Towards A Framework for Cyber Social Status Based Trusted Open Collaboration

Jaehong Park
Institute for Cyber Security
University of Texas at San Antonio
jae.park@utsa.edu

Yuan Cheng
Institute for Cyber Security
University of Texas at San Antonio
ycheng@cs.utsa.edu

Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio
ravi.sandhu@utsa.edu

***Abstract*—Collaboration takes place in both closed and open environments. While closed collaboration focuses on information or resource sharing amongst selected participants, open collaboration assumes and emphasizes that anyone can participate. In open collaboration, although participation is open to anyone who wishes to contribute or observe, it does not follow that everyone participates on an equal footing. Open collaboration is inherently a social activity. Establishment of trust in this context inevitably requires some form of social computing. Our premise is that such social computing derived trust requires a discriminative approach by utilizing cyber social status so as to enable selective and weighted trustworthiness of users and their activities and resources. In this paper we identify and discuss various kinds of cyber social status that can be used to facilitate trust in open collaboration. More specifically, we focus on social activity-based social status creation and management and articulate how these cyber social statuses of participants and resource can be generated. Furthermore, we show how these cyber social statuses are used in real world open collaboration systems such as Amazon, YouTube and eBay.**

I. Introduction

The explosive growth and diversity of social computing in cyber space is remarkable to say the least. Social computing enables new forms of sharing information and services. We use it to keep in touch with family and friends; to share news, knowledge, opinion, art, business documents; to play multi-user games, share others' reviews and recommendations, find friends at nearby locations, collaborate with other users, and build new social networks.

With increasing popularity of social computing its potential benefits for collaboration have been noted [6]. In particular "open collaboration" is recognized as different from traditional "closed collaboration" in that there is no pre-selected group of participants and anyone can contribute to and benefit from the collaboration efforts. Open collaboration has turned out to produce results on par and better than closed collaboration, in part due to hitherto unknown expertise drawn from a large population.

The notion of opening collaboration to anyone, however, brings to the fore the issue of trustworthiness of participants, their activities, and their shared resources. One method to inject trustworthiness in open collaboration system is by discriminating users and resources based on their cyber social status. Cyber social status can be conferred by authority or derived from various social activities of participants via social computing. In this paper, we introduce the notion of "cyber social status based trusted open collaboration"[1] and identify different kinds of cyber social statuses that we believe are crucial for embedding trust aspects in open collaboration. This is a necessary first step towards a comprehensive framework for cyber social status based trusted open collaboration.

II. Social Computing vs. Social Networking

In this paper, we use the term "Social Computing" rather than the popular term "Social Networking". The term "Social Networking" or "Social Networks" has been used extensively not only in computer science community but also in the general population. Typically we use the term "Social Networking" to recognize the recent (mostly web-based) information or service sharing computing services which utilize user relationship based social graphs to share certain "social" interests. A social network builds upon and fosters social connections between users. Popular social networking services include Facebook, LinkedIn, Twitter, etc. However, there are other services that do not utilize a social graph but still facilitate sharing of social interests, and thereby are not considered to be social networks. Examples include Amazon.com's recommendation system, eBay's reputation system, a collaboration application like Groove, crowdsourcing application like Wikipedia and a discussion board like Mac user forum. These applications or services are similar to social networking applications in that they allow users to share knowledge, news, opinion and more of their interests. By using the term "Social Computing", we relax the definition of social networking and cover a broader area of computing services than typical social networking definition. While social networking requires participants' social network connections to other users, social computing does not require this characteristic and covers any user-participated

[1]The term "trusted collaboration" has become well accepted in the research community. For consistency and simplicity, we use the term "trusted open collaboration" to capture the notion of trust in open collaboration. While it makes perfect sense to use the term "trusted closed collaboration", note that the term "trusted open collaboration" could be considered paradoxical in a sense that collaboration with unverified participants who share unverified resource can hardly guarantee any trustworthiness of the collaboration. While the terms "trust" and "open" are contradicting each other, by saying "trusted open collaboration", we do not mean an open collaboration system with a guaranteed trustworthiness but rather mean that a discriminative measure (for example, cyber social status in our case) can be facilitated in open collaboration to provide certain degree of trust to participants.

information and resource sharing services that facilitates a way to share certain "social" interests.

Note that it is not our goal to introduce an air tight definition for social computing. Rather we try to identify a recent and high impact computing phenomenon that emphasizes sharing of our social interests with others. With this definition, we can discuss how trust in open collaboration can be realized. Open collaboration is inherently a social activity. Establishment of trust in this context inevitably requires some form of social computing, but not necessarily social networking.

III. Trust and Open Collaboration

According to the definition in Merriam-Webster dictionary, collaboration means working together with others in an intellectual endeavor. Security research on cyber collaboration has largely focused on trust and control issues in closed collaboration systems [2], [9]. Recently we have witnessed previously unimagined success in open collaboration efforts such as Wikipedia and various open source projects. While there has been considerable research in the area of trusted closed collaboration, trust issues in open collaboration are relatively new and need to be modeled and analyzed so as to derive maximum benefit to human society from this new mode.

