Internet Engineering Task Force (IETF) C. Ma
Internet Draft J. Chen
Intended status: Informational X. Fan
Expires: June 21, 2024 M. Chen
Z. Li
China Academy of Information and Communications Technology
December 21, 2023

Security Services for the Industrial Internet Identifier Data Access Protocol (IIIDAP)
draft-mcd-identifier-access-security-08

Abstract

The Industrial Internet Identifier Data Access Protocol (IIIDAP) provides "RESTful" web services to retrieve identifier metadata from Second-Level Node (SLN). This document describes information security services, including access control, authentication, authorization, availability, data confidentiality, and data integrity for IIIDAP.

Table of Contents

1. Introduction

One goal of IIIDAP is to provide security services, including access control, authentication, authorization, availability, data confidentiality, and data integrity. This document describes how each of these services is achieved by IIIDAP using features that are available in other protocol layers. Additional or alternative mechanisms can be added in the future.

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

HTTP: Hypertext Transfer Protocol

JSON: JavaScript Object Notation

IIIDAP: Industrial Internet Identifier Data Access Protocol

SLN: Second-Level Nodes

ELN: Enterprise-Level Nodes

TLS: Transport Layer Security

3. Information Security Services and IIIDAP

IIIDAP itself does not include native security services. Instead, IIIDAP relies on features that are available in other protocol layers to provide needed security services, including access control, authentication, authorization, availability, data confidentiality, and data integrity. A description of each of these security services can be found in "Internet Security Glossary, Version 2" [RFC4949]. No requirements have been identified for other security services.

3.1. Access Control

As described in the following sections, IIIDAP includes features to identify, authenticate, and authorize clients, allowing server operators to control access to information based on a client's identity and associated authorizations. Information returned to a client can be clearly marked with a status value (see Section 13 of [IDENTIFIER-RESPONSES]) that identifies the access granted to the client.

3.2. Authentication

This section describes security authentication mechanisms and the need for authorization policies to include them. It describes requirements for the implementations of clients and servers but does not dictate the policies of server operators. For example, a server

operator with no policy regarding differentiated or tiered access to data will have no authorization mechanisms and will have no need for any type of authentication. A server operator with policies on differentiated access will have to construct an authorization scheme and will need to follow the specified authentication requirements.

IIIDAP's authentication framework needs to accommodate anonymous access as well as verification of identities using a range of authentication methods and credential services. To that end, IIIDAP clients and servers MUST implement the authentication framework [RFC9110]. The "basic" scheme can be used to send a client's user name and password to a server in plaintext, base64-encoded form. The "digest" scheme can be used to authenticate a client without exposing the client's plaintext password. If the "basic" scheme is used, HTTP over TLS [RFC9110] MUST be used to protect the client's credentials from disclosure while in transit (see Section 3.5).

Servers MUST support either Basic or Digest authentication; they are not required to support both. Clients MUST support both to interoperate with servers that support one or the other. Servers may provide a login page that triggers HTTP authentication. Clients should continue sending the HTTP authentication header once they receive an initial 401 (Unauthorized) response from the HTTP server as long as the scheme portion of the URL doesn't change.

The Transport Layer Security protocol [RFC8446] includes an optional feature to identify and authenticate clients who possess and present a valid X.509 digital certificate [RFC5280]. Support for this feature is OPTIONAL.

IIIDAP does not impose any unique server authentication requirements. The server authentication provided by TLS fully addresses the needs of IIIDAP. In general, transports for IIIDAP must either provide a TLS-protected transport (e.g., HTTPS) or a mechanism that provides an equivalent level of server authentication.

Work on HTTP authentication methods continues. IIIDAP is designed to be agile enough to support additional methods as they are defined.

3.3. Authorization

Server operators MAY offer varying degrees of access depending on policy and need in conjunction with the authentication methods described in Section 3.2. If such varying degrees of access are supported, an IIIDAP server MUST provide granular access controls

(that is, per identifier metadata) in order to implement authorization policies. Some examples:

- Clients will be allowed access only to data for which they have a relationship.

