分布式系统安全保障新体系的研究

黎忠文[1] ,熊光泽[2] ,李乐民[1]
(1. 电子科技大学通信学院 ,四川成都 610054 ;2. 电子科技大学计算机学院 ,四川成都 610054)

摘 要: 安全问题是阻碍分布式系统发展和实用化的主要因素之一. 分布式系统的安全性包括 security 和 safety 两个重要且紧密相关的方面 ,然而目前绝大多数的研究只限于 security. 可是随着软件的大量应用 ,分布式系统正面临严峻的防危考验 ,迫切需要新的 safety 保障技术. 本文在深入分析分布式系统安全需求的基础上 ,提出了建立集 security 和 safety 保障为一体的分布式系统安全保障新体系的设想 ,并对该体系应具有的特点和设计目标进行探讨. 然后针对把防危核这种 safety 保障新技术用于大型分布式系统存在的困难 ,提出了基于实时操作系统的解决方案. 最后建立了一种新的安全保障体系 SADS (security and safety assurance structure of distributed system) ,并在实时 Linux 平台上 ,以交通灯指挥系统为对象建立了 SADS ,验证了该 SADS 的可行性和有效性.

关键词: 分布式系统; safety 核; 安全保障体系; 防危策略; 实时操作系统
中图分类号: TP306⁺. 3 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0564-05

Research on New Security and Safety Assurance Structure of Distributed System

LI Zhong-wen[1] ,XIONG Guang-ze[2] ,LI Le-min[1]
(1. *Communications College , UEST of China , Chengdu , Sichuan* 610054 , *China ;*
2. *Computer Science and Engineering College , University of Electronic Science and Technology , Chengdu , Sichuan* 610054 , *China*)

Abstract: Security and safety are important and related factors that baffle the development and practicality of modern distributed system. However ,most of researches on distributed system focus on security. Unfortunately ,since software is being used largely in the complex distributed systems ,the possibility of serious damage resulting from a software defect is considerable and growing ,and then the complex distributed systems are plunging into safety crisis. In fact ,distributed systems are in urgent need of new safety assurance technologies. After analyzing security and safety requirements of distributed system ,we put forward new ideas for setting up the security and safety assurance structure of distributed system. We also analyze characteristics ,designing aims for this structure. Since there are a lot of shortcomings in the current methods of realizing safety kernel (that is a new concept of safety assurance) in distributed system , we advance a program for RTOS to supply safety kernel mechanism. Based on all of these ,we set up SADS (security and safety assurance structure of distributed system) . At last ,taking the control system in the traffic lights as example ,prototype experiment of SADS has been done on the RT-Linux platform in the lab ,and this experiment has proved the validity of SADS.

Key words: distributed system ;safety kernel ;security and safety assurance structure ;safety policy ;RTOS

1 引言

对分布式系统安全保障机制的研究包括 safety 和 security 两个方面 ,它们分别代表系统面临自身缺陷(如软件开发中没有完全排除的故障)和受外界恶意攻击时如何保障系统的安全性. 两者决不能互相代替 ,且缺一不可. 长期以来 ,人们对对 safety 的研究非常少 ,而且在研究过程中 ,security 和 safety 往往被分离开来. 近年来 ,随着软件的大量应用 ,safety 问题日益突出 ,事故频频发生[1]. 大规模、复杂系统软件的开发是当今所面临的极富挑战性的课题之一[2,3]. 究其原因在于软件的大量应用使得设计型软件错误成为大型系统事故的主要来源 ,然而传统 safety 和可靠技术对于这类软件错误却渐感力不从心. 据统计 ,就一般复杂度的软件 ,用测试法只能使软件错误率降低到每小时 10^{-4} 个 ,对于复杂度稍高的软件 ,测试法还达不到这种效果. 而与 safety 相关的控制系统的错误率要求是每小时 10^{-9} 个 ,甚至有的是每小时 10^{-10} 个[1]. 事实上目前还有许多系统(包括国家级)仍然建立在“脆弱”的软件之上[4]. 为此西方发达国家近年来纷纷投入大量的人力、物力开展新 safety 保障技术和新软件开发技术的研究. 防危核(safety kernel)[5,6]正是应运而生的一种新 safety 保障技术. 本文的研

收稿日期:2001-08-10;修回日期:2002-07-15

究以探讨分布式系统安全需求为基础,研究防危核技术移用于大型分布式系统可行性,然后建立集 safety 和 security 保障为一体的分布式系统的安全体系,减少系统中两者的有缝连接.

