Integrated Framework for Authentication and Access Control in Peer to Peer Groups

No Author Given
No Institute Given

Abstract. Collaborative applications like video/audio conferencing, IP telephony, file sharing, collaborative work spaces, and multi-user games, having varied security requirements, require a secure and reliable group communication system to provide co-ordination among the processes. Peer to peer computing allows users to interact with each other and find and share resources without requiring a centralized server. This gives rise to the need of a secure group layer which integrates authentication, admission control, authorization, fine-grained access control and key management. Currently there are some integrated solutions for secure group communication, but very few allow for the development of trust in a dynamic fashion. We propose a generic integrated framework for secure group communication in decentralized peer to peer groups with a hybrid access control model for peers in groups requiring multi-level access control. Our approach is adaptive, flexible and scalable and integrates aspects of incremental trust, along with role-based and policy based access control. The access policy framework allows peers in a group to dynamically change their levels, as well as modify existing rules in the policy.

1 Introduction

Web based collaborative groups are becoming increasingly popular as peers with common interests form a network among themselves and automatically tend to create interest groups among each other, called communities. The group is governed by a set of rules that describe the conditions required to be part of the group.

Security in such dynamic collaborative groups is governed by membership control, authentication, access control and key management. Membership control and authentication is required to allow only authorized members to join the group. In the dynamic scenario where peers are constantly leaving and joining this becomes a difficult task. Another major challenge is access control since decisions need to be made based on collaborations from all peers and feedback mechanisms based on trust.

In the decentralized environment, peers in self-organising groups should have the right to collaboratively modify the access control policies governing their levels and the levels below them. Current solutions do not allow dynamic change of access levels or policies, with incremental building of trust during the communication. Nor do they allow dynamic authentication of participants who were previously part of the group and later wish to rejoin. In view of the varied security requirements for diverse peer to peer applications, there is a need for an integrated framework for secure communication in dynamic groups with no dependance on a centralized server. We propose such an integrated framework, which has an adaptive, flexible, dynamic and totally decentralized access control mechanism, integrated with authentication and dynamic rekeying.

2 Related Work

Security in collaborative groups is addressed by group membership, authentication, access control, and group key management. Distributed establishments typically involve peers that do not know each other and have never met before. This brings in the concept of
risk when peers perform transactions without knowing the reputation of those whom they are interacting with. This has precipitated work on trust and reputation mechanisms in peer-to-peer networks [5] [20] [18] [6]. Trust is a measure of how much a peer is willing to transact with another peer. Reputation [8] is one specific way of establishing trust.

Several efforts have been made towards securing group communication systems, for e.g Secure Spread [13], Antigone project [12] and Secure group layer SGL [14]. Secure Spread [13] is a secure group communication system that uses a fully distributed group key generation protocol, but it does not provide any authentication or group access control mechanisms and focusses primarily on LAN and interconnected LAN environments.

Antigone project [12] includes a flexible framework for secure group communication and utilizes a centralized member admission approach which is controlled by a session leader SL who interacts with an on-line trusted third party TTP in order to admit a new member. The TTP shares a symmetric key both with the SL and every potential new member. However Antigone is not designed for peer-to-peer networks.

Secure group layer SGL [14] is a secure group communication system aimed at WAN environments. It bundles a reliable group communication system, a group authorization and access control mechanism and a group key agreement protocol to provide a comprehensive and practical secure group communication platform. However the access control mechanism is not dynamic or scalable.

Some frameworks are focussed on peer to peer applications. Kim et al [1] [2] proposed an admission control framework which revolves around two basic elements, viz: a group charter which has well defined admission policies and a group authority which is an entity that can certify group admission. However their scheme lacks the attributes of peers and cannot simplify authorization in collaborative environments. Further access control has not been considered, all members have equal access rights, and neither does it integrate admission control with group key agreement.

3 Proposed Integrated Framework

In the decentralized and dynamic peer group scenario it is necessary to have an adaptive access control mechanism where peers have the right to collaboratively make access control decisions, modify these decisions and frame rules based on attributes as well as trust evolved in the group. We propose a hybrid access control framework which integrates policy based access control and trust based access control with multi-level access control.

We present here a flexible architecture framework for secure group communication in decentralized peer groups, based on our proposed access control framework. The architecture is suitable for applications that involve sharing of high value resources, e-commerce applications, as well as general collaborations where security is not a major issue. The access policy framework is flexible and allows peers to change their levels as well as change the rules for membership within an existing level.