- Unauthenticated or anonymous access status may not yield any contact information.

- Full access may be granted to a special group of authenticated clients.

The type of access allowed by a server will most likely vary from one operator to the next. A description of the response privacy considerations associated with different levels of authorization can be found in Section 13 of [IDENTIFIER-RESPONSES].

3.4. Availability

An IIIDAP service has to be available to be useful. There are no IIIDAP-unique requirements to provide availability, but as a general security consideration, a service operator needs to be aware of the issues associated with denial of service. A thorough reading of "Internet Denial-of-Service Considerations" [RFC4732] is advised.

An IIIDAP service MAY use an HTTP throttling mechanism to limit the number of queries that a single client can send in a given period of time. If used, the server SHOULD return an HTTP 429 (Too Many Requests) response code as described in "Additional HTTP Status Codes" [RFC6585]. A client that receives a 429 response SHOULD decrease its query rate and honor the Retry-After header field if one is present. Note that this is not a defense against denial-of-service attacks, since a malicious client could ignore the code and continue to send queries at a high rate. A server might use another response code if it did not wish to reveal to a client that rate limiting is the reason for the denial of a reply.

3.5. Data Confidentiality

IIIDAP uses HTTP over TLS [RFC9110] to provide that protection by encrypting all traffic sent on the connection between client and server. HTTP over TLS MUST be used to protect all client-server exchanges unless operational constraints make it impossible to meet this requirement. It is also possible to encrypt discrete objects (such as command path segments and JSON- encoded response objects) at one endpoint, send them to the other endpoint via an unprotected transport protocol, and decrypt the object on receipt. Encryption

algorithms as described in "Internet Security Glossary, Version 2" [RFC4949] are commonly used to provide data confidentiality at the object level.

There are no current requirements for object-level data confidentiality using encryption. Support for this feature could be added to IIIDAP in the future.

As noted in Section 3.2, the HTTP "basic" authentication scheme can be used to authenticate a client. When this scheme is used, HTTP over TLS MUST be used to protect the client's credentials from disclosure while in transit. If the policy of the server operator requires encryption to protect client-server data exchanges (such as to protect non-public data that cannot be accessed without client identification and authentication), HTTP over TLS MUST be used to protect those exchanges.

A description of privacy threats that can be addressed with confidentiality services can be found in Section 4. Section 13 of [IDENTIFIER-RESPONSES] describes status values that can be used to describe operator actions used to protect response data from disclosure to unauthorized clients.

3.6. Data Integrity

Web services such as IIIDAP commonly use HTTP over TLS [RFC9110] to provide that protection by using a keyed Message Authentication Code (MAC) to detect modifications. It is also possible to sign discrete objects (such as command path segments and JSON-encoded response objects) at one endpoint, send them to the other endpoint via a transport protocol, and validate the signature of the object on receipt. Digital signature algorithms as described in "Internet Security Glossary, Version 2" [RFC4949] are commonly used to provide data integrity at the object level.

There are no current requirements for object-level data integrity using digital signatures. Support for this feature could be added to IIIDAP in the future.

The most specific need for this service is to provide assurance that HTTP 30x redirection hints [RFC9110] and response elements returned from the server are not modified while in transit. If the policy of the server operator requires message integrity for client-server data exchanges, HTTP over TLS MUST be used to protect those exchanges.

4. Privacy Threats Associated with Industrial Internet Identifier Data

The identifiers' information of ELN SHOULD be uploaded to SLN. The standardization of IIIDAP does not change or impact the data that operators of SLN may require to be collected from ELN, but it provides support for a number of mechanisms that may be used to mitigate privacy threats to ELN should SLN choose to use them.

IIIDAP includes mechanisms that can be used to authenticate clients, allowing servers to support tiered access based on local policy. This means that all identifier data need no longer be public, and personal data or data that may be considered more sensitive can have its access restricted to specifically privileged clients.

IIIDAP data structures allow servers to indicate via status values when data returned to clients has been made private, redacted, obscured, by a proxy. "Private" means that the data is not designated for public consumption. "Redacted" means that some identifier data fields are not being made available. "Obscured" means that data has been altered for the purposes of not readily revealing the actual identifier information.

