TAXII 1.0 (DRAFT)

Detailed Walk-through

Charles Schmidt & Mark Davidson

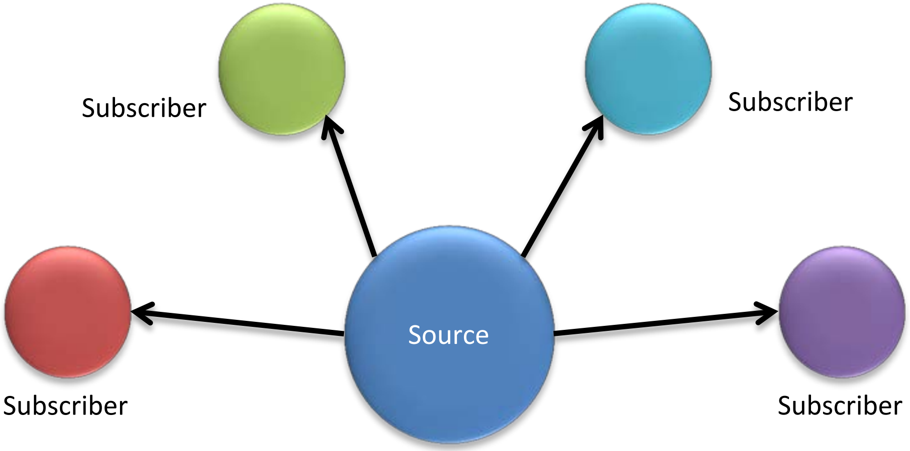
Approved for Public Release; Distribution Unlimited: 12-4167

About This Talk

- **Look at the XML and HTTP messages to support a simple sharing scenario using TAXII 1.1**

A Source/Subscriber Sharing Model

- **Vendor has multiple sharing level**
  - Different “contract” levels get different data
  - Customers purchase contracts to gain access to data feeds
- **Assume:**
  - Content already expressed in STIX
  - Vendor has already organized their content into data feeds based on contract levels
  - Vendor hosts Discovery, Feed Management, & Poll services



New Customer Contacts Discovery Service

- **Customer wishes to learn of available TAXII Services**
  - The Discovery Service address is published through other means
- **TAXII HTTP Protocol Binding defines this as a GET message with no body**

Header fields as HTTP parameters

```
GET /?message_type=discovery_request&message_id=
a84798beffe840ee3722c893288bd375 HTTP/1.1

Host: taxiiserver.company.com
Accept: application/xml
Content-Type: application/xml
User-Agent: TAXII client application
X-TAXII-Accept: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTP_BINDING_1.0
```

TAXII HTTP Headers

Vendor’s Discovery Service Responds to Customer’s Request

```
HTTP/1.1 200 OK
Content-Type: application/xml
Content-Length: 2474
Date: Thu, 15 Nov 2012 08:12:31 GMT
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTP_BINDING_1.0
```

TAXII HTTP Headers

TAXII XML Message Body

```
<?xml version="1.0" encoding="UTF-8"?>
<TAXII_DiscoveryResponse
    xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="984987DE-FEAA-95FF-894C-CBCC432988839023"
    in-response-to="a84798beffe840ee3722c893288bd375">
     <service-instance service-type="FEED-MANAGEMENT"
                  service-version="TAXII_1.0">
             <protocol-binding>TAXII_HTTPS_BINDING_1.0</protocol-binding>
             <message-binding>TAXII_XML_BINDING_1.0</message-binding>
             <service-address>https://taxiiserver.company.com/feeds/pay
             </service-address>
             <message>Used to for for-pay data feeds. To purchase a
                  subscription, go to http://www.company.com/sales and
                  follow the on-screen instructions.</message>
      </service-instance>
      <service-instance service-type="POLL" service-version="TAXII_1.0">
             <protocol-binding>TAXII_HTTPS_BINDING_1.0</protocol-binding>
             <message-binding>TAXII_XML_BINDING_1.0</message-binding>
             <service-address>https://taxiiserver.company.com/feeds/pay
             </service-address>
             <message>To support polling of for-pay data feeds.</message>
      </service-instance>
```

Customer Queries Vendor About Available Feeds

- **Customer wishes to learn of available TAXII Data Feeds**
  - Contacts the Feed Management Service learned earlier
- **TAXII HTTP Protocol Binding defines this as a GET message with no body**

Header fields as HTTP parameters

```
GET /feeds/pay/?message_type=feed_information_request&
message_id=a84798beffe840ee3722c893288bd376 HTTP/1.1

Host: taxiiserver.company.com
Accept: application/xml
Content-Type: application/xml
User-Agent: TAXII client application
X-TAXII-Accept: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTPS_BINDING_1.0
```

TAXII HTTP Headers

Vendor Responds with a List of Feeds

TAXII HTTP Headers

```
HTTP/1.1 200 OK
Content-Type: application/xml
Content-Length: 1464
Date: Thu, 15 Nov 2012 09:11:43 GMT
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXI-Protocol: TAXI_HTTP_BINDING_1.0
```

