Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security

Wanying Zhao, Gregory White
The University of Texas at San Antonio
wzhao@cs.utsa.edu, greg.white@utsa.edu

Abstract

Communities are becoming more vulnerable to cyber attacks as their reliance on critical cyber infrastructures is growing. Due to the interdependency among different cyber infrastructures, collaborative information sharing is necessary and important to help a community detect potential risks, prevent cyber attacks at an early stage, and facilitate incident response as well as preparedness activities in communities.

In this paper we propose a group-centric collaborative information sharing framework that aims to improve community cyber security. By analyzing specific information sharing requirements in the community, we design a formal policy model for this framework. Our model is illustrated by several information sharing scenarios in the community.

1. Introduction

As the reliance of communities on critical cyber infrastructures is growing, they are becoming more vulnerable to a wide variety of cyber attacks. Generally, a community consists of all of the entities within a geographical region. This includes local government, academic, and industry organizations. As such, a community consists of both public and private infrastructures, including finance, utilities (e.g. energy and water), health care and other important sectors. Cyber attacks and other cyber threats can cause disastrous impacts in a community, especially for a coordinated attack targeting multiple critical infrastructures in the community simultaneously. Due to the interdependency among many critical services, a service shutdown caused by a cyber attack may bring down multiple services in nearby areas.

For this reason, collaborative information sharing among different sectors becomes necessary and important to community cyber security. Many cyber threats are difficult to detect and identify by a single organization. By correlating the shared information, a more effective method for a community to detect potential risks and prevent cyber attacks at an early stage can be developed. With an analysis of comprehensive incident-related information shared collaboratively, it will be possible to analyze the impact of an incident on the whole community. Collaborative information sharing can also facilitate incident response as well as preparedness activities in communities.

In recent years, a Community Cyber Security Maturity Model (CCSMM) [1] was proposed to help communities establish viable and sustainable cyber security programs. While much of a community cyber security incident response capability has been developed in this model [2], an important part of the CCSMM, Information Sharing, has significant aspects that still need to be investigated and explored.

There are several information sharing services developed by federal government and state governments. The U.S. Department of Homeland Security (DHS) developed United States Computer Emergency Readiness Team (US-CERT). The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents. Similarly, the Multi-State Information Sharing and Analysis Center (MS-ISAC) hosts a library of cyber security resource documents and enables secure email using the US-CERT Portal. The problem with these information sharing services is that the organizations directly share information with government entities to a centralized location. What is lacking is collaboration among different organizations in the same sector or across different sectors in a community.

We propose a collaborative information sharing framework specifically designed for a community. Our framework aims to facilitate collaborative information sharing among the organizations and entities in the community itself. The framework is based on the group-centric Secure Information Sharing (g-SIS)
model [3]. We extended the basic g-SIS model and developed new features and inter-group relationships to support collaborative information sharing among different groups. The design of this framework will benefit communities in that it enables multi-level aggregation and correlations in order to provide the maximum amount of information for further sharing with state and national entities.

By analyzing the specific information sharing requirements and information flow in the community, we design a formal policy model for our collaborative information sharing framework. Our policy model is represented in formal specifications at high level, thus it enables enough flexibility for enforcement and implementation in various communities.

The rest of the paper is organized as follows. Section 2 proposes a collaborative information sharing framework for community cyber security. Section 3 discusses information sharing requirements for different purposes related to incident management in the community. Section 4 presents the formal policy model specifically designed for our framework. Section 5 gives several possible information sharing scenarios by using our model. Section 6 discusses future work and section 7 concludes the paper.

2. Collaborative information sharing framework for community cyber security

In traditional information sharing, each side communicates directly with one another. When a large number of entities need to share information for a common goal, the traditional way can be inefficient. One natural and effective way to facilitate information sharing among a larger number of entities is to gather information and participants together in groups.

Group-centric Secure Information Sharing (g-SIS) model [3] is an Access Control (AC) model that utilizes groups to bring users and information together. It is a flexible sharing framework suited for use in highly dynamic environments such as found in computer and network incident response. It provides a way to share information but at the same time protect information deemed sensitive by its owners. We propose the creation of a collaborative information sharing framework specifically for community cyber security based on the g-SIS model. We introduce different types of groups with various inter-group relationships to extend the basic g-SIS model.

