THE MITRE CORPORATION

The Trusted Automated eXchange of Indicator Information (TAXII™)

Julie Connolly, Mark Davidson, Charles Schmidt

5/2/2014

Trademark Information

Feedback

Community input is necessary for the success of TAXII. Feedback on TAXII 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 the MITRE TAXII team by sending a message to taxii@mitre.org

Overview

This document describes the Trusted Automated eXchange of Indicator Information (TAXII™) effort, a Department of Homeland Security (DHS) led, community-driven effort to develop standard services and message exchanges to facilitate cyber threat information sharing across organization and product/service boundaries. Cyber threat information sharing, or *threat sharing*, is the exchange of actionable cyber threat data—from adversary-used IP addresses, x-mailers, and malware to discovered vulnerabilities and defensive courses of action—between trusted partners that can be used to inform and instrument network defenses. This document reviews the motivation and goals of TAXII, TAXII's scope, TAXII specifications and documentation, TAXII's benefits, and current TAXII status and next steps.

Background

Cyber threat information sharing is critical in the fight against today's sophisticated cyber adversaries. As noted in the Security for Business Innovation Council report [1] "Sharing cyber-risk intelligence and defensive strategies has become imperative in today's threat landscape. No organization can realistically sit in isolation and still be able to defend itself." The President and Congress have also underscored the importance of threat sharing as evidenced in the Cybersecurity Executive Order (EO) [2], the Presidential Policy Directive 21 (PDD-21) [3], and the Cyber Intelligence Sharing and Protection Act (CISPA) [4]. For cyber defenders, threat sharing paints a richer picture of adversary activity and helps them prioritize their organization's cyber defenses. One organization's detection becomes another organization's prevention. In addition, threat sharing provides a way to make collective advances against otherwise "anonymous" adversaries attacking one's enterprise; their attacks become less successful because their attack patterns are known, detectable, and obstructed by sharing partners.

Today's cyber threat information sharing state of the practice, however, is either a time-consuming, manual process or a set of separate, community-specific automation solutions. The capability to share cyber threat information broadly with multiple sharing partners and communities in an automated manner has been made possible by TAXII. The community-driven TAXII effort defines technical mechanisms for cyber threat information sharing that are applicable to a wide range of sharing needs yet flexible enough to support existing cyber threat information sharing models. Specifically, TAXII defines services and message exchanges that can be part of an automated sharing infrastructure, as well as makes possible a single set of services and clients that can be used to interact with multiple parties, allowing a single investment in infrastructure and procedures to apply to multiple sharing communities.

Motivation and Goals

Seeking a solution to current threat sharing challenges not addressed by existing standards or sharing technologies, DHS funded MITRE to develop a cyber threat information sharing capability to meet the following goals:

- Enable timely and secure sharing of threat information within and between and within cyber defender communities

- Enable robust, secure, high-volume exchanges of expressive sets of cyber threat information.
- Support a broad range of use cases and practices common to cyber threat information sharing communities.
- Support the use of existing mechanisms wherever possible in order to minimize the changes needed for adoption.
- Long term, seek eventual adoption by one or more international standards organizations.

The end result is TAXII. The following sections describe TAXII in more detail.

An Exchange Framework

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 defines services, 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 all while using a single, common, set of tools.

Scope

TAXII is intended for use by any cyber threat information producers, cyber threat information consumers, and developers of cyber threat management capabilities, including government, industry, and academia. TAXII supports all widely used threat sharing models, including hub-and-spoke, peer-to-peer, and source-subscriber.

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.

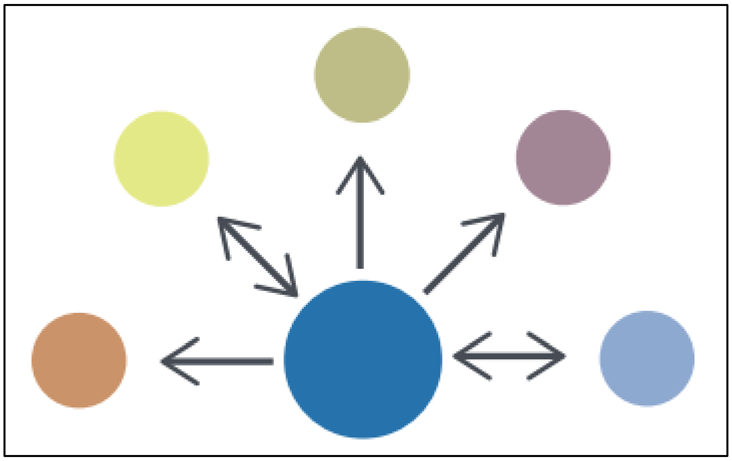


Figure 1 - Hub and Spoke Diagram

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.

