Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: March 23, 2013

S. Hollenbeck
Verisign Labs
N. Kong
CNNIC

September 19, 2012

Security Services for the Registration Data Access Protocol
draft-ietf-weirds-rdap-sec-00

Abstract

The Registration Data Access Protocol (RDAP) provides "RESTful" web services to retrieve registration metadata from domain name and regional internet registries. This document describes information security services and their application to RDAP.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on March 23, 2013.

Copyright Notice

Table of Contents

1. Introduction

The Registration Data Access Protocol (RDAP) core is specified in two documents: "Unified Registration Data Access Protocol Query Format" [I-D.ietf-weirds-rdap-query] and "JSON Responses for the Registry Data Access Protocol" [I-D.ietf-weirds-json-response]. One goal of RDAP is to provide security services that do not exist in the WHOIS [RFC3912] protocol, including authentication, availability, data confidentiality, data integrity, and non-repudiation (note: some of these might be a stretch).

This document describes each of these security services from the perspective of RDAP requirements and applicability. Where applicable, informational references to requirements for a WHOIS replacement service [RFC3707] are noted.

2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2.1. Acronyms and Abbreviations

DNR: Domain Name Registry

RDAP: Registration Data Access Protocol

RIR: Regional Internet Registry

3. Information Security Services and RDAP

RDAP itself does not include native security services. Instead, RDAP relies on features that are available in other protocol layers to provide needed security services including authentication, availability, data confidentiality, data integrity, and non-repudiation. A description of each of these security services can be found in RFC 4949 [RFC4949].

3.1. Authentication

WHOIS does not provide features to identify and authenticate clients. As noted in section 3.1.4.2 of RFC 3707 [RFC3707], there is utility in allowing server operators to offer "varying degrees of access depending on policy and need". Clients have to be identified and authenticated to provide that utility.

There are multiple ways to identify and authenticate RDAP clients. Candidate technologies include:

- HTTP Basic Authentication [RFC2617]: The "basic" scheme can be used to send a client's user name and password to a server in plaintext, based64-encoded form. If this scheme is used another protocol (such as HTTP Over TLS [RFC2818]) MUST be used to protect the client's credentials from disclosure while in transit.

- HTTP Digest Authentication [RFC2617]: The "digest" scheme can be used to authenticate a client without exposing the client's plaintext password.

- X.509 Digital Certificates [RFC5280]: The Transport Layer Security Protocol [RFC5246] includes an option to identify and authenticate clients who possess and present a valid X.509 digital certificate. Web clients do not typically possess digital certificates so this option is likely impractical.

- OAuth [I-D.ietf-oauth-v2]: The OAuth authorization framework describes a method for clients to access protected web resources using access tokens issued by a third party authorization server with the permission of the resource owner. If widely deployed it would permit clients to access servers without having to manage credentials on a per-server basis.

- (What else?)

3.2. Availability

An RDAP service has to be available to be useful (need to talk about denial of service, anycasting, and anything else that addresses availability).

3.3. Data Confidentiality

WHOIS does not provide the ability to encrypt data while in transit to protect it from inadvertent disclosure. Web services commonly use HTTP Over TLS [RFC2818] to provide that protection. Examples of data confidentiality utility include:

- Encryption to protect plaintext passwords exchanged when using the HTTP "basic" authentication scheme.

- Encryption to protect personal or otherwise sensitive data returned in response to RDAP queries.

- (What else?)

If data confidentiality is useful, we should also plan to review the JSON Web Encryption draft [I-D.ietf-jose-json-web-encryption].

3.4. Data Integrity

TBD: is there value in signed responses? If so, the work being done in the JOSE working group (such as what's described in the JSON Web Signature draft [I-D.ietf-jose-json-web-signature]) may be useful. There's no mention of a "signed response" requirement in RFC 3707.

3.5. Non-repudiation

TBD: does it make sense to talk about proof of integrity and data origin authentication for responses? It might in the context of law enforcement actions. Again, there's no requirement mentioned in RFC 3707.

4. IANA Considerations

This document does not specify any IANA actions.

5. Security Considerations

TBD

6. Acknowledgements

The authors would like to acknowledge the following individuals for their contributions to this document: Andrew Newton.

7. References

7.1. Normative References

[I-D.ietf-weirds-json-response]
Newton, A. and S. Hollenbeck, "JSON Responses for the Registy Data Access Protocol (RDAP)", draft-ietf-weirds-json-response-00 (work in progress), September 2012.

[I-D.ietf-weirds-rdap-query]
Newton, A. and S. Hollenbeck, "Unified Registration Data Access Protocol Query Format", draft-ietf-weirds-rdap-query-00 (work in progress), September 2012.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2617] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and L. Stewart, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, May 2008.

7.2. Informative References

[I-D.ietf-jose-json-web-encryption]
Jones, M., Rescorla, E., and J. Hildebrand, "JSON Web Encryption (JWE)", draft-ietf-jose-json-web-encryption-05 (work in progress), July 2012.

[I-D.ietf-jose-json-web-signature]
Jones, M., Bradley, J., and N. Sakimura, "JSON Web Signature (JWS)", draft-ietf-jose-json-web-signature-05 (work in progress), July 2012.

[I-D.ietf-oauth-v2]
Hardt, D., "The OAuth 2.0 Authorization Framework", draft-ietf-oauth-v2-31 (work in progress), August 2012.

[RFC3707] Newton, A., "Cross Registry Internet Service Protocol (CRISP) Requirements", RFC 3707, February 2004.

[RFC3912] Daigle, L., "WHOIS Protocol Specification", RFC 3912, September 2004.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

Appendix A. Change Log

Initial -00: Adopted as working group document.

Authors' Addresses

Scott Hollenbeck
Verisign Labs
12061 Bluemont Way
Reston, VA 20190
US

Email: shollenbeck@verisign.com
URI: http://www.verisignlabs.com/

Ning Kong
China Internet Network Information Center
4 South 4th Street, Zhongguancun, Haidian District
Beijing 100190
China

Phone: +86 10 5881 3147
Email: nkong@cnnic.cn