THE MITRE CORPORATION

TAXII Overview

Version 1.1

Mark Davidson, Charles Schmidt

1/13/2014

Trusted Automated eXchange of Indicator Information (TAXII ™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries.

Trademark Information

Feedback

Feedback on this or any of the other TAXII specifications is welcome and can be sent to taxii-discussion-list@lists.mitre.org after signing up on the community registration page (http://taxii.mitre.org/community/registration.html). You may also provide feedback directly to MITRE by sending a message to taxii@mitre.org.

Comments, questions, suggestions, and concerns are all appreciated.

Table of Contents

1 Introduction

Trusted Automated eXchange of Indicator Information (TAXII ™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across organization and product/service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative or application and does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing. Instead, TAXII empowers organizations to achieve improved situational awareness about emerging threats, and enables organizations to easily share the information they choose with the partners they choose.

1.1 Scope

This section describes the scope of TAXII by illustrating the spectrum of information sharing models TAXII supports. TAXII's scope includes, but is not limited to, the following information sharing models, as well as variants and combinations of the sharing models.

Hub and Spoke - In a hub and spoke information sharing architecture, one organization acts as a clearinghouse (the hub) for all sharing participants (the spokes). A spoke shares information with the hub, which then re-shares this information with all other spokes. The hub may perform analytics or filtering before re-sharing information. In this architecture, information may flow from spoke to hub and from hub to spoke.

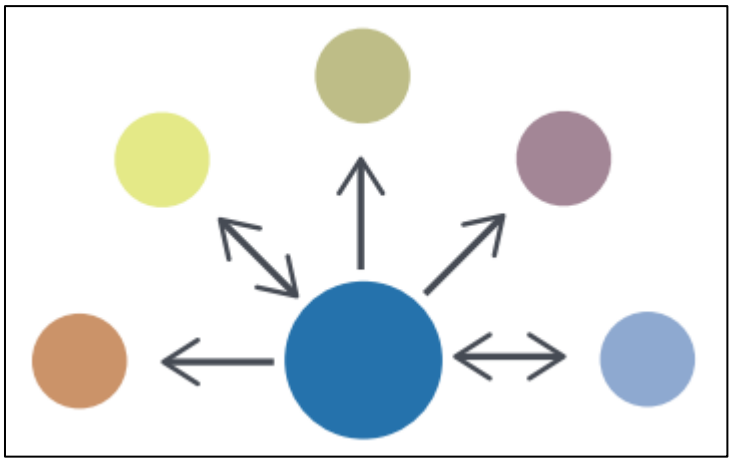

Figure 1 - Hub and Spoke Diagram

Source/Subscriber - In a source/subscriber information sharing architecture, one organization acts as a single source of information for all subscribers. In this architecture, information flows from the source to a subscriber.

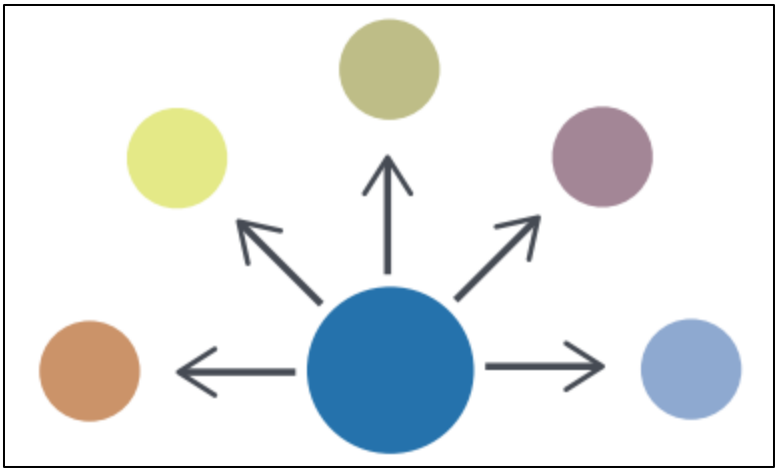

Figure 2 - Source/Subscriber Diagram

Peer to Peer - In the Peer to Peer information sharing architecture, any number of organizations act as both producers and consumers of information. In this architecture, information flows from one peer to another peer.