TAXII XML Message Body

```
<?xml version="1.0" encoding="UTF-8"?>
<TAXII_FeedInformationResponse
    xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="984987DE-FEAA-95FF-894C-B845503EEF3319AC"
    in-response-to="a84798beffe840ee3722c893288bde376">
    <feed feed-name="Platinum">
        <description>Our most comprehensive data feed containing up-to-
             the-minute threat information and professional analysis of
             impact and context. </description>
        <delivery-method>TAXII_HTTP_BINDING_1.0</delivery-method>
        <delivery-method>POLL</delivery-method>
        <message-binding>TAXII_XML_BINDING_1.0</message-binding>
        <content-binding>STIX_XML_1.0</content-binding>
    </feed>
    <feed feed-name="Gold">
        <description>Up-to-the-minute threat information covering global
             threats but with no additional analysis.</description>
        <delivery-method>TAXII_HTTP_BINDING_1.0</delivery-method>
        <delivery-method>POLL</delivery-method>
        <message-binding>TAXII_XML_BINDING_1.0</message-binding>
        <content-binding>STIX_XML_1.0</content-binding>
    </feed>
```

Customer Purchases Contract

- **Happens outside of TAXII**
  - Contact web site and fill out purchase
- **Establish authentication credentials**
  - In this case, assume a certificate-based authentication verified using TLS client-authentication

Customer Subscribes to a Data Feed

```
POST /feeds/pay HTTP/1.1
Host: taxiiserver.company.com
Accept: application/xml
Content-Type: application/xml
Content-Length: 578
User-Agent: TAXII client application
X-TAXII-Accept: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTPS_BINDING_1.0
```

TAXII HTTP Headers

TAXII XML Message Body

```
<?xml version="1.0" encoding="UTF-8"?>
<TAXII_SubscriptionManagementRequest
    xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="a84798beffe840ee3722c893288bd377">
    <feed-name>Gold</feed-name>
    <action>SUBSCRIBE</action>
    <subscription>
        <delivery-method>TAXII_HTTPS_BINDING_1.0</delivery-method>
        <message-binding>TAXII_XML_BINDING_1.0</message-binding>
        <content-binding>STIX_XML_1.0</content-binding>
        <send-to>https://www.customer.com/taxii/inbox</send-to>
    </subscription>
</TAXII_SubscriptionManagementRequest>
```

Vendor Responds that Request was Successful

TAXII HTTP Headers

```
HTTP/1.1 200 OK
Content-Type: application/xml
Content-Length: 758
Date: Wed, 21 Nov 2012 11:12:31 GMT
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTPS_BINDING_1.0
```

TAXII XML Message Body

```
<?xml version="1.0" encoding="UTF-8"?>
<TAXII_SubscriptionManagementResponse
    xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="984987DE-FEAA-95FF-894C-CCB893840004CF67"
    in-response-to="a84798beffe840ee3722c893288bd377">
    <feed-name>Gold</feed-name>
    <message>Thank you for your business. Your subscription is paid
          up for 6 months.</message>
    <subscription subscription-id="customer.com-JGK8H84BF">
        <delivery-method>TAXII_HTTPS_BINDING_1.0</delivery-method>
        <message-binding>TAXII_XML_BINDING_1.0</message-binding>
        <content-binding>STIX_XML_1.0</content-binding>
        <send-to>https://www.customer.com/taxii/inbox</send-to>
    </subscription>
</TAXII_SubscriptionManagementResponse>
```

Customer Polls the Data Feed

- **In their first request, customer asks for all prior posts on feed**
  – Does not include bounding timestamps

```
POST /feeds/pay HTTP/1.1
Host: taxiiserver.company.com
Accept: application/xml
Content-Type: application/xml
Content-Length: 336
User-Agent: TAXII client application
X-TAXII-Accept: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTPS_BINDING_1.0

<?xml version="1.0" encoding="UTF-8"?>
<TAXII_PollRequest xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="a84798beffe840ee3722c893288bd389">
    <feed-name>Gold</feed-name>
    <subscription-id>customer.com-JGK8H84BF</subscription-id>
</TAXII_PollRequest>
```

TAXII HTTP Headers

TAXII XML Message Body

Vendor Responds to the Poll Request

- **Vendor timestamps bound range of reported information**

```
HTTP/1.1 200 OK
Content-Type: application/xml
Content-Length: 518
Date: Mon, 10 Dec 2012 11:52:22 GMT
X-TAXII-Content-Type: TAXII_1.0/TAXII_XML_BINDING_1.0
X-TAXII-Protocol: TAXI_HTTPS_BINDING_1.0

<?xml version="1.0" encoding="UTF-8"?>
<TAXII_PollResponse xmlns="http://taxii.mitre.org/messages/xml/1"
    message-id="984987DE-FEAA-95FF-894C-800F7EACA647A6A"
    in-response-to="a84798beffe840ee3722c893288bd389">
    <begin-timestamp>2012-07-07T00:00:00Z</begin-timestamp>
    <end-timestamp>2012-12-06T14:43:34Z</end-timestamp>
    <subscription-id>customer.com-JGK8H84BF</subscription-id>
    <content-binding>STIX_XML_1.0</content-binding>
    <STIX xmlns="http://stix.mitre.org"/>
</TAXII_PollResponse>
```

TAXII HTTP Headers

TAXII XML Message Body

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/

Help out

- **TAXII 1.0 is still in DRAFT form**
- **Please tell us if TAXII is going in the right direction**
  - Does it adequately cover your use cases?
  - Are the TAXII services reasonable divisions of activity?
  - What are your thoughts on the TAXII bindings?
- **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