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

James Gould
jgould@verisign.com
IETF-107 REGEXT Working Group

Introduction

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

Elements of Approach (Review)

- Strong Random Authorization Information
  - Draft defines a mechanism for creating a strong random authinfo 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 authinfo value
  - Client should only set the authinfo value during the transfer process
  - Registrar (client) manages any (authinfo) Time-To-Live (TTL) based on its local policy and unsets the authinfo upon TTL expiration
- Storing Authorization Securely
  - Registrar (client) does not store the authinfo value
  - Registry (server) stores the authinfo value using a cryptographic hash

Updates from Prior Versions

- Support of secure authinfo for purposes other than transfer
- Reference use of SHA-256 for authinfo storage
- Empty authinfo is stored with a NULL value
- Addition of “Authorization Information Matching” section
  - Any authinfo input value MUST NOT match an unset value
  - An empty authinfo value MUST NOT match any set value
  - A non-empty authinfo value MUST be hashed to match against the stored hashed value
- Support indication of set or unset authinfo in the *info* response for Sponsoring Registrar

Updates:
New Transition Considerations Section

- Definition of Classic Authorization Information Model
  - Registry requires a non-empty authinfo for life of the domain
    - Authinfo required on create and no ability to unset the authinfo
  - Registry stores the authinfo as an encrypted value
  - Registry returns the plain text authinfo in the *info* response to the Sponsoring Registrar
  - Registry does not touch the authinfo upon a successful transfer
  - Registry does not validate the entropy (length and randomness) of the authinfo

Updates: New Transition Considers Section

- Transition Phase 1 – Features
  - Authinfo optional on *create*
  - Authinfo can be unset on *update*
  - Authinfo automatically unset by Registry on successful transfer
  - Authinfo not returned in *info* response
  - No indication of authinfo being set or unset (except for Sponsoring Registrar)
- Transition Phase 2 – Storage
  - Hash new authinfo values
  - Support encrypted and hashed authinfo values during transition
  - Hash existing authinfo values
- Transition Phase 3 – Enforcement
  - Disallow authinfo on *create*
  - Validate entropy of authinfo value

Conclusion

- EPP Secure Authorization Information for Transfer improves the security of authinfo
  - No need for a new EPP extension
  - Authinfo can exist only during the transfer process
  - Authinfo can have a client-managed TTL
  - Authinfo 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