3.1 Proposed Architecture

We consider a peer based model where every peer $P_i$ has a unique user identity $UUID_i$ associated with it. A group is a named set of peers or a subset of a community that is governed under a set of rules that describe the conditions required to be part of the group, and is formed based on a particular interest criterion. The dynamic membership of the group implies that no peer will be highly available. The challenges are rapid admission of
new members with appropriate access rights, dynamic elevation of access levels of existing members and dynamic revocation of access rights of leaving or defaulting members.

![Fig. 1. Integrated Framework](image)

Peers should be individually capable of performing the tasks of authentication, admission control, access control and key management. However the extent to which each peer should be capable of performing these tasks need not be uniform. A peer in a maximal role would be expected to have the following functional components:

- **Attribute Manager**: Responsible for storing the attributes and certificates of the peers. The Attribute Manager is also responsible for updating the certificates of the peers with the new rating.

- **Authentication Manager**: Verifies the validity of the identity and invokes the voting algorithm.

- **Trust Engine**: Responsible for calculating the trust values of each peer, based on responses from other peers. It thus has a calculation engine and a feedback engine associated with it.

- **Access Policy Manager**: Frames rules or policies based on attributes, behavior of peers and inputs from trust engine. It also checks the rules to allow members to join. It is called upon either by the Authentication Manager in case of a new member join, or the Updation Manager in case of an existing member level updation.

- **Updation Manager**: Responsible for checking the rating levels of peers after they have collected feedback from other peers and gives the input to the Access policy manager. It is also responsible for granting or revoking access rights to peers based on the dynamic policy.

- **Key Management System**: Invoked whenever a new peer joins or an existing peer’s access level is changed depending on the dynamic policies, and is responsible for computing the group key. These components interact as shown in the figure.

### 3.2 Model Overview

Our initial membership admission protocol is similar to the protocol proposed by Kim et al. and allows all peers to collaboratively decide whether a new user should be allowed
entry into the group and if so decide the hierarchy level or role in which he can join the
group. First time authentication is based on user identity (e.g. an X.509 credential), or a
self generated pseudo certificate and other attributes presented during initial admission
request phase. This is handled by the Authentication Manager and Attribute Manager.
If permitted to join a peer is given a signed membership certificate which serves as an
authentication token. For all practical purposes a new peer will be allowed to join a group
at the lowest level initially. The membership certificate contains a field which has the trust
level or rating of the member.

Subsequent per session authentication could be based on an authentication token re-
ceived in prior session and recognized by all peers. This would require inputs from the
Access Policy Manager and the Trust engine.

Once a member of the group, the access control policy could be dynamically changed
and the user could be switched from a low hierarchy level to a higher hierarchy level
depending on his performance in the group as well as the rating given to him by other
peers in the group. A rating of a peer can either be periodically updated by all existing
peers in the group or a peer can request for rating certificates from other peers in the
group with whom he has had transactions.

Rekeying algorithm would be invoked by the peer whose rating increases, so that he
could switch to a higher hierarchy. If a member who was previously part of the group and
has left, wishes to rejoin the group, then based on the rating token and credentials that
he possesses, he could easily rejoin without having to be subjected to the voting process,
or if he has a high rating i.e. a high trust level, then he may be permitted to join as a
trusted member even though the votes of remaining members are less than the threshold
i.e. 50 percent i.e the admission policy changes if the member is an old member.
The credentials provided by the user could have various levels of trust, that could be
incremental.

4 Working of Proposed Model

In dynamic peer groups the different cases needed to be supported are:

1. A New peer wishing to join an existing group
2. An existing peer wishing to have his level updated
3. A peer who was previously part of the group wishing to rejoin in a new session

Peers could also be dynamically leaving the group. We propose protocols to handle these
different cases of join and leave based on our integrated framework. The Notations used
in our protocols are:

- $P_{new}$ : New Peer
- $P_i$ : Existing Peer
- $SK_i$ : Private key of $i$
- $PK_i$ : Public key of $i$
- $Cert_i$ : Certificate of $i$ which contains the ID, Public key, Level/rating, Validity period.

4.1 Protocol for New Member Join

A new member wishing to join an existing group would have the following phases.
**Fig. 2. New Member Join**

**Group Initialization and Advertisement** In case of peer groups, it is essential that the initiator of the group should publish and advertise his group along with documents that specify the parameters of the group, such as group type, admission policies, group name, group members etc. The group advertisement should be periodically broadcast by the peers of the group.

