draft-gould-regext-secure-authinfo-transfer Extensible Provisioning Protocol (EPP) Secure Authorization Information for Transfer

James F. Gould
jgould@verisign.com
IETF-105 REGEXT Working Group

Introduction

- Problem
  - With the dependence on the use of the EPP authorization information to process transfers, how can the practices related to authorization information be improved while still using the existing EPP RFCs?
- Out-of-scope
  - Transfer process policy is out-of-scope (e.g., form of authorization, immediate transfer, duration of an authorization information value)
- EPP Secure Authorization Information for Transfer (draft-gould-regext-secure-authinfo-transfer)
  - https://tools.ietf.org/html/draft-gould-regext-secure-authinfo-transfer

Elements of Approach

- Strong Random Authorization Information
  - Draft defines a mechanism for creating a strong random authorization information value.
  - Recommendation is to use at least 128 bits of entropy; 20 characters (when using all printable ASCII characters except space 0x20).
- Short-Lived Authorization Information
  - Registry (server) currently supports setting and unsetting the authorization information value
  - Client should only set the authorization information value during the transfer process
  - Registrar (client) manages the (authinfo) Time-To-Live (TTL) based on its policy and unsets upon TTL expiration
- Storing Authorization Securely
  - Registrar (client) does not store the authorization information value
  - Registry (server) stores the authorization information value using a cryptographic hash

Transfer Flow with Secure Authorization Information

1. Registrant requests to register the object with the registrar
2. Registrar sends the create command with empty authorization information
3. Registrant requests the authorization information from the losing registrar
4. Losing registrar generates a secure authorization information value, sends it to the registry, and returns it to the registrant
5. Gaining registrar (optionally) verifies the authorization information using the info command
6. Gaining registrar sends authorization information on transfer request command
7. Registry unsets the authorization information upon a successful transfer

EPP RFC Support for Setting / Unsetting Authorization Information

- On create use empty authInfo
  - eppcom:pwAuthInfoType specifies a normalizedString with no length constraints
  - Example: <domain:authInfo><domain:pw/></domain:authInfo>
- On update authInfo can be unset
  - Use of <domain:null> or empty authInfo in RFC 5731
    - Example: <domain:authInfo><domain:null/></domain:authInfo>
    - Example: <domain:authInfo><domain:pw/></domain:authInfo>
  - Use of empty authInfo in RFC 5733
    - Example: <contact:authInfo><contact:pw/></contact:authInfo>
- On update use a strong, random authInfo value
  - eppcom:pwAuthInfoType has no length constraints
  - eppcom:pwAuthInfoType only has issues with inclusion of space (0x20)
- Info response does not return the authInfo
  - Authorization information is optional in RFC 5731 and RFC 5733

Conclusion

- EPP Secure Authorization Information for Transfer improves the security of authorization information
  - No need for a new EPP extension
  - Authorization information can exist only during the transfer process
  - Authorization information can have a client-managed TTL
  - Authorization information is not stored by the registrar and stored as a hash by the registry
- Please review the draft and provide feedback on the mailing list