维普资讯 http://www.cqvip.com

安全操作系统研究的发展(下)*)

The Development of Research on Secure Operating Systems(2)

石文昌 孙玉芳

(中国科学院软件研究所 北京 100080)

Abstract Prior to the work of this paper, our knowledge of the evolution history of secure operating systems was limited and primarily anecdotal. This paper proposes a classification method which divides the progress process of the research on secure operating systems into foundation period, cookbook period, multi-policy period and dynamic-policy period. The originating and developing procedure of the fundamental concepts, technologies and methods of secure operating systems is analyzed systematically according to the proposed classification method. As a result, a comprehensive perspective of the evolution course of the research on secure operating systems is presented. The discussion of the topic in question consists of two parts. This is the secont part.

Keywords Secure operating system, Evolution history, Development period, Multi-policy, Dynamic-policy

6 动态政策时期[0]

从单一政策支持到多种政策支持,安全操作系统迈出了向实际应用环境接近的可喜一步。然而,R. Spencer 等指出[17],从支持多种安全政策到支持政策灵活性,还有相当一段距离。政策灵活性是动态政策时期的重要特征,1999 年,Flask 系统的诞生是动态政策时期的帷幕徐徐打开的标志。

6.1 基于 Fluke 的 Flask 安全操作系统

Flask 是以 Fluke 操作系统为基础开发的安全操作系统原型。Fluke 是一个基于微内核的操作系统,它提供一个基于递归虚拟机思想的、利用权能系统的基本机制实现的体系结构[66,67]。

Flask 系统的安全体系结构是从 DTOS 原型系统的安全体系结构衍生而来的。尽管 DTOS 的安全体系结构是独立于特定安全政策的,但它却存在无法支持动态安全政策的不足。与此相反,Flask 的安全体系结构克服了 DTOS 体系结构中的不足,实现了动态安全政策,支持政策灵活性。

6.1.1 *项目的背景和目标* 在 DTOS 项目中,美国安全计算公司(SCC)和国家安全局(NSA)开发了 DTOS 安全体系结构,该体系结构的原型建立在 Mach 微内核之上。DTOS 项目之后,Mach 微内核的工作没有得到持续的支持,因而 NSA 和 Utah 大学合作启动了 Fluke 保障计划项目,把 DTOS 安全体系结构集成到 Utah 大学开发的 Fluke 操作系统中,同时,对该体系结构进行了改造,后来形成的就是 Flask 安全体系结构。自然,SCC 也参加了整个 Fluke 保障计划项目。

Fluke 保障计划项目的目标[68]是从两个方面去实现 Fluke 项目的安全性目标和保障能力目标,即,一方面是应用已知技术去帮助确定 Fluke 技术关键内容的保障能力,另一方面是通过新的研究去进一步拓展保障技术,解决 Fluke 特有的问题。

而 Fluke 项目的安全性目标和保障能力目标的内容是:

(1)安全性:主要的安全性目标是在 DTOS 安全体系结构的基础上建立一个政策灵活的访问控制模型的原型,重点是对动态安全政策的支持。

(2)保障能力:保障能力目标是通过运用形式化描述和推理手段实现对关键安全功能的验证。

6.1.2 *Flask 安全体系结构* Flask 安全体系结构描述两类子系统之间的相互作用以及各类子系统中的组件应满足的要求,两类子系统中,一类是客体管理器,实施安全政策的判定结果,另一类是安全服务器,做出安全政策的判定。该体系结构的主要目标是不管安全政策判定是如何作出的,也不管它们如何随时间的推移而可能发生变化,都确保这些子系统总是有一个一致的安全政策判定视图,从而,在安全政策方面提供灵活性。该体系结构的第二个目标包括应用的透明性、防御的深层性、保障的容易性和性能的小影响。

Flask 安全体系结构为客体管理器提供三个基本要素。首先,该体系结构提供从安全服务器检索访问、标记和多例化判定的接口。访问判定描述两个实体间(典型地,是一个主体与一个客体间)的一个特定权限是否得到批准。标记判定描述分配给一个客体的安全属性。多例化判定描述一个特定的请求应该访问多例化资源中的哪一个成员。其次,该体系结构提供一个访问向量缓存(AVC)模块,该模块允许客体管理器缓存访问判定,以便缩小性能开销。第三,该体系结构为客体管理器提供接收安全政策变化通知的能力。

