
# Filtering MD5 password hashes from the WHOIS database

Amreesh Phokeer

AFRINIC

# MNTNER - ACTUAL

| | |
|---|---|
| mntner: | YCHADEE-MNT |
| admin-c: | YC5-AFRINIC |
| tech-c: | YC5-AFRINIC |
| auth: | MD5-PW $1$nJ2l/vql$/YKI/fdADSuJHvCllVUICL/ |
| auth: | CRYPT-PW TTASsdaqLqhVp$a |
| auth: | X509-37 |
| auth: | PGPKEY-FFD39337 |
| mnt-by: | YCHADEE-MNT |
| changed: | yogesh@afrinic.net 20120419 |
| source: | AFRINIC |

# Mail update security issue

- **MD5 and CRYPT - BROKEN**
  - Known pre-image attack against MD5
  - Not collision resistant
  - US-CERT : “cryptographically broken and unsuitable for further use”
- Overall global problem with plain text e-mail authentication with WHOIS update via e-mail

# MNTNER - PROPOSED

| | |
|---|---|
| mntner: | YCHADEE-MNT |
| admin-c: | YC5-AFRINIC |
| tech-c: | YC5-AFRINIC |
| auth: | MD5-PW # Filtered |
| auth: | X509-37 |
| auth: | PGPKEY-FFD39337 |
| mnt-by: | YCHADEE-MNT |
| changed: | yogesh@afrinic.net 20120419 |
| source: | AFRINIC |

# STATISTICS

- **mntner** object authentication method stats:
  - MNTNER objects : 1641
  - MD5 : 1549
  - CRYPT : 70
  - PGPKEY : 54
  - X509 : 4

# RECOMMENDATIONS

- Filter out the password hashes (MD5/ CRYPT) – *done*
- Investigate use of SHA256 instead of MD5
- Phase out password authentication system by:
  - Encourage PGPKEY and x509 certificate
  - Extend MyAFRINIC to securely handle MNTNER objects – Q1 2013
  - Provide a secure web interface to allow bulk WHOIS updates – Q1 2013

# IMPACT – MNTNER UPDATES

- Update `mntner` by members using email method auto-dbm@afrinic.net
- Members will need to save their full object for future updates
- Only hostmaster has access to the full object
- In case MD5 hash or password lost, send mail to afrinic-dbm@afrinic.net for password reset.

# IMPACT - DOCUMENTATION

- Training documentation
- Need to Update few WHOIS related documentation online. E.g:
  - http://www.afrinic.net/en/library/membership-documents/210-afrinic-db-security
  - http://www.afrinic.net/en/library/membership-documents/197-database-afrinic-database-reference-manual- (section 2.6)
  - …