2　分布式系统安全保障体系 SADS 的设计目标

2.1　分布式系统的安全需求

分布式系统具有多个节点,其安全保障分为域内和域间(即互联)两方面. 域表示端系统(end-system,它有多种形态,这里设为单节点),互联表示数据通信设备和网络.

(1)域间安全需求

域与域之间的关系可分为对等和主从两种. 对等关系中,域与域之间是完全平等的,都有各自的安全保障政策. 在主从关系中,安全保障政策具有继承性,即子域要共享母域的政策. 此外,子域还可以有自己的政策. 必须要保证域间传递的信息具有保密性、完整性. 这里的安全显然是指 security,因此利用 security 的成果进行安全保障.

(2)域内安全需求

同一域内的安全保障系统必须统一设计,这样才能保证该域内的全局安全性. 域内的安全性要求包括外来信息处理的安全和域内信息处理的安全两部分. 域内的安全保障包括 safety 和 security 两方面.

2.2　SADS 的设计目标

安全保障体系 SADS 是一个集安全服务、安全机制和安全管理及其它与安全有关的内容为一体的概念. SDAS 至少要具有功能性和适应性两个特点. 功能性指 SADS 提供的安全服务包括 safety 和 security 两方面;适应性则指 SADS 能适应形形色色的应用形态.

SADS 的设计目标是:

(1)灵活性:仅当需要安全保障服务时才提供该功能.

(2)透明性:用户尽可能的感觉不到它的存在.

(3)安全保障服务的周密性:安全保障系统既要向用户提供丰富的安全保障服务,又提供各种管理功能,以便对该系统进行安装、监测和重建.

(4)全保障实施的独立性:安全保障措施由安全保障系统全权负责实施.

(5)适应性:安全系统既能适用于从单个 PC 到 LAN,甚至于开放系统等环境,又能适用于多种用户、应用和数据.

(6)易开发和易验证:安全保障系统不能太复杂,必须要易于开发、测试和验证.

3　分布式系统安全保障体系 SADS 的结构

3.1　SADS 的外部视图

在结构上将 SADS 设计为三层.

(1)安全保障系统的管理层:它由完成安装、调试、监视、维护和重建安全保障系统的模块组成.

(2)安全保障服务代理层:它由各个安全代理组成,它们之间相互配合,保障系统的安全.

(3)安全保障服务实现层:它就是安全保障系统提供的安全保障服务的集合,具体完成安全保障的职能.

(4)安全管理数据库:它存放所有与系统安全相关的信息. 它是集中式还是分布式管理视具体系统而定.

3.2　安全服务代理及相互关系

SADS 中设置下述几类安全保障服务代理:

(1)应用代理:保存本域支持的所有类型应用的说明,标准的安全信息;记录应用的安全需求;根据标准的安全信息,审查应用安全需求的合理性,并做出适当的响应.

(2)用户代理:记录用户的请求,根据严格的规则来判断其合法性,并做出适当的响应;协助用户进行其安全管理;向用户提供帮助信息.

(3)全管理代理:与监视代理、恢复代理协同工作和安全管理数据库代理协同工作.

(4)防危核代理:防危核代理是防危系统的中心控制和操作代理,主要负责提供防危核服务.

(5)安全管理数据库代理:凡是要访问安全管理数据库的代理均需通过安全管理数据库代理.

(6)监视代理:接收安全管理代理所收集的数据并通过安全管理数据库代理把它们记录在安全管理数据库中.

(7)恢复代理:恢复代理负责探测系统的安全性是否被破坏,在系统进入非安全状态时将系统恢复到安全状态.

(8)环境代理:对用户、应用和域外数据进行初步的安全审查,合格者交给相应的代理,不合格者禁止访问本域;负责域间网络安全,确保域间数据的保密性和完整性.

(9)域外数据代理:在异构分布式控制系统中,域外数据代理用于处理异构问题,如数据格式的转化等.

各服务代理相互之间的关系见图 1 所示.

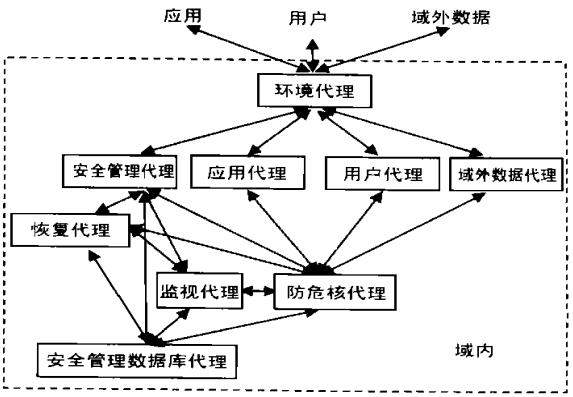

图 1　安全服务代理之间的关系

3.3　安全服务

安全服务是安全保障系统的功能,为支持安全服务代理,SADS 主要提供下面二类安全服务.

