RIPE NCC
RIPE NETWORK COORDINATION CENTER

Discontinuing MD5 Hashed Passwords

Impact Analysis and Migration Plan

Ed Shryane | RIPE NCC | 31 October 2024

Discontinuing MD5 Hashed Passwords

Introduction

- We plan to discontinue MD5 hashed passwords in 2025
- Presented at RIPE 88
- Impact Analysis published to DB-WG in September
- API Keys
- Less secure transfer of credentials
- Migration plan

API Keys

API Keys: A More Secure Alternative to Passwords

- API keys are for automated (non-interactive) updates
- API Keys are intended to be a “drop-in” replacement for passwords
  - Create, list and revoke API keys in the DB web application
  - Can be optionally scoped to a maintainer
  - Key will have a “public” part and a “secret” part (only shown once)
  - Use standard HTTP “Basic” authentication for updates (no custom header)
- API keys are linked to a RIPE NCC Access account
  - 80% of maintainers already use auth: SSO account so no need to update
  - API keys are not stored in the maintainer
- Available in **early 2025**
  - Documentation including examples
  - Training materials
- Other alternatives
  - You don’t have to wait for API keys to stop using passwords
  - PGP (used by 6% of maintainers) and X.509 signing (used by a minority)
  - client certificate authentication

Shared Credentials

- API keys will be linked to an **individual** RIPE NCC Access account
  - They are not intended to be shared (same as passwords)
  - When multiple people share the same credentials, it creates security risks
  - Changes by an individual can be audited (for accountability and compliance)
  - We will not encourage the sharing of RIPE NCC Access accounts. It is a better practice for individuals to manage their own credentials separately
- **When someone leaves**, just remove their RIPE NCC Access account
  - Their API keys will no longer authenticate as the maintainer
- We will help an **LIR** manage how API keys are used
  - List users with API keys
    - On the LIR Portal "User Accounts" page, display an "API Key" label
    - For admin users for their own LIR account only
  - Add warning
    - Add a warning when removing an LIR Portal user or changing their role, if they have any API keys, as automation may stop working

API Key Expiry

- API keys will have a mandatory **expiry date**
  - User can choose the expiry date but not longer than one year
  - Trade-off between security and ease of use
  - Secrets with a long lifetime pose a security risk
  - If they are unknowingly exposed they can be misused
- Avoiding Downtime
  - A procedure to rollover the API key is necessary no matter the validity period
    - The longer the expiry the less frequently this will be done
    - The procedure must track the expiry date
  - We will notify the RIPE NCC Access user in advance by email and on our web interface(s), if any of their API keys are due to expire soon

Future Work

- Add more fine-grained limits on API keys, for example:
  - Additional maintainer(s)
  - An environment (Production, Test, RC, Training)
  - Source prefix(es)
  - Object type(s)
  - Read-only / Read-write
- OAuth 2.0 Support
  - Automate key rollover, more complicated
  - Needs client support
- Extend API Keys to other RIPE NCC Services

A Single API Key is Used for Authentication

- Whois allows for **multiple** credentials to be used for authentication in a single update
  - When maintainers in parent and object itself are different
- We will only support a ***single* API key** in each update request
  - Same for client certificate authentication and OAuth 2.0 (in future)
- Impact
  - We found that multiple passwords were used in *< 0.4%* of updates
- Alternatives
  - Use PGP or X.509 to sign an update multiple times
  - *"If you wish to avoid having to supply multiple credentials, it is best to set up hierarchical authorisation by adding a "mnt-routes:" attribute to all of your resource objects and consistently use this maintainer to create and manage route(6) objects."* - DB documentation

Less Secure Transport of Credentials

Less Secure Transport of Credentials

Upcoming changes will only allow credentials to be sent securely

- Mailupdates:
  - Passwords are deprecated (warning since September) (in 16% of updates)
  - Only PGP or X.509 signed mailupdates will be supported
  - API Key will not be supported
- Syncupdates:
  - HTTP is deprecated (warning since September last year) (in 50% of updates)
  - Passwords will be deprecated (16% of updates)
  - API Key will be supported
- REST API:
  - Credentials over HTTP are already not allowed (403 Forbidden)
  - Passwords will be deprecated (76% of total)
  - API Key will be supported

Migration Plan

Migration Plan

How many maintainers are affected?

Most maintainers do **not** use passwords:

- There are 62k maintainers in the RIPE database
- About 18k (29%) of maintainers have at least one MD5 hashed password
- 3K maintainers **only** have MD5 hashed password(s)

In the last year:

- About **half** of all updates in the past year were authenticated by a password
- 1.4k maintainers authenticated with a password in the last year

Migration Plan

How will maintainers migrate away from passwords?

- The RIPE NCC notifies the community in advance by email to DB-WG
- The RIPE NCC emails all maintainers with an MD5 hashed password **in early 2025:**
  - Warn that we plan to drop support for passwords **six months later**
  - Ask them to switch to an alternative (SSO account, API Keys, PGP, X.509)
- Wait **three months** for maintainers to migrate themselves
- The RIPE NCC selects batches of maintainers from **three months** later:
  - Warn that we will remove their MD5 hashed passwords in one month
  - Assist anyone who asks for help to switch to an alternative
  - Remove MD5 hashed passwords in batches
- From **six months** later:
  - Remove support for MD5 hashed passwords
  - Follow "Forgot Maintainer Password" process (or contact DB support) if locked out

Questions & Comments

eshryane@ripe.net

RIPE NCC
RIPE NETWORK COORDINATION CENTER

THANK YOU!