Ecosystem of Independent, Cooperative Cyber Trust Communities
in Support of
Automated Cyber Threat Information Sharing
and
Integrated Adaptive Cyber Defense

Brokering Functional Description

Background

We (the good guys) are working as fast as we can on as much as we can but cyber-attacks work at cyber scale and speed while we humans do not have do-loops or multi-processors. The cyber bad guys are leveraging each other's tools/knowledge to get better at what they do, faster than we are getting better at what we do. Two tools[1] will help us change this calculus:

- Automation that works at the speed and scale that our adversaries are working – but uses business rules that are customized for each of our unique needs.
- Information sharing to leverage each other's efforts
  - to improve confidence in our own results
  - to gain time to prevent rather than respond to threats
  - to de-duplicate expensive, time-consuming analytic efforts (discovery and course of action development)

Cybersecurity Trust Community

To share information and optionally work together, organizations/entities gather together to form a Community around some set of shared goals and, more specifically, around some formal or informal Trust Model that defines (implicitly or explicitly) purpose/goals, membership, terms (including further sharing outside the Community), and governance. A Trust Community can revolve around human-to-human sharing but, because of the nature (speed/scale) of cybersecurity information, is more likely to be supported by Community Shared Infrastructure that permits/enables information sharing and other synchronization via machine-to-machine processing[2], either in lieu of or in addition to slower, human-to-human sharing. A member has the option of actively participating, passively monitoring, using information as confirmatory of the member's own analysis, using information about others' discoveries to raise/lower internal alarm thresholds or even taking automated defensive actions. If a member determines that a Trust Community is not meeting expectations a member can leave the Trust Community and join another.

Definitions

Community Trust Model: A Community agreed-upon (either formal or informal) shared purpose, terms, operating mores, membership requirements, and governance. The trust model includes a description of what rules must be honored if information from the Trust Community is permitted to exit the Trust Community's boundaries.

Trust Community: A group of entities that agree to work together under the auspices of a common Trust Model. Communities and membership may be transitory or permanent. Entities can join more than one Community and their interactions with each community are per the Trust Model for each.

[1] Other important tools (e.g. enduring, behavior-based discovery analytics and non-technical tools like deterrence, diplomacy, and norms) are important but are handled/discussed in other venues.

[2] The emergency of machine-to-machine processing capabilities are enabled by standards such as STIX and TAXII which define a language and transport mechanism. The language and transport end up being the "easy" part of the challenge. Ensuring that the knowledge model or semantics are also shared within a Trust Community is likely to be an emerging area of research and development.

Each Trust Community, via member-determined rules, independently self-forms, governs, evolves, and potentially dissolves over time. Each Trust Community serves different needs. One Trust Community may be organized to by the business of the members (examples: FS-ISAC, USG ESSA). Other Trust Communities may be organized by geographic area, by the level of sophistication of the member's cyber analytic skills or by the agreed-upon confidence level of the shared information. Some Trust Communities may be organized on a for-profit basis where members pay a central authority to provide one-way services (Anti-Virus subscription services). While the members of the Trust Community must observe the rules of that Community, certain Trust Communities can be organized with few, if any, rules and a low bar for entry, not even requiring on-line identity authentication. Other Trust Communities have stringent membership vetting and penalties for non-abidance.

Definition: Shared Infrastructure

Hosted, shared Infrastructure available within a Community for members to exchange information with each other according to the Trust Model for that particular Community. The Infrastructure may include services for member enrollment and authentication, information enrichment and consolidation, anonymization, logging (if required). The Infrastructure hosts message hubs such as a TAXII server and on-line collaboration tools. The host of the shared infrastructure may have some unique role with the Community or the host may simply be a Member who has volunteered to provide the capabilities.