We design our framework acknowledging the basic information flow found with groups. Our design of a collaborative information sharing framework is illustrated in Figure 1 and 2.

Figure 1. Collaborative information sharing framework (during periods with no incident occurring)

Figure 2. Collaborative information sharing framework (during periods with incidents occurring)

In our framework, community information sharing entities basically include:

- **Sector Group**: A community includes multiple Sector Groups. These groups represent the major sectors found in communities of any size. These include energy, water, finance, healthcare, emergency services, telecommunications, transportation, etc. In a Sector Group, information sharing occurs among different organizations that all are part of the same overriding sector. For example, members from Wells Fargo, Bank of America, and other financial organizations would share information in the finance Sector Group.

- **Non-Sector Organizations**: Not all organizations within a community may be part of the recognized critical sectors. These Non-Sector Organizations still are important to the community and need to be part of the information sharing process. Non-Sector Organizations may provide important information for cyber incidents in the community.
These organizations may obtain information from academia, other industry entities, and even individual citizens.

- **Super Group:** In every community there is a need for an organization to provide functions comparable to the functions performed by a fusion center [4] or the National Cybersecurity and Communications Integration Center (NCCIC). In our framework, a community will have a Super Group that will provide similar functions. The Super Group is responsible for obtaining information from internal sources (Non-Sector Organizations) and external sources (such as neighboring communities and the state government). It interfaces with the Collaboration Group and performs intelligence information analysis to identify risks. It is responsible for coordinating information sharing and incident management/response among different Sector Groups when an incident is identified. It also shares incident response, mitigation strategies, recovery recommendations, applicable alerts or warnings to community members. The Super Group should be staffed by cyber security domain experts.

A community needs a certain level of routine information sharing during steady state when no incident has been identified, and incident-specific information sharing when incidents occur. In our framework, there are two types of groups for supporting routine information sharing and incident-specific information sharing among sectors:

- **Collaboration Group:** The purpose of the Collaboration Group is to facilitate information sharing among different sectors in the community and to provide an established, long-term collaboration mechanism. The Collaboration Group supports routine and incident-related information sharing. The incident information handled by the Collaboration Group consists of information applicable to all members in the community (such as community-wide alerts or warnings, and general recovery recommendations.) It also provides the foundation for sectors to correlate incident details to determine when to establish an Incident Group for sharing information about specific incidents. Membership in the Collaboration Group is granted to representatives from Sector Groups and the Super Group. The administrators from the Super Group and each Sector Group perform co-administration in the Collaboration Group.

- **Incident Group:** An Incident Group is a dynamically established, temporary collaborative group. The purpose is to support incident-specific information sharing when incidents occur in the community. Based on the analysis of the information gathered and correlated in the Collaboration Group, if a threat to the community is identified related to an incident or a specific type of incidents, an administrator of the Collaboration Group creates a new Incident Group and provides a reference for related Sector Group members to join the Incident Group to share further details about the incident(s). The Super Group members assisting with the incident mitigation may share mitigation plans or strategies in the Incident Group. Membership in the Incident Group is granted to members in the Collaboration Group. As Figure 2 shows, a community may have multiple Incident Groups at the same time. An Incident Group may be disbanded once the corresponding incidents in the Incident Group are resolved.

### 3. Information sharing requirements in the community

There are some research [5] and [6] that discuss the architecture and the method of collaborative intrusion detection. Our research focus is different from these works in that our work mainly focuses on what information needs to be shared, and in what way can the information be shared effectively and securely. The specific methodologies and techniques related to information aggregation, correlation and analysis are out of the scope of this paper.

Additionally, our collaborative information sharing not only intends to share information relevant to the detection of an incident, but also share all other information related to community cyber incident management. Information sharing assists coordination and collaboration in all the phases of a cyber incident response cycle including prevention, protection, detection, assessment, response and resolution.

