



# NONE Considered Harmful

Shane Kerr, RIPE NCC

# Historical Context

- In the beginning... no authentication/authorisation
- mntner introduced
- PGP support added
- RPSL
  - Maintainers required for almost all objects
  - Detailed authorisation rules defined
- MD5-PW added
- MAIL-FROM deprecated

*General Trend Towards Improved Security!*



# Today

- Continued “tweaking” of rules:
  - Default to protected for inetnum/inet6num/domain
  - Reclaim functionality
  - “mnt-ref:”
- X.509

# “auth: NONE”

- This “authentication” offers no protection
  - Useful when notification is desired, but not protection
  - Allows use of “mnt-by:” as a tag
- Many maintainer objects exist with “auth: NONE”
  - About 500, or 5% of all maintainers
  - Mostly historical – *very* rare in new maintainers



# NONE is... the weakest link

- Unprotected data affects the entire community
  - Accidental updates
  - Hijacking concerns
- Password authentication is easy to use
- PGP or X.509 can be even easier

*Proposal: Deprecate NONE*



# #include <std-dbchange.h>

Usual procedure for changing the database:

1. Announce change (web page, mailing lists)
2. Notify specific users
3. Wait for users to fix data
4. Clean up / notify specific users
5. Announce completion (web page, mailing lists)
6. Champagne



# The “Band-Aid” Approach

- Usual approach is bad in this case:
  - Security concerns
  - Users only vaguely aware of phases
- So Just Do It™
- Differences from usual method:
  - No announcement
  - No waiting for users
  - Heavy reliance on easy-to-use recovery mechanisms



# Details for maintainers

- Remove “auth: NONE”
- If necessary, add generated MD5-PW password
- E-mail contacts
  - Explanation
  - Password
- Can also get passwords from [ripe-dbm@ripe.net](mailto:ripe-dbm@ripe.net)
- After a period of time, stop e-mailing passwords





# RIPE-NCC-NONE-MNT

- A very special maintainer
  - Added to objects during RPSL conversion
  - Also used to *unprotect* non-RIPE NCC resources
  - Currently “protects” about 6% of inetnum objects
- RIPE-NCC-RPSL-MNT with public password
- Most “mnt-by:” become RIPE-NCC-LOCKED-MNT
- Provide CGI link to unlock these objects:
  - Create a new maintainer
  - Change “mnt-by:” to the new maintainer



# Other maintainers

- RIPE-NCC-PN-NONE-MNT
  - Historical – from 2001 person cleanup
  - No current purpose: remove from “mnt-by:”
- LIM-MNT
  - Critical operational maintainer
  - Use public password
  - Pending approval from Secret-WG