Ecosystem of Independent, Cooperative Cyber Trust Communities

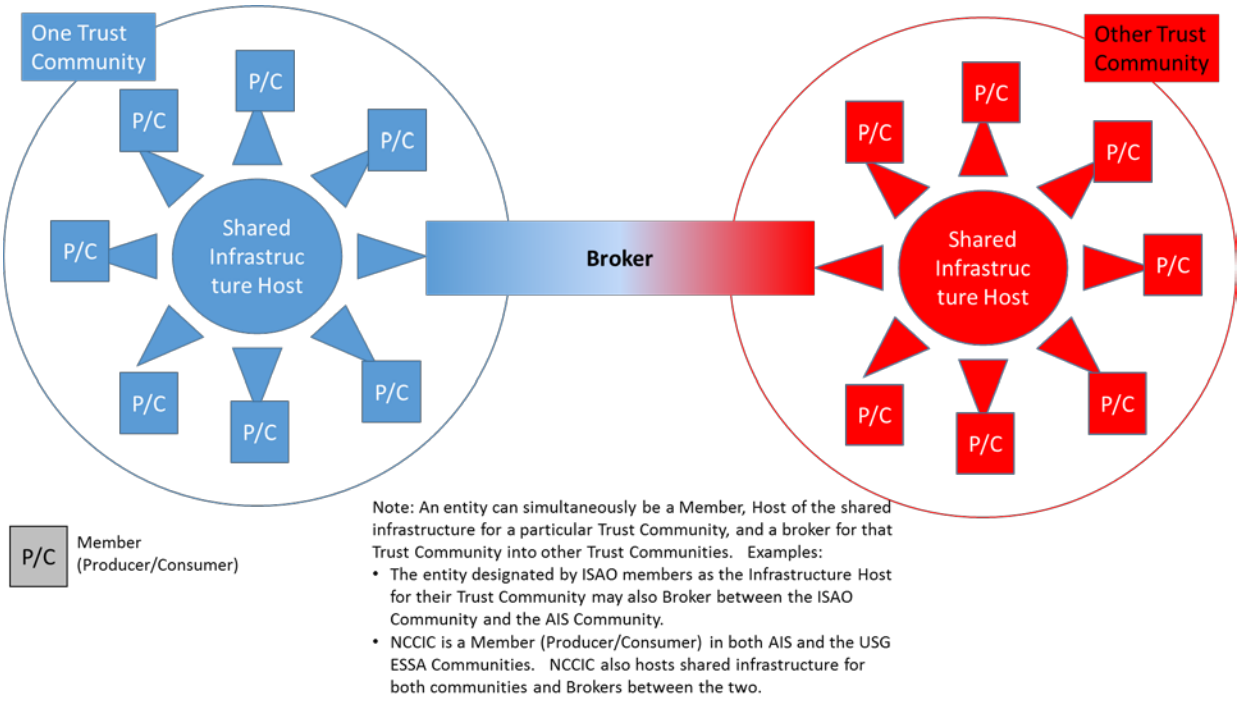
It stands to reason that the more sharing and synchronization that occurs, the better off we are. There are three ways to scale Trust Communities and all are important. The last is the focus of this document.

- If working together for a common goal provides benefits to all Trust Community members, it stands to reason that the more members a Trust Community has, the more beneficial it would be to all. Certainly some Trust Communities can choose to scale in this manner.
- An organization can join more than one Trust Community, expanding the amount of information to which they have access. When a member joins multiple Trust Communities, they follow the different rules for each individual Trust Community engagement. Due to this complexity of individual engagement with each Community, only those organizations with a certain level of technical maturity or resources will choose to belong to more than one Trust Community.
- Community-to-Community interactions or sharing provides a means for individual Communities to work together while maintaining their independence. This is not a 100% pass-through (or there would be no need for separate Communities.)

The key component to building an Ecosystem from of a collection of independent Trust Communities is the brokering between individual Trust Communities. Brokering allows interactions between Trust Communities while still observing the different rules of each individual Trust Community. While this brokering between Trust Communities is varied/customized, it is possible to define a set of brokering functions that maintain independence within each Trust Community while simultaneously promoting cooperation and information sharing.

The Trust Model for each Trust Community explicitly defines whether the brokering functions can be performed by a member of the Trust Community or by a brokering organization selected by the community (or both). There is a certain economy to be achieved if the Broker is also the host of the machine-to-machine shared capabilities (e.g. TAXII server, membership manager) for that Community. A Broker may also have some kind of "oversight" role within the Trust Community but this is not required.

Definition: Broker
The entity who works between two or more Independent Cyber Trust Communities to filter, translate, and transfer information in accordance with the individual Trust Models for each collaborating Trust Community.



