TAXII 1.0 (DRAFT) Messages

Message data model and XML binding

Charles Schmidt & Mark Davidson

Approved for Public Release; Distribution Unlimited: 12-4167

MITRE

About This Talk

- **Look at the messages and exchanges defined in TAXII**
  - What information the TAXII services receive/send
- **We are discussing a draft specification**
  - There are multiple open questions – we do not have all the answers
- **We want your input**
  - Please ask questions
  - Please feel free to provide suggestions for changes

Approved for Public Release; Distribution Unlimited: 12-4167

TAXII Message Definitions

- **TAXII message definitions are split between specifications**
  - TAXII Services specification defines a message data model
    - Identifies what information each message conveys
  - TAXII Message Binding specifications define how to express each TAXII message in the given format (e.g., XML)
  - TAXII Protocol Binding specifications may define expressions of certain messages when integrated to the protocol components
- **Goal is to provide a stable understanding of message content (data model) while allowing flexibility in its expression (binding)**
- **TAXII 1.0 currently defines only a single message binding: XML**
- **The TAXII HTTP Protocol Binding defines expressions for two TAXII message types without using a message binding**

Approved for Public Release; Distribution Unlimited: 12-4167

Message Construction

- **Header fields**
  - Fields common to all TAXII messages
  - Some bindings (e.g. XML) do not distinguish between TAXII headers and body
- **Data model defines *what* is in fields, but no *how* it appears**
  - Does not specify data types
  - Indicates if field is required
    - I.e., whether field content must be conveyed in the message
  - Indicates if a field may provide multiple values
  - Example:
    - Data model says that all messages must have a single globally unique identifier
    - XML message binding says this is a string consisting of 32 hex digits (case insensitive) with or without separating characters

Approved for Public Release; Distribution Unlimited: 12-4167

Multiple Points of Extensibility

- **All messages can be given vendor/user/etc. defined fields**
  - Part of the “header” – (i.e. “Any message can have them”)
  - Name-value pairs, but both name and value may have any structure
  - Message recipients ignore fields they do not recognize
- **Some fields allow vendor/user/etc. defined values**
  - Error types
    - For custom error handling
    - Unrecognized error types map to the generic FAILURE type
  - Bindings
    - For custom message/protocol bindings
    - Unrecognized bindings are just “not supported”

Approved for Public Release; Distribution Unlimited: 12-4167

TAXII Messages

- **TAXII Error Message**

  Indicate an error condition. Sent from any service.

- **TAXII Discovery Request**
- **TAXII Discovery Response**

  Request/response to a Discovery service to learn of the presence and contact details of other TAXII services

- **TAXII Feed Information Request**
- **TAXII Feed Information Response**

  Request/response to a Feed Management service to learn of the presence of TAXII data feeds

- **TAXII Manage Feed Subscription Request**
- **TAXII Manage Feed Subscription Response**

  Request/response to a Feed Management service to manage and/or create a data feed subscription.

- **TAXII Poll Request**
- **TAXII Poll Response**

  Request/response to a Poll service to retrieve some range of content from a TAXII data feed.

- **TAXII STIX Message**

  Send STIX content to a TAXII Inbox service.

Approved for Public Release; Distribution Unlimited: 12-4167

MITRE

TAXII Error Message

- **Any service can send in response to a message**
- **Fields include:**
  - Error type – from an enumeration or sender-defined
  - Error detail – machine-readable information about the error
    - Binding specs specify format
  - Message – optional human-readable information about the error
- **Data model enumerates 11 error types:**
  - Bad Message, Unsupported Service, Unauthorized, Denied, Unsupported Protocol, Unsupported Message Binding, Unsupported Content Binding, Not Found, Unrecognized Value
  - Pending = request could not be completed immediately – repeat request after a specified interval
  - Failure = Generic error; services can always send this instead of a more specific error message

Approved for Public Release; Distribution Unlimited: 12-4167

TAXII Discovery Request/Response

- **Between a TAXII Client and a Discovery Service**
- **Request just contains header fields (i.e., no special parameters)**
- **Response contains a record for each reported service:**
  - Service type
  - TAXII version
  - Supported protocol binding
  - Address to use when contacting the service
  - Supported message, and (if appropriate) STIX bindings
  - Optionally, whether requester is known to have access to the service
  - Optional additional human-readable message
- **Discovery service might not report some services based on requester identity or for other reasons**