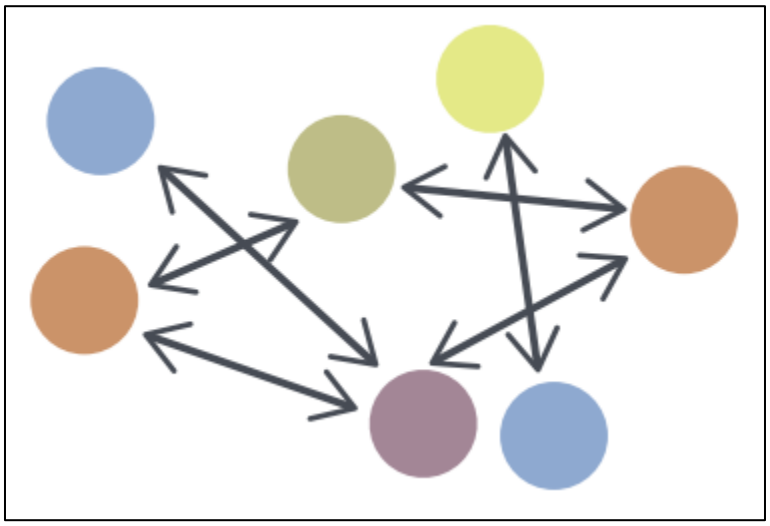

Figure 3 - Peer to Peer Diagram

1.2 TAXII Documents

TAXII is defined by a collection of interrelated documents. This section describes those documents.

TAXII Overview - The TAXII Overview (this document) defines the primary concepts of TAXII, as well as the organization of TAXII component documents.

Services Specification - The Services Specification defines TAXII Services, as well as the information conveyed by TAXII Messages and TAXII Message Exchanges. It provides normative requirements that govern TAXII Services and Message Exchanges.

Message Binding Specification - A Message Binding Specification defines normative requirements for representing TAXII Messages in a particular format (e.g., XML). There may be multiple Message Binding Specifications created for TAXII where each Message Binding Specification defines a binding of TAXII Messages using a different format.

Protocol Binding Specification - A Protocol Binding Specification defines normative requirements for transporting TAXII Messages over some network protocol (e.g., HTTP). There may be multiple Protocol Binding Specifications created for TAXII where each Protocol Binding Specification defines requirements for transporting TAXII Messages using a different network protocol.

Query Format Specification - A Query Format Specification defines a query format that can be used to define query expressions that are used within TAXII Messages to provide characteristics against which content records are compared. Query Expressions allow requestors to collect only content that meets these criteria. A Query Format Specification my include how to express the given format in a particular Message Binding, or this may be handled by a separate Message Binding Specification.

Content Binding Reference - The Content Binding Reference is a non-normative document that lists Content Binding IDs for use within TAXII.

Figure 4 shows how these specifications relate to each other.