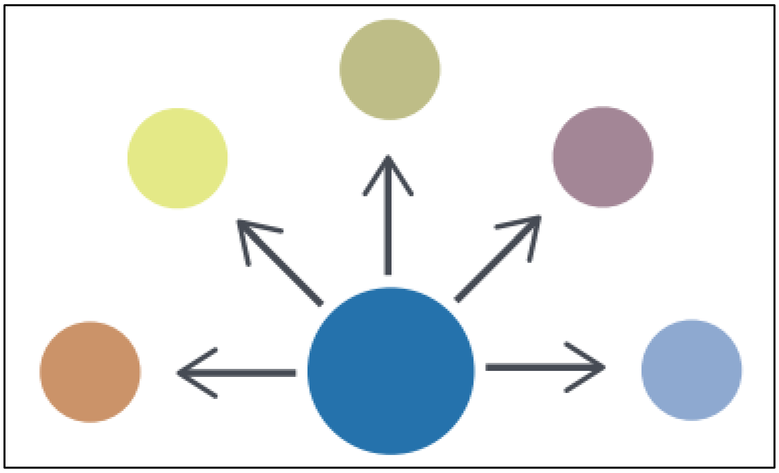


Figure 2 - Source/Subscriber Diagram

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.

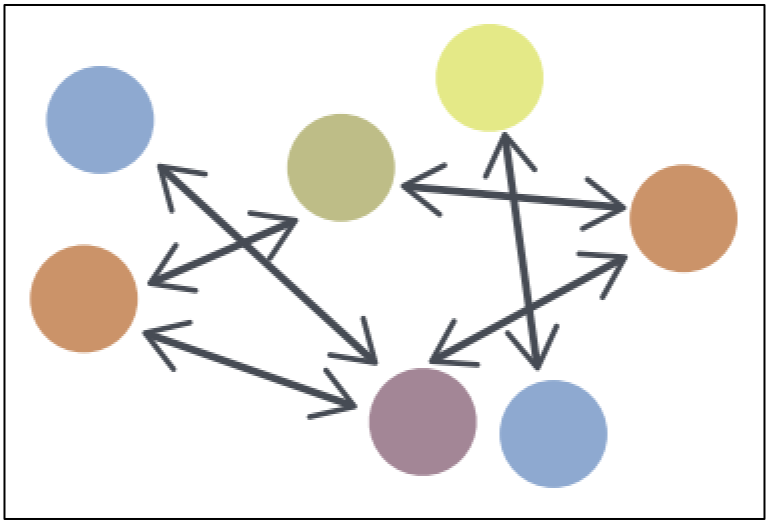


Figure 3 - Peer to Peer Diagram

TAXII Specifications and Documentation

TAXII is a set of modularly-designed technical specifications and supporting documentation. To support multiple threat sharing communities with different network protocol and message format constraints, TAXII is not tied to a specific protocol or format. Instead, TAXII's core components, services and message exchanges, are defined separately from the implementation details of those components. When there is a need for a new protocol or message 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 cannot communicate directly with each other, but because they are still using TAXII's services and message exchanges at the core of their communications it is possible to create gateways that allow interaction to occur.

The specifications and documents that comprise TAXII are described below.

TAXII Overview - The TAXII Overview 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 requirements that govern TAXII Services and Message Exchanges.

Message Binding Specifications - A Message Binding Specification defines 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.