Approved for Public Release; Distribution Unlimited: 12-4167

TAXII Feed Information Request/Response

- **Between a TAXII Client and a Feed Management Service**
- **Request just contains header fields**
- **Response contains a record for each reported TAXII data feed:**
  - Feed name – the string used as a handle for this feed
  - Description – human readable description of the feed
  - Delivery methods – how feed content can be delivered (protocol binding and/or POLL)
  - Supported message and STIX bindings
  - Optionally, whether the requester is known to have access to this feed
- **Feed Management Service might not report some feeds based on requester identity or for other reasons**

TAXII Manage Feed Subscription Request/Response

- **Between a TAXII Client and a Feed Management Service**
- **Request identifies an action to take on a named data feed**
  - Actions: SUBSCRIBE, UNSUBSCRIBE, PAUSE, RESUME, MODIFY, STATUS
  - When creating or modifying a subscription, specify
    - Delivery method (protocol binding and Inbox service address OR POLL)
    - Message and content binding
  - When managing existing subscriptions, identify subscription
- **Response indicates successful action (failure gives an Error)**
  - Repeats subscription parameters and includes a subscription ID value
  - Responses to a STATUS action will produce records for each of the requester's subscriptions to the named data feed
  - May also include a human-readable message

TAXII Poll Request/Response

- **Between a TAXII Client and a Poll Service**
- **Request names a data feed and provides a timestamp range**
  - Timestamp range may be open on either or both end
  - Also give a subscription ID or a content binding
    - The latter to address cases where producer does not require an existing subscription to poll the feed
- **Response provides STIX content and the timestamp range from which this content was drawn**
  - Timestamp range may have no lower bound, but upper bound must be given
  - STIX content binding is explicitly identified
  - Content may not represent all records within the identified range
    - Producers can always elide information based on requester identity or for other reasons
  - May include a human readable message
  - May identify the polled subscription (if it exists)

Approved for Public Release; Distribution Unlimited: 12-4167

STIX Message

- **Sent from a TAXII Client to an Inbox Service**
- **Contains STIX content**
  - STIX content binding is explicitly identified
  - May contain a human-readable message
  - May identify an appropriate subscription ID
- **Can support solicited and unsolicited content**
  - Solicited = a pre-arranged agreement with a producer to provide content (e.g., a subscription)
  - Unsolicited = no prior agreement with the producer (e.g., volunteered information from a previously unknown source)

The TAXII XML Message Binding

- **TAXII 1.0 defines one message binding: XML**
  - The XML binding uses relatively basic XML forms
- **Includes an XML schema but the schema is not normative**
- **Defines structures for all message types**
  - Note that the HTTP binding doesn't use two of these message structures – XML binding is not bound to the HTTP binding

Approved for Public Release; Distribution Unlimited: 12-4167

Thoughts and Conclusion

- **Messages need to be flexible but unambiguous**
- **TAXII messages have no support for authentication or encryption**
  - TAXII relies on network protocols for this
- **TAXII messages support the TAXII services**
  - Goal is to support a range of use cases while minimizing implementer effort

Approved for Public Release; Distribution Unlimited: 12-4167

For more information

- **http://taxii.mitre.org/**
- **Sign up for the TAXII Discussion and Announcement mailing lists**
  - http://taxii.mitre.org/community/registration.html
- **Related sites**
  - https://stix.mitre.org/
  - http://cybox.mitre.org/

Approved for Public Release; Distribution Unlimited: 12-4167

MITRE

Help out

- **TAXII 1.0 is still in DRAFT form**
- **Please tell us if TAXII is going in the right direction**
  - Do the TAXII messages adequately support the TAXII services and targeted use cases?
  - Are the messages sufficiently unambiguous?
- **Draft specifications are available on the TAXII web site**

We need your help to make sure TAXII meets its goal of simplifying the sharing of structured threat information

Approved for Public Release; Distribution Unlimited: 12-4167