Available online at www.sciencedirect.com
ScienceDirect
Future Generation Computer Systems 23 (2007) 776–786
FGCS FUTURE GENERATION COMPUTER SYSTEMS
www.elsevier.com/locate/fgcs

Dual-Level Key Management for secure grid communication in dynamic and hierarchical groups

Xukai Zou, Yuan-Shun Dai*, Xiang Ran

Department of Computer and Information Science, Purdue University School of Science, Indiana University, Purdue University, Indianapolis, 46202, USA

Received 31 March 2006; received in revised form 26 September 2006; accepted 11 December 2006
Available online 22 December 2006

Abstract

Grid computing is a newly developed technology for complex systems with large-scale resource sharing and multi-institutional collaboration. The prominent feature of grid computing is the collaboration of multiple entities to perform collaborative tasks that rely on two fundamental functions: communication and resource sharing. Since the Internet is not security-oriented by design, there exist various attacks, in particular malicious internal and external users. Securing grid communication and controlling access to shared resources in a fine-tuned manner are important issues for grid services. This paper proposes an elegant Dual-Level Key Management (DLKM) mechanism using an innovative concept/construction of Access Control Polynomial (ACP) and one-way functions. The first level provides a flexible and secure group communication technology while the second level offers hierarchical access control. Complexity analysis and Simulation demonstrate the efficiency and effectiveness of the proposed DLKM in both computational grid and data grid. An example is illustrated.

Keywords: Grid computing; Grid security; Group communication; Hierarchical access control; Key management

1. Introduction

Grid computing [14] is a recently emerging technology focusing on large-scale resource sharing and multi-institutional collaboration, see e.g. [19,11,17,15,3]. One of the most important issues in the Grid is security [20,25]. The Internet and networks are not security-oriented by design. Numerous hackers constantly explore security holes existing in hardware, software, processes, or systems to launch various attacks. There are two types of attacks: passive and active [4,18,27]. Passive attackers steal useful information by eavesdropping and/or performing traffic analysis. Active attacks interfere with legal communication and are typically in the forms of masquerading, replaying, modification, and denial of services (DOS). The countermeasures against attacks utilize encryption/decryption for confidentiality, message authentication code for integrity, digital signature for authentication, undeniable digital signature for non-repudiation, access control for authorization, and intrusion detection/defence for availability/DOS [24]. Most of these technologies are based on cryptography in which keys and key management are the most important but complicated issues.

The Internet-based grid computing encounters the same attacks and involves all the security requirements discussed above. Furthermore, grid computing systems are group-oriented, including a large number of users and shared resources. They are also complex, dynamic, distributed and heterogeneous. As a result, the attacks to grid systems may become more serious and to defend them becomes more difficult. For example, due to the distributed and heterogeneous features of grid computing systems, centralized authentication is generally unavailable and multiple-site co-authentication is difficult to implement. Thus, the Single-Sign-On [16] authentication comes into play. For another example, grid computing is aimed at providing collaborative services. These services are featured by two important functions: group-oriented communication and information sharing/exchange [30]. As long as communication and information exchange are conducted over the Internet, communication messages should be encrypted with a common key for confidentiality. However,

Abbreviations: KMS: Key Management Server, DLKM: Dual-Level Key Management, CA: Central Authenticator, RMS: Resource Management System, ACP: Access Control Polynomial, HAC: Hierarchical Access Control.

* Corresponding author. Tel.: +1 317 274 3473.
E-mail address: ydai@cs.iupui.edu (Y.-S. Dai).