In this section we first review three principles for open source collaboration identified by Riehle et. at. We then discuss these principles from the perspective of trusted open collaboration. We further discuss additional characteristics found in trusted open collaboration. Then we define a collaboration taxonomy and the scope of this paper with respect to the taxonomy.

A. Three Principles for Open Source Collaboration

Recently, Reihle et. al. identified three principles for open (source) collaboration namely egalitarian, meritocratic, and self-organizing [7]. Open collaboration is **egalitarian** in the fact that everyone can contribute. For example, open source projects are usually accessible on the Internet and anyone can join and contribute to the project community. It is **meritocratic** in a sense that contributions are judged and valued based on their quality and merits. In open source collaboration, developed source code is discussed and evaluated publicly and available for reference to the community. Also open collaboration is considered **self-organizing**. This means there is no pre-defined process and participants determine how to use the shared work in the collaboration community.

These three principles are mainly derived from open source collaboration practice and not all principles fit perfectly for general open collaborations found in today's social computing environment. Furthermore, trust aspects in open collaboration require additional concepts as discussed below.

B. Trusted Open Collaboration: Principles and Criteria

Just like open collaboration, trusted open collaboration adheres to the principle of "**egalitarian**". Trusted open collaboration is egalitarian in the fact that anyone can participate.[2] Being egalitarian does not mean that all contributions are valued equally. In other words, trusted open collaboration is meritocratic. Although Riehle et. al. identified the principle of meritocracy for open collaboration, they did not specifically discussed the principle in terms of trusted open collaborations. We think the principle of "**meritocratic**" well captures aspects of trusted open collaboration. However, we also believe this is true only to a certain degree. One reason is that the principle could be somewhat self-contradictory. In trusted open collaboration, once a participant's trustworthiness is weighted based on the quality of the participant's contribution, the participant is allowed to have a discriminated social standing or privilege in the collaboration community. This standing or privilege in turn can allow the participants a power to influence other participants' social standing or privilege which could violate the very meaning of "meritocratic".

Another reason is that, in trusted open collaboration, discrimination may not be completely based on merit. In social computing, discrimination can be based on other cyber social activities or even authority-given social status which may not be meritocratic. Therefore we propose a new principle of "**discriminative**" to capture this. The principle of discriminative is a more generalized term than meritocratic. We say trusted open collaboration is discriminative to emphasize that trust in open collaboration can be realized based on discriminated participants and resource by facilitating various cyber social statuses which can be generated and managed by either authorities or participants' social activities.

Riehle et. al. argue that, in open collaboration, there is typically no defined process imposed from the outside so the project community itself determines how to go about its collaborated work, hence self-organizing. This could be true in some open source collaboration projects but not necessary the case for all open collaborations. For example, Wikipedia could be viewed as system-organized (as opposed to self-organized) in that, for example, there is a contribution decision process defined by a collaboration system so that experts can override (e.g., delete) certain documents contributed by other participants. Also, in an open collaboration like Amazon recommendation system, an evaluation process of user contributions is pre-defined and controlled by the system. Therefore, trusted open collaboration can be either **self-organized** or **system-organized** depending on whether the contribution evaluation process is defined by collaboration community or collaboration system provider.

Another crucial criteria that characterizes trusted open collaboration will be based on what kinds of cyber social statuses are used to discriminate participants and their resources. Here, a cyber social status can be either **self-governed** or **authority-governed**. The authority-governed cyber social status means that the social statuses are assigned to participants or their

[2] Although, strictly speaking, to be egalitarian, a collaboration system should not require an user account for participation, in general a system could be still considered egalitarian if the system allows anyone to create an account and if a user with an account can participate in a collaboration.

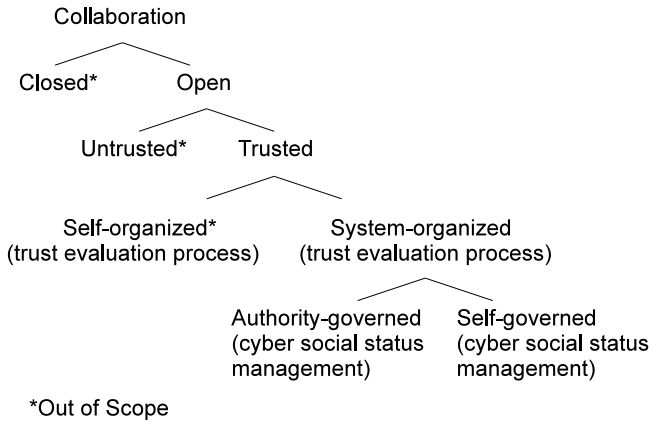

Fig. 1. A collaboration Taxonomy

resource by an entity other than collaboration participants who holds an authority to manage cyber social statuses. For self-governed cyber social status it is the collaboration community itself (or more precisely the participants' activities) who generates and manages cyber social statuses.