**Admission Request** A new peer wishing to join a group would first search for an advertisement of a group that matches his requirements. He would then submit a signed request to any peer which would include his credentials that he obtains from a CA say X.509 certificates or self-generated certificates, along with a request for the role that he wishes to join in. Given that each peer has his own certificate which could be self signed or signed by a CA, a peer credential is created by hashing the concatenation of unique user ID UUID and public key fields and then signing this hash with the private key of the user and using this digital signature as the identity of the peer. This identity could be used as the peer’s credential in the messages.

\[
P_{\text{new}} \rightarrow P_i : \{ \text{JoinREQ} \}_{SK_{\text{new}}}, Cert_{\text{new}}
\]

where

\[
Cert_{\text{new}} = UUID_{\text{new}}, PK_{\text{new}}, Rating_{\text{new}}, \{ H[UUID||PK_{\text{new}}] \}_{SK_{\text{new}}}
\]

For a new user his Rating_{\text{new}} field will contain a single value signed by himself.

**Authentication** The peer receiving this signed request will obtain the identity of the requesting peer from the Certificate. If it is a signed certificate then the verification is easy. If however the Public Key pair is pseudo generated then the receiving peer will compute the hash of UUID and PK_{i} and tally this with received message. If the two hashes match then the user is authenticated and will be granted access permissions based on the access control policy. If the user’s credentials contain a rating field with a single entry he will be treated as a fresh user and the voting process will be invoked by broadcasting this join.
request to the other peers. The certificate of the new peer is co-signed by the broadcasting peer, so that further verification of ID is not required by other peers.

\[ P_i \rightarrow \text{All}P_n : \{\text{JoinREQ}\}_{SK_{\text{new}}}, \{\text{Cert}_{\text{new}}\}_{SK_i}, Votereq \]

**Voting and Authorization** The peers all verify the authenticity of the new peer from his credentials. The peers return the results of voting to Access Policy Manager of the peer who had initiated it.

\[ P_n \rightarrow P_i : \{Vote, Level\}_{SK_n} \]

**Access control** The Access Manager verifies the votes and if the votes are > 50% then the later then gives a signed membership token to the new peer and calls the rekeying algorithm. Since this is signed with the current group key which is unknown to the peer the later cannot modify it and forwards this directly to the Key Management System (KMS) for rekeying needed to join the group.

\[ P_i \rightarrow P_{\text{new}} : \{GC_{\text{new}}\}_{G_{\text{key}}} \]

The entry of the new peer is broadcast to all peers of the group. The membership token \(GC_{\text{new}}\) would contain details of the action granted to a joining peer, for e.g: join, invite, escort, attend or reject.

**Key Management** The Key Management component of the existing peer who receives the signed Group Membership certificate performs the group rekeying at the necessary level. TGDH [19] protocol can be used for computing the key.

### 4.2 Protocol for Existing Member Level Updation

Once a member of the group, a peer can periodically request the members of the group to rate him based on his performance and the trust level he has already acquired. Appropriate access privileges are granted to a peer based on a scoring system. A rating certificate can be used as a means of recommendation. This certificate would contain the original trust value of the peer along with the recommended rating value given by each peer. The recommendation would be signed by the recommending peer thus preventing a peer from being able to modify the recommendations/ratings given to him by other peers.

Each peer has a local Trust calculator which is able to compute the rating of every other peer. The rating certificate would also contain an expiry date to prevent the recommended peer from recycling good rating certificates beyond the specified period. When a certificate is about to expire, the peer can contact the recommending peer and get the validity of the certificate extended. Thus for each peer it has interacted with, the peer needs to keep a copy of the certificates it issued to that peer for validation purpose and for trust and contribution score updating. In addition a peer could maintain a revocation list of peers who are not to be trusted and periodically this information could be exchanged amongst peers. The fields in the rating certificate are Recommending peer’s identity, Recommended peer’s identity, Original trust value, Issuing date and time, Expiry date and time, Contribution score and Signature of recommending peer.
Request for Updation

\[ P_i \rightarrow P_j : \{\text{UpdateREQ}\}_{SK_i}, \text{Cert}_i \]

where \( \text{Cert}_i \) contains rating certificates from other peers. \( P_j \) computes the global rating value after verifying the authenticity of individual ratings. The Updation Manager interacts with the trust Engine to calculate the rating of the peer. It then forwards this request with rating score to the Policy Manager.

Access Control Access rights will be assigned based on a combination of the credentials, self rating and behavioral rating as well as rating given by other peers. Trust threshold, denoted as \( A_{ij} \) is a summation quantity. Any peer who has its overall trust value and overall contribution score equal to or greater than the corresponding thresholds, can get the corresponding hierarchial access right. The policy would be flexible so that it could be modified contributively above a certain level. Thus maybe peers at access level 3 could modify the policy rules for entry into that level. The following section gives the details of the algorithm used to calculate the rating.

