Toward Relationship Based Access Control for Secure Sharing of Structured Cyber Threat Intelligence

Md. Farhan Haque(✉) and Ram Krishnan

Electrical and Computer Engineering,
University of Texas at San Antonio, San Antonio, USA
{md.farhan.haque,ram.krishnan}@utsa.edu

Abstract. Cyber Threat Intelligence (CTI) represents cyber threat information which are critical to an organization. Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Intelligence Information (TAXII) provide a standard to represent and share CTI in an efficient, structured and machine readable manner. In this paper, we provide a CTI sharing scenario in an organizational context and develop a Relationship Based Access Control (ReBAC) implementation to securely share CTI structured in STIX. We further discuss an organization's scope for future analyses and actions on shared CTI.

Keywords: Cyber Threat Intelligence (CTI) · Structured Threat Information Expression (STIX) · Trusted Automated Exchange of Intelligence Information (TAXII) · Relationship Based Access Control (ReBAC)

1 Introduction and Motivation

Cyber Threat Intelligence (CTI) is a type of cyber threat information which goes through certain cyber security standards through the scrutiny of cyber security experts and are collected from reliable sources. CTI provide essential cyber threat information which can be critical to maintain safety and protect integrity of an organization in cyber space. These CTI can also provide valuable insights about cyber attacks and a significant amount of research material to counter against future cyber attacks. In today's data driven world, there is a high demand for CTI sharing in a large quantity. An efficient CTI sharing can boost Cyber Threat Intelligence of an individual organization. Haass, Ahn and Grimmelmann [17] presented the importance of CTI sharing to develop a fast and efficient threat response system.

CTI generally contain detailed information related to a cyber attack. For example - a simple Phishing [20] email attack can have several key features such as attacker information, attack techniques used, target of attack, tools and software used to launch the attack. A well agreed standard is required in order to

S. K. Sahay et al. (Eds.): SKM 2019, CCIS 1186, pp. 21–37, 2020.
https://doi.org/10.1007/978-981-15-3817-9_2

clearly express and share several key features of an attack process in an efficient and machine readable manner.

Structured Threat Information Expression (STIX™) [4] is a language and serialization format used to exchange CTI maintained by OASIS [2]. STIX enables organizations to share CTI in machine readable manner, allowing other organizations and security communities to better understand an attack and take preventive measures.

Organizations can benefit from sharing these CTI in a controlled manner. For example - Three organizations A, B and C where A trusts B more than C. The level of sharing between A and B might be significantly different than that of between A and C due to Information leakage [8], Privacy [22] concerns etc. Haass et al. [17] raised concerns over irresponsible sharing of classified CTI from government organizations into private sectors.

Organizations require some Access control [27] over CTI sharing based on the different sharing requirements. There are various forms of access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC) and Relationship Based Access Control (ReBAC) etc. It is not well understood the effectiveness of all these access control models for CTI sharing. In our work, we investigate the applicability of ReBAC for CTI sharing. ReBAC seems a natural fit as organizations are able to facilitate different levels of sharing based on the sharing relationships established among them.

Gates [16] coined the term Relationship Based Access Control (ReBAC) which is a access control model based on the relationship between accessor and owner/controller of a resource. We adopt a variant of Cheng, Park and Sandhu's [9] regular expression based User-to-User Relationship-Based Access Control (UURAC) model to control CTI sharing. The advantages of this model are discussed in Sect. 5. We focus on sharing CTI in a structured manner and adopt STIX [4] standards in our implementation. We also provide further insights on the analysis of CTI to improve organizational cyber defense system.

To summarize, our contributions in this paper are as follows

1. We demonstrate the applicability of ReBAC for effective sharing of CTI by presenting an example CTI sharing scenario.
2. We develop a prototype implementation of a CTI sharing ecosystem named as CTI System and instantiate the system for an example sharing scenario and demonstrate the system's operations.

2 Background

In this section, we discuss few key concepts involving our work.

2.1 Structured Threat Information Expression

Structured Threat Information Expression or STIX [4] is a standard to express CTI in a structured way. STIX standards has two key components - STIX Domain Objects (SDO) and STIX Relationship Objects (SRO).

STIX Domain Objects or SDOs are individual information blocks to express certain CTI categorically. Each block communicates a high level CTI concept and builtin properties inside each block explain the specific details about that concept. For example - Threat Actor SDO represents individuals, groups or organizations which may have malicious intent and more likely pose cyber security threats to other individuals or organizations. Threat Actor SDO has few properties such as name, goals and motivation of the threat actor. We can also specify skill level of the threat actor (beginer, intermediate, expert etc.) in the properties. SDO properties consist of a well combination of pre-established vocabularies and open ended descriptions and provide the flexibility to capture a wide range of CTI. These kind of structured representation makes easier for industries to understand and share CTI with minimum human intervention. There are twelve SDOs in STIX which involve crucial CTI related to vulnerabilities, attack pattern, course of action etc.

STIX Relationship Objects connect two SDOs and demonstrate inter SDO relationships. The Malware SDO represents CTI related to malicious codes or programs to compromise a system. We can link Threat Actor SDO and Malware SDO by using a "Uses" relationship - Threat Actor (SDO) Uses (SRO) Malware (SDO). We can use multiple SDOs, SROs together to represent complicated CTI in a very structured manner.