As summary, in this section we identified three principles of "egalitarian", "meritocratic", and "discriminative" for trusted open collaboration (which are different from the open source collaboration principles identified from Riehle et. al.). We also identified two criteria for trusted open collaboration that we utilize to build a collaboration taxonomy in the next subsection.

C. A Collaboration Taxonomy and Our Scope

Based on the discussion above, we introduce a taxonomy for collaboration as illustrated in Figure 1.[3] As discussed earlier, a collaboration can occur in both closed environment (where only selected user group(s) are allowed to participate in the collaboration), and open environment (where anyone can participate in the collaboration). These collaboration environments can be distinguished into untrusted and trusted collaborations based on whether a trust feature is facilitated or not in collaboration environment. As discussed in [4], [8], unlike reputation which is a collaborated understanding on an entity, trust is a subjective probability that can be used to measure how much an entity can expect from another entity. Therefore, ultimately trust in open collaboration can not be guaranteed equally to all participants but rather can be facilitated to help participants' subjective and personal decision by utilizing various factors such as cyber social statuses (including reputations) of participants and their resources. In this paper, by saying "trusted", we mean there exist cyber social statuses that can be used to discriminate participants and their resource. Based on who defines trust evaluation process, trusted open collaboration can be either self-organized or system organized. In self-organized trusted open collaboration, initially there exists no system defined trust evaluation process. One or more trust evaluation processes are likely to be created and evolved over time by collaboration community itself. Although not shown in the taxonomy, we think these evolved processes are likely to be similar to that of system-organized trusted open collaboration. In system-organized trusted open collaboration, based on who generates and manages cyber social statuses, a collaboration system can be either authority-governed or self-governed.

Note that in Figure 1, although closed collaboration could be classified into similar classifications as open collaboration, we only show classifications of open collaboration side since closed collaboration is not part of our scope. However, untrusted collaboration is not likely to fit into the classification scheme of trusted collaboration. This is because, by definition, there is no cyber social status that can be used to discriminate participants and their resources in untrusted collaboration. Most open collaborations may start with an "untrusted" state but will likely evolve into "trusted" collaboration. We do not discuss untrusted collaboration in this paper since our focus is on trusted open collaboration. Furthermore, within trusted open collaboration, we mainly focus on system-organized side since there is no defined cyber social status management process on self-organized side.

IV. Cyber Social Status Based Trust for Open Collaboration

A collaboration system can utilize various cyber social statuses to enable trustworthiness of participants and their resource in the collaboration environment. In system-organized trusted open collaboration environment, cyber social statuses of both participants and shared resource are either authority-governed or self-governed. In this section, we discuss various types of cyber social statuses for user and resource in terms of how these statuses are generated and managed.

A. User Cyber Social Status (u-CSS) Management

Cyber Social Statuses (CSS) for collaboration participants can be governed either by authority (Authority-governed in Figure 1) or collaboration community itself (Self-governed in Figure 1). Here, "Self-governed" means cyber social statuses of participants are generated based on the participants' various cyber social activities. In Figure 2, we illustrate several types of these user cyber social statuses (u-CSS). Specifically, we discuss one authority-governed and five self-governed user cyber social statuses. Please note that we do not intend to produce a complete list of how to generate CSSes. Rather we show our initial understanding on how CSSes can be generated so we can use them as a basis for understanding on how real world open collaboration systems realize trustworthiness of participants and their resources.

As the name says, in **Authority-given** u-CSS, user CSSes are provided to participants by authority. For example a collab-

[3]For simplicity, we develop this taxonomy as a collection of binary categories. In reality, a given system may have aspects that follow one binary choice and other aspects that follow the other binary choice. Most systems are likely to be hybrids in this regard. Further open collaboration systems are likely to evolve over time and therefore may change their characteristics through their life cycle.