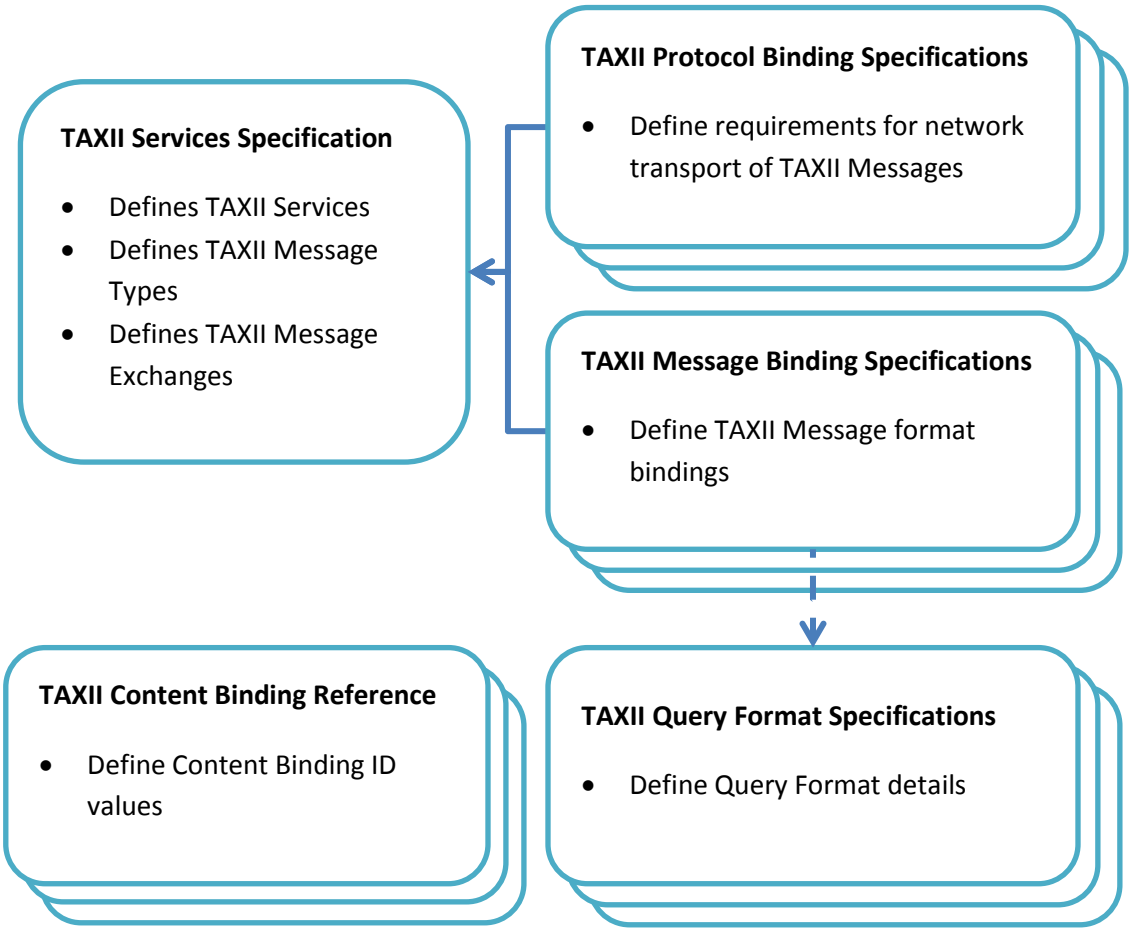

Figure 4 - TAXII Specification Hierarchy

Separation of the TAXII Specifications exists to support flexibility as TAXII evolves. Threat information sharing communities often have specific constraints on the types of network protocols and message formats they are able to support, the types of content they can exchange, and the types of queries their infrastructure can support. Rather than tying TAXII to a specific mechanism that excludes portions of the community, TAXII's core concepts (i.e., its services and exchanges) are defined separately from the implementation details of those concepts. When there is a need for a new binding, it can be created, either as part of a new official release of TAXII or as a third-party extension for TAXII, without affecting TAXII's core components. Groups that use different protocol or message bindings for TAXII will not be able to communicate directly with each other, but because they are still using TAXII Messages and Services at the core of their communications it is possible to create gateways that will allow interaction to occur.

1.2.1 Suggested Reading Order

For those wishing to become familiar with TAXII, this section suggests reading the TAXII documents in a specific order. The documents build on each other, so following the suggested reading order can make understanding TAXII easier:

1. The TAXII Overview (this document)
2. The TAXII Services Specification
3. Protocol and/or Message Binding Specifications based on requirements to support a given format or protocol
4. Query Format Specifications based on requirements to support a given query model

The Content Binding Reference can simply be consulted as needed to identify appropriate Content Binding ID values. The Content Binding Reference serves as a dictionary of Content Binding IDs and is generally not read beginning-to-end.

1.3 Specification Versioning

Changes to TAXII Specifications that impact content or tools are indicated by either a Major release or a Minor release.

Major release - A major release incorporates changes that require breaking backward compatibility with previous versions or represent fundamental changes to concepts. For a major release, the MAJOR version is incremented by one and the MINOR version is set to zero.

Minor release - A minor release incorporates changes that do not break backward compatibility with previous versions. For a minor release, the MINOR component is incremented by one.

1.4 Terms and Definitions

This section defines terms that are assigned a specific meaning within all TAXII specifications.

1.4.1 TAXII Roles

TAXII Roles are used to denote participants in TAXII according to their high-level objectives in the use of TAXII Services.

Producer - An entity (e.g., a person, organization, agency, etc.) that is the source of structured cyber threat information.

Consumer - An entity that is the recipient of structured cyber threat information.

Note that these roles are not mutually exclusive - one entity might be both a Consumer and a Producer of structured cyber threat information.

1.4.2 TAXII Functional Units

TAXII functional units represent discrete sets of functionality required to support TAXII. Note that this does not mean that separate software is needed for each functional unit - a single software application could encompass multiple functional units or multiple applications could cooperate to serve as a single functional unit. A functional unit simply represents some component with a well-defined role in TAXII.