2.2 Trusted Automated Exchange of Intelligence Information

Trusted Automated Exchange of Intelligence Information or TAXII [11] is a suggested application protocol to exchange CTI over the network. CTI in STIX format can also be transported with other communication protocols. TAXII supports two sharing models - Collection and Channel.

1. **Collection:** Collection operates on a request-response model where CTI data can be hosted on a TAXII server and consumer can get CTI data by request. We adopt this model of CTI sharing in our work and applied Access control [27] to prevent any leakage of unauthorized sensitive CTI data.
2. **Channel:** Channel sharing operates on publish-subscribe model. CTI producers publish the CTI data on TAXII server and consumers need to be subscribed to get the CTI data.

2.3 Relationship Based Access Control

Access control is a known mechanism to control access to resources in computer based systems. There are several forms of access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) [27] etc. There is a more recent form of access control model named as Relationship Based Access Control (ReBAC) [16]. For example, please see [9,12–14]. ReBAC operates based on the relationship between two entities and access to a resource is determined based on the relationship types between those entities. ReBAC is popular in online social networks [15] scenario because of its intuitive relationship based structure. We use ReBAC in our implementation because organizations may not be related or may be loosely related and only come together to share different levels of CTI. This kind of sharing requirement can easily be facilitated with the establishment of sharing relationships among different organizations.

3 Related Work

Johnson et al. [21] defined cyber threat information is as any information that can help an organization identify, assess, monitor, and respond to cyber threats. The authors put emphasize on the importance of CTI sharing and provided few use cases for cyber threat information sharing such as nation-state attacks against a specific industry sector, distributed denial of service attack against another industry sector, financial conference phishing attack etc. Haass et al. [17] demonstrated a case study for information sharing challenges within a public/private not-for-profit partnership organization called ACTRA - Arizona Cyber Threat Response Alliance, Inc. STIX [4] is a language to represent CTI in a structured way for organizations to consume CTI in an automated and machine readable manner. STIX is maintained by OASIS [2] and well accepted standard to represent structured CTI.

Gates [16] introduced Relationship Based Access Control (ReBAC) where access to a resource depends on the relationship between owner and accessor. Over the years, several numbers of ReBAC models have been proposed in the literature. Fong [13] proposed a modal logic based relationship based access control policy in a social network context. Crampton and Sellwood [12] provided a relationship based access control policy based on path conditions which are similar to regular expression. Cheng et al. [9] provided a regular expression policy based relationship based access control model for online social networks. Cheng et al.'s model makes an authorization decision based on multiple policies which is beneficial for our organizational CTI sharing scenario in a non social network context.

There are plenty of opportunities to perform analysis on STIX structured CTI to extract meaningful information and apply them to better organizational cyber security. Iannacone et al. [19] provided an ontology to develop for cyber security knowledge graph similar to Google's knowledge graph which incorporates information from both structured and unstructured information sources. Syed, Padia, Finin, Mathews and Joshi [28] proposed Unified Cybersecurity Ontology (UCO) which integrates and incorporates data from various cyber security standards and also mapped with archived STIX 1.0 [6]. We plan to design a CTI Knowledge base compatible with STIX 2.0 to extract useful information and integrate into organizational cyber defense system.

4 Cyber Threat Intelligence Sharing Scenario

4.1 Sharing Requirements

In this section, we discuss about different sharing requirements based on geographical location (Intracity, Nationwide), intra organization system (Intrasystem), inter organization system (Nationwide) and collaboration with law enforcement agencies (Lawenforcement).

4.1.1 Sharing Requirement 1 - Intracity

Imagine there is a surge of Ransomware [23] attacks directed towards critical organizations in San Antonio, Texas such as banks, airports, hospitals etc. These attacks are circulated through Email spoofing [26] and Social engineering [29] tactics. Three health institutions Sacred Lake, Ace Health and Church Hospital in San Antonio understand these cyber threats against the city and can agree share CTI related to threat-actor (attacker information) and malware CTI.

4.1.2 Sharing Requirement 2 - Intrasystem

Institutions under Ace Health system want to boost their cyber defense system and protect privacy of valuable patient data. These organizations can agree to share system vulnerability CTI since they trust each other.

4.1.3 Sharing Requirement 3 - Lawenforcement

Cyber criminals [7] can launch plenty of cyber attacks; some of which may have serious consequences in real world and pose serious security risks towards infrastructures and employees of an organization. These cyber crimes may need to be reported to law enforcement agencies and share CTI related to attacker's identity. Organizations can agree to share threat-actor (attacker information) CTI with law enforcement agencies.

4.1.4 Sharing Requirement 4 - Nationwide

Health organizations across different cities understand the risk of attack with similar high level attack techniques such as phishing emails of online deals from a suspicious organization. These organizations can agree to share attack-pattern (attack technique) CTI.

4.2 CTI Categorization in STIX

The above section shows the need for categorization of CTI based on different sharing requirements. STIX provides an standard to structure and categorize CTI aligned with the above sharing needs. Figure 1 shows the high level view of STIX generation process of an organization named as Ace Health SA.