We summarize the different types of information required to be shared by their purposes in Table 1. For each type of information, we provide a description and specify the information flow among different groups in our framework. We give several specific examples for information required to be shared. Notice that the required information includes but is not limited to the examples given in the table. Based on the source where the information comes from, the information examples given in the table can be divided into **Human Intelligence** and **Technical Intelligence**. Human Intelligence is the information gathered by means of observation or recorded by a person. Information of this type may
### Table 1. The information sharing requirements for community cyber security

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Information Flow</th>
<th>Required Information Sharing Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routine and Awareness</td>
<td>Sector Group to Collaboration Group, Super Group to Collaboration Group, Collaboration Group to Sector Group, Collaboration Group to Super Group</td>
<td>General information that addresses awareness.</td>
<td>Routine security status update, daily cyber feed, external feed brought from outside of the community, general guidelines</td>
</tr>
<tr>
<td>Warning and Prevention</td>
<td>Sector Group to Collaboration Group, Super Group to Collaboration Group, Collaboration Group to Sector Group, Collaboration Group to Super Group</td>
<td>Information that helps incident prevention. Early indicators of potential incident.</td>
<td>Technical Intelligence: Port scanning records, exploited vulnerabilities from anti-virus application and system, tracked threats, IDS/IPS alerts, Human Intelligence: Warnings from other communities. Reports about abnormal activities for potential incident, such as suspected war driving.</td>
</tr>
<tr>
<td>Incident Reporting</td>
<td>Sector Group to Collaboration Group and Incident Group, Super Group to Collaboration Group and Incident Group, Incident Group to Super Group</td>
<td>Detailed information regarding the incident. Information about the type of attack, the source, started time, detected time of the incident, description, event data, symptoms, the destination port numbers involved, etc.</td>
<td>Technical Intelligence: Firewall logs, IDS/IPS alerts, system logs, data logs, port scanning records, network performance data, data from routers and anti-virus applications, Human Intelligence: Reports about abnormal activities (such as human errors) that caused a cyber incident.</td>
</tr>
<tr>
<td>Assessment</td>
<td>Sector Group to Incident Group, Super Group to Incident Group, Incident Group to Super Group</td>
<td>Information about impact, scope and severity and other information related to risk assessment.</td>
<td>Reports about the number of systems and sites impacted by the incident, the percentage of population denied access to the service.</td>
</tr>
<tr>
<td>Mitigation</td>
<td>Super Group to Collaboration Group and Incident Group, Incident Group to Sector Group, Collaboration Group to Sector Group, Incident Group to Super Group</td>
<td>Information related to the incident mitigation, response and recovery.</td>
<td>Mitigation resolution, incident action plan, recovery status report.</td>
</tr>
</tbody>
</table>

need to be processed and analyzed by a special analyst. Technical Intelligence is the information generated and collected from computers and networks. Most information of this type could be processed automatically or semi-automatically using tools.

The information shared among different groups should be organized, categorized, structured, and uniformly described, so as to make it useful in the context. In this section we take the first step toward this goal by categorizing the information types that are required in our framework and providing descriptions and examples. Further steps toward this goal include designing a standard data format for information sharing and designing a method to validate the information according to the standard data format. These latter steps, not undertaken in this paper, will be studied in our future research.

4. Formal model for the collaborative information sharing framework

In the basic g-SIS model proposed in [3], users join and leave groups, and objects are added to and removed from groups. Users gain access to objects via membership relationships they have with groups that contain those objects. The basic g-SIS model only supports information sharing in isolated groups without information flow from or to other groups. The framework proposed in [7] supported collaboration among bilateral organizations, however, the policy model in that work does not apply to our designed framework in section 2. In order to support inter-group relationship and information flow among different types of groups in the community, we specified a formal policy model for our framework described in Section 2.

We do not consider administrative operations inside organizations participating in collaboration due to organizational variations. Non-Sector Organizations can be difficult to formally specify in our model due to the same reason. Moreover, the information from Non-Sector Organizations and external sources of the community (such as other communities, state government, federal government) will be brought to the community collaboration by the Super Group. For these reasons, our model specified in this section will focus only on the Sector Groups, Super Group, Collaboration Group and Incident Groups.

Moreover, in our model, we do not enable read-and-
write access since writing (or updating) an existing object will bring many complex problems in design and implementation, such as it could cause inconsistency of reading different versions, the object being read is not up to date, and the difficulty to maintain different versions. Read access could satisfy most of the information sharing requirements discussed in the previous section. Instead of write operation, our model allows creating a new object with new content.

To formally specify our policy model, we develop several attributes for users, objects and groups that are used in the model. We also develop the operations related to user membership, object membership and information flow, group administration and inter-group level relationship. We specify the authorization policies for each operation.