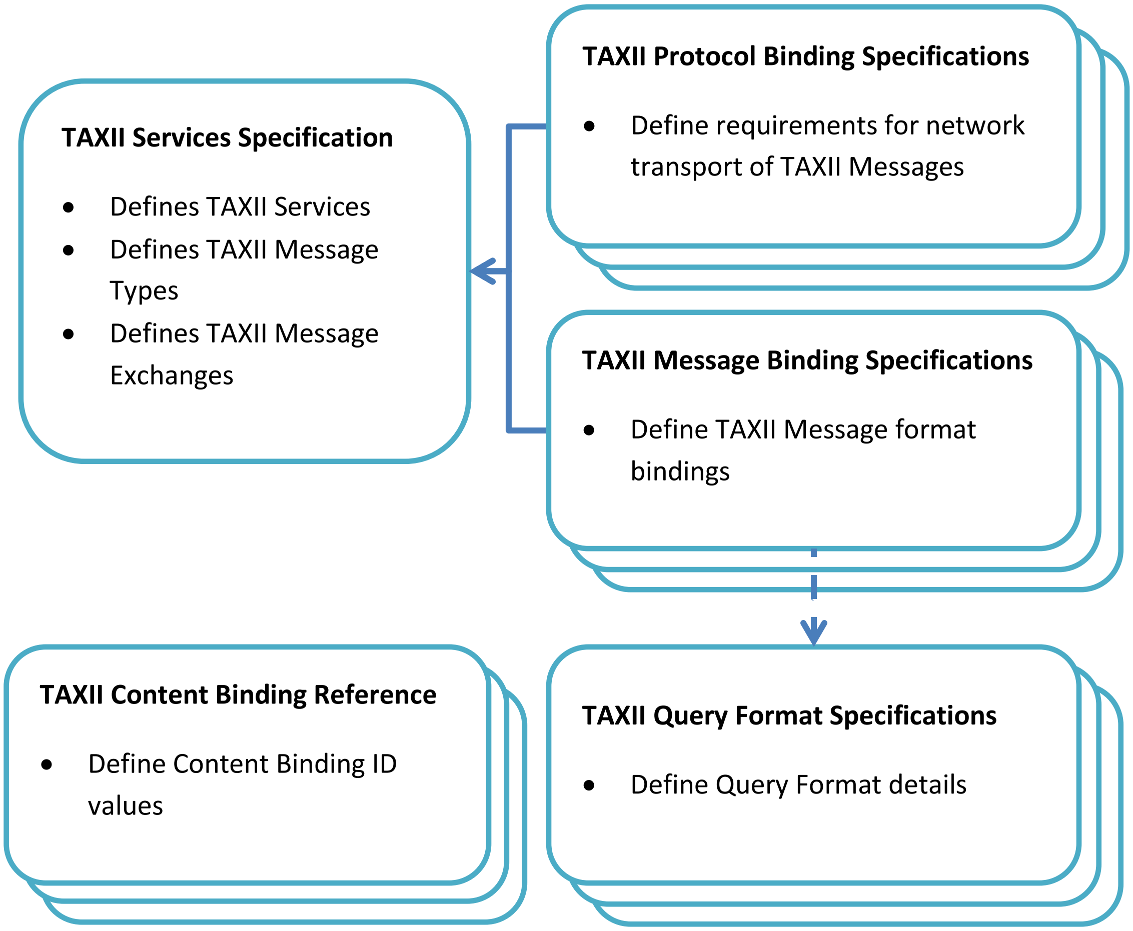
Protocol Binding Specifications - A Protocol Binding Specification defines requirements for transporting TAXII Messages over some network protocol (e.g., HTTP). There may be multiple Protocol Binding

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 reference document that lists canonical Content Binding IDs for use within TAXII. TAXII can convey a wide range of cyber threat information types and formats and Binding IDs (either canonical or defined within a sharing community) help parties identify the information they are requesting or receiving.

Figure **4** shows the relationship between the TAXII specifications.