客体管理器负责定义为客体分配标记的机制。每个客体管理器必须定义和实现一个控制政策,该控制政策描述如何利用安全判定来控制管理器提供的服务,它为安全政策提供对客体管理器提供的所有服务的控制,客体管理器允许根据安全威胁来配置这些控制,从而以最通用的方式对威胁进行处理。每个客体管理器必须定义响应政策变化时调用的处理例程。对多例化资源的使用,每个客体管理器必须定义选择资源的合适实例的机制。

6.1.3 *安全服务器的实现* Flask 原型系统的安全服务

*)国家自然科学基金项目(60073022)、国家 863 高科技项目(863-306-ZD12-14-2)和中国科学院知识创新工程项目(KGCX1-09)资助。石文昌 博士生,研究员,主要研究方向为系统软件与计算机安全。孙玉芳 研究员,博士生导师,主要研究方向为系统软件和中文信息处理。

维普资讯 http://www.cqvip.com

器实现了由四个子政策组成的安全政策，这几个子政策是多级安全(MLS)政策、类型裁决(TE)政策、基于标识的访问控制(IBAC)政策和基于角色的访问控制(RBAC)政策[69]。安全服务器提供的访问判定必须满足每个子政策的要求。

由 Flask 的安全服务器封装的安全政策通过两种方式定义，一种方式是由程序代码定义，另一种方式是由政策数据库定义。能够由 Flask 原型的政策数据库语言表示的安全政策可以简单地通过修改政策数据库来实现。对于其它的安全政策，需要修改程序代码或完全重写安全服务器，以改变安全服务器的内部政策框架，从而获得支持。值得注意的是，不管是否需要修改安全服务器的程序代码，都无需对客体管理器做任何修改。

就系统已实现的几个安全政策而言，除了标记本身以外，多级安全政策的政策逻辑大部分是通过安全服务器的程序代码来定义的，其它子政策的政策逻辑主要通过政策数据库语言来定义。

6.2 基于 Linux 的 SE-Linux 安全操作系统

SE-Linux 是以 Linux 操作系统为基础的基于 Flask 安全体系结构的安全操作系统，2001 年，P. Loscocco 等发布了该系统的研究成果[70,71]。

Flask 是基于微内核的系统原型，Linux 是非微内核的操作系统。Flask 项目完成后，作为 Flask 系统的主要开发者的美国国家安全局(NSA)启动了把 Flask 的安全体系结构集成到 Linux 操作系统中的项目，网络伙伴公司(NAI)的实验室、安全计算公司(SCC)和 MITRE 公司等协助 NSA 完成集成工作。NSA 已经在 Linux 内核的主要子系统中实现了 Flask 安全体系结构，这些子系统包括进程、文件和 socket 等操作的强制访问控制。NAI 实验室与 NSA 合作进一步开发和配置这个安全增强的 Linux 系统，SCC 和 MITRE 协助 NSA 开发应用层的安全政策和增强的实用程序。

Flask 安全体系结构的突出特点是通过安全判定与判定实施的分离实现安全政策的独立性，借助访问向量缓存(AVC)实现对动态政策的支持。安全请求的判定由安全服务器负责，判定结果的实施由客体管理器完成，AVC 是客体管理器的一部分，它用于存放由安全服务器提供的供客体管理器使用的访问判定计算。安全服务器是封装安全政策逻辑的一个独立的操作系统组件，它对外提供获取安全政策判定的通用接口。在 SE-Linux 实现中，安全服务器和 AVC 是在 Linux 操作系统中增加的两个新组件，安全服务器是 Linux 内核中的一个子系统，内核中的其它子系统属于客体管理器。

SE-Linux 实现的安全服务器定义了一个由类型裁决(TE)政策、基于角色的访问控制(RBAC)政策和多级安全(MLS)政策组合成的安全政策，其中 TE 和 RBAC 政策总是系统实现的安全政策的有机组成，而 MLS 政策是可选的政策，当内核配置选项 CONFIG_FLASK_MLS 打开时，系统提供 MLS 政策支持。