While each Trust Community is autonomous in terms of how members work together and share information/tools within the Community, brokering will be individually and collectively faster and more cost-effective if Communities:

- Leverage best practices, standards and commercial tools for integration/sharing – both within a Trust Community and intra-Trust Communities (via Brokering)
- Tag the exchanged information and response actions with access control or usage restrictions to allow automated processing by members and the Brokers
- Use technology to enforce constraints associated with the Trust Model within a Community including constraints associated with privacy; civil liberties; liability, legal, and intellectual property protection; and policy.

There is unlikely to be a single über-Broker for all Trust Communities in existence --- and there is no need for a single broker. But we can define what brokers do for the Communities they serve.

Ecosystem Brokering Functions

There are a number of core brokering functions:

- **Vetting.** A Trust Community is likely to require some form of vetting of external Trust Communities prior to initiating brokering with that Community. The formality/degree of external Community vetting is likely one of the key components of any given Community's Trust Model. Vetting may also include conditional approvals, pending the quality or quid-pro-quo of information from external Trust Communities. The vetting and vetting processes are transparent and documented within a Trust Community (including the broker) and may not be shared outside the Trust Community.
- **Filtering:** The broker determines which information can pass outside the trust community. In general, to support the speed and scale of cyber, the filtering determination is automated so that information can exit a Trust Community as fast as possible (to be useful in preventing attacks). The filtering may be a simple "yes/no" to sharing, more complex "Yes, but source must be anonymized", or very complex "Yes to Trust Communities with these characteristics, No to others." This determination may be based on pre-arranged rules for the producing Trust Community, tags associated with each piece of information by the originating member, different sharing areas with different filtering rules, etc. The broker may also filter based on receiving the Trust Community's rules. Examples: "Let external information filter into our Trust Community if the information is high confidence as defined by …"
- **Translating:** Key to the Ecosystem concept is the concept of autonomy for each Trust Community. While it would be easier if everyone used the same language and semantic knowledge model, the former is possible while the latter is improbable. Thus, brokering involves translating (language and semantics) between Trust Communities. By definition, the broker understands the needs of each Community it brokers between so the translation can be targeted/specific rather than a ubiquitous, Rosetta stone of translations which is practically impossible to create, gain agreement on, and maintain.
- **Transferring.** The Broker provides a secure, reliable means to transfer the information from one Trust Community to the other, where the transfer is consistent/compatible with the IT safeguards of each. Note that this transfer may be one way or two way.
- **Controlling Access:** Once information exits a trust community, the information may carry restrictions defined by the originating Trust Community. Brokering includes the interpretation of undocumented or ambiguous intra-Trust-Community access restrictions into an unambiguous terms that can be honored outside the originating Trust Community. The Trust Model/Agreement for a Trust Community will likely over time want to remove the ambiguity related to access control/restrictions within their Community. A common way to add these terms is to tag the shared information either from the start or at a minimum before it exits the originating Trust Community.
- **Stewarding:**
  - In the event that the originator of the information desires anonymity prior to further sharing outside the Trust Community or if the Trust Community itself always anonymizes source prior to sharing outside the Community, the broker assumes the role of originator/owner for information. There are also cases where a broker could be brokering for multiple Trust Communities and the Trust Communities themselves wish anonymity from each other with only the Broker knowing the source Trust Community for each piece of information.

- The broker has a gatekeeper role in the life cycle of previously shared information. When the information expires or the information is found to be erroneous, the steward ensures that notification is sent to external Trust Communities that received the information. Once notice is received, each Trust Community handles Member notification per internal-to-Trust Community procedures.
- The Broker logs information shared between Trust Communities per rules defined in the Trust Models of each Trust Community.
- The broker provides a single point of external feedback on previously shared information. The processing of the feedback is unique and defined for each Trust Community.

- **Consolidating/Enriching.** By virtue of access to more than one Trust Community, a two-way Broker has more information than any individual member in either Trust Community. That richer data set allows the broker to potentially enrich information for Trust Communities within which it operates (while still ensure access restrictions and filtering is observed per Trust Community rules.) Enrichment also can include assigning of confidence assessments of particular shared information and the assuring of quality, all based on knowledge that may not be readily available to individual Trust Communities or their members.
- **Controlling Traffic:** Because information can exit a trust community, there is also potential for the information to enter another trust community, and be automatically looped back to the originating trust community. This loop-back would eventually result in a DDOS unless the broker detects and prevents loop-backs.

Appendix A – Use Cases - to be supplied