Sanctioning Mechanisms in Virtual Communities

Elisa Bertino  
*Purdue University, USA*

Anna Cinzia Squicciarini  
*Università degli Studi di Milano, Italy*

Elena Ferrari  
*Università dell’Insubria, Italy*

**INTRODUCTION**

A virtual community is a composition of heterogeneous and independently designed subsystems, sharing services, resources, information, and knowledge to achieve a common goal. The concept of virtual community is very general and open to a number of interpretations (Ao & Misky, 2003; Sadighi & Sergot, 2002). Members belonging to a virtual community, indeed, may be represented by human beings, if the virtual community is a collection of people sharing common interests and ideas, or roles, programs or software/hardware modules, if the community is an automated system for sharing computing resources (Welch & Foster, 2002). The resource shared among a community may be computational resources as well as documents, information, or data. Whichever is the community-specific goal and features, assuming a community composed by interacting entities, several open issues need to be addressed, for instance, how to manage access policies to coordinate resource sharing, how to establish a community, how to oblige member communities to respect community policies, and so on. In the real world, to set up an organization it is necessary to perform some fundamental steps. First, the founder members have to draft a constitution, specifying the object and purpose of the organization, the rules, the kind of services and information provided. The constitution may be directly released to members or officially published in a registry’s Office. Furthermore, constitution must establish rules and responsibilities that each member has to follow. To join the community, a subject commonly has to apply for membership. The application consists of a procedure, where the applicant communicates his/her personal data, subscribes to the regulation of the community, and informs whether he/she has something to share, and which are the conditions under which he/she will release his/her services.

Similarly, in order to start up a virtual community, it is necessary to define participant roles and resources to be shared, as well as a regulatory system composed of community laws and/or local laws defined by single members. Protocols to define how to establish sharing relationships between participants must be enforced: each member entering into a community has to agree on what it is permitted to do and also on what it is obliged to do. Sharing of resources must be monitored, with resource providers clearly and carefully defining what is shared, who is allowed to share, and the conditions under which the sharing occurs. Such issues have been thoroughly explored by a number of researchers (see, for instance, Ao & Minsky, 2002; Bertino, Ferrari, & Squicciarini, 2003).

In addition to the above-discussed issues, a number of complementary issues have to be addressed to realize an efficient virtual community. Such issues have not been deeply investigated so far, but we strongly believe they are key requirements for the design of an effective framework for managing virtual communities. Such issues concern accountability, delegation, violation detection, and sanctioning mechanisms.

The concept of accountability concerns the responsibility of member behavior, and thus is strictly related with identity management in a virtual community. If a community allows members to have multiple identities at the same time, it is actually very hard to implement a system able to make the members accountable for their actions. Also, systems making use of pseudonyms give a weak handle for accountability insurance. A same entity may disappear and appear with a different identity without incurring any form of sanctions. A possible approach for achieving accountability is making use of reputation systems, facilitating the propagation of ambient knowledge about trustworthiness of the entities. Such mechanisms give the users incentive to properly behave in order to not to lose privileges and trust among the other community members.

The delegation issue concerns the possibility of authorizing other members to act as representative in exer-
cising actions in the community. Mechanisms for delegating authorities and privileges may be useful especially in large-scale communities having a considerable number of members playing different roles.

Further, a key aspect of a virtual community is to monitor that services are provided in accordance with the community policies and local policy rules, and to detect violations as they occur. A number of security protocols have to be adopted to prevent false claims by agents and guarantee evidence of actions proving parties behavior. Members may not be able to repudiate their actions or claiming for actions they have not committed and vice versa. Finally, sanctioning mechanisms need to be devised, to encourage agents to comply with community rules and to control subjects’ behavior during the community life. Several forms of sanctioning may be provided, from the temporary banning from the community to more sophisticated forms, that make use of “bonds” or “marginal accounts.”

In what follows, we briefly define an overall architectural framework for a virtual community, characterized by a flexible and dynamic structure where participants share resources in an efficient and decentralized way. Then, based on the model we depict, we focus on sanctioning functions and provide an insight on the possible forms of sanctions that may be adopted and their effectiveness.

A VIRTUAL COMMUNITY MODEL

We now give a model for a virtual community, overviewing the main components we have identified (Bertino, Ferrari, & Squicciarini, 2003), and a possible policy regulation system governing the community.

Virtual Community Components

A virtual community may be modeled as a tuple: $\langle S, AR, R, NS \rangle$, where:

- $S$ is the set of subjects belonging to the community. Each community member is qualified by means of digital credentials and can play different roles in a virtual community. Further, each member possesses the Membership credential, proving the community membership, and issued as the member join the community.
- $AR$ is the set of administrative roles played throughout the community. Each administrative role corresponds to specific functions that must be played by one or more community members for the correct functioning of the community. Administrative roles can be implemented by use of credentials, to be issued as a member joins the community by third trusted authorities or other reference members. Such credentials will be likely implemented using an XML-based language. The administrative roles considered in our model, which may be eventually extended if needed, are as follows:
  - **Resource Provider**: denoting subjects sharing their resources across the community or other community members.
  - **Resource Manager**: denoting subjects entitled to manage a resource by a resource provider.
  - **Witness**: denoting subjects entitled to monitor that a specific resource request by a subject to a service provider has been correctly processed according to the enforced policies. A witness must then be able to detect possible community laws violation as they occur in the processes it witnesses. Witnesses can also be in charge of exercising additional functions, for instance, they may also randomly control sharing processes that they do not directly witness.
  - **Community Guard**: denoting the members empowered to accept or refuse the joining of new members.

Functions such as community policies specification and normative state updates or resource credentials issuing are in charge of a set of community members, entitled by the administrative roles they are authorized to play, as defined in the description associated with the corresponding administrative role. Indeed, the whole description of rights and duties associated with each administrative role has to be clearly defined and published in the community repository.

- $R$ denotes the set of shared resources. Each resource in $R$ is uniquely identified. Additionally, for certain type of resources, such as computing resources, it may be necessary to describe each resource by means of a set of properties that can be exploited in the specification of the corresponding access control policies. For instance, a storage resource can be characterized by space availability, disk bandwidth, types of data that can store, mechanisms used for file transfer and backup. Like subjects, resource properties may be collected into credentials associated with the resources themselves. **Resource credentials** are issued by community guards when the corresponding resource is included into the set $R$ of shared resources, and they are stored at resource provider’s site. Resources in a community can be either local or community. Resources belonging to single members are called local resources, whereas resources belonging to