Special Interest Group

PGP Key Management

March 1st, Korea, Seoul

Assumptions

- Basic Knowledge of PGP
  - http://www.pgpi.org/
  - http://www.gnupg.org/
- Passing knowledge of RIPE-189
  - http://www.ripe.net/ripe/docs/ripe-189.html
- Understanding of how to PGP sign a message

Problem Definition

- *How to protect that which protects*
    - PGP valid auth method on APNIC maintainer objects
    - Protect your interests
- *Basic Security precautions*
    - Like physical key or credit card, stolen is bad and can cost

How Secure?

Possible weaknesses in PGP

- http://axion.physics.ubc.ca/pgp-attack.html
- PGP is as good as the system running it

Most exploits are due to easily guessed passphrases

- Eavesdroppers

‘Pretty Good’ Privacy, not ‘James Bond’ Privacy

Selecting a Passphrase

- Make it hard to guess
  - Simple passphrases easily guessed, more-so by those who know you
  - No birthdates (easily guessed)
  - Obscure book quotes (not your favourite book, see above)
  - Diceware (http://www.diceware.com)
  - Pronounceable line noise (‘zackalimvelich’)
  - Random number sub7titut1on

Sharing?

- ISP environment, several people may need to update objects

- Sharing the passphrase of one PGP key
  - Accidental leakage
  - Need to change passphrase when staff leave and inform remaining staff of change
  - Bad habit

Sharing (2) ?

- Multiple Auth
  - Maintainer objects can have multiple auths or valid PGP keys
  - Each staff member has own PGP key (in APNIC database)
  - Chain is only as strong as its weakest link; encourage each staff member to have strong passphrase
  - Only need to remove reference to their PGP key from mntner when staff leave

Backdoors?

- Chain is only as strong as its weakest link
  - PGP auth method in Maintainer object vunerable if less secure auth methods are also specified in same Maintainer object
  - Protecting a ‘key-cert’ object with a maintainer that uses ‘MAIL-FROM’ or ‘CRYPT-PW’ is against common sense
  - ‘Post-It’ notes on your monitor with your passphrase

References

- PGP
  - http://www.pgpi.org/
  - http://www.gnupg.org/
- RIPE NCC database
  - http://www.ripe.net/ripe/docs/ripe-189.html
- APNIC
  - http://www.apnic.net/db/

Further Discussion

Questions?