P.O.Box 8718, Beijing 100080, China	Journal of Software, Oct. 2005,16(10):1774-1783
E-mail: jos@iscas.ac.cn	ISSN 1000-9825, CODEN RUXUEW, CN 11-2560/TP
http://www.jos.org.cn	Copyright © 2005 by The Editorial Department of *Journal of Software*

多级安全DBMS的通用审计策略模型

何永忠, 李 斓, 冯登国

何永忠1,2, 李 斓3, 冯登国1
1(信息安全国家重点实验室(中国科学院 软件研究所),北京 100080)
2(中国科学院 研究生院,北京 100049)
3(上海交通大学 信息安全工程学院,上海 200030)
作者简介: 何永忠(1969－),男,重庆人,博士生,主要研究领域为密码学,系统安全;李斓(1977－),男,博士,主要研究领域为系统安全;冯登国(1965－),男,博士,研究员,博士生导师,主要研究领域为网络与信息安全.
联系人: 何永忠 Phn: +86-10-62528254 ext 803, E-mail: yzhe@is.iscas.ac.cn

Received 2004-07-27; Accepted 2004-10-10

Abstract
This paper proposes a generic audit policy model on multilevel secure DBMS. The model is powerful expressively which not only expresses audit policy based on periodical time constraints, but also implements audit policy deduction based on rules. Furthermore, fine-grained audit policies are possible in this model with the introduction of object attribute predicate. The decidability of the model is proven and a decidability algorithm is presented.

He YZ, Li L, Feng DG. A generic audit policy model on multilevel secure DBMS. *Journal of Software*, 2005,16(10):1774-1783.
DOI: 10.1360/jos161774
http://www.jos.org.cn/1000-9825/16/1774.htm

摘要
提出了一种基于多级安全数据库管理系统的通用审计策略模型.该模型具有丰富的表达能力,既可以表达基于时间的审计策略,也可以实现基于规则的审计策略推衍.通过引入对象的属性谓词,还可以表达细粒度的审计策略.证明了该模型的可判定性,并给出了判定任意一个事件是否需要审计的算法.

基金项目：Supported by the National Natural Science Foundation of China under Grant Nos.60025205, 60373048, 90304007 (国家自然科学基金); the National High-Tech Research and Development Plan of China under Grant No.2004AA147070 (国家高技术研究发展计划(863))

References:

[1] National Computer Security Center. A guide to understanding covert channel analysis of trusted systems. Technical Report, NCSC-TG-030, National Computer Security Center, 1993.

[2] DE BL, LaPadula LJ. Secure computer systems: Unified exposition and multics interpretation. Technical Report, MTR-2997, Bedford: MITRE Corporation, 1976.

[3] Bertino E, Bettini C, Ferrari E, Samarati P. A temporal access control mechanism for database systems. IEEE Trans. on Knowledge and Data Engineering, 1996,8(1):67-80.

[4] Wee C.LAFS: A logging and auditing file system. In: Proc. of the 11th Annual Computer Security Applications Conf. Los Alamitos: IEEE Computer Society Press, 1995. 231-240.

[5] Bishop M. A standard audit trail format. In: Proc. of the 18th National Information Systems Security Conf. Washington DC: National Computer Security Center, 1995. 136-145.

[6] Helman P, Liepins G. Statistical foundations of audit trail analysis for the detection of computer misuse. IEEE Trans. on Software Engineering, 1993,19(9):886-901.

[7] Biskup J, Flegel U. Transaction-Based pseudonyms in audit data for privacy respecting intrusion detection. LNCS 1907, Berlin: Springer-Verlag, 2000. 28-48.

[8] Sandhu R, Chen F. The multilevel relational (MLR) data model. ACM Trans. on Information and System Security, 1998,1(1): 93-132.

[9] Lunt TF, Denning DE, Schell RR, Heckman M, Shockley WR. The SeaView security model. IEEE Trans. on Software Engineering, 1990,16 (6):593-607.

[10] National Computer Security Center. A guide to understanding security modeling in trusted systems. Technical Report, NCSC-TG-010, National Computer Security Center, 1992.

[11] Jajodia S, Samarati P, Subrahmanian VS. A logical language for expressing authorizations. In: Proc. of the 1997 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1997. 31-42.

[12] Bertino E, Bettini C, Ferrari E, Samarati P. An access control model supporting periodicity constraints and temporal reasoning. ACM Trans. on Database Systems (TODS), 1998,23(3):231-285.