Secure Admission Control in Peer Groups on the Internet

Yongdae Kim
Department of Computer Science and Engineering,
University of Minnesota, Twin Cities

Abstract. Security in peer groups is challenging due to lack of a centralized authority, and due to varied security requirements of its applications. Significant work has been done to solve the security issues of peer groups such as key management and anonymity. However, admission control, an important prerequisite for peer group security is not addressed yet (or assumed), which is extremely challenging as the decision to admit a prospective member to the group has to be collectively made by the current group members. This project aims to provide secure and efficient admission control protocols for group communication system. During the course of this project we intend to design schemes to provide admission control, publish these schemes, and develop a suite of mechanisms that will address the requirements of different peer group applications, such as file sharing, group communication system, and ad-hoc networks.

1 Present Status of Knowledge

1.1 Introduction

A peer-peer network is not controlled by a centralized server and each node in the network has equivalent capabilities and responsibilities. The lack of a centralized entity poses a challenge to complement security with these systems. In a network with centralized manager (client/server architecture) most of the security mechanism such as admission control, key management are performed by the manager itself. For example, in our university the system administrator decides which user to add to the system, i.e., the administrator performs the admission control tasks. However, in peer group due to absence of such a centralized entity, these decisions have to be made by the current group members themselves. The group members should communicate securely and collectively decide whether to accept prospective member to the group. While providing admission control, a number of problems could be faced, such as one or more group members could be malicious, there might not be adequate group members available to reach a decision, or an attacker might forge the identity of one the legitimate group members. Furthermore, the dynamic nature (frequent leaving and joining of members) of the group aggravates the problem. As evidence from the prior work suggests, peer group key management, it is very hard to design multi-party, multi-round protocols that are – at the same time – secure, efficient and robust [17, 12, 1].

The recent proliferation of group-oriented applications, such as IP telephony, video/audio conferencing, file sharing, collaborative workspaces, multi-user games, wireless ad hoc networks, have triggered the need for specialized group security services and mechanisms. These applications have diverse group settings and have different security requirements, such as conferencing require synchronous operation while Gnutella-style [8] file sharing operates in disconnected asynchronous manner. Communication models vary as well from one-to-many or few-to-many (e.g., GPS [7]) to
any-to-any peer groups (e.g., Gnutella). These applications are not only restricted to the Internet, but are also important for Army\(^1\) operations.

One related work [14] has been done in the context of large multicast-style groups with one or few senders and a multitude of receivers. In this setting, it is natural to assume or impose a centralized authority (be it the sender or an on-line trusted third party) that can perform many security chores e.g., key management, admission/access control and member authentication. Due to the presence of this authority developing security policies and mechanisms [11, 10, 14] for these systems is relatively easy. However, currently there are no known solutions that provide admission control in peer-peer groups.

My goal is to start by developing a framework for peer group admission control and, in doing so, analyze and propose a set of cryptographic mechanisms suitable for different peer groups. These protocols will be implemented on cryptographic libraries, and further integrated with peer group applications.

### 1.2 Related Work

The Antigone [14] project is the closest related work. Antigone includes a flexible framework for secure group communication and utilizes a centralized admission approach geared primarily towards secure multicast scenarios. Antigone offers flexible mechanisms for defining policies about membership, application messages, and other aspects. However, it is important to note that Antigone is not designed for peer-to-peer networks.

In Antigone, member admission is mediated by a Session Leader (SL), which interacts with the on-line TTP (Trusted Third Party) in order to admit a new member. The TTP shares a symmetric key both with the SL and every potential new member. Everyone is expected to know in advance the identity of the SL.

There have been other efforts to develop standard frameworks for creating peer-to-peer applications, for example, JXTA [18] by SUN and Peer-to-Peer Trusted Library (PtPTL), also an open-source project sponsored by INTEL [19]. JXTA uses SSL/TLS as its security mechanism while PtPTL supports a wide variety of options. There is also an active working group within the IETF (P2PWG) [20] created with the charter to facilitate and accelerate the advancement of common mechanisms peer-to-peer computing. One of the documents produced by P2PWG is an Internet draft addressing the security requirements for peer-to-peer applications. In this draft *authorization* (admission control) is identified as one of the major issues.

### 1.3 PI’s Related Work

During my doctoral research I took active part in designing new group key management protocols for peer groups such as, TGDH (Tree-based Group Diffie-Hellman) [12], and STR (Skinny TRee) [13]. TGDH provides computational efficiency while enjoying provable security, where as STR optimizes the communication cost. These protocols have been implemented [4] on OpenSSL [16] cryptographic library and integrated [1, 2] with Spread group communication system [3]. However, these protocols focused on key management while assuming the existence of admission control mechanism. With this experience in hand I am interested in proceeding further to designing protocols for ensuring admission control in peer groups.