In addition to privacy risks to the information of identifiers, there are also potential privacy risks for those who query identifier data. For example, the fact that a SLN employee performs a particular query may reveal information about the employee's activities that he or she would have preferred to keep private. IIIDAP supports the use of HTTP over TLS to provide privacy protection for those querying identifier data, unless operational constraints make it impossible to meet this requirement.

5. Security Considerations

This document describes the security services provided by IIIDAP and associated protocol layers, including authentication, authorization, availability, data confidentiality, and data integrity.

As an HTTP-based protocol, IIIDAP is susceptible to code injection attacks. Code injection refers to adding code into a computer system or program to alter the course of execution. There are many types of code injection, including SQL injection, dynamic variable or function injection, include-file injection, shell injection, and HTML-script injection, among others. Data confidentiality and integrity services provide a measure of defense against man-in-the-middle injection attacks, but vulnerabilities in both client- and server-side software make it possible for injection attacks to

succeed. Consistently checking and validating server credentials can help detect man-in-the-middle attacks.

There is a risk of too promiscuous, or even rogue, CAs being included in the list of acceptable CAs that the TLS server sends the client as part of the TLS client-authentication handshake and lending the appearance of trust to certificates signed by those CAs. Periodic monitoring of the list of CAs that IIIDAP servers trust for client authentication can help reduce this risk.

The Transport Layer Security protocol [RFC8446] includes a null cipher suite that does not encrypt data and thus does not provide data confidentiality. This option MUST NOT be used when data confidentiality services are needed. Additional considerations for secure use of TLS are described in [RFC9325].

Data integrity services are sometimes mistakenly associated with directory service operational policy requirements focused on data accuracy. "Accuracy" refers to the truthful association of data elements (such as names, addresses, and telephone numbers). Accuracy requirements are out of scope for this protocol.

Additional security considerations are described in the specifications for HTTP [RFC9110], HTTP Basic and Digest access authentication [RFC9110], HTTP over TLS [RFC9110], and additional HTTP status codes [RFC6585].

6. IANA Considerations

7. References

References to IIIDAP are subject to the latest edition.

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC6585] Nottingham, M. and R. Fielding, "Additional HTTP Status Codes", RFC 6585, April 2012, <http://www.rfc-editor.org/info/rfc6585>.

[RFC9110] Fielding, R., Ed., M. Nottingham, Ed. and J. Reschke, Ed., " HTTP Semantics", RFC 9110, June 2022, <http://www.rfc-editor.org/info/rfc9110>.

7.2. Informative References

[RFC4732] Handley, M., Ed., Rescorla, E., Ed., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, December 2006, <http://www.rfc-editor.org/info/rfc4732>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, August 2007, <http://www.rfc-editor.org/info/rfc4949>.

[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, <http://www.rfc-editor.org/info/rfc5280>.

[RFC8446] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, August 2018, <http://www.rfc-editor.org/info/rfc8446>.

[RFC9325] Y. Sheffer, P. Saint-Andre and T. Fossati "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", RFC 9325, November 2022, <http://www.rfc-editor.org/info/rfc9325>.

[IDENTIFIER-RESPONSES] Ma, C., "JSON Responses for the Industrial Internet Identifier Data Access Protocol (IIIDAP)", Work in Progress, draft-mcd-identifier-access-responce, December 2023.

Authors' Addresses

Chendi Ma
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 177 1090 9864
Email: machendi@caict.ac.cn

Chen Jian
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 138 1103 3332
Email: chenjian3@caict.ac.cn

Xiaotian Fan
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 134 0108 6945
Email: fanxiaotian@caict.ac.cn

Meilan Chen
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 139 1143 7301
Email: chenmeilan@caict.ac.cn

Zhiping Li
CAICT
No.52 Huayuan North Road, Haidian District
Beijing, Beijing, 100191
China

Phone: +86 185 1107 1386
Email: lizhiping@caict.ac.cn