Threat Detection System is a representation of a system which monitors different system parameters and is able detect varieties of cyber threat components

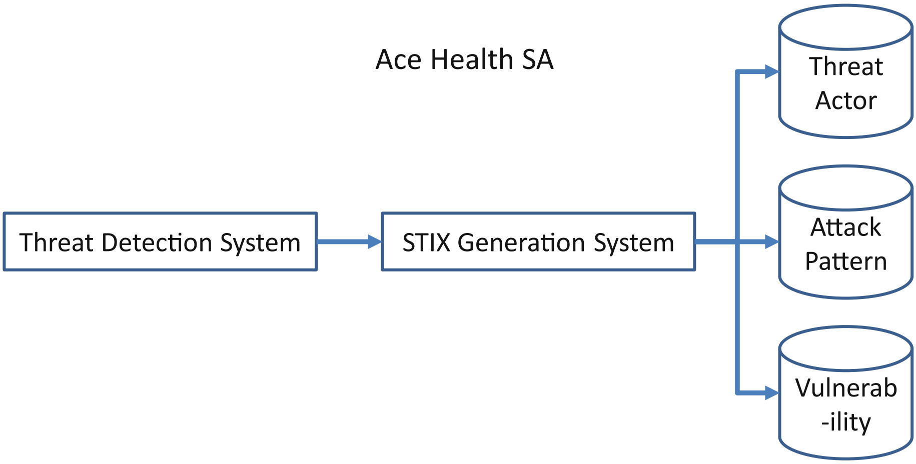

Fig. 1. Organizational STIX Generation

such as attacker identity, vulnerability, attack technique etc. The STIX Generation System receives the cyber threat components from Threat Detection System and generates STIX documents of different predefined STIX categories such as Threat Actor, Attack Pattern, Vulnerability etc.

STIX standard is open ended specification to structure CTI and provides the flexibility of STIX design at the discretion of security engineers. We take advantage of this feature of STIX and develop the STIX structures for predefined STIX categories. For example - a Threat Actor type STIX is required to have a threat-actor SDO, may or may not have malware SDO and must have a relationship between threat-actor and malware SDOs if malware SDO is present. Figure 2 demonstrates Threat Actor type STIX when malware SDO is present. We also specify the property requirements for threat-actor SDO. Figure 3 shows the required builtin properties that should be present in threat-actor SDO of Threat Actor type STIX.

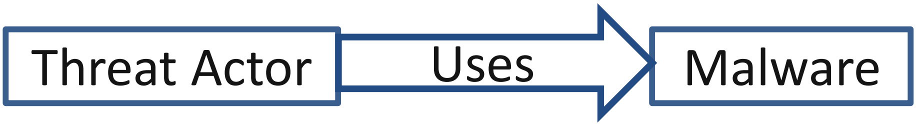

Fig. 2. Threat Actor STIX Structure

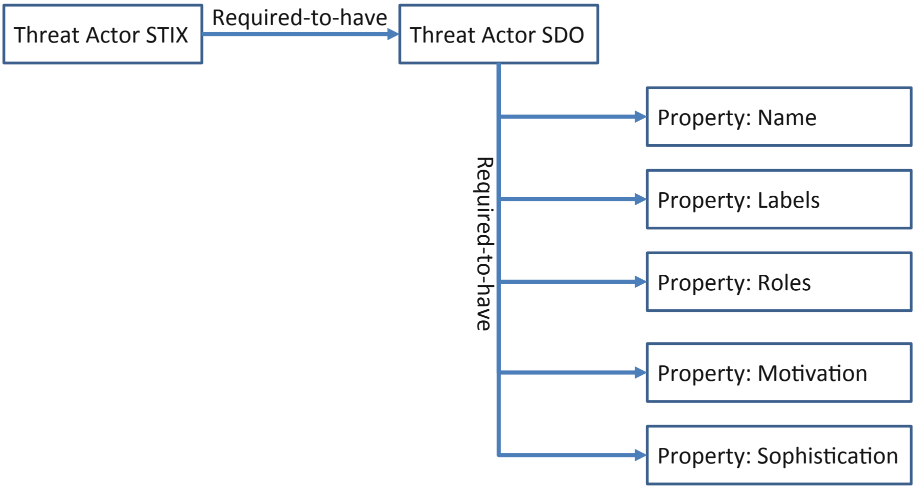

Fig. 3. Threat-Actor SDO properties Structure

5 Relationship Based Access Control Policies for Cyber Threat Intelligence Sharing

We explore the applicability major forms of access control models such as Mandatory Access Control (MAC), Discretionary Access Control (DAC) and Role Based Access Control (RBAC) model for our CTI sharing scenario.

Access Control List (ACL) [27] is one of the DAC approaches where we have to maintain a list of subject's access rights for each object. In our scenario, each individual STIX type would be objects and organizations would be subjects. Then we have to maintain access control list for each STIX type for each organization. For example - we keep a list of organizations allowed to read Threat Actor type STIX of Ace Health SA. We can also do the same for other STIX types. This kind of approach is cumbersome work for an individual organization and consumes huge amount of system and human resources.

RBAC [27] is a popular form of access control in enterprise scenario where access to a resource is granted based on the role. But RBAC may be ineffective in organizational CTI sharing scenario because organizations may only want to share CTI when there is an active sharing need between them. Fong et al. [13] demonstrated few advantages of ReBAC with respect to RBAC model.