Rating Algorithm For calculating the trust/reputation rating we use the concept proposed by Eigen Trust [9] with some modifications. We state that the factors on which reputation depends are Peer Feedback, Weighted Cost of transaction and Credibility of peer who is giving the rating.

Thus each peer has a local trust value, based on his initial credentials and his performance in the system, as well a global trust value which is based on the ratings provided to him by other peers.

Weighted Cost We introduce the concept of weighted cost to overcome the drawback of the eBay [21] reputation system where buyers and sellers can easily default on large orders after gaining a good reputation value by successfully completing small orders. We put an upper bound on transaction as \( \Theta \) and state that for all transactions whose cost or...
weight is < Θ the reputation is calculated normally but for every transaction with weight > Θ, the reputation value is multiplied by a constant which is a multiple of this threshold value. This would ensure that smaller transactions generate lower trust value than larger transactions.

Thus local rating or reputation index \( RI \) for a peer \( i \) is calculated by peer \( j \) as follows:

\[
RI_i = RI_j \times \sum T_{ij} \times Trans\_cost
\]

for transactions whose cost or weight is > Θ, where \( T_{ij} \) is the opinion peer \( j \) makes about peer \( i \) per based on transactions and behavior. The global rating of Peer \( i \) is then a summation of the local ratings computed by all the peers it interacts with. A peer cannot modify its trust and contribution rating even though it stores the rating locally in the form of certificates.

**Key management:** The necessary rekeying is done by the Key Management system. In order to ensure multiple levels of access privilege for group members, there can be separate key trees for users with same separate access privileges i.e each hierarchy of users would have a separate group key for encrypting their data. This can be done by calling the key agreement protocol separately at each hierarchical level. Thus each user would have to maintain different sets of keys and when a user switches from one level to another, he could call the rekeying algorithm to ensure that backward secrecy is maintained. We propose a key management graph similar to the one in [10]. However the rekeying algorithm is not a one way function controlled by a KDC, but is a variant of the TGDH algorithm.

### 4.3 Per-Session Authentication of Previous Member

Authentication of a peer is based on his credentials, authentication token received in earlier sessions, and/or rating granted to him in earlier session. The role assigned to him is based on his attributes and the rating. It would be the task of the access policy manager to check whether the old rating certificates have expired or not or whether, the members who had given the rating earlier are revoked or not.

### 4.4 Dynamic Leaving of Members

When a peer leaves a group, it may not be identified immediately. Peers may send a query message to find out when a particular peer last communicated. If the peer is still a current member of the group, response would be immediate. However if a certain threshold of members reply stating that the last communication was not very recent then the group may assume that this particular peer is no more a current member of the group. Periodic rekeying or batch rekeying could be another solution to tackle security threats from peers who leave without informing.

### 5 Access Decision Policy

A major contribution of our work is that the access policy is totally dynamic. The Functionality of a peer in a group depends upon the role that the peer wants to play in the group. We identify the following roles:

1. **Member peer** A peer in this role participates in the activities of the group like gaming, conferencing, file transfer etc, but does not contribute to the admission of new peers, nor updation of levels of existing peers. Thus this peer need not store certificates of every other peer nor have the components like Updation Manager, and need not invoke voting either.
2. **Admission Control Peer** A peer with this role would participate in the voting algorithm, and would therefore store public keys of every other peer. However it need not store the updated ratings.

3. **Maximal role peer** A peer in this role would have all the functional components and would participate in updation levels of existing peers also.

The role of a peer is independent of the level of the peer in the group. The access policy would decide the role a peer assumes, based on the request of the peer and his credentials as well as rating calculated by Trust engine.

**Dynamism in Policy**

The policy can be dynamic at each level. Rules can be modified by the peers themselves at a certain level. For example in a multi-player gaming application, a rule could initially state that players need to have a rating of 8 and > 70 per cent votes to play at level 3 say. However suppose all players at level 3 have accumulated 200 points then a new level could be introduced where only players with > 400 points could get updated. The group size could also be a factor for determining the hierarchy levels permitted. Different hierarchial levels in a group thus have different policies for implementation. We define a Policy language framework to handle this dynamism.