安全属性是安全政策判定的重要依据。安全属性在 Flask 安全体系结构中由安全标记表示。Flask 体系结构为安全标记定义了两个独立于政策的数据类型：安全背景和安全标识符(SID)。安全背景是由可变长字符串表示的安全标记，在系统内部，安全服务器用私有数据类型的结构存放安全背景。SID 是由安全服务器映射到安全背景上的一个整数。客体管理器负责把安全标记绑定到客体上，所以，它把 SID 绑定到活动的客体上。客体管理器以盲操作的方式处理 SID 和安全背景，它不对安全背景中的单个属性进行操作，所以，安全标记的格式或内容的变化不会导致产生对客体管理器进行修改的要求。在 SE-Linux 实现中，安全背景由用户标识、角色、类型和可选的 MLS 等级或等级范围组成。

SE-Linux 系统提供一个与安全服务器相配套的安全政策配置语言，该语言用于对安全服务器中的安全政策的配置进行描述。构造安全政策时，系统生成一个由政策配置语言表示的配置文件。由配置语言表示的配置文件可由一个称为 checkpolicy 的独立程序编译成二进制形式，安全服务器在引导时读取二进制形式的配置数据，配置其中的安全政策。

表 2 安全操作系统历史发展进程视图

	奠基时期	食谱时期	多政策时期	动态政策时期
起始年度	1967	1983	1993	1999
开始标志	美国国防部计算机安全特别部队组建，Adept-50 系统项目启动	美国国防部颁布 TCSEC 标准	美国国防部制定 DGSA 框架	美国国家安全局等推出 Flask 安全体系结构
促进因素	美国军方意识到资源共享的计算机系统的安全威胁	美国国防部要求被采纳的系统必须 TCSEC 标准	网络应用范围扩大，美国国防部要求被采纳的系统必须与 DGSAG 一致	真实世界的环境要求系统应该处理政策的变化特征
主要特点	摸索基本的思想、技术和方法	单一政策；系统研制有蓝本；有 C2-A1 各等级的系统推出	多种政策；系统开发有抽象框架，无蓝本	政策灵活性；进一步探索新的体系结构
主导开发方法	基于威胁的方法	基于标准的方法	基于威胁的方法	基于威胁的方法
代表性思想或系统	Adept-50、主体、客体、访问控制矩阵、引用监控机、安全核、隐通道、BLP 模型、权能、访问控制表、系统设计原则、操作系统保护理论、Multics、Mitre 安全核、UCLA 安全 Unix、KSOS、PSOS	可信计算基、系统安全等级、LINUS IV、安全 Xenix、System/V MLS、TUNIS、A-SOS	多安全政策共存、算法的安全政策支持结构、访问控制程序、看守员、安全服务器、客体管理器、DTOS	安全政策灵活性、安全政策配置、Flask、SELinux
突出技术难点	创立基本的思想、技术和方法	高安全等级系统的研制	多种安全政策的共存	政策变化特征的处理
主要问题	初始创新难度大	系统与变化的应用需求脱节	确定系统支持结构有难度	

结束语 在本文的工作之前，有关安全操作系统技术发展历史方面的已有信息是零碎的、不全面的。本文提出了奠基时期、食谱时期、多政策时期和动态政策时期的阶段划分方法，比较系统地对安全操作系统基本思想、技术和方法的形成和发展过程进行了全面的分析，给出了安全操作系统研究演

维普资讯 http://www.cqvip.com

化进程的一个全景视图，我们通过表 2 给出这个视图的简要归纳。

本文考察的时间范围是 1967 年至 2001 年，分析的第一个系统是 Adept-50，最后一个系统是 SE-Linux。本章以时间为主线，注重提供安全操作系统技术发展的历史资料，重点勾画安全操作系统基本思想、技术和方法的形成和发展过程，同时给出这些基本思想、技术和方法的基本内涵的归纳和总结，力图为揭示安全操作系统的发展规律和发展方向以及确立符合技术进步和实际应用需要的安全操作系统开发方法建立基础。