\(^1\) NTDR (Near Term Digital Radio) is an ad-hoc network in use by the US Army.
2 Plan of Work

2.1 Overview of the Proposed Approach

Various applications have different group characteristics and different security requirements. To begin with, different applications will be surveyed to precisely categorize groups depending on their requirements and characteristics. Based on these categories different group charters will be defined.

Our preliminary research introduces basic elements of the admission control system explained below.

- **Group Charter**: Any peer group must have well defined policies and procedures for admitting new members. *Group Charter* is an electronic document codifying admission rules that a prospective member should satisfy in order to gain membership of the group.

- **Group Charter Certification Authority (GCCA) and Group Charter Certificate (GCC)**: The prospective group member must be able to verify if the group charter belongs to the group that he/she intends to join. Therefore, a group charter must have its *Group Charter Certificate (GCC)* signed by *Group Charter Certification Authority (GCCA)*. By verifying this GCC the prospective member can confirm that the group he/she intends to join is the authentic group and no one else is forging the identity of that group.

- **Group Authority (GAUTH) and Group Membership Certificate (GMC)**: *GAUTH* renders membership decisions and issues a *GMC* to every member of his group. Members of a group can verify whether an individual is his peer group member by verifying the GMC. A GAUTH may serve more than one group. Examples of GAUTH include an independent Certification Authority (CA) or its delegate, the group itself, and the group founder.

Figure 1 gives an overview of the preliminary admission control mechanism:

1. In the first step a group charter is created.
2. Second step depicts the interaction between a prospective member and the group. The prospective member sends a joining request to the group. As a result of this request the prospective member receives the charter of that group.
3. The third step is the crucial stage of group admission, which can vary widely among different groups. The main focus of this project will be dedicated precisely to the exploration of this peer group admission processes.
4. In the forth step, the prospective member provides the decision from group admission process to GAUTH, who then checks that admission requirements are indeed satisfied and, if so, issues a Group Membership Certificate.
5. In the last step, the new member joins the group by showing its Group Membership Certificate to other members.
2.2 Design of admission control protocols

No protocol is optimal in all settings. Several security protocols will be developed to satisfy different group characteristics. Usually, cryptographic protocols are expensive and in our environment these protocols might require use of digital signatures, which are very expensive. Therefore, our attempt will be focused to build cryptographic protocols that are efficient and scalable.

Some of the mechanisms useful in our proposed project are akin to limited forms of voting. Electronic voting schemes have been extensively studied starting with the seminal work of Benaloh [5]. Most approaches are based on mix-nets, homomorphic encryption [6] or blind signatures [15]. Usually, voting schemes must satisfy many different requirements, such as privacy, anonymity, un-coerceability, and receipt-freeness [9]. However, the framework I will develop for this project, does not deal with secret-ballot election. Instead, I will focus on mechanisms for registering consensus about a particular event type (new member admission).
Proof of security is central in cryptographic protocols. Concrete proofs that will show that the securities of designed protocols are as strong as well known hard mathematical problems will be provided.

2.3 Protocol implementation and evaluation

Based on cryptographic libraries such as OpenSSL, complete implementation of protocols will be provided. We will compare the performance of implementations of different protocols. The final results will be used as a central building block to develop new secure peer-to-peer file sharing/computing systems, ad hoc networks, and secure group communication systems.

2.4 Expected Results

By the end of the project term we would have published, designed, and implemented reliable and efficient admission control protocols. Using these results as the core I will pursue for external funding from NSF, DARPA, and few companies. I am specifically looking forward to apply for NSF Career Proposal on “Peer-to-peer network security”. Other proposal I am planning on based on the result from this project include ”Security of Ad-hoc Networks”, an attractive research issues for military and networking community. The results of this work (peer group admission control) will play an important role for both of these proposals.

3 Budget Justification

Research Assistant (RA) is crucial for getting preliminary results that are needed to submit long-term strong proposals described above. Main duties of the RA will be developing new admission control mechanisms, their implementation and comparison of their performance. Currently, I do not have any funds available to support this project.

4 Need Justification

I have used part of my departmental startup funds to buy desktop/laptop computers. However, I need to set up a security lab for research and educational purposes, which requires at least 6 to 7 personal computers as well as network equipments. This lab will be used for implementing and testing secure peer-to-peer file sharing systems, and for demonstrating system vulnerabilities and defending tools to students, which cannot be taught in an common labs. Hence I would not need additional funding for my equipment. Remaining portion of my startup funds will be used for my summer salary, fringe, and travel expenses for participating in conferences and visiting funding agencies. Funds from Internet Security Co. Ltd. will be used to support visiting scholars living expenses and fringe.

Currently, I am applying two NSF grants which are listed in Insert # 3.

5 Word Count

1967 words
References