, Bathwater, . . .
  - \+ Shares weaknesses (cleartext password, brute force attack)
  - – Stronger: Passphrases, more expensive hash, better salt
- Might work as *drop in replacement* for `CRYPT-PW`
- Need a non-PGP method for `mntner`-bootstrapping