Available online at www.sciencedirect.com
ScienceDirect
Future Generation Computer Systems 23 (2007) 774–775
FGCS
FUTURE GENERATION COMPUTER SYSTEMS
www.elsevier.com/locate/fgcs

Editorial

Special section: Security on grids and distributed systems

María S. Pérez[a,*], Bin Xiao[b]

[a] *Universidad Politécnica de Madrid, Madrid, Spain*
[b] *Hong Kong Polytechnic University, China*

Received 31 January 2007; accepted 2 February 2007
Available online 8 February 2007

Future Generation Computer Systems, the International Journal of Grid Computing: Theory, Methods and Applications is focused on the research performed in the grid and distributed computing systems. Grid and distributed systems provide global sharing of computational resources through high-speed networks, allowing applications to significantly improve their performance. To ensure trustworthy resource sharing and access control, the security issue deserves more attention and analysis in the wired and/or wireless grid and distributed environments.

Providing security poses a great challenge in the grid and distributed systems. The main challenge of grid computing is the complete integration of heterogeneous computing systems and data resources with the aim of offering a global computing space. The achievement of this goal is involving revolutionary changes in the field of computation and, more concretely, in the security aspect, because it enables resource sharing across networks. The challenge of distributed systems comes from security threats, which exploit the weakness of protocols as well as operating systems, and also extended to attack applications such as database systems, file sharing systems, real-time and multimedia online applications. The attacks, including distributed denial of service, viruses, buffer overflows and worms, are causing more economic damage and attracting more attention. To achieve a secured distributed system in future networks and applications, the cyber-security aspects, namely, data confidentiality, authentication, nonrepudiation, data integrity, privacy, access control, key management and availability, should be fully addressed.

The purpose of this special section is to show new and emerging frameworks, protocols and systems for grid and distributed environments, which aim to provide trustworthy and secure services in wired or wireless networks. Five papers have been finally selected to provide a suitable overview of topics, such as key management, access control, trusted frameworks and grid systems. The acceptance rate has been approximately 30%.

Xukai Zou, Yuanshun Dai et al. propose an elegant dual-level key management (DLKM) mechanism using an innovative concept/construction of an access control polynomial (ACP) and one-way functions. This dual-level key management mechanism offers securing grid communication and controlling access to shared resources in a fine-tuned manner for grid services. The dual-level key is implemented with the first level providing 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 and data grids.

Lijun Liao and Mark Manulis also address the key management for establishing shared keys in mobile ad hoc groups using a contributory group key agreement (CGKA), which allows group members to compute the group key on the basis of their individual contributions providing a verifiable trust relationship between participants. It is novel to apply the CGKA protocol in mobile ad hoc networks, which shows an optimal trade-off between communication and computation efficiency.

Song Fu and Cheng-Zhong Xu discuss new challenges to resource access control where resource sharing in the grid coalition environment creates certain temporal and spatial requirements for access by mobile entities. The access control is formalized through a shared resource access language, SRAL, to model the behaviours of mobile codes. SRAL is structured and compositional so that the program of a mobile code can be constructed recursively from primitive accesses. In addition, a constraint language, SRAC, is defined to specify spatial

* Corresponding address: DATSI, Facultad de Informatica, Campus de MontegancedoDespacho 4204, 28660 Madrid, Spain. Tel.: +34 91 336 73 80; fax: +34 91 336 73 76.
E-mail addresses: mperez@fi.upm.es (M.S. Pérez), csbxiao@comp.polyu.edu.hk (B. Xiao).

0167-739X/$ - see front matter
doi:10.1016/j.future.2007.02.001

constraints for shared resource accesses. The access control model, with proved concept and technical feasibility, has been implemented in a mobile agent system, which emulates mobile execution in grids by software agents.

Mais Nijim, Ziliang Zong and Xiao Qin present a quality of security framework or StReD for storage resources in data grids. The framework leverages the adaptor to dynamically control quality of security for disk requests, thereby achieving good trade-offs between security and storage system throughput. The framework is able to dynamically adjust quality of security to meet the flexible security needs of complex data-intensive applications. Experimental results based on a simulated grid with storage resources show that the proposed framework is capable of significantly improving the quality of security and guaranteeing desired response times of disk requests.

Jinpeng Huai, Yunhao Liu et al. describe an implemented system CROWN Grid, and present ROST, an original scheme of Remote and hOt Service deployment with Trustworthiness. By dynamically updating runtime environment configurations, ROST avoids restarting the runtime system during deployment. Moreover, the incorporated trust negotiation mechanism in ROST can greatly increase flexibility and security of CROWN Grid. ROST has been successfully implemented, showing that ROST is viable and significantly improves the service efficiency and quality of CROWN. The wide deployment of ROST would also benefit other grid systems.

Finally, the guest editors wish to thank all the people that have collaborated with us in order to make this special section successful. Thanks to the editor-in-chief, Peter Sloot, for his invitation to organize this special section and his accessibility; to the reviewers, for their on-time reviews; to the editorial staff, for their excellent work, and to the authors, for their valuable papers.

María S. Pérez received the MS degree in Computer Science in 1998 at the Universidad Politecnica de Madrid, the Ph.D. degree in Computer Science in 2003 and the Extraordinary Ph.D. Award at the same university. From 1998 she has been an Associate Professor at the Universidad Politecnica de Madrid. Her research interests include high-performance and grid computing, parallel I/O, autonomic computing and data mining. She is coauthor of four books, four book chapters and she has published more than 60 articles in journals and conferences. She has been involved in the organization of several grid related workshops and conferences, and she has edited several proceedings books and special issues. Currently she is involved in the Ontogrid European project (FP6-511513), whose main goal is to provide a reference semantic grid architecture. She is also a member of the editorial board of the journal of Autonomic and Trusted Computing.

Bin Xiao received B.Sc. and M.Sc. degrees in Electronic Engineering from Fudan University, China, in 1997 and 2000 respectively and a Ph.D. degree from University of Texas at Dallas, USA, in 2003, in Computer Science. Since 2003, he has been an Assistant Professor in the Department of Computing of Hong Kong Polytechnic University, Hong Kong. His research interests include communication and security in computer networks, peer-to-peer networks, grid computing, wireless ad hoc and sensor networks, He is the editor of two books and has published more than 30 technical papers in journals and conferences. He has been involved in the organization of several security related workshops and conferences, such as SNDS05, SecUbiq05, SNDS06 and ATC07.