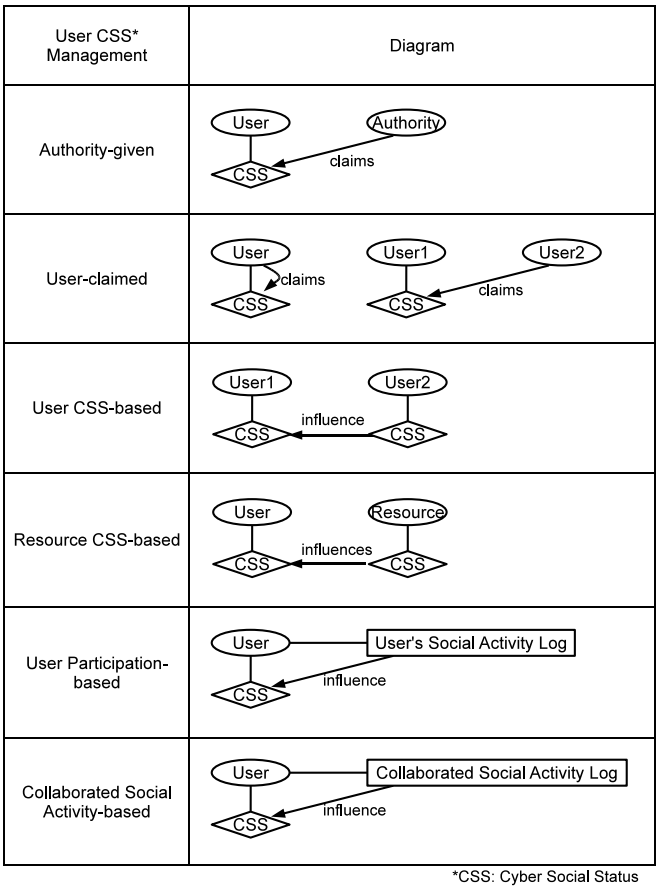

Fig. 2. User Cyber Social Status Management Types

oration system allows anyone can join the system but verifies participants, and then assigns cyber social statuses. Unlike other CSSes, authority-given u-CSS does not directly rely on participants' (collective) opinions or activities but incorporates authority's decision. Because of this reason, a collaboration system with authority-given u-CSS is not meritocratic if used alone without other CSSes. A collaboration system can utilize this u-CSS together with other u-CSSes to incorporate users' influence on measuring trustworthiness of users. We include authority-given u-CSS in our list since it is one way of generating u-CSS for a discriminative trust in collaboration environment.

User-claimed u-CSS means user CSSes are claimed by either the user herself or another user. In case there is no information to be used to discriminate trustworthiness of users in a collaboration system, the self-claimed u-CSS can be used perhaps temporarily until, for example, the system accumulates enough information to be able to generate cyber social statuses that are based on users' cyber social activities. In case of other user-claimed u-CSS, a user's CSS is given by a user other than the u-CSS holder. In a sense, this could be seen as a simplest (or initial) form of collaborated social activity-based u-CSS though there is no multi-user collaborated u-CSS. User-claimed u-CSS based collaboration system is not meritocratic.

In **User CSS-based** u-CSS, a user's CSS is determined (or influenced) by another user's CSS. This can make sense typically in case these users are related to each other. For example, suppose Alice is new to a collaboration community and does not have high-trust standing, while Bob is considered highly trustworthy in the community. If Alice and Bob are local collaborators for a specific subject matter and Alice represents the local collaboration, Alice's u-CSS for the subject could be improved due to the Bob's u-CSS or Bob's u-CSS is delegated to Alice automatically. Although this kind of u-CSS is likely to be generated by a collaboration system, since it is based on users' cyber social activities (in this case, the local collaboration), not based on authority's decision, we consider this "self-governed". Since this u-CSS type assumes there exist other u-CSSes in a collaboration system, it requires the collaboration system to include another way to generate u-CSSes. A collaboration system that utilizes u-CSS-based u-CSSes may or may not be meritocratic depending on how the u-CSSes that influence other u-CSSes are generated in a prior time. If this type of collaboration system utilizes u-CSSes that are generated based on other user's collaborated social activities, the system could be considered meritocratic. If these u-CSSes are assigned by an authority, the system is not meritocratic.

A u-CSS can be generated based on CSSes of resources. This is called **Resource CSS-based** u-CSS. Here, a user (whose u-CSS is influenced by a CSS of a resource) is likely to maintain a certain relationship with the resource. For example, a user could be the provider of a resource (e.g, product review) or a resource includes certain information about the user (e.g., buyers' feedbacks and ratings on a seller). A collaboration system with this type of u-CSS can be meritocratic depending on how resource CSSes are generated. If resource CSSes are generated based on user collaborated social activities such as product recommendations or buyers' feedback ratings, the collaboration system can be considered meritocratic. The details of how resource CSS can be generated are discussed in the next subsection.

In **User Participation-based** u-CSS, a user's CSS is based on her own cyber social activities. For example, the longer one participates in a collaboration or the more comments one posts, the higher trust level she can receive. However, this does not incorporate any activities or opinion from other users hence does not belong to the collaborated social activity-based u-CSS type which is discussed next.

Perhaps the most complex (but often considered the most trustworthy) way to generate u-CSS is **Collaborated Social Activity-based**. By saying "social activity", we mean cyber social activity. Here, a user's CSS is determined based on the results of other users' collaborated social activities. For example, Alice's u-CSS is determined based on the number of other users' recommendations or the average rating on her reputation.

