

P.O.Box 8718, Beijing 100080, China	Journal of Software, Oct. 2004,15(10):1528-1537
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2004 by The Editorial Department of Journal of Software

面向XML文档的细粒度强制访问控制模型

李 澜, 何永忠, 冯登国

[Full-Text PDF](#) [Submission](#) [Back](#)

李 澜, 何永忠, 冯登国

(中国科学院 软件研究所 信息安全国家重点实验室,北京 100080)

作者简介: 李澜(1977—),男,江西新干人,博士生,主要研究领域为系统与网络安全;何永忠(1969—),男,博士生,主要研究领域为系统安全,密码学;冯登国(1965—),男,博士,研究员,博士生导师,主要研究领域为密码学,信息安全.

联系人: 李 澜 Phn: +86-10-62528254 ext 803, E-mail: lilan@is.iscas.ac.cn, http://www.is.iscas.ac.cn

Received 2003-09-11; Accepted 2003-11-11

Abstract

Information stored in XML documents should be protected by access control policy. Current access control models for XML documents are all based on DAC (discretionary access control) or RBAC (role-based access control). High security system uses MAC (mandatory access control) to secure information in system. XML document model is extended to include label information in this paper, and some rules that the extended model has to satisfy with are presented. Fine-grained MAC model for XML documents is described in detail by discussing four operations on XML documents. The fine-grained MAC model is based on XML schema, and its finest granularity of access control is element or attribute. The architecture and some mechanisms used to implement the fine-grained MAC model are discussed too.

Li L, He YZ, Feng DG. A fine-grained mandatory access control model for XML documents. *Journal of Software*, 2004,15(10):1528~1537.

<http://www.jos.org.cn/1000-9825/15/1528.htm>

摘要

XML文档存放的信息需要受到访问控制策略的保护.现有的一些面向XML文档的访问控制模型都是基于自主访问控制策略或基于角色的访问控制.高安全等级系统需要强制访问控制来保证系统内信息的安全.首先扩展了XML文档模型使其包含标签信息,并给出了扩展后的文档模型需要满足的规则.然后通过讨论XML文档上的4种操作,描述了面向XML文档的细粒度强制访问控制模型的详细内容.该模型基于XML模式技术,它的控制粒度可以达到文档中的元素或者属性.最后讨论了该模型的体系结构和一些实现机制.

基金项目: Supported by the National Natural Science Foundation of China under Grant Nos.60025205, 60273027 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035802 (国家重点基础研究发展规划(973)); the National High-Tech Research and Development Plan of China under Grant No.2002AA141080 (国家高技术研究发展计划(863))

References:

- [1] World Wide Web Consortium (W3C), Extensible Markup Language (XML) 1.0. 2000. <http://www.w3.org/TR/REC-xml>
- [2] Damiani E, Vimercati SDC, Paraboschi S, Samarati P. A fine-grained access control system for XML documents. *ACM TISSEC*, 2002,5(2):169~202.
- [3] World Wide Web Consortium (W3C), XML Schema Part 0: Primer. 2001. <http://www.w3.org/TR/xmlschema-0>
- [4] World Wide Web Consortium (W3C), XML Schema Part 1: Structures. 2001. <http://www.w3.org/TR/xmlschema-1>
- [5] World Wide Web Consortium (W3C), XML Schema Part 2: Datatypes. 2001. <http://www.w3.org/TR/xmlschema-2>

- [6] Damiani E, Vimercati SDC, Paraboschi S, Samarati P. Design and implementation of access control processor for XML documents. *Computer Network*, 2000,33(1-6):59~75.
- [7] Bertino E, Castano S, Ferrari E, Mesiti M. Specifying and enforcing access control policies for XML document sources. *World Wide Web*, 2000,3(3):139~151.
- [8] Beritino E, Castano S, Ferrai E. Securing XML documents with Author-x. *IEEE Internet Computing*, 2001,5(3):21~31.
- [9] Chandramouli R. Application of XML tools for enterprise-wide RBAC implementation tasks. In: SIGSAC ed. *Proc. of the 5th ACM Workshop on Role-Based Access Control*, Berlin: ACM Press, 2000. 11~18.
- [10] Hitchens M, Varadharajan V. RBAC for XML document stores. In: Qing SH, Okamoto T, Zhou JY, eds. *Proc. of the Int'l Conf. on Information and Communications Security. Lecture Notes in Computer Science 2229*, Springer-Verlag, 2001. 131~143.
- [11] Vuong NN, Smith G, Deng Y. Managing security policies in a distributed environment using eXtensible markup language (XML). In: SIGAPP ed. *Proc. of the 2001 ACM symposium on Applied computing*. Las Vegas: ACM Press, 2001. 405~411.
- [12] Fu HY, Li H, Wang YM. Research on XML access control technologies. *Net Security Technologies and Applications*, 2002,9: 17~20 (in Chinese with English abstract).
- [13] Zhao X, Huai JP. XML-Based multi-granularity access control system. *Computer Engineering and Applications*, 2002,38(21): 155~159 (in Chinese with English abstract).
- [14] Zhang XW, Park J, Sandhu R. Schema based XML security: RBAC approach. Technical Report, IFIP WG 11.3, 2003.
- [15] Osborn S, Sandhu R, Munawer Q. Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM TISSEC*, 2000,3(2):85~106.
- [16] Bell DE, LaPadula LJ. Bell-LaPadula model for secure computer systems. Technical Report, 1976.
- [17] World Wide Web Consortium (W3C), XML Path Language (XPath). 2002. <http://www.w3.org/TR/xpath20>

附中文参考文献:

- [12] 傅海英,李晖,王育民.XML访问控制技术研究.网络安全技术与应用,2002,9:17~20.
- [13] 赵遐,怀进鹏.基于XML的多粒度访问控制系统.计算机工程与应用,2002,38(21):155~159.