0167-739X/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.future.2006.12.004

Notations

SID_i	Every valid user/machine is assigned a permanent secret key SID_i
z	A random integer which is changed and made public every time
$A(x)$	Access Control Polynomial (ACP)
$P(x)$	Public polynomial sent to users for key distribution, $P(x) = A(x) + K$
P	The system prime used for modular computation
U_i	A group member in a certain group
v_j	A certain vertex in the second level hierarchy
$\hat{k}_i$	A secret group key
k_i	A private group key
$f(x, y)$	The public one-way hash function
ID_i	A unique public identity assigned to each vertex in the second level hierarchy
m	The number of users in a certain node
n	The number of vertices in the hierarchy structure
$p_{i,j}$	The public edge value on the edge from v_i to v_j
%	Modular operation

due to the high dynamic nature of grid computing, how to update group key(s) efficiently and effectively becomes a challenging problem. As for resources sharing among different nodes/organizations in the grid, every participating node would like to offer its resources to be used by other nodes. However this sharing must be in a controllable and fine-tuned manner. Thus, security is of great concern to grid computing and the solutions for different security problems need to be studied and designed in a holistic manner.

To solve the above critical security problems that set obstacle for the further deployment and applications of grid computing, this paper presents a novel Dual-Level Key Management (DLKM) scheme that is appropriate to grid context. At the first level, Dynamic Groups and Key Distribution are the focus, where a novel and efficient scheme using Polynomial as public information to hide a group key is presented. These dynamic and independent polynomials enable secret information to be distributed to arbitrary and dynamic user groups. At the same time, they are able to defend against different attacks including collusion of malicious internal users. The second level is aimed at solving Hierarchical Access Control (HAC) and makes use of a new hybrid scheme. The HAC scheme allows a member to derive the key of any of its descendants efficiently, but the reverse is prohibited. Moreover, the first-level is the basis of the second level and helps accurately distribute secret information to any particular node in the second level hierarchy. One important feature with DLKM is that it allows users, processes, and resources to freely enter or leave a grid system without jeopardizing required security. Thus, this technology could help promote grid computing to a new era, in which security-critical services offered on the grid is enabled.

The rest of the paper is organized as follows. Section 2 describes grid computing and presents a novel Dual-Level Key Management (DLKM) System for grid computing and services. Section 3 analyzes security-related measures, robustness and complexity of the proposed DLKM. In Section 4, DLKM is implemented into a grid service, where a numerical example is illustrated and some performance measures from a real grid computing case are depicted. Section 5 briefly discusses the relation of the proposed DLKM with the grid security architecture and with the existing SGC and HAC techniques.

2. Secure grid communication

2.1. Grid computing and security challenges

The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations [17]. The sharing that we are concerned with is not primarily file exchange but rather direct access to computers, software, data, and other resources. This is required by a range of collaborative problem-solving and resource-brokering strategies emerging in industry and science.

However, there is a significant security challenge on the Grid resource sharing, that is, the data privacy to others outside the group of shared resources. When those resources involved in a task communicate with one another, the task owner may not want other untrusted/unauthorized people to know the communication data. Unfortunately, the Internet contains many malicious factors (such as hackers, virus) especially for the grid. One cannot expect everybody on the Internet to be trustworthy. Thus, the information transmitted among remote sites/resources should be encrypted.

Point-to-point cryptographic schemes have been well developed such as RSA, but Grid computing is featured by collaboration among a group of users and their sharing of computational or data resources. Therefore, it is very inefficient to unicast common information one to another, but multicasting shared information among the group is much more efficient. The multicast information needs to be encrypted (by a group key) so that others cannot understand the information even though they might intercept it. Groups can be dynamic, because users, resources or sites can attend or leave a group at any time, and groups are organized in real-time according to the availability and workload of various resources. In addition, one member may belong to multiple groups simultaneously. Thus, the follow-up challenges emerge as how to authenticate the group members, how to distribute the group key to the group members and how to update the group key securely and efficiently when the group members change.

Another important feature of grid computing is Hierarchical Access Control (HAC). This scenario is mainly related to the management in grid computing. The grid environment consists of resources and users (the number of users and resources can vary from a few to millions). There are different relations among users and resources. Some special members/nodes have been authorized to monitor the tasks of certain resources or to check the communication among some grid resources, such as system administrators, service/resource providers, Resource Management Systems (RMS) and so on. Hence, they should