Although not shown in the list, a user could be allowed to agree or disagree on assigned u-CSSes. This includes

(dis)agreement of u-CSS owner as well as (dis)agreement of other user(s). For example, a u-CSS owner can (dis)agree a u-CSS assigned to her by an authority, or one may (dis)agree on a u-CSS that is assigned to another user. This can occur in all types of u-CSS managements with an exception of self-claimed u-CSS based system, since it is meaningless for a user to agree or disagree on her own claim. Furthermore, an option for agreement or dispute can be made per each social activity that is collectively used to generate u-CSSes. For example, a seller may dispute on a buyer's review on the seller. How to resolve this kind of disagreement is beyond the scope of this paper, hence not discussed here.

B. Resource Cyber Social Status (r-CSS) Management

Similar to user cyber social status, resource cyber social status (r-CSS) can be used to discriminate trustworthiness of resource. In Figure 3, we show five types of resource CSS managements that are similar to u-CSS management types. Among them, "authority-given" belongs to authority-governed r-CSS management category while others belong to self-governed r-CSS category. In this subsection, we further discuss these r-CSSes.

Similar to authority-given u-CSS, **Authority-given** r-CSS means r-CSS is assigned by authority, hence not meritocratic. However it can be used together with other self-governed r-CSSes to enable collaborated evaluations of the resource contribution. Examples could be found in real world open collaboration systems such as YouTube. In YouTube, a video clip can be badged as a featured video by the YouTube. An r-CSS for a video clip can be also generated based on users' collaborated social activities.

In **User-claimed** r-CSS, an r-CSS is directly assigned by either the provider of the resource or other users. This is different from collaborated social activity-based r-CSS in that there is only one user's decision on an r-CSS at a given time. If a collaboration system utilizes this type of r-CSS, the system needs a mechanism to resolve issues caused by multiple users' claims on an r-CSS of a resource.

In **User CSS-based** r-CSS, an r-CSS is based on a user's CSS. Similar to user claimed r-CSS, it can be based on either the provider's CSS or another user's CSS. Typically, a user has certain relationship with the resource. For example an r-CSS inherits the resource provider's u-CSS. Here if a system also utilize user-claimed r-CSS, a u-CSS of the user who claimed r-CSS of a resource can influence r-CSS of the resource. More specifically, suppose Alice who holds a low-trust (u-CSS) in a collaboration environment posted a product review then assigned a high-trust (r-CSS) on the review. If the system also utilize user CSS based r-CSS, the r-CSS of the product review is likely to be degraded to reflect Alice's low-trust social standing.

Resource CSS-based r-CSS means r-CSS is influenced by an r-CSS of another resource. One example could be that if a resource is a copy of another resource, then it will carry same r-CSS of the original resource. Another example could be that if a resource is a collection of other resources, then its r-CSS is reflected by r-CSSes of some or all of the resources used in the resource. The r-CSS-based r-CSS could be meritocratic if r-CSS of the referenced resource is generated based on users' collaborated evaluation of its contribution.

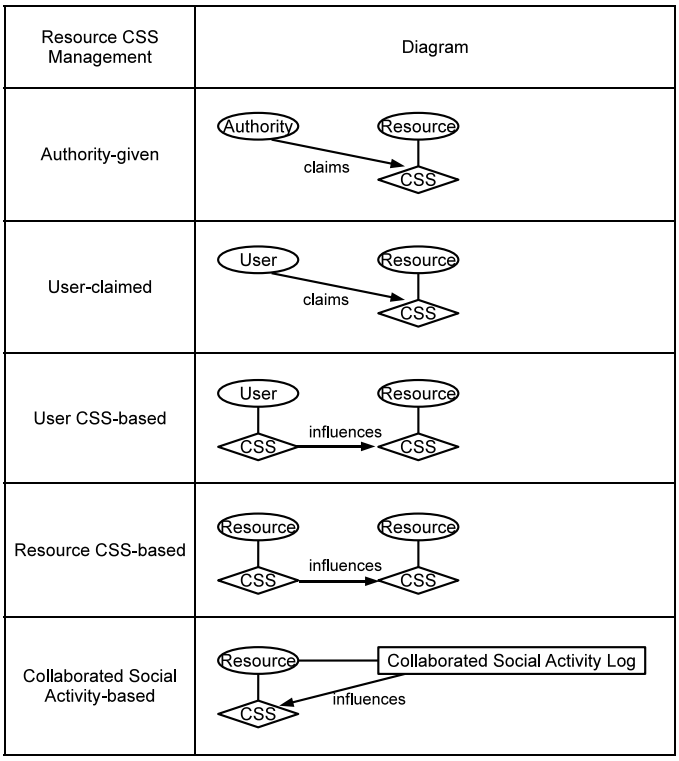

Fig. 3. Resource Cyber Social Status Management Types

Collaborated Social Activity-based r-CSS means r-CSS is generated based on collaborated social activities performed by participants. It may include how many times a resource is viewed or how many users liked the resource. It may also include an average rating voted by users. This collaborated social activity-based r-CSS is meritocratic since it is based on collective result of users' social activities that can be used to measure trustworthiness of resource. Examples could be the feedback systems found in many real world systems like eBay, YouTube, and Amazon.