4.1. Attributes

The following sets are used in defining the attributes in our model.

- **U**: A set of existing users in the community.
- **O**: A set of existing objects in the community.
- **G**: A set of existing groups of all types in the community.
- **SG**: A set of existing Sector Groups in the community.
- **IG**: A set of existing Incident Groups in the community.

In our model, we use **cg** to represent the only Collaboration Group in the community, and **spg** to represent the only Super Group in the community. So \( G = SG \cup IG \cup \{cg\} \cup \{spg\} \), and \( cg \notin SG \cup IG \), \( spg \notin SG \cup IG \), \( SG \cap IG = \emptyset \). That is, \( G \) consists of all types of group sets. Different group sets share no common element.

4.1.1. User attributes. We define the following user attributes according to the requirements.

\[
\begin{align*}
  UgMem : U &\rightarrow SG \cup \{spg\} \cup \{NULL\} \\
  UcgMem : U &\rightarrow \{True, False\} \\
  UigMem : U &\rightarrow \mathcal{P}(IG)
\end{align*}
\]

The attribute \( UgMem \) represents the user membership in the Super Group or one of the Sector Groups. In our model, a user can be a member of only one of these two types of groups; either the Super Group \( spg \) or one of the existing Sector Groups. The attribute \( UcgMem \) represents whether the user is a member of the only Collaboration Group \( cg \) in our model. At the same time, the user can be a member in multiple Incident Groups. The attribute \( UigMem \) represents the set of Incident Groups in which the user has the membership. \( \mathcal{P}(IG) \) stands for the power set of \( IG \).

4.1.2. Object attributes. We define the following object attributes according to the requirements.

\[
\begin{align*}
  OMem : O &\rightarrow G \cup \{NULL\} \\
  OriginG : O &\rightarrow G \cup \{NULL\} \\
  Disclose : O &\rightarrow \{Public, Restricted\} \\
  ExportG : O &\rightarrow \mathcal{P}(G)
\end{align*}
\]

The attribute \( OMem \) represents the group in which the given object is in. In our design, an object contains the information to be shared, and an object should belong to only one group (of all types). Although there is information flow among different groups, when the information needs to be transferred to another group, a new copy is created in the destination group with a different object identifier, thus we do not view them as the same object in our model.

\( OriginG \) represents the group where the object is created or added. (Add operation is only for Super Group and Sector Groups, Create operation is for all types of groups). This attribute is designed for privacy concern and traceback purpose. ExportG represents the group set the given object is allowed to be exported to. If the attribute Disclose is “Public”, there is no restriction for the object to be exported to any other groups, or if this attribute is “Restricted”, only the groups in the set of ExportG the object can be exported to. These two attributes are designed for privacy concern. For instance, some organizations in the community might want to protect their privacy-sensitive information from outside of the Sector Group. In certain circumstances (e.g. the threat alert level of the community increases), they may be willing to share more information with other entities by modifying the ExportG attribute to include more groups (such as a specific Incident Group or the Collaboration Group).

4.1.3. Group attributes. We define the following group attributes according to the requirements.

\[
\begin{align*}
  ConnectCG : SG \cup \{spg\} &\rightarrow \{True, False\} \\
  AdminG : U \times G &\rightarrow \{True, False\}
\end{align*}
\]

The ConnectCG attribute is for the Super Group \( spg \) and Sector Groups, it represents whether the group is connected with the Collaboration Group \( cg \) to share information with it. Ideally, \( spg \) and all Sector Groups should be connected with \( cg \). But some newly formed Sector Groups may be in early information sharing phase so that they did not join the collaboration yet. AdminG attribute shows whether a given user is an administrator of a given group.

4.2. Operation model for user membership

We specify the basic requirements for authorizing each operation related to user membership in Table 2,
along with the sets and attributes updates upon the authorization.

In Table 2, the first column specifies an operation. The second column provides a brief description of the operation. The third column specifies the basic requirements for this operation to be authorized. Because there are various requirements in different communities, some additional community-specific requirements are not listed. A community may specify additional requirements as they need. When a request for an operation is made, this operation is only authorized if all the requirements listed in the third column are satisfied. (Plus that all community-specific requirements are also satisfied.) If the operation is authorized, the updates of attributes and sets are listed in the fourth column. We denote the attribute and set names with prime to represent the existing values after the update, and those without prime to represent the existing values before the update. These rules also apply to Table 3 and Table 4.