参 考 文 献

0 石文昌，孙玉芳. 安全操作系统研究的发展(上). 计算机科学，2002，29(6)

1 Gligor V D. 20 Years of Operating Systems Security. In: Proc. of the 1999 IEEE Symposium on Security and Privacy, Oakland, California, May 1999. 108～110

2 Weissman C. Security Controls in the ADEPT-50 Time Sharing System. In: Proc. of the 1069 AFIPS Fall Joint Computer Conference, AFIPS Press, 1969. 119～133

3 Saltzer J H, Schroeder M D. The Protection of Information in Computer Systems. Proceedings of the IEEE, 1975, 63(9): 1278～1308

4 Landwehr C E. The Best Available Technologies for Computer Security. IEEE Computer, 1983, 16(7): 86～100

5 Foley S N, Li Gong, Qian Xiaolei. A Security Model of Dynamic Labeling Providing a Tiered Approach to Verification. In: Proc. of the IEEE Symposium on Security and Privacy, May 1996. 142～153

6 Whitmore J, et al. Design for MULTICS Security Enhancements. ESD-TR-74-176, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA, USA, Dec. 1973

7 CSC-STD-001-83, Department of Defense Standard. Department of Defense Trusted Computer System Evaluation Criteria. DoD Computer Security Center, Aug. 1983

8 Ware W H. Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security: [Technical Report]. the Rand Corporation, Santa Monica, CA, published for the Office of the Director of Defense Research and Engineering, Washington, DC, Feb. 1970

9 DoD 5200. 28-STD, Department of Defense Standard. Department of Defense Trusted Computer System Evaluation Criteria. National Computer Security Center, Ft. Meade, MD, USA, Dec. 1985

10 Lampson B W. Dynamic Protection Structures. In: Proc. of the AFIPS Fall Joint Computer Conference, volume 35, Las Vegas, Nevada, Nov. 1969. 27～38

11 Anderson J P. Computer Security Technology Planning Study Volume II. ESD-TR-73-51, Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA, USA, Oct. 1972

12 Lampson B W. A Note on the Confinement Problem. Communications of the ACM, 1973, 6(10): 613～615

13 Bell D E, LaPadula L J. Secure Computer Systems: Mathematical Foundations. ESD-TR-73-278, Vol. I, AD 770 768, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, MA, USA, Nov. 1973

14 Bell D E, LaPadula L J. Secure Computer Systems: A Mathematical Model. ESD-TR-73-278, Vol. II, AD 771 543, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, MA, USA, Nov. 1973

15 Bell D E, LaPadula L J. Secure Computer Systems: A Refinement of the Mathematical Model: [ESD-TR-73-278]. Vol. III, AD 780 528, Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, MA, USA, Apr. 1974

16 Bell D E, LaPadula L J. Secure Computer Systems: Mathematica l Foundations and Model. M74-244, The MITRE Corporation, Bedford, MA, USA, Oct. 1974

17 Bell D E, LaPadula L J. Secure Computer System: Unified Exposition and MULTICS Interpretation. MTR-2997 Rev. 1, The MITRE Corporation, Bedford, MA, USA, Mar. 1976

18 Biba K J. Integrity Considerations for Secure Computer Systems: [ESD-TR-76-372]. Electronic Systems Division, Air Force Systems Command, Hanscom Air Force Base, Bedford, MA, USA, Apr. 1977

19 Landwehr C E. Formal Models for Computer Security. ACM Computing Surveys, 1981, 13(3): 247～278

20 Pfleeger C P. Security in Computing, Second Edition. Prentice Hall PTR, Upper Saddle River, NJ, USA, 1997

21 Summers R C. Secure Computing: Threats and Safeguards. McGraw-Hill, New York, NY, USA, 1997

22 Harrison M A, Ruzzo W L, Ullman J D. Protection in Operating Systems. Communications of the ACM, 1976, 19(8): 461～471

23 Ritchie D M, Thompson K. The UNIX Time Sharing System. Communications of the ACM, 1974, 17(7): 365～375

24 Karger P A, Schell R R. MULTICS Security Evaluation, Volume II: Vulnerability Analysis. ESD-TR-74-193, Vol. II, Electronic Systems Division, Air Force Systems Command, Hanscom Field, Bedford, MA 01731, June 1974