TAXII Services Specification

- Defines TAXII Services
- Defines TAXII Message Types
- Defines TAXII Message Exchanges

TAXII Protocol Binding Specifications

- Define requirements for network transport of TAXII Messages

TAXII Message Binding Specifications

- Define TAXII Message format bindings

TAXII Content Binding Reference

- Define Content Binding ID values

TAXII Query Format Specifications

- Define Query Format details

Figure 4 - TAXII Specification Hierarchy

Current versions of these specifications and documents can be found on the TAXII website, http://taxii.mitre.org

Benefits

TAXII enables more organizations to securely share threat information faster. Specifically, full realization of TAXII means:

- **Speed**. Cyber threat information sharing is faster. Defined services and message exchanges enable automation for what is now a largely manual undertaking. Defenders can receive threat data in real time.
- **Security and Privacy**. Since TAXII defines standard mechanisms for protecting the confidentiality, integrity, accurate delivery, and attribution of cyber threat information, these capabilities can be built into tools to automatically ensure the appropriate level of security and privacy protection.
- **More Participation**. TAXII reduces the technical hurdles to participating in threat sharing communities, enabling more organizations to participate.
- **Enhanced Analysis**. Standardization and automation permit organizations to redirect analyst time; effort previously directed towards manual production and receipt of threat data—such as cutting and pasting IP addresses from a PDF file and to a web portal—they can instead be focused on threat data analysis.
- **Product Interoperability**. Vendor products and services can use TAXII instead of proprietary exchange mechanisms. Users of TAXII-enabled vendor products can achieve seamless exchange and interoperability with other TAXII-enabled software, thus enabling threat sharing automation.

Ultimately, the result is improved situational awareness and better cyber defense against today's advanced adversaries. Cyber defenders that leverage TAXII have access to more threat data to help correlate and track adversary activity, and a growing number of organizations can develop cyber intelligence capabilities. TAXII's benefits can be help sharing participants regardless of the sharing model or security requirements.

Current Status

To date, the following TAXII development activities have taken place:

- **Engaged a broad government and industry community.** This community includes subject matter experts interested in cyber threat information sharing, such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) [5], government cyber threat producers, threat management product/service vendors, and more.
- **Published TAXII 1.1.** Building on TAXII's initial release, the TAXII team published TAXII 1.1 in January 2014. TAXII 1.1 includes a set of technical specifications that detail requirements for exchanging XML messages over HTTP and HTTPS.

TAXII's accomplishments to date would not have been possible without the participation of many cyber security community members. Their insights, feedback, and support have been invaluable.

Next Steps

With the release of version 1.1, TAXII is now in the hands of cyber defender community. In addition to fielding community feedback, the TAXII team will continue to actively support TAXII through a range of support activities:

- **TAXII application and use.** The TAXII team is actively identifying and participating in a number of pilot engagements in order to demonstrate TAXII within different operational environments.
- **Utility development.** In coordination with community needs, the TAXII team is developing software utilities (libraries, etc.) to aid in the implementation and fielding of TAXII services and clients.
- **Specification and schema maintenance and updates**. TAXII is an evolving effort that will be updated and maintained in coordination with the needs of the community.
- **Active community engagement**. Conference and workshop participation will continue, along with outreach to individuals and organizations, in order to raise TAXII awareness and use.

Summary

TAXII is a community-driven effort to address cyber threat information sharing needs, including automation, security, consistency, and interoperability. TAXII enables increased sharing of cyber threat information and can integrate with existing practices and technologies utilized by a wide range of existing communities and prospective sharing participants.

DHS, MITRE and the rest of the TAXII community welcome your participation in TAXII. If you would like to contribute to the further evolution of TAXII, implement TAXII, find products that implement TAXII, or just maintain awareness about TAXII, please join the community.

Website: http://taxii.mitre.org
Email: send 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 contact the MITRE TAXII team by sending a message to taxii@mitre.org

References

[1] "Getting Ahead of Advanced Threats: *Achieving Intelligence-Driven Information Security,* Recommendations from Global 1000 Executives," Security for Business Innovation Council, January 2012.

[2] Executive Order, "Improving Critical Infrastructure Cybersecurity," issued February 12, 2013 by President Barack Obama.

[3] Presidential Policy Directive 21: Critical Infrastructure Security and Resilience, issued February 12, 2013.

[4] Cyber Intelligence Sharing and Protection Act (CISPA), 113th Congress 1st session House Resolution 624, April 22, 2013; URL http://www.gpo.gov/fdsys/pkg/BILLS-113hr624rfs/pdf/BILLS-113hr624rfs.pdf

[5] The Financial Services Industry Sharing and Analysis Center (FS-ISAC). URL http://www.fsisac.com/