Upon joining a group, the user can get access to the objects in that group. Depending on different types of groups, we specify JoinG for a user joining the Super Group or a Sector Group, JoinCG for a user joining the Collaboration Group, and JoinIG for a user joining an Incident Group. According to our design, a user can join either the Super Group spg or exactly one of the Sector Groups by JoinG. For JoinCG, authorization is only given to the user if he is a member of the spg or a Sector Group that connected to the Collaboration Group cg. Since only selected representatives of a Sector Group could join cg. Additional requirements could be developed for selecting the qualified member joining cg depending on the specific demand of the community. For instance, cg could require the user to be trusted by all members from different sectors. For JoinIG, the basic requirement for a user joining the Incident Group is that he should be a member of the Collaboration Group.

When a user leaves a group, depending on the different type of group, we specify LeaveG for a user leaving the Super Group or a Sector Group, LeaveCG for a user leaving the Collaboration Group cg, and LeaveIG for the user leaving an Incident Group. LeaveIG will revoke only the membership of the Incident Group the user leaves. LeaveCG will revoke the user’s membership in the Collaboration Group and all Incident Groups. LeaveG will revoke user membership in all types of groups, since the user will no longer be an active participant for community collaboration. Upon leaving a group, the user loses access to the objects in that group.

### 4.3. Operation model for object membership and information flow

We specify the basic requirements for authorizing each operation related to object membership and information flow in Table 3, along with the sets and attributes updates upon the authorization.
Add objects only applies to Sector Groups and the Super Group, for that they bring in existing information from organizations and other entities in the community or from outside of the community. For a user to Add an object to a given group, the user needs to be a member of that group. The Remove operation applies to groups of all types, the Remove operation will delete the membership of the object in the group. In some design, Remove may require deleting the object.

CreateO operation is for creating a new object in the group, this operation applies to groups of all types. The user needs to be a member of the group in which he creates the object. Upon the creation of a new object, a new object identifier is created, and the OriginG attribute of the object is updated to the group where it is created.

For transmitting the information in an object from one group to another, the Publish operation is developed. As previously stated, each object belongs to only one group in our model. By publishing an object in the source group to the destination group, a new copy of the object will be created in the destination group. There are two cases of Publish according to Table 1: (1) From Sector Group or Super Group to Incident Group or Collaboration Group. (2) From Incident Group or Collaboration Group to Sector Group or Super Group, either way, the user performing this operation needs to be a member in both the source group and the destination group. Publish is only permitted if the source object is set to “Public” disclose or the destination group belongs to one of the exporting groups listed in object attribute ExportG. And the created object in destination group will maintain the same Disclose and ExportG attribute values of the source object.

SetExport operation is required when a user wants to allow exportation of an object to a given group by modifying the exportation group list. The user performing this operation should be a member of the group in which the objects resides. Additional requirements may be needed such as the user needs to be the creator of the object.

Read operation is for a user to read an object in the group. To authorize this operation, both the user and the object should be a member of that group.