5.1 ReBAC in CTI Sharing Scenario

We now present a relationship based organizational CTI sharing scenario in Fig. 4. Organizations have established different types of sharing relationships among themselves to facilitate various levels of CTI sharing. We consider four sharing relationships - Intracity, Intrasystem, Lawenforcement and Nationwide

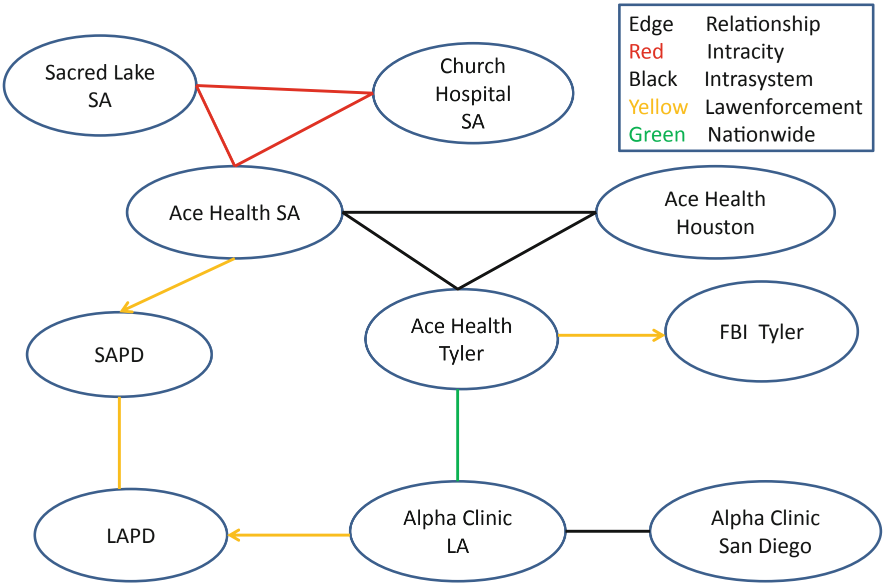

Fig. 4. Organizational CTI sharing scenario (Color figure online)

in accordance with our sharing requirements. Each type of sharing relationship is represented in a different color. For example - Intracity is represented in red, Intrasystem is in black, Lawenforcement is in yellow and Nationwide is in green. We can state ReBAC policies which align with our sharing requirements in Sect. 4.

1. **Intracity:** Intracity relationship will give access to threat-actor and malware type STIX CTI.
2. **Intrasystem:** Intrasystem relationship will give access to vulnerability type STIX CTI.
3. **Lawenforcement:** Lawenforcement relationship will give access to only threat-actor type STIX CTI.
4. **Nationwide:** Nationwide relationship will give access to attack pattern type STIX CTI.

There are many ReBAC models available in the literature and discussed in the previous sections. Cheng et al.'s ReBAC model utilizes multiple access control policies to make proper authorization decisions and provides more finer grained control over the sharing of resources. We adopt this ReBAC model into our implementation due to this feature. The model defines both user and resource as potential target for an authorization decision in online social networks [15] context. A typical example of user as target is when an user performs an action on another user such as poking in a social network like Facebook.

In our sharing scenario, users are organizational employees and we do not consider them as actionable targets. We rather focus on CTI resources owned by an organization as targets. Thus allows us to consider three policies from Cheng et al.'s access control policy taxonomy. They are system specified policy (SP) for a resource, outgoing action policy for users denoted as Accessing User Policy (AUP) and incoming action policy for a resource named as Target Resource Policy (TRP).

1. **System Specified Policy:** System specified policy (SP) determines the access or denial of a system wide Access Request [9] from a requesting/accessing user or employee of an organization to access a CTI resource owned by another organization under same CTI sharing ecosystem. An instantiation of SP for our ReBAC based CTI sharing scenario - (read, Threat Actor, (Requesting Organization, (Lawenforcement, 5))).
2. **Accessing User Policy:** Each organization's system admin sets up an Accessing User Policy (AUP) to control all the outgoing requests from the employees and prevents any unsolicited outgoing request from that organization. An instantiation of AUP for our ReBAC based CTI sharing scenario - (read, (Ace Health SA, (Intracity-Lawenforcment, 3))).
3. **Target Resource Policy:** System admin of an organization also sets up Target Resource Policy (TRP) for each resource of that organization to control the access of their own CTI resources. This policy provides organizations more control over their own CTI as organizations do not have any control over joining or leaving organizations in the CTI sharing ecosystem.

   In Fig. 4, Ace Health SA trusts SAPD with Lawenforcement relationship and wants to share Threat Actor (attacker information) CTI. CTI sharing ecosystem also denoted as CTI System which maintains System specified Policies (SP) that may allow the sharing of Threat Actor CTI with any two organizations having direct or indirect Lawenforcement relationship between them. Later when SAPD establishes another Lawenforcement relationship with LAPD, LAPD will then gain the access to Ace Health SA's Threat Actor CTI according to System specified Policy (SP) for Threat Actor type CTI. But if Ace Health SA is unwilling to share it with LAPD, they can control LAPD's access to their Threat Actor CTI through the enforcement of their own Target Resource Policy (TRP) for Threat Actor type CTI. An instantiation of TRP for our ReBAC based CTI sharing scenario - (read-inverse, Threat Actor, (Ace Health SA, (Lawenforcment-Intrasystem, 4))).