TAXII Transfer Agent (TTA) - A network-connected functional unit that sends and/or receives TAXII Messages. A TTA interacts with other TTAs over the network and handles the details of the protocol requirements from one or more TAXII Protocol Binding Specifications. A TTA provides TAXII Messages to

a TAXII Message Handler (defined below) allowing the TAXII Message Handler to be agnostic to the utilized network protocol. By the same token, the TTA can be agnostic as to the content of TAXII Messages, leaving the handling of this information to the TAXII Message Handler.

TAXII Message Handler (TMH) - A functional unit that produces and consumes TAXII Messages. The TMH is responsible for parsing inbound TAXII Messages and constructing outbound TAXII Messages in conformance with one or more TAXII Message Binding Specifications. A TMH interacts with the TTA, which handles the details required to transmit those messages over the network. The TAXII Back-end interacts with the TMH to turn the information from the Back-end into TAXII Messages and to perform activities based on the TAXII Messages that the TMH receives.

TAXII Back-end - A term covering all functional units in a TAXII architecture other than the TTA and the TMH. This could cover data storage, subscription management, access control decisions, filtering of content prior to dissemination, and other activities. The TAXII specifications provide no requirements on how capabilities are implemented in a TAXII Back-end beyond noting that TAXII Back-ends need to be able to interact with a TMH. Individual implementers and organizations can decide which TAXII Back-end capabilities are necessary given the TAXII Services they wish to support and how they wish to provide this support.

TAXII Architecture - The term TAXII Architecture covers all functional units of a single Producer or Consumer's infrastructure that provide and/or utilize TAXII Services. A TAXII Architecture includes a TTA, a TMH, and a TAXII Back-end. As noted above, implementation details of a TAXII Back-end are outside of the scope of the TAXII specifications.