(1)域间消息传递的安全服务

在 SADS 中我们引用国际标准化组织 ISO 为 OSI 环境规定的五种标准通信安全服务.

(2)域内安全服务分为三类:①防危核服务:防危核服务分为四类,分别用于维护设备控制策略、应用软件的状态策略、设备错误诊断策略和错误响应策略. ②数据库 security 服

务:数据库 security 服务引用开放系统环境中的数据库 security 服务,即除了 OSI 的访问控制、数据保密和数据完整 security 服务外,还提供保持数据流防危一致性和防止推知数据两项 security 服务. ③管理安全服务:安全审核服务(它实现探测和调查与安全性有关的事件)和安全恢复服务(在安全性破坏发生后,该服务采取一定的措施将系统恢复到安全状态).

4 防危核机制的实现

防危核[6]是一种 safety 保障新技术,它通过执行 safety 策略以防因软件的缺陷造成对设备的误操作:凡是对受保护设备的访问,都必须经过防危核的审查控制,合法者予以支持,反之则采取相应的出错处理措施. 这样就能很好的避免软件错误造成的灾难后果.

4.1 由操作系统提供防危核机制

防危核的实现方式一般分为集中式和分散式两种,而且都是置于应用层的位置,对每一个系统而言其 safety 策略和防危核都必需全新设计,因此其可重用性、移植性和实时性差,且不适合大型分布式系统[9]. 我们设计把防危核放入实时操作系统(RTOS)中:防危核机制仍然由操作系统来提供,但不把它与操作系统的内核融为一体,而是把之作为一个单独的机制与操作系统的内核分开. 这样一方面能更多地考虑防危核与应用的关系;另一方面又能更好的体显灵活性,不需要防危服务时,系统就不提供. 我们分析了 CRTOS Micro 和 RT-Linux 两个 RTOS,防危核机制的提供方式分为下列几种:

(1)库的方式:生成.o 文件,在编译时联入.

(2)扩展系统调用:相当于增加了用于防危的系统调用.

(3)修改系统函数 API:修改系统函数的 API,在原 API 上加入类似于转向防危核的功能.

(4)内核模块法:这种方法用于实时 Linux. 把防危核做成一个核心模块加入到实时 Linux 的内核中去.

4.2 防危核的重用算法

防危核机制的重用性主要表现在防危策略上. 相同行业中,应用软件的防危策略所涉及的内容大体相同,只是参数不同而已. 我们把防危策略的封装分为可重用部分和不可重用部分,后者需要系统开发人员根据系统的特殊性进行设计. 在图 1 的基础上,我们设计了一种重用算法,其主要过程如下:

(1)各用户向环境代理提出防危请求;

(2)建立用户与应用服务代理之间的连接,然后用户以参数的形式把各自应用的防危需求告知应用代理;

(3)应用代理使用应用过滤器对应用进行归类;

(4)应用代理根据应用所属类别的防危常规与用户进行“协商”,去除应用中不合理的防危参数;

(5)应用代理使用标准的防危参数翻译器把经过“协商”的防危参数(这时的防危参数被称为用户级防危参数,即以便于用户处理的形式表达的)翻译成系统认可的防危参数(这时的防危称为系统级的防危参数);

(6)应用代理把系统级的防危参数传递给防危服务代理;

(7)防危服务代理的过滤器对应用代理传递过来的参数进行归类,然后把它们交给相应的防危服务子代理;

(8)防危核的防危服务子代理根据防危参数的形式把它们分成设备控制策略、应用软件的状态策略、设备错误诊断策略和错误响应策略等四类,从而把它们分别传递给相应的防危模型.

5 原型实验

5.1 交通灯控制系统及其安全需求

实验室中模拟的交通灯控制系统 TCS 由两个十字路口(CROSS1 和 CROSS2)和一个交通指挥中心组成. 其中每个十路口都有一个交通指挥系统,它通过传感器发来的交通流量情况,改变两盏交通灯的颜色来指挥本路口的交通;交通指挥中心的任务是协调这两个路口的交通指挥系统,保证整个系统交通畅通. 在交通灯正常工作的情况下,TCS 的安全需求:交通指挥系统 1 和 2 无论收到指挥中心的指令与否都要正确地改变交通灯的颜色,避免同一个路口出现两个方向的交通灯同时为绿的情况.