6 Implementation

In this section, we discuss about our implementation for the development of a sample CTI sharing ecosystem involving all the organizations showed in Fig. 4 with the application of ReBAC as an access control model. We divide our implementation into two parts - implementation framework and secure communication protocols. Implementation framework provides the necessary features to initialize the CTI System and update the system for later use. Secure communication protocols demonstrate the CTI System's operating procedure after system has been properly setup through implementation framework components.

6.1 Implementation Framework

Our implementation framework has three key components which are demonstrated in Fig. 5.

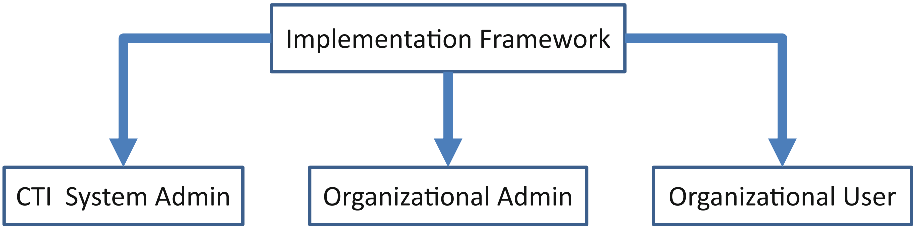

Fig. 5. Implementation framework

6.1.1 CTI System Admin

CTI System Admin is responsible for managing CTI sharing ecosystem which involves maintenance of various access control policies and sharing ecosystem graph. The admin also maintains a white list of suggested organizations allowed to join the sharing ecosystem. The admin also keeps a list of allowable relationship types that can be established among these suggested organizations.

The CTI System admin manages System specified Policies (SP) integral to the implementation of Cheng et al.'s access control model. System specified policy (SP) is a per action per resource type policy. Some typical actions for our implementation are read, write, copy etc. Resource types are defined from Report Label Vocabulary [3] of STIX literature. A few examples of resource types are attack-pattern, threat-actor (attacker information), tool, vulnerability etc. There is also a graphical user interface available to monitor the CTI sharing ecosystem represented in a Graph Data Structure where organizations are denoted as nodes and sharing relationships among the organizations are denoted as edges. The graph is implemented in popular graph database Neo4j [25].

6.1.2 Organizational Admin

Each organization may have one or more dedicated admins who perform two major operations. First operation is to maintain two organizational policies: Accessing User Policy (AUP) and Target Resource Policy (TRP). AUP is per action policy and puts control over all the employee's outgoing requests in the organization. TRP is per action per resource policy and provides control over organization's own CTI resources. Second operation is to send a sharing relationship add or delete request to another organization. We have implemented the add request feature and plan to incrementally implement deletion request in future.

6.1.3 Organizational User

Organizational employees are authorized to request CTI resource types such as attack-pattern, threat-actor (attacker information), tool, vulnerability etc. from another organization. The decision on request to access a CTI resource type is determined through the evaluation of three policies - Accessing User Policy (AUP) of requesting organization, Target Resource Policy (TRP) of requested resource type from owner organization and System specified Policy (SP) for the same resource type from CTI sharing ecosystem. The implementation is also applicable for employees requesting CTI resources from their own organization but that does not present an interesting implementation scenario.

6.2 Secure Communication Protocols

In this section, we demonstrate two protocols for secure processing of communication requests between organizations. The first protocol is sharing relationship addition request protocol which demonstrates the back and forth communication among two organizations and CTI System to securely establish a sharing relationship between organizations. The second protocol is resource request protocol which demonstrates the secure processing of a resource request from an employee of an organization to the resource owner organization.

These protocols are machine to machine or server to server communication protocols between organizations and CTI System and are built on top of known communication protocols such as Needham-Schroeder [24]. These protocols are an approach which demonstrate the handling of a request initiated from an organization in CTI sharing ecosystem. Organizational admins are authorized to initiate sharing relationship addition request protocol and organizational users are only authorized to initiate resource request protocol for an organization. CTI System processes the requests and makes decisions to allow or deny requests based on access control policies and identities of organizations. We plan to implement a sharing relationship deletion request protocol in future.

Both the protocols have two implementation prerequisites in order to establish a secure communication. First prerequisite is to implement Needham-Schroeder [24] public key protocol to mutually authenticate two participating organizations and CTI System. Second prerequisite is to share a session key between those two organizations for further communication in a secure manner after Needham-Schroeder protocol has been implemented.

6.2.1 Prerequisite 1 - Needham-Schroeder Public Key Protocol

The Needham–Schroeder protocol is an authentication protocol between two entities. The protocol has two variations - symmetric key and public key. We adopt public key protocol with the assumption that each organization and CTI System have their respective RSA public-private key pairs. We implement the modified version of the protocol free from man-in-the-middle attack. An instantiation of Needham-Schroeder public key exchange among Sacred Lake SA, CTI System and Ace Health SA is shown in Fig. 6.