C. Sybil Attacks in Trusted Open Collaboration

In today's social computing world, it is possible that a single entity utilizes multiple pseudonym identities to manipulate the result of collaborated user evaluation activities on herself. This result then influences the user's cyber social status. This kind of attack is called the Sybil attack which is named after the same name book by Schreiber [10]. The Sybil attack is considered a serious issue especially for open collaboration systems because of the fact that anyone can create multiple accounts. In this subsection, we discuss how the Sybil attack can influence open collaboration environments with various user cyber social statuses.

In a collaboration system that is based on authority given u-CSS, as argued in [1], no Sybil attack is possible since u-

CSS is given by an authority. In case of user-claimed u-CSS based collaboration system, if self-claimed u-CSS is used in a system, the attack is meaningless. If other user claimed u-CSS is used, since anyone can join the collaboration system, the vulnerability of the system depends on how difficult a user to claim someone else's u-CSS. If u-CSS is based on another user's CSS, sybil attack may not be an issue since if one user can create another user identity with certain u-CSS so she can use this new identity's u-CSS to influence the original identity's u-CSS, she probably can make the original user identity's u-CSS as she wished at the first place. If u-CSS is based on r-CSS, the vulnerability of the system depends on how difficult the attacker to generate an r-CSS that can influence the attacker's u-CSS. In this case, if the r-CSS is assigned by an authority, no sybil attack is possible. If the r-CSS can be claimed by a user other than the r-CSS holder, since creating an identity is trivial, the vulnerability depends on how difficult an attacker with a new identity to assign an r-CSS for the attacker's original identity. If r-CSS is generated based on collaborated social activities, the attacker can generate many identities to influence r-CSS which in turn can influence her own u-CSS. In a collaboration system that is based on user participation-based u-CSS, the Sybil attack is not possible since u-CSS can be influence only by the u-CSS owner's social activities. A collaboration system that utilizes collaborated social activity based u-CSS is probably the most vulnerable to the Sybil attack since u-CSS is generated based on the result of other user's social activities on which the main idea of Sybil attack is based.

As we discussed, different u-CSS types shows different level of vulnerability to the Sybil attack. A trusted open collaboration system could reduce the vulnerability to the Sybil attack by incorporating multiple u-CSS types in the collaboration system. Note that unlike other Sybil attack articles in computer science literature such as [5] it is not our focus to provide a solution for the Sybil attack hence not explored in this paper.

V. Discussion

In the previous section, we have identified various user and resource cyber social statuses that can be used to discriminate trustworthiness of the users and resources. These cyber social statuses are building blocks to enable trustworthiness in open collaboration. Many real world collaboration systems are likely to utilize multiple cyber social statuses to enhance trustworthiness of participants and shared resources. In this section we discuss three real world trusted open collaboration examples. We show the CSS management types presented in this paper are sufficient to model these trusted collaboration systems.[4]

A. Case 1: Amazon-like Trusted Open Collaboration System

Figure 4 shows how Amazon-like review and feedback system utilizes cyber social statuses identified in this paper.

[4]It is worth noting that one of the earliest trusted open collaborations may well be the PGP system, originally known as Pretty Good Privacy, which established trust in public keys via social computing [3].

