RDAP Security Requirements

Scott Hollenbeck
Verisign Labs
Background

• Sources
  – RFC 3707, “Cross Registry Internet Service Protocol (CRISP) Requirements”
  – SSAC 23, 27, 33, 40
  – Inventory of WHOIS Service Requirements Final Report (Sheng, Piscitello, and Gasster July 2010)
  – Anything else I could think of

• Protocol security vs. operational security
  – Specify the former, support the latter

• See RFC 4949 for security service definitions
Authentication

• Define an authentication framework for WHOIS that is able to accommodate anonymous access as well as verification of identities using a range of authentication methods and credential services
• Entities accessing the service (users) MUST be provided a mechanism for passing credentials to a server for the purpose of authentication.
• The protocol MUST provide a mechanism capable of employing many authentication types and capable of extension for future authentication types.
• Support federation
Authorization

• Implement an authorization framework that is capable of providing granular (per registration data object) permissions (access controls)
• The protocol MUST NOT prohibit an operator from granularly assigning multiple types of access to data according to the policies of the operator.
• The protocol MUST provide an authentication mechanism and MUST NOT prohibit an operator from granting types of access based on authentication.
• The protocol MUST provide an anonymous access mechanism that may be turned on or off based on the policy of an operator.
Availability

• Security consideration: DDoS protection
  – Refer to RFC 4732
• Explicit requirement: support abuse contacts
Data Confidentiality

- WHOIS services must provide mechanisms to protect the privacy of registrants
- A WHOIS service must discourage the harvesting and mining of its data
- MUST be capable of tagging values with labels
- Protect “in transit” credentials
Data Integrity

• Much talk of integrity and accuracy in the context of collected data, but not in the context of client-server interaction
  – Protocol data exchange: in scope
  – “Bogus” data detection: out of scope

• No explicit requirements identified
Non-repudiation

- No requirements identified
Open Questions: Authentication

• Client – Server authentication
  – Assume MUST be existing HTTP mechanism
    • Basic (encryption required) or Digest
  – Require one or allow both?
    • Require one: easier interoperability
      – Too limiting?
    • Allow both: more flexible
      – Interoperability risk
  – One thought: HTTP allows both

• Server – Server authentication?
Open Questions: Authorization

- Allow client to determine if the origin of the response was authorized to provide the data?
Open Questions: Data Confidentiality

• From RFC 3707
  – When a value in an answer to a query is given, the protocol MUST be capable of tagging the value with the following labels:
    1. do not redistribute
    2. special access granted

• Is this a requirement for RDAP?
Open Questions: Data Accuracy

• Not really a security requirement
  – Where does it belong?

• Data validation/verification
  – Requirement to flag that data has been “validated” or “verified”?
    • If so, how?