AFRINIC
The Internet Numbers Registry for Africa

DB Security Proposal

Simon Seruyinda

DBWG Online | September 2020

Background

- Following recent cases of fraudulent activity observed on the database
- Risk of interception of plain text passwords (auto-dbm or webupdate)
- Password sharing with third-party to update objects on their behalf
- The need for tracebility

Tracebility

- Unreliable changed attribute
- Auto-dbm, email can be from anyone
- Webupdate: originating IP not enough to identify who has done changes

Password authentication

- Weak authentication algorithms
- Though deprecated, several objects are still protected by MD5 and CRYPT hashes

Stats

Auth Method	Number of Maintainers
	18003 auto-generated by WHOIS for person/role objects protection
BCRYPT	**1322** created by object owner
	Total: 19325
PGP	151
CRYPT	63
MD5	2619
X509	7

Proposed Mitigation

Slowly deprecate password based authentication and replace it with PGP.

Implement email whitelist for auto-dbm requests

Proposed Action plan

- Develop tools to enable members easily create their PGP keys
- Develop training material to build capacity of the members
- Organize webinars to help members to adapt to using PGP
- Communicate intention to deprecate password authentication to members and community
- Communicate to CRYPT & MD5 maintainer owners

Proposed Action plan

- Provide Support to CRYPT & MD5 maintainer owners to transition to PGP
- Send reminder that around say end of Q3 2021 we are dropping support for MD5 & CRYPT
- Drop CRYPT & MD5 around say end of Q3 2021
- Communicate to BCRYPT Users
- Provide support to BCRYPT users to transition to PGP

Proposed Action plan

- Drop BCRYPT auth, except for auto-generated maintainers that are less than 6 months old
- Enforce expiry of key-cert Object
- Deprecation of changed attribute for all object types and replace it with created and last updated attributes.
- Setup email alerts x months before expiry of key-cert objects.
- Explore the use of tokens as an alternative authentication scheme to PGP

Thank you for your Attention

Questions?


twitter.com/ afrinic


flickr.com/ afrinic


facebook.com/ afrinic


linkedin.com/company/ afrinic


youtube.com/ afrinic media


www. afrinic .net