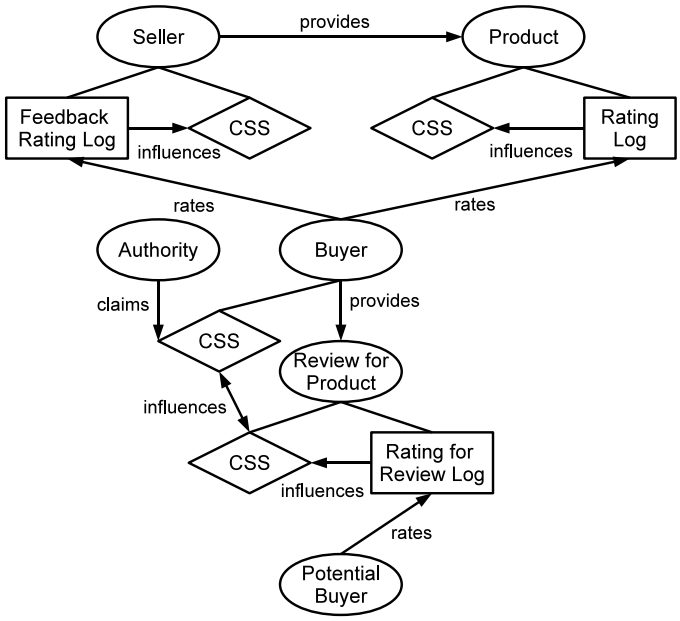

Fig. 4. Amazon-like trusted open collaboration system

Amazon online store has used customer review and feedback system to help customers make purchase decision, for years. After making a purchase, a customer can provide a rating as well as a product review about her experience on a specific product to the product page. This rating is stored in a rating log together with other users' ratings and used to influence cyber social status of the product (collaborated social activity-based r-CSS). In Amazon system, although this r-CSS may not be an objective assessment of the product quality, it may still reveal overall customer satisfaction of the product to a certain degree to the potential customers. If the purchase is made from a third party seller on Amazon, the customer also has a chance to provide a feedback rating for the seller. This feedback rating is then stored in a feedback rating log which is then used to generate a seller's CSS (collaborated social activity-based u-CSS). This u-CSS of seller can imply the trustworthiness of the seller (u-CSS), and thus provide a guidance to potential buyers. If a review provider holds high-trust standing, potential buyers can have more confidence in the review. Therefore, we can say the r-CSS of the review can be influenced by the u-CSS of the provider (u-CSS based r-CSS). When a potential buyer reads a product review on a product page, the buyer is allowed to rate the review as helpful or not. This rating is stored in rating review log and collectively influence r-CSS of the product review (collaborated social activity-based r-CSS). A review with more "helpful" votes is considered more valuable, then may influence the trustworthiness of the review provider. In other words, the r-CSS of the review can influence the u-CSS of the review provider (r-CSS based u-CSS). Also, if a review is made by a customer whose real name is verified by the Amazon system (Authority-given u-CSS), it may suggests high trustworthiness (u-CSS based r-CSS) to potential buyers. As

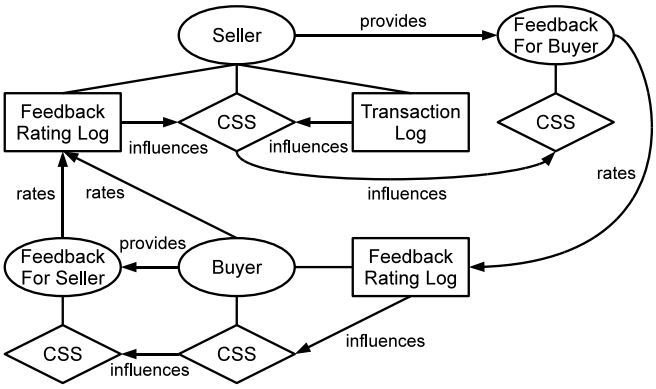

Fig. 5. eBay-like trusted open collaboration system

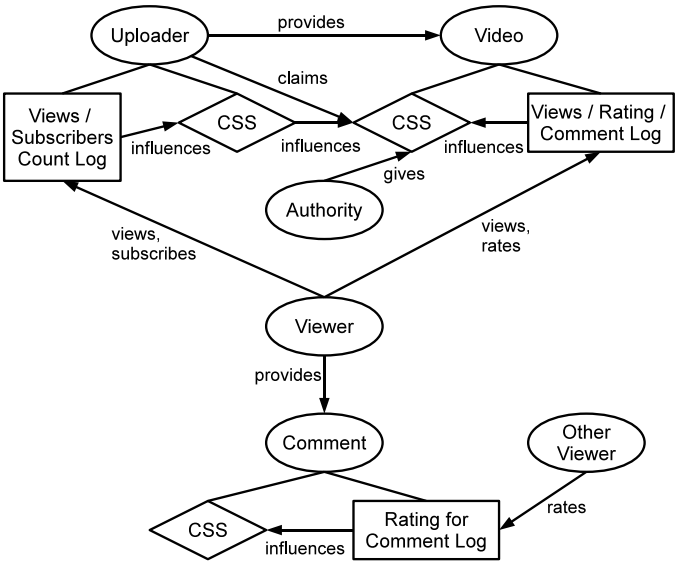

Fig. 6. YouTube-like trusted open collaboration system

a summary, in Amazon-like system, trustworthiness of users are facilitated by utilizing authority-given, r-CSS based, and collaborated social activity-based u-CSS while trustworthiness of resources are facilitated by utilizing u-CSS based, and collaborated social activity-based r-CSS.

B. Case 2: eBay-like Trusted Open Collaboration System

eBay is a popular online auction and shopping platform with feedback system. The major difference between its feedback mechanism and Amazon's is that eBay allows a buyer and a seller to give feedback to each other, and the feedback is made on the transaction participants rather than the product. Buyers can leave a positive, negative, or a neutral rating plus a comment (to the seller's feedback rating log), while sellers can leave a positive rating plus a comment (to the buyer's feedback rating log). Also, buyers are allowed to leave a detailed seller rating anonymously (to the feedback for seller). Both the seller's sales history (in the transaction log) and buyers' collaborative ratings and comments (in the feedback rating log) can influence seller's reputation or trustworthiness (user participation-based u-CSS and collaborated social activity-based u-CSS). For example, a seller with more positive ratings from past customers is supposed to provide better product or service, hence attracts more potential buyers. And if a seller's accumulated transactions counts as well as the number of received positive ratings meet the requirement, the seller could be qualified as a top-rated seller. Once a buyer rates the seller, seller can give a feedback back to the buyer. The buyer's reputation is affected by its accumulated rating from sellers (collaborated social activity based u-CSS). When the transaction participants provide feedbacks to each other, the feedbacks include the past rating of buyer, the past rating of the seller and a current rating. Here, their reputation (u-CSS) in the eBay community can influence the trustworthiness of their feedback (u-CSS based r-CSS) since the reader of these feedback can see the participants' past ratings. However, the buyer's detailed anonymous rating on the seller do not influence the buyer's reputation. As a summary, in eBay system, trustworthiness of users are facilitated by utilizing user participation-based and collaborated social activity-based u-CSS while trustworthiness of resources are facilitated by utilizing u-CSS based r-CSS.

