P.O.Box 8718, Beijing 100080, China	Journal of Software，Aug. 2004,15(8):1124-1132
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

基于Clark-Wilson完整性策略的安全监视模型

卿斯汉, 温红子, 雷　浩, 王　建

Full-Text PDF　Submission　Back

卿斯汉1,2, 温红子1,2, 雷　浩2,3, 王　建2,4，　1(中国科学院　软件研究所　信息安全技术工程研究中心,北京　100080)2(中国科学院　研究生院,北京　100039)
3(中国科学院　软件研究所　信息安全国家重点实验室,北京　100080)4(中国科学院　计算机网络信息中心　超级计算中心,北京　100080)
作者简介: 卿斯汉(1939－),男,湖南隆回人,研究员,教授,博士生导师,主要研究领域为信息安全理论与技术;温红子(1969－),男,工程师,主要研究领域为信息安全理论与技术;雷浩(1975－),男,博士生,主要研究领域为系统安全与信息安全技术;王建(1976－),男,博士生,主要研究领域为并行非线性最优化技术,并行计算安全技术.
联系人: 温红子　Phn: +86-10-62561197 ext 8006, E-mail: wenhongzi@msn.com, http://www.iscas.ac.cn

Received 2003-11-03; Accepted 2004-03-31

Abstract

The redundant data in log files and the delay for detecting abnormal trails are the inherent problems existing in the traditional secure monitoring subsystem of a computer system. In this paper, it is identified that the system security policies determine the logging data items in a secure monitoring function. By formally describing and analyzing the famous Clark-Wilson integrity policies with the corresponding relation patterns, the minimal logging data items set involved in these security policies is precisely determined. A formal secure monitoring model based on Clark-Wilson integrity policies (CW-SMM) is proposed. The CW-SMM has the characteristics of both minimal logging data and auto-detecting of the system abnormal trails in time, and can thoroughly solve the problems mentioned above.

Qing SH, Wen HZ, Lei H, Wang J. A secure monitoring model based on the Clark-Wilson integrity policies. *Journal of Software*, 2004,15(8):1124~1132.
http://www.jos.org.cn/1000-9825/15/1124.htm

摘要

传统的计算机设计系统的安全监视功能存在日志数据冗余和异常线索检测时延过长等固有问题.由于安全监视功能的日志数据项主要是由系统实施的安全策略所决定,所以采用关系模式,通过形式地描述、分析著名的Clark-Wilson完整性策略,从而精确确定了与各条策略相关的最小日志项集,然后将其应用于基于Clark-Wilson完整性策略的形式化安全监视模型(CW-SMM).该模型不但可以有效解决Clark-Wilson安全策略适用系统的日志数据冗余问题,而且也可以彻底解决异常线索检测中的时延问题.

基金项目：Supported by the National Natural Science Foundation of China under Grant No.60083007 (国家自然科学基金); the National Grand Fundamental Research 973 Program of China under Grant No.G1999035810 (国家重点基础研究发展规划(973))

References:

[1] Seiden, KF, Melanson JP. The auditing facility for a VMM security kernel. In: IEEE Symp. on Security and Privacy. New York: IEEE Computer Society Press, 1990. 262~277.

[2] Simone FH. IT-Security and Privacy. Berlin: Springer-Verlag, 2001. 35~104.

[3] Bishop M. A model of security monitoring. In: IEEE 5th Annual Computer Security Applications Conf. New York: IEEE Computer Society Press, 1990. 46~52.

[4] National Computer Security Center. A guide to understanding audit in trusted systems, Version 2. Technical Report, NCSC-TG-001, Fort Meade: National Computer Security Center, 1988.

[5] Clark DD, Wilson DR. A comparison of commercial and military computer security policies. In: IEEE Symp. on Security and Privacy. New York: IEEE Computer Society Press, 1987. 184~194.

[6] Qing SH, Liu WQ, Wen HZ, Liu HF. Operation System Security. Beijing: Tsinghua University Press, 2004. 73~114 (in Chinese).

[7] ?zsu MT, Valduriez P. Principle of Distributed Database Systems. 2nd ed., Upper Saddle River: Prentice Hall, 1989. 25~51.

[8] Denning DE, Lunt TF. A multilevel relational data model. In: IEEE Symp. on Security and Privacy. New York: IEEE Computer Society Press, 1990. 220~234.

[9] Woodcock J, Davies J. Using Z. Upper Saddle River: Prentice Hall, 1996.

[10] Picciotto J. The design of an effective auditing subsystem. In: IEEE Symp. on Security and Privacy. New York: IEEE Computer Society Press, 1987. 13~22.

[11] Markantonakis C. Secure logging mechanisms for smart card [Ph.D. Thesis]. Egham: University of London, 1999.

[12] Mayfield T, Roskos JE, Welke SR, Boone JM. Integrity in automated information systems. Technical Report, 79-91, Fort Meade, 1991.

[13] Bishop M. A standard audit trail format. Technical Report, Department of Computer Science, University of California at Davis, 1995.

[14] Bishop M, Wee C, Frank J. Goal-Oriented auditing and logging. 1996. http://seclab.cs.ucdavis.edu/papers/tocs-96.pdf

附中文参考文献:
[6] 卿斯汉,刘文清,温红子,刘海峰.操作系统安全.北京:清华大学出版社,2004.73~114.