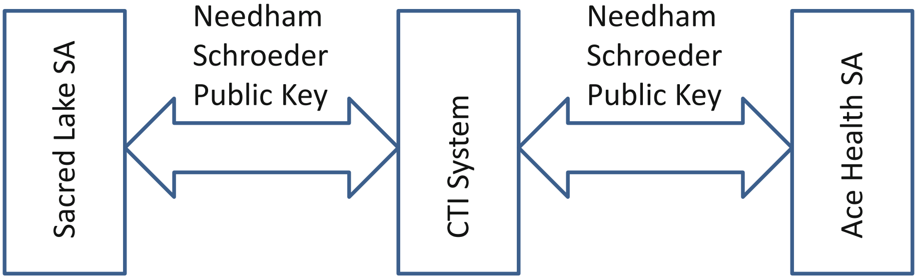

Fig. 6. Needham-Schroeder public key protocol

6.2.2 Prerequisite 2 - Session Key Share

Needham-Schroeder public key protocol in Fig. 6 provides a three way mutual authentication among Sacred Lake SA, Ace Health SA and CTI System. Since Needham-Schroeder pubic key protocol does not establish a shared session key; Sacred Lake SA and Ace Health SA need to share a session key for secure communication and data exchange after Needham schroeder authentication. Figure 7 shows secure sharing of session key between Sacred Lake SA and Ace Health SA after Needham-Schroeder public key protocol has been implemented. These two prerequisites are mandatory process before both protocol 1 and 2 are implemented.

6.2.3 Protocol 1 - Relationship Addition Request Protocol

Needham-Schroeder implementation ensures the identities of both Sacred Lake SA and Ace Health SA. CTI System is the central body which processes any request from any of the organizations and updates sharing ecosystem graph or makes access authorization decisions. To establish an Intracity sharing relationship with Ace Health SA, Sacred Lake SA sends an encrypted and Integrity [1] protected request to Ace Health SA. Ace Health SA verifies the integrity of the request and forwards the request to CTI System along with their own signed approved request. After successful verification of signed requests from

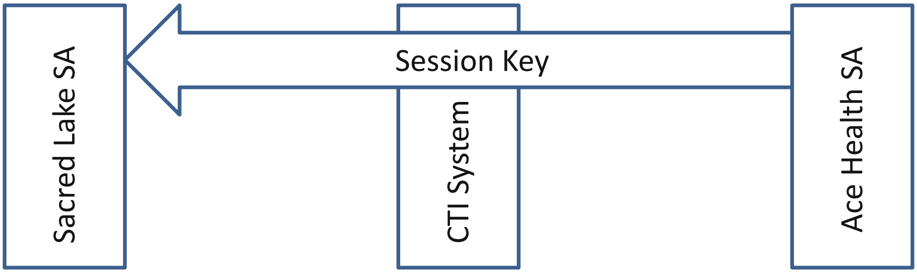

Fig. 7. Session key share

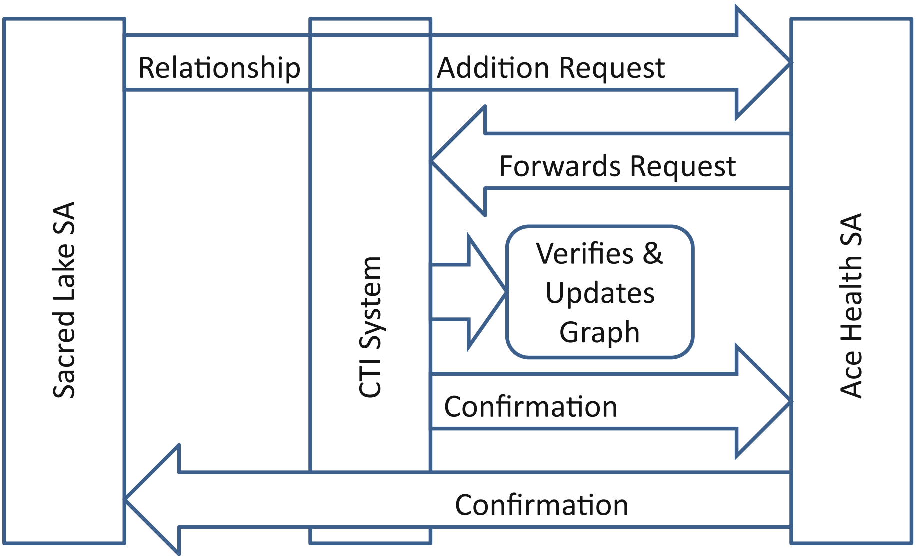

Fig. 8. Relationship request protocol

both Sacred Lake SA and Ace Health SA, CTI System establishes the requested sharing relationship between them and updates the sharing ecosystem graph. The brief communication protocol is shown in Fig. 8.

6.2.4 Protocol 2 - Resource Request Protocol

The protocol operates almost similar way as protocol 1. Sacred Lake SA wants to read Threat Actor [5] type CTI which typically contains attacker information owned by Ace Health SA and sends an encrypted and integrity (signed) protected request to Ace Health SA after both prerequisite 1 and 2 have been completed. Ace Health SA verifies the request and forwards the request to CTI System along with their own approved signed request. After successful verification of signed requests from both Sacred Lake SA and Ace Health SA, CTI System makes an authorization decision by verifying the Accessing User Policy (AUP) of Sacred Lake SA, Target Resource Policy (TRP) for Threat Actor type CTI of Ace Health SA and System specified Policy (SP) for Threat Actor type CTI of CTI System with respect to sharing ecosystem graph. CTI System then sends the authorization decision to Ace Health SA. Based on the authorization decision; Ace Health SA may or may not pull Threat Actor type CTI from their TAXII [11] server and send towards Sacred Lake SA. The brief resource request protocol is shown in Fig. 9.