C. Case 3: YouTube-like Trusted Open Collaboration System

YouTube serves as the biggest video sharing website in the world. Users can upload videos and create his own channel on the website, while others can watch the video, subscribe the channel, and post comments to the video. The popularity (u-CSS) of the uploader is based on other users' social activities, such as the number of subscribers and total view count of his videos (collaborated social activity-based u-CSS). The r-CSS of the video can be influenced in many different ways. Videos from a reputed uploader are more likely to have good quality (u-CSS based r-CSS). Furthermore, an uploader can claim one of his videos as a featured video candidate. Once approved by the system, the featured video badge would make the video more striking (authority-given r-CSS). However if an uploader is allowed to name a video as a featured on without YouTube's approval, the badge could be considered as a user-claimed r-CSS. Perhaps the more popular mechanism used in YouTube system to measure the popularity of a video is the number of views (collaborated social activity-based r-CSS). The more viewers watch, the more popularity it gains. The quality of the video can be inferred from the viewer's comments and ratings. Viewer can post a comment, or thumb up/down to the video he watches (collaborated social activity-based r-CSS). Meanwhile, others are allowed to rate the comments if they agree or disagree (collaborated social activity-based r-CSS). The rating may suggest the quality or popularity of that comment (r-CSS) in the community. As a summary, in YouTube-like system, trustworthiness of users can be facilitated by utilizing collaborated social activity-based u-CSS while trustworthiness of resources can be facilitated by utilizing authority-given, user-claimed, u-CSS based, and collaborated social activity-based r-CSS.

VI. Conclusion

Open collaborations that share questions and issues and seek answers and solutions are commonplace in cyber space. The basis for participants to determine trustworthiness of other participants and their shared resource is a key element for the success of these open collaborations. In this paper, we proposed the central notion of cyber social status as the basic building block for trusted open collaboration. As an initial step toward building a framework for cyber social status based trusted open collaboration, we identified and discussed various user cyber social status and resource cyber social status that can be used to discriminate trustworthiness of participants and their shared resources in open collaborations. We showed how these user and resource cyber social statuses are used in several well-known real world open collaboration systems.

Acknowledgment

This work is partially supported by NSF grant CNS-0831452 and by the State of Texas Emerging Technology Fund.

References

[1] John R. Douceur. The Sybil Attack. In IPTPS '01: Revised Papers from the First International Workshop on Peer-to-Peer Systems, (London, UK), 2002, pp. 251-260.

[2] Steven Dawson, Shelly Qian, and Pierangela Samarati. Providing Security and Interoperation of Heterogeneous Systems. Distributed Parallel Databases, 8(1):119-145, 2000.

[3] T. Grandison and M. Sloman. A Survey of Trust in Internet Applications. IEEE Communications Surveys and Tutorials, 3(4):2-16, 2000.

[4] Audun Jøsang, Roslan Ismail, and Colin Boyd. A survey of trust and reputation systems for online service provision, Decis. Support Syst., vol. 43, no. 2, 2007, pp. 618-644, Elsevier Science Publishers B. V..

[5] Brian Neil Levine, Clay Shields, and N. Boris Margolin. A Survey of Solutions to the Sybil Attack. University of Massachusetts Amherst technical report 2006-052, (Amherst, MA), Oct. 2006.

[6] Manoj Parameswaran and Andrew B Whinston. Research Issues in Social Computing. Journal of AIS, 2007, vol. 8, pages 336–350.

[7] Dirk Riehle, John Ellenberger, Tamir Menahem, Boris Mikhailovski, Yuri Natchetoi, Barak Naveh, Thomas Odenwald. Open Collaboration within Corporations Using Software Forges. IEEE Software vol. 26, no. 2 (March/April 2009). Page 52-58.

[8] Paul Resnick, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. Reputation systems. Commun. ACM, vol. 43, no. 12, 2000, pp. 45-48, ACM.

[9] Mohamed Shehab, Elisa Bertino, and Arif Ghafoor. Secure collaboration in mediator-free environments. In Proceedings of the 12th ACM Conference on Computer and Communications Security, 2005, Page 58-67.

[10] Flora Rheta Schreiber. Sybil. Warner Books, 1973.