**Policy Language**

The language has different components:

- Role Sets RS: This comprises of the different roles permitted.
- Group Hierarchy GH:
- Service Set SRVC

A JOIN_REQ or an UPDATE_REQ is defined as a triple < role, level, srv > where role ∈ RS, level ∈ GH and srv ∈ SRVC. Based on the join or update request, the system determines the applicable access policy for the requested service. The access policy for a role service pair is a set of clauses consisting of multiple access conditions. We use attribute-based credential specification. There is no reliance on X.509 identity-based certificates to encode user authentication information. The authentication credential comprises of self signed user attributes which are used for role assignment. The credential specification in our framework facilitates a combination of rule-based role assignment and role-based authorization. Thus roles are of two types: Attribute-Roles and Group Roles. Attribute Roles would correspond to role the peer is assigned in the group based on his attributes and rating i.e in case of A University it could be role of Professor or student or Director. Whereas group-role corresponds to the functionality of the peer in the group, which the peer could choose at the time of joining and could modify later while in the group.

6 **Implementation of Secure Multi-Chat**

We implemented a prototype chat application based on peer to peer framework, where all the system components and processes described earlier have been implemented. For this sample application the components of our policy language were as follows:

\{RS\} = \{Director, Professor, T.A, Student\}
\{GH\} = \{level 1, level 2, level 3\}
\{SRVC\} = \{message\_send, message\_receive\}

The group roles are member, admission control peer and level control peer.
Technologies used

Java programming language was used for implementation of all components. We used JXTA as the base platform for application development to demonstrate how a secure group layer which integrates authentication, admission control, authorization, fine-grained access control and key management can be created to achieve secure group communication.

**JXTA** JXTA uses a small number of protocols, is easy to implement and integrate into P2P services and applications. It is independent of transport protocols and can be implemented on top of TCP/IP. The main components in a JXTA network are: Peers and peer groups, Messages, Pipes, Services and applications, Advertisements. A peer group forms a boundary that prevents non authorized users from accessing the group. JXTA divides software into three layers:

- JXTA core - handles peer discovery and monitoring
- JXTA services - Generic services like files sharing and indexing
- JXTA application layer is reserved by application developed by JXTA community.

Fig. 4. JXTA Framework

**XML** Currently we have used XML to specify set of rules for policy language framework, as it provides a customizable and extensible framework to represent messages. A sample rule is shown here.

```xml
<?xml version = "1.0" encoding = "UTF-8" ?>
<rules>
  <rule>
    <requestname = "join">permission = "grant"</requestname>
  </rule>
  <rule>
    <requestname = "update">
      <newlevel id = "1">
        <permission = "grant">
          <condition>
            <parametername = "Rating">minbound = "1"</parametername>
            <parametername = "vote<bound">minbound = "50"</parametername>
          </condition>
        </newlevel>
        <newlevel id = "2">
          <parametername = "rating">minbound = "8"</parametername>
        </newlevel>
      </newlevel>
    </requestname>
  </rule>
</rules>
```

Fig. 4. JXTA Framework
We have analyzed two possible approaches and have developed test applications for both.

1. Central Server for Authentication: When a peer instance is initiated it registers itself to central server by proving its possession of public key which is then stored on central server. Central server acts as a trusted third party and gives new peer a X.509 certificate signed by him. For verifying his identity, other peers contact the central server to access his public key and then send messages encrypted with public key of peer.

2. Trust Based Peer to Peer communication: Here the system works in a purely distributed manner. When a new peer joins a group after proper authentication it broadcasts its public key to all other members of the group. Every peer thus can store the public key of every other peer. Once other peer gets his public key, his identity is bound to that public key.

After successfully joining the group, peer membership can be controlled by feedback mechanism. Currently our implementation is such that peer himself can only initiate his level updation request but it is easy to extend it such that other peers can initiate level updation for fellow group members. Peers falling below some threshold may be ejected from the group.

7 Conclusion

Currently there are some integrated solutions for secure group communication over wide area networks, but very few allow the development of trust and switching of users between hierarchial levels in an incremental fashion. We have modeled an integrated framework for decentralized groups, which will allow us to implement secure communication between different peers using admission and trust based access control along with key management. We propose a dynamic access control policy which is integrated with trust based access control and permits peers to collaboratively frame, and modify policies at various levels. The policy also permits peers to update their access rights within a group. Idea of per session authentication is also proposed which depends on the incremental trust factor and eliminates the need of the voting process. The access control policies can be dynamically changed by the members of the group based on this incremental trust. We have successfully implemented a prototype chat application of our integrated framework based on JXTA.

References

7. Thomas Repantis, Vana Kalogeraki: Decentralized Trust Management for AdHoc Peer-to-Peer Networks, MPAC, November 27-December 1, ACM 2006