Figures 6, 7, 8 and 9 show the generalized and brief overview of exchanges among Sacred Lake SA, Ace Health SA and CTI System. A more detailed description of these exchanges and the complete implementation project can be found at github [18].

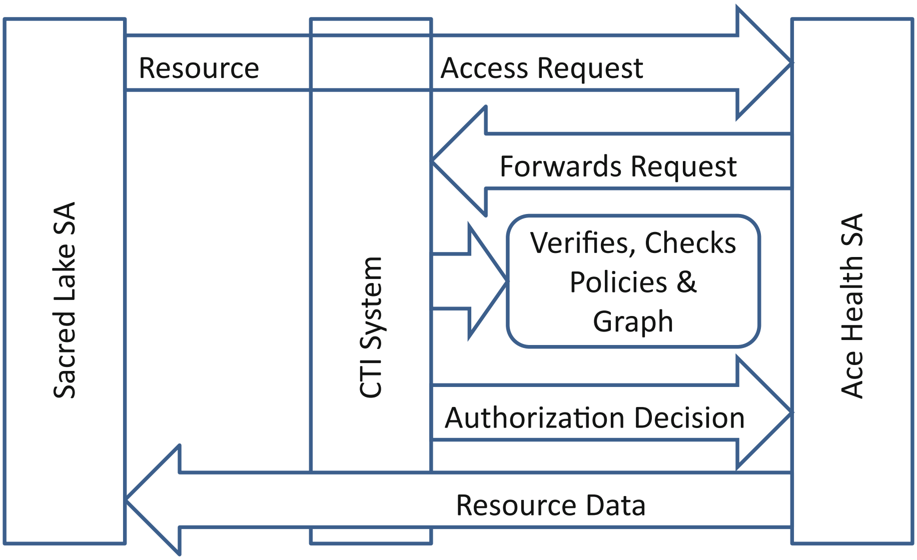

Fig. 9. Resource (CTI) request protocol

7 Relationship Based Access Control Authorization Decision Process

The request to access a CTI resource is processed by CTI System. In order make an authorization decision, the CTI System takes account of three policies. They are - Accessing User Policy (AUP) of accessing/requesting organization, Target Resource Policy (TRP) of owner organization for the requested resource type and overall System specified Policy (SP) of CTI System for the same resource type. These three policies are verified against the CTI System sharing ecosystem graph. Each policy evaluation result is represented by a boolean result of true or false. If the requesting organization and resource owner organization are matched with relationship type and are within the maximum allowable distance or hop count limit specified in the policy, the policy yields in a true result. The specific details about these policies and their structures are elaborated in Cheng et al.'s UURAC [9] model.

These three type of policies may yield in different boolean results individually and can cause a decision conflict. In case of a decision conflict, Cheng et al. propose disjunctive, conjunctive or prioritized approach to resolve the conflict. We incorporate and enforce conjunctive approach in our implementation which interprets as the access to a resource is granted only if all the three policies into consideration yield in a boolean true result individually.

8 Future Work

In this paper, we present a practical approach to share structured CTI in a secure and automated manner through the application of ReBAC. Our work lays the foundation for an elaborate analyses of these shared CTI resources in future. We now propose some of the scopes of those analyses-

1. **Attack Reconstruction:** There may be a need for an organization to reconstruct/extrapolate the complete attack scenario from a received CTI of a particular type. For example- a CTI of Threat Actor [5] type focuses on attacker information. But the receiving organization may need to know further high level attack related information which involves that attacker in order to understand the attack and attacker's method of operations at a detail level. One possible approach could be to apply a machine learning algorithms to predict attack related information such as attack techniques, attack tools used etc. based on the Properties [5] received as a content of Threat Actor type CTI.
2. **Course of Action:** Organizations can establish their own security defense mechanisms to counter different cyber attacks. For example - a mass email could be sent to all the employees within the organization in case of sighting of a phishing attack to warn about the suspicious email. Organizations could use machine learning algorithms discussed in previous point to construct the full attack from received CTI containing partial attack features and map those attacks to appropriate Course of Actions [10].
3. **Cyber Threat Intelligence Knowledge Graph:** The knowledge graph is a knowledge base used by Google and it's services to enhance search engine's results with information gathered from a variety of sources. A machine learning based approach could be applied to develop a similar type of knowledge graph for structured CTI. The graph could provide useful relevant information to a CTI receiving organization such as attacks of similar nature, previous course of actions taken for similar type of attacks etc.

9 Conclusion

To summarize, we present the necessities to share CTI in an organizational scenario and provide a framework implementation to share structured CTI in a secure and machine readable manner. We also use Trusted Automated Exchange of Intelligence Information (TAXII) protocol to host CTI resources on organizational servers and exchange those CTI within organizations in a Request-response model. Our adoption of Cheng et al.'s [9] relationship based access control model demonstrates the applicability of this form of access control outside social network context. We further analyze STIX [4] framework and propose few directions in Future Work section to extract valuable insights from shared CTI. These insights could be incorporated into an organization's cyber defense system in order to develop a more secure and responsive cyber security infrastructure at an organizational level.