### Table 3. Operation model for object membership and information flow

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Requirements for Authorization</th>
<th>Updates Upon Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add(u, o, g)</td>
<td>User u adds an existing object o to the Super Group or a Sector Group g</td>
<td>u ∈ U, o ∈ O, g ∈ SG ∪ {spg}, UgMem(u) = g, OMem(o) = NULL</td>
<td>OMem'(o) = g, OriginG'(o) = g</td>
</tr>
<tr>
<td>Remove(u, o, g)</td>
<td>User u removes the object o from the group g</td>
<td>u ∈ U, o ∈ O, OMem(o) = g, (g ∈ SG ∪ {spg} ∧ UgMem(u) = g) (\forall (g = cg ∧ UgMem(u) = True) \lor (g ∈ IG ∧ g ∈ UgMem(u)))</td>
<td>OMem'(o) = NULL, O' = O (\cap {o}) if deleting o is necessary</td>
</tr>
<tr>
<td>CreateO(u, o, g)</td>
<td>User u creates a new object o in the group g</td>
<td>u ∈ U, o ∉ O, (g ∈ SG ∪ {spg} ∧ UgMem(u) = g) (\forall (g = cg ∧ UgMem(u) = True) \lor (g ∈ IG ∧ g ∈ UgMem(u)))</td>
<td>O'Mem(o) = g, OriginG'(o) = g</td>
</tr>
<tr>
<td>Publish(u, o1, o2, g1, g2)</td>
<td>User u publishes the content of object o1 from the source group g1 to a newly created object o2 in the destination group g2</td>
<td>u ∈ U, o1 ∈ O, o2 ∉ O, OMem(o1) = g1, Disclose(o1) = Public(\forall g2 \in ExportG(o1)), one of following cases: * case 1: (g1 ∈ SG ∪ {spg} ∧ UgMem(u) = g1, (g2 = cg ∧ UgMem(u) = True) \lor (g2 ∈ IG ∧ g2 ∈ UgMem(u))) * case 2: (g2 ∈ SG ∪ {spg} ∧ UgMem(u) = g2, (g1 = cg ∧ UgMem(u) = True) \lor (g1 ∈ IG ∧ g1 ∈ UgMem(u)))</td>
<td>O'Mem'(o) = O' (\cup {o2}), OriginG'(o2) = OriginG(o1), ExportG'(o2) = ExportG(o1)</td>
</tr>
<tr>
<td>SetExport(u, o, g1, g2)</td>
<td>User u adds g2 to the object exportation group list of the object o in g1</td>
<td>u ∈ U, o ∈ O, OMem(o) = g1, OriginG(o) = g1, g2 ∉ ExportG(o), (g1 ∈ SG ∪ {spg} ∧ UgMem(u) = g1) (\forall (g1 = cg ∧ UgMem(u) = True) \lor (g1 ∈ IG ∧ g1 ∈ UgMem(u)))</td>
<td>ExportG'(o) = ExportG(o) (\cup {g2})</td>
</tr>
<tr>
<td>Read(u, o, g)</td>
<td>User u reads the object o in the group g</td>
<td>u ∈ U, o ∈ O, OMem(o) = g, (g ∈ SG ∪ {spg} ∧ UgMem(u) = g) (\forall (g = cg ∧ UgMem(u) = True) \lor (g ∈ IG ∧ g ∈ UgMem(u)))</td>
<td>None</td>
</tr>
</tbody>
</table>
Table 4. Operation model for group administration and inter-group relationship

<table>
<thead>
<tr>
<th>Operation</th>
<th>Description</th>
<th>Requirements for Authorization</th>
<th>Updates Upon Authorization</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreateIG(u, ig)</td>
<td>User u creates an Incident Group with new identifier ig</td>
<td>( u \in U, \text{UcgMem}(u) = \text{True}, \text{ig} \notin \text{IG} )</td>
<td>( IG' = IG \cup {\text{ig}} )</td>
</tr>
<tr>
<td>DisbandIG(u, ig)</td>
<td>User u disbands the Incident Group ig</td>
<td>( u \in U, \text{UcgMem}(u) = \text{True}, \text{AdminG}(u, \text{cg}) = \text{True}, \text{ig} \in IG )</td>
<td>( \forall u \in U, ig \in \text{UigMem}(u), \text{UigMem}'(u) = \text{UigMem}(u) - {\text{ig}}, \forall o \in \text{OUMem}(o) = \text{ig}, \text{OMem}'(o) = \text{NULL}, IG' = IG - {\text{ig}} )</td>
</tr>
<tr>
<td>Connect(u, g)</td>
<td>User u connects the Super Group or a Sector Group g with the Collaboration Group</td>
<td>( g \in \text{SG} \cup {\text{spg}}, u \in U, \text{UgMem}(u) = g, \text{AdminG}(u, g) = \text{True}, \text{ConnectCG}(g) = \text{False} )</td>
<td>ConnectCG'(g) = True</td>
</tr>
</tbody>
</table>

4.4. Operation model for group administration and inter-group relationship

We specify the basic requirements for authorizing each operation related to group administration and inter-group relationship in Table 4, along with the sets and attributes updates upon the authorization.