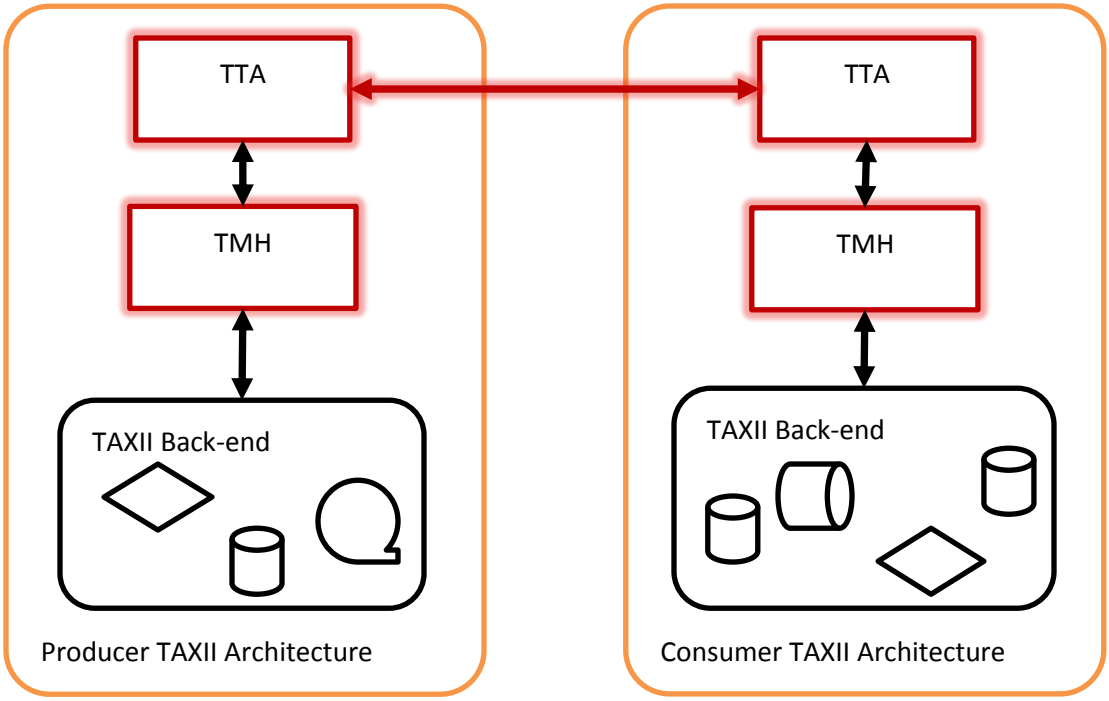

Figure 5 - The Interaction of TAXII Functional Units

Figure 5 shows a notional interaction between a TAXII Producer and a TAXII Consumer. The two TTAs communicate with each other over the network using protocols defined in a Protocol Binding Specification. The recipient's TTA then extracts the TAXII Message from the network and passes it to the TMH. The TMH parses the TAXII Message and interacts with the TAXII Back-end to determine the appropriate response. The TMH then takes this response, packages it as a TAXII Message, and passes it on to the TTA for transmission. The TAXII specifications provide normative requirements for the components that appear in red. Specifically, they provide requirements with regard to how TAXII Messages are exchanged between TAXII Architectures and also provide requirements which dictate the behavior of TTAs and TMHs. Note that the TAXII specifications do not require or anticipate uniformity in the implementation of TAXII Back-ends.

2 TAXII Capabilities

TAXII exists to provide specific capabilities for sharing structured cyber threat information. TAXII Capabilities are the highest level at which TAXII actions can be described. There are three Capabilities that the current version of TAXII supports: push messaging, pull messaging, and discovery.

2.1 Push Messaging

Structured cyber threat information can be pushed from a Producer to a Consumer. This can reflect a pre-existing relationship between the Producer and Consumer, where the Consumer has requested to receive periodic content pushes from the Producer. On the other end of the spectrum, push messaging can be used in a case where a Consumer is willing to accept contributions from any party and any Producer can volunteer content at any time without any pre-existing relationship. An example of the former is a Consumer who subscribed to a Producer's data feed, while an example of the latter is a Consumer that is acting as a repository of published information and allows anyone to volunteer data.

2.2 Pull Messaging

A Consumer can request to pull structured cyber threat information from a Producer. This not only allows the Consumer to control when it receives cyber threat data, but allows the Consumer to receive data without having to listen for incoming connections. As with push messaging, the Producer and Consumer can have an existing agreement for the Consumer to have access to the Producer's content. Alternately, a Producer can make its information available publicly and any Consumer can contact it requesting the data.

2.3 Discovery

TAXII implementers have a great deal of flexibility in choosing which TAXII Capabilities they support. As noted earlier, TAXII is bound to neither a particular network protocol nor to a particular message binding. In order to facilitate automated communication, TAXII includes the ability to discover the specific TAXII Services a TAXII user (or group of TAXII users) fields, as well as their network address and supported bindings. This does not remove the need for human involvement in the establishment of sharing agreements - sharing agreement negotiation is outside the scope of TAXII. Discovery does,

however, allow for the automated exchange of information about which TAXII Capabilities a Producer might support and the technical mechanisms they employ in doing so.

2.4 Query

TAXII Consumers may wish to receive only content that match certain criteria (e.g., pertain to a particular event or mention some specific text). TAXII Query allows Consumers to define criteria that content must match in order to be sent from Producer to Consumer. TAXII Query capabilities are discoverable and can be used with both Push and Pull Messaging.

3 TAXII Conformance

In order to claim conformance with TAXII, products and software need to:

1. Be conformant with at least one version of the Services Specification.
2. Be conformant with at least one version of a Message Binding that is compatible with the Services Specification in #1.
3. Be conformant with at least one version of a Protocol Binding that is compatible with the Services Specification in #1.

In all cases either the Version ID associated with a TAXII Binding Specification or the title of the specification can be used to identify particular TAXII bindings when identifying an entity's TAXII conformance.

4 Development

TAXII and its component specifications are expected to continue to evolve based on user needs. Feedback, suggestions, and comments with regard to this or any of the other TAXII specifications are welcome. The TAXII web site (http://taxii.mitre.org/) contains the latest news and resources with regard to TAXII, including the latest versions of all TAXII specifications. There is a mailing list for the discussion of the specifications and where users can pose questions. Interested parties can sign up for this mailing list via the TAXII web site (http://taxii.mitre.org/community/registration.html). Finally, there is a repository on GitHub.com (https://github.com/TAXIIProject/). This repository will host code development efforts as well as modified versions of the TAXII specifications with changes that might be included in future releases of TAXII.

Users of TAXII are encouraged to make use of these resources, both to empower their own use of TAXII and to provide feedback that will help TAXII evolve to meet the needs of its users.