Acknowledgment. This work is partially supported by DoD ARO Grant W911NF-15-1-0518, NSF CREST Grant HRD-1736209 and NSF CAREER Grant CNS-1553696.

References

1. Confidentiality, Integrity, Availability: The three components of the CIA Triad. https://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/. Accessed 13 Aug 2019
2. Oasis Cyber Threat Intelligence (CTI) TC. https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti. Accessed 09 July 2019
3. Report Label. http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709303. Accessed 02 July 2019
4. STIX: A structured language for cyber threat intelligence. https://oasis-open.github.io/cti-documentation/. Accessed 01 July 2019
5. Threat Actor. https://oasis-open.github.io/cti-documentation/stix/intro. Accessed 04 July 2019
6. Barnum, S.: Standardizing cyber threat intelligence information with the structured threat information expression (STIX). Mitre Corp. **11**, 1–22 (2012)
7. Burden, K., Palmer, C.: Internet crime: cyber crime-a new breed of criminal? Comput. Law Secur. Rev. **19**(3), 222–227 (2003)
8. Chaabane, A., Acs, G., Kaafar, M.A., et al.: You are what you like! Information leakage through users' interests. In: Proceedings of the 19th Annual Network & Distributed System Security Symposium (NDSS). Citeseer (2012)
9. Cheng, Y., Park, J., Sandhu, R.: A user-to-user relationship-based access control model for online social networks. In: Cuppens-Boulahia, N., Cuppens, F., Garcia-Alfaro, J. (eds.) DBSec 2012. LNCS, vol. 7371, pp. 8–24. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-31540-4_2
10. Course of Action. https://oasis-open.github.io/cti-documentation/stix/intro. Accessed 08 July 2019
11. Connolly, J., Davidson, M., Schmidt, C.: The trusted automated exchange of indicator information (TAXII). The MITRE Corporation, pp. 1–20 (2014)
12. Crampton, J., Sellwood, J.: Path conditions and principal matching: a new approach to access control. In: Proceedings of the 19th ACM symposium on Access control models and technologies, pp. 187–198. ACM (2014)
13. Fong, P.W.: Relationship-based access control: protection model and policy language. In: Proceedings of the First ACM Conference on Data and Application Security and Privacy, pp. 191–202. ACM (2011)
14. Fong, P.W., Siahaan, I.: Relationship-based access control policies and their policy languages. In: Proceedings of the 16th ACM Symposium on Access Control Models and Technologies, pp. 51–60. ACM (2011)
15. Garton, L., Haythornthwaite, C., Wellman, B.: Studying online social networks. J. Comput.-Mediat. Commun. **3**(1), JCMC313 (1997)
16. Gates, C.: Access control requirements for web 2.0 security and privacy. IEEE Web **2**(0) (2007)
17. Haass, J.C., Ahn, G.J., Grimmelmann, F.: ACTRA: a case study for threat information sharing. In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, pp. 23–26. ACM (2015)
18. Haque, Md.F.: REBAC Model and TAXII Merged (2019). https://github.com/farhan071024/ReBACModel. https://github.com/farhan071024/TaxiiMerged

19. Iannacone, M.D., et al.: Developing an ontology for cyber security knowledge graphs. CISR **15**, 12 (2015)
20. Jagatic, T.N., Johnson, N.A., Jakobsson, M., Menczer, F.: Social phishing. Commun. ACM **50**(10), 94–100 (2007)
21. Johnson, C., Badger, M., Waltermire, D., Snyder, J., Skorupka, C.: Guide to cyber threat information sharing. Technical report, National Institute of Standards and Technology (2016)
22. Lane, J., Stodden, V., Bender, S., Nissenbaum, H.: Privacy, Big Data, and the Public Good: Frameworks for Engagement. Cambridge University Press, Cambridge (2014)
23. Mansfield-Devine, S.: Ransomware: taking businesses hostage. Netw. Secur. **2016**(10), 8–17 (2016)
24. Meadows, C.A.: Analyzing the Needham-Schroeder public key protocol: a comparison of two approaches. In: Bertino, E., Kurth, H., Martella, G., Montolivo, E. (eds.) ESORICS 1996. LNCS, vol. 1146, pp. 351–364. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-61770-1_46
25. Miller, J.J.: Graph database applications and concepts with Neo4j. In: Proceedings of the Southern Association for Information Systems Conference, Atlanta, GA, USA, vol. 2324 (2013)
26. Pandove, K., Jindal, A., Kumar, R.: Email spoofing. Int. J. Comput. Appl. **5**(1), 27–30 (2010)
27. Sandhu, R.S., Samarati, P.: Access control: principle and practice. IEEE Commun. Mag. **32**(9), 40–48 (1994)
28. Syed, Z., Padia, A., Finin, T., Mathews, L., Joshi, A.: UCO: a unified cybersecurity ontology. In: Workshops at the Thirtieth AAAI Conference on Artificial Intelligence (2016)
29. Thornburgh, T.: Social engineering: the dark art. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, pp. 133–135. ACM (2004)