CreateIG operation is to create a new Incident Group, the user needs to be a member of the Collaboration Group to perform this operation. Generally, the Collaboration Group administrator will create an Incident Group for a potential threat to the community based on the analysis of information gathered in the Collaboration Group. There are many factors that affect the forming of an Incident Group, such as the occurring time period and characteristics of the incident(s). How a particular Incident Group is defined varies from community to community. If a Collaboration Group member wants to report an incident and finds no relevant Incident Group available, he needs to request creation of a new Incident Group. The DisbandIG operation is to disband an existing Incident Group. The user performing this operation needs to be an administrator of the Collaboration Group. Upon DisbandIG, all the user memberships in this Incident Group will be revoked, and the objects in this group will be removed.

Connect operation will connect the Super Group or a Sector Group to the Collaboration Group cg. We consider this connection is long-term once the operation is performed. The user performing this operation needs to be a group administrator of the group that wants to connect with cg.

5. Scenarios of information sharing by using our Model

Our policy model focuses on the important issues at a higher level of abstraction at the policies, various enforcement and implementation models can be developed in different communities. The separation of the policy model from enforcement and implementation as illustrated in [8] allows enough flexibility for communities to enforce and implement the model according to their specific requirements.

Since the information aggregation, correlation and analysis methods are not our research focus. We assume that in each Sector Group, there are tools, methodologies to determine how to aggregate the information gathered, and appropriate guidance when to report it to the Collaboration Group or a Incident Group. (e.g. aggregated information will be sent out in a predefined time interval, say, every 10 minutes.) We also assume that in the Collaboration Group, there are tools, methodologies and mechanisms to correlate the information gathered and perform analysis to determine if there is a potential threat to the community. (e.g. If there were 100 IDS alerts in the Collaboration Group coming from all sectors. The alerts relate to one IP address and they reached the threshold for a threat to the community.) Such techniques and methods can be found in the work [6]. We assume that the Collaboration Group members are able to form appropriate Incident Groups and there are guidelines for them to match the incident he wants to report with the existing Incident Groups by the characteristics and description according to the Incident Group definition in a community. (e.g. There could be an Incident Group for Denial of Service attacks occurring during the time period from today to tomorrow, and there could be another Incident Group for intrusion attacks from a specific IP address.) In this section, we provide several possible scenarios for information sharing by using our model based on the above assumptions. We will describe the information sharing process and the operations need to be performed.
5.1. Scenario 1: Sharing information about a warning for the community

The first scenario is a simple one, suppose that the Super Group received a warning message from another community about an explored security vulnerability. The Super Group members share this information and some preventive measure resources such as the patches to the Collaboration Group by using the Publish operation so that Sector Group members could be aware of this vulnerability and protect their sector from attacks. If Sector Group members in the Collaboration Group considered their sectors relevant to this vulnerability, they will Publish the objects containing warning and resources to their Sector Groups.

5.2. Scenario 2: Sharing information about port scanning for incident prevention

Suppose a user $u_1$ in the energy Sector Group $sg_1$ detects port scanning from a specific IP address for port range 0-1024 in his organization which is considered a potential threat. For incident prevention purposes, he may want to share this information in $sg_1$.

Based on predefined sector group guidance, information containing the Source IP address, and port range being scanned should be structured and presented in object $o_1$ and be shared to $sg_1$ by an Add operation to the group. Other members in $sg_1$ could Read the information in $o_1$ and they could take preventive actions such as enhanced monitoring on these ports if necessary.

In this scenario we assume that no related threat was identified in the community, and the aggregated information (if there is any) will be shared to the Collaboration Group in a time interval predefined by community guidance. Suppose in this predefined time interval there are another 10 users in $sg_1$ sharing information about port scanning from the same IP address. This information will be aggregated and correlated in $sg_1$. The aggregated information may cause a new object to be created with the operation CreateO by user $u_{rep1}$, who is a representative in $sg_1$ and also a member of Collaboration Group $cg$. The aggregated information will be shared by $u_{rep1}$ to $cg$ by the Publish operation.

