draft-ietf-regext-login-security
Login Security Extension

James F. Gould
jgould@verisign.com
IETF-104 REGEXT Working Group

Introduction

- Problems
  - RFC 5730 supports passwords with a maximum length of just 16 characters
  - EPP does not support the server providing login security warnings to the client (e.g. password expiry, cert expiry, insecure ciphers, etc.)
  - EPP does not support the client providing user agent information to the server
- Login Security Extension (draft-ietf-regext-login-security)
  - https://tools.ietf.org/html/draft-ietf-regext-login-security
  - Addresses the problems with an extension to the EPP Login command and response

Allow Passwords Longer Than 16 Characters

- Extend the Login Command
  - Enable overriding the current password (<pw>) or new password (<newPw>)
  - Use of *[LOGIN-SECURITY]* constant value to indicate override in extension
    - RFC 5730 requires a 6 to 16 character value for the <pw> or <newPw> element
    - Using the 16 character constant value makes the override explicit by the client
  - Client may continue to use the RFC 5730 elements if the password is 6 to 16 characters long
  - Login Security Extension must be used if the password is greater than 16 characters long
- <loginSec:pw> and <loginSec:newPw>
  - Uses XML schema “token” type with a minimum length of 6 and no maximum

Server: to Provide Login Security Warnings and Errors

- Extend the Login Response
- Support for a list of security events
  - A server may identify many security events for a session
  - Examples include expiring password, expiring certificate, insecure ciphers, etc.
- Extension added to the response only if
  - Client supports the Security Event extension based on the login services
  - There is at least one login security event

Login Security Event Attributes

- “type” – Extensible enumerated list of event types
  - “password”
  - “certificate”
  - “cipher”
  - “tlsProtocol”
  - “newPw”
  - “stat”
  - “custom”
- “name” – Optional name of “custom” or “stat” type event
- “level” – “warning” or “error” (for any event type)
- “exDate” – Optional expiration date for an expiry event (e.g., “password”, “certificate”)
- “value” – Optional value of a “stat” type event
- “duration” – Optional duration of a “stat” type event
- “lang” – Optional language of the event description with “en” default value
- Description – Human-readable description of the event element

Client: User Agent Information

- Extend the Login Command
  - Provide option for client to provide client agent information to the server
  - Provides the client software and platform used
  - Server can identify functional and security constraints, current security issues, and potential future functional and security issues for the client

Feedback from Mailing List

- Addressed
  - Setting of minimum password length to 6 characters
  - Make case of newPW consistent
  - Ensure the <loginSec:loginSec> element is non-empty
  - Revise the Security Considerations section
  - Changed XML namespace to be EPP-scoped
- Discussed
  - Support for additional authentication methods (2FA, Digest)?
  - Use of *[LOGIN-SECURITY]* constant value
  - Format of the password
    - Use of XML schema ”token” type
    - PRECIS framework (RFC 7564 and 8265)

Conclusion

- Login Security Extension addresses the 3 problems via
  - Login Command Extension
    - Extending the password past the RFC 5730 16-character maximum
    - Enabling the client to provide user agent information to the server
  - Login Response Extension
    - Enabling the server to provide login security warnings and errors
- Please review the draft and provide feedback on the mailing list