25 Schiller W L. The Design and Specification of a Security Kernel for the PDP-11/45. MTR-2709, The MITRE Corporation, Bedford, MA, USA, Jun . 1973

26 Schiller W L. Design of a Security Kernel for the PDP-11/45. MTR-2934, The MITRE Corporation, Bedford, MA, USA, Mar. 1975

27 Popek G J, Kampe M, Kline C S, Walton E J. UCLA Data Secure Unix. AFIPS Conf. Proc., Vol. 48, 1979 National Computer Conf. AFIPS Press, Arlington, VA, USA, 1979. 355～364

28 Walker B J, Kemmerer R A, Popek G J. Specification and Verification of the UCLA Unix Security Kernel. Communication of the ACM, 1980, 23(2): 118～131

29 Aerospace F, Communications Corporation. Secure Minicomputer Operating System (KSOS) Executive Summary: Phase I: Design of the Department of Defense Kernelized Secure Operating System. WDL-781, Palo Alto, CA 94303, Mar. 1978

30 McCauley E J, Drongowski P J. KSOS: The Design of a Secure Operating System. AFIPS Conf. Proc., Vol. 48, 1979 National Computer Conf. e, AFIPS Press, Arlington, VA, USA, 1979. 345～353

31 Neumann P G. A Provably Secure Operating System: Final Report. DAAB03-73-C-1454, Stanford Research Institute, Menlo Park, California 94025, Jun. 1975

32 Feiertag R J, Neumann P G. The Foundations of a Provably Secure Operating System (PSOS). In: Proc. of the National Computer Conf. Vol. 48, 1979. 329～334

维普资讯 http://www.cqvip.com

33 Organick O. The Multics System: An Examination of its Structure. MIT Press, Cambridge, MA, USA, 1972

34 Good D I, London R L, Blesdsoe W W. An Interactive Program Verification System. IEEE Transactions on Software Engineering, 1975, 1(1): 59～67

35 Linden T A. Operating System Structures to Support Security and Reliable Software. Computing Surveys, 1976, 8(4): 409～445

36 Nibaldi G H. Specification of a Trusted Computing Base. M79-228, The MITRE Corporation, Bedford, MA, USA, 1979

37 Nibaldi G H. Proposed Technical Evaluation Criteria for Trusted Computer Systems. M79-225, The MITRE Corporation, Bedford, MA, USA, Oct. 1979

38 Kcramer S. Linus IV - An Experiment in Computer Security. In: Proc. of the 1984 Symposium on Security and Privacy, Oakland, California, USA, IEEE Computer Society Press, 1984. 24～32

39 Ritchie D M. On the Security of UNIX. In the UNIX Programmer's Manual, Jun. 1977

40 Gligor V D, et al. On the Design and the Implementation of Secure Xenix Workstations. In: Proc. of the 1986 IEEE Symposium on Security and Privacy, Apr. 1986. 102～117

41 Gligor V D, et al. Design and Implementation of Secure Xenix. IEEE Transactions on Software Engineering, 1987, SE-13(2): 208～221

42 Gligor V D, et al. A New Security Testing Method and its Application to the Secure Xenix Kernel. IEEE Transactions on Software Engineering, 1987, SE-13(2): 169～183

43 Flink II C W, Weiss J D. System V/MLS Labeling and Mandatory Policy Alternatives. AT&T Technical Journal, May/Jun 1988. 53～64

44 Grenier G L, Holt R C, Funkenhauser M. Policy vs Mechanism in the Secure TUNIS Operationg System. 1989 IEEE Symposium on Security and Privacy, 1989. 84～93

45 Siber W O, et al. UNIX and B2: Are They Compatible?. In: Proc. of the 10th National Computer Security Conf. Baltimore, MD, USA, Sept. 1987. 142～149

46 Levin R, et al. Policy/Mechanism Separation in Hydra. In: Proc. of the Fifth Symposium on Operating System Principles, ACM, 1975. 132～140

47 Waldhart N A. The Army Secure Operating System. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, 1990. 50～60

48 Vito B L Di, et al. Specification and Verification of the ASOS Kernel. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, 1990. 61～74