The Collaboration Group $cg$ correlates all the information gathered from other Sector Groups and analyzes the information to determine if there is a potential threat to the community. If the total numbers reach a community defined threshold (suppose the threshold is 50, $cg$ received 10 alerts from $sg_1$, 25 from $sg_2$, and 16 from $sg_3$), a potential threat to the community is identified. The Collaboration Group administrator will create an Incident Group $ig_1$ with the operation CreateIG for upcoming incident details, and provide reference for related and potentially affected Sector Group members to join this Incident Group to share further information. The Super Group members in $cg$ will assist with information analysis and incident response by sharing preventive strategies or mitigation plans in $ig_1$. The members from effected sectors then can Publish the strategies, mitigation plans and other resources from $ig_1$ to their Sector Groups. For other members in $cg$, warning message and general precaution recommendation could be shared with them in $cg$. In this simple scenario, the attack is low-level and not much more than is seen hundreds of times on a daily basis. No specific attack was tried, but it did show an interest in various organizations around the community. If after additional focused monitoring the same individual was seen attempting specific attacks, additional measures might be taken and a larger alert posted by a Publish operation.

If the threshold is not reached and no significant threat is identified for the community, feedback and some general prevention suggestions (e.g. enforce monitoring, block some ports, install security updates) will be shared with effected Sector Groups.

5.3. Scenario 3: Sharing information for an intrusion incident reporting

Suppose a user $u_2$ in the finance Sector Group $sg_2$ wants to report an intrusion through an application that uses port 12345 for communication in his organization. He needs to share object $o_2$ containing the details about the incident, including the source IP address, scanned port, detected time of the incident, symptoms, etc. as predefined by community guidance.

The representative $u_{rep2}$ in $sg_2$ (who is also a Collaboration Group member) will check the Collaboration Group $cg$ for existing Incident Groups. Suppose that previously in $cg$ several port scanning reports were received from sector $sg_3$ about scanning on port 12345 on their systems from different IP addresses. By correlation and analysis, a potential threat was identified and $sg_2$ was already created for the emerging incident related to port 12345. $u_{rep2}$ could join $ig_2$ and Publish $o_2$ to $ig_2$. $spg$ members could assist with mitigation by sharing resources to $ig_2$, and they could share appropriate recommendation for the sectors that previously reported scanning but where no intrusion occurred. (e.g. Recommendation to block the traffic heading to port 12345 if these sectors do not have to use this application.)
If there is no existing Incident Group relevant to this incident, \( u_{rep2} \) could publish \( o_2 \) to \( cg \) and make a request to create a new Incident Group. Depending on incident severity and scope, and by analysis and correlation with previously received information in \( cg \), the \( cg \) administrator will authorize CreateIG operation for a new Incident Group \( ig_3 \) if a threat is identified. Effected sectors will be provided with the reference for joining \( ig_3 \) to share more information. Other \( cg \) members could also join \( ig_3 \) to report ongoing port scanning to \( ig_3 \). Similarly, mitigation and prevention recommendation will be provided to \( ig_3 \).

We assume that in the above three scenarios, the shared information was labeled as “Public” in their disclose attributes, some privacy sensitive information about specific organizations (such as the IP address of the organization, location, physical device information) should be separated from public information. The Sector Group members may choose not to share this information or share them only in Sector Group with a “Restricted” label, later if the Collaboration Group or Incident Group requires more details, the Sector Group members could modify the the exportation scope by SetExport operation if they are willing to.

6. Future Work

The first task we need to do in our future work is to develop a proposed standard data format so that the information contains the exact information required by correlation and analysis services. A method to validate the information according to the standard data format should be developed as well.

Another important issue of secure information sharing is trust. We need an authentication mechanism to guarantee that the information comes from a trusted participant by using a certification authority to generate the credentials of the participants.

Administration is another common issue, especially concerning who specifically within a community will be tasked with the collection and dissemination of information and the establishment of the groups. The answer to this varies depending on the level of cyber security maturity of the community. Where possible, established emergency management structures, such as emergency operation centers or fusion centers, should be utilized. At the local organization level, information sharing needs to be cultivated at the individual security administrator level. Both individual sectors and the community as a whole also need to come together as their information sharing processes mature in order to establish the guidance that all will follow concerning what, when, and how to share information. The establishment of an information sharing process within a community is not a simple task and will involve much time and effort by individuals and organizations within the community.

7. Conclusion

Our paper proposes a collaborative information sharing framework which can be used to improve community cyber security. We analyzed specific information sharing requirements and designed a formal policy model for this framework. We illustrate our model using information sharing scenarios in the community. Although there are multiple future steps to apply our model in practice, as an important and under-developed part of the CCSMM model, our research on collaborative information sharing for community cyber security will greatly enrich the overall model.

References