49 Good D I, Vito B L Di, Smith M K. Using the Gypsy Methodology. Institute for Computing Science, University of Texas at Austin, Jun. 1984

50 Feustel E A, Mayfield T. The DGSA: Unmet Information Security Challenges for Operating System Designers. ACM Operating Systems Review, 1998, 32(1): 3～22

51 Center for Standards. Department of Defense Goal Security Architecture, Version 3. 0. Defense Information Systems Agency, Washington, DC, 30 Apr. 1996

52 Halfmann U, Kuhnhauser W E. Embedding Security Policies into a Distributed Computing Environment. ACM Operating Systems Review, 1999, 33(2): 51～64

53 Theimer M M, Nichols D A, Terry D B. Delegation through Access Control Programs. In: Proc. of the 12th International Conference on Distributed Systems. IEEE Computer Society Press, 1992. 529～536

54 Härtig H, Kowalski O, Kühnhauser W E. The BirliX Security Architecture. Journal of Computer Security, 1993, 2(1)

55 Kühnhauser W E. On Paradigms for User-Defined Security Policies in Multipolicy Environments. In: 11th IFIP Intl. Information Security Conf., Cape Town, 1995

56 Kühnhauser W E. A Paradigm for User-Defined Security Policies. In: 14th IEEE Symposium on Reliable Distributed Systems. Bad Neuenahr, IEEE Press, 1995

57 Hosmer H H. Metapolicies II. In: Proc. of the 15th National Computer Security Conf. NIST-NCSC, United States Government Printing Office, 1992. 369～378

58 Secure Computing Corporation. DTOS Lessons Learned Report. CDRL Sequence No. A008, Secure Computing Corporation, Roseville, Minnesota, Jun. 1997

59 Saydjari O S, et al. Synergy: A Distributed, Microkernel-Based Security Architecture: [Technical Report: R231]. INFOSEC Research and Technology, Nov. 1993

60 Olawsky D, Fine T, Schneider E, Spencer R. Developing and Using a Policy Neutral Access Control Policy. In: Proc. of the UCLA Conf. on New Security Paradigms Workshops, ACM, USA, Sep. 1996

61 Secure Computing Corporation. DTOS Generalized Security Policy Specification. DTOS CDRL A019, Secure Computing Corporation, Roseville, Minnesota, Jun. 1997

62 Boebert W E, Kain R Y. A Practical Alternative to Hierarchical Integrity Policies. In: Proc. of the 8th National Computer Security Conf. Gaithersburg, MD, Oct. 1985. 18～27

63 Badger L, et al. Practical Domain and Type Enforcement for UNIX. 1995 IEEE Symposium on Security and Privacy, 1995. 66～77

64 Carney M, Loe B. A Comparison of Methods for Implementing Adaptive Security Policies. In: Proc. of the 7th USENIX Security Symposium, 1998. 1～14

65 Spencer R, et al. The Flask Security Architecture: System Support for Diverse Security Policies. In: Proc. of the 8th USENIX Security Symposium, Washington, DC, USA, Aug. 1999. 123～139

66 Lepreau J, Ford B, Hibler M. The Persistent Relevance of the Local Operating System to Global Applications. In: Proc. of the 7th ACM SIGOPS European Workshops, Sep. 1996

67 Secure Computing Corporation. Assurance in the Fluke Microkernel: Formal Security Policy Model. CDRL Sequence No. A003, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota 55113, Feb. 1999

68 Secure Computing Corporation. Assurance in the Fluke Microkernel: Final Report. CDRL Sequence No. A002, Secure Computing Corporation, 2675 Long Lake Road, Roseville, Minnesota 55113, Apr. 1999

69 Sandhu R, Coyne E, Feinstein H, Youman C. Role-Based Access Control Models. IEEE Computer, 1996, 29(2): 38～47

70 Loscocco P, Smalley S. Integrating Flexible Support for Security Policies into the Linux Operating System: [Technical report]. NSA and NAI labs, Jan. 2001

71 Smalley S, Fraser T. A Security Policy Configuration for the Security-Enhanced Linux: [Technical report]. NAI Labs, Jan. 2001