5.2 安全保障统的设计与实现

5.2.1 TCS 的仿真 实验室分别用三台 PC 机仿真 TCS,PC 机通过局域网与 HUB 相连. 仿真 TCS 采用的软件是 RT-Linux,其版本为 Kernel 2.2.14-RT-Linux 2.2. 其中,PC1 仿真交通指挥中心,PC2 和 PC3 分别仿真 CROSS1 和 CROSS2. PC1、PC2 和 PC3 各设成一个安全域,分别为域 1、域 2 和域 3. PC1 上用软件 Server 实现交通指挥中心的功能:Server 收到域 2(或域 3)的消息后,向域 2(或域 3)发封装在数组 KD 中的控制指令 A1、A2 和 A3;数组 CD 封装了改变交通灯颜色的一系列命令. PC2(或 PC3)上软件 COMM 根据 CD 和 SC 接收的指令发命令改变冲突方向交通灯的颜色;软件 P 模拟交通灯,P 根据 COMM 的命令改变颜色;如果交通灯连续 5 次没有根据 COMM 的命令改变颜色,软件 SC 就向 PC1 发消息 M1、M2 或 M3,请求其干预. 域 2 和域 3 是两个处于平等关系的域;域 1 是域 2 和域 3 的母域.

5.2.2 域间安全的实现 通信安全服务不是本论文的重点,因此在实验中我们使用简化的方式处理域间安全保障:采用 socket 编程,选用 TCP/IP 协议,并在通信双方严格记录消息的来源、时间及内容,以备审查.

5.2.3 域内安全的实现

(1)域 1 的安全系统

安全服务代理层只设有环境代理、防危核代理和安全管理数据库代理三种代理,分别由任务 Proc1、Proc2 和 Proc3 来实现. 安全管理数据库 SDL1 存放了与全局安全有关的信息(实验中设为其它安全域的地址、消息的格式、数组 KD). 域 1 的安全系统见图 2 所示.

(2)域 2 和域 3 的安全系统

域 2 和域 3 的安全系统相同,下面以域 2 为例进行详细说明. 域 2 的安全系统见图 3 所示.

域 2 的 SADS 中,环境代理、防危核代理和安全管理数据库代理分别由任务 SC、SK 和 Proc 来实现,安全管理数据库是 SDL2. SC 的功能与域 1 的 proc1 类似,为了减化 SC 的设计,每当防危核连续处理了 5 个有错的交通灯访问命令,就向 SC 发

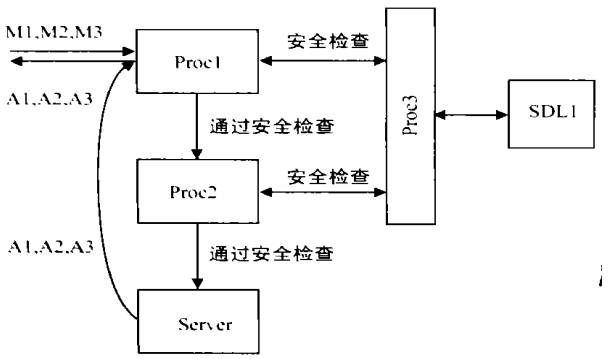

图 2　域 1 的安全系统

异常消息,而不再由 SC 去收集异常消息;SK 提供防危核服务;WD 模拟 SK 的监视器,一旦它发现 SK 有异常行为就立即停止该 SK,并启动另一个防危核 SK′,SK′是 SK 的一个备份. SDL2 存放了有关本域安全的信息.

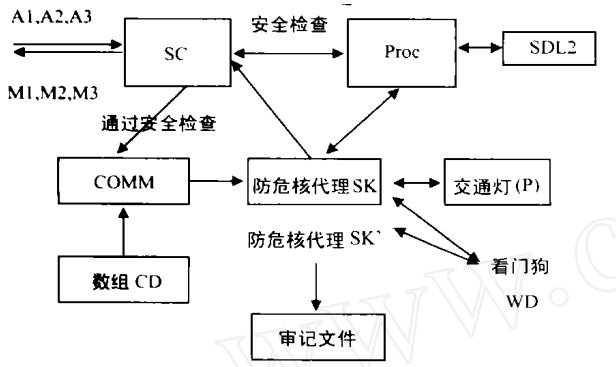

图 3　域 2 的安全系统

5.3　实验结果

(1)实验的有效性

为验证实验的有效性,我们为 COMM 设置了三组数据 Data1,Data2 和 Data3:Data1 由改变交通灯颜色的正确命令组成;Data2 在 Data1 的基础上加入了不正确的命令,检验域 2 在没有域 1 干预情况下的安全保障功能;Data3 则在 Data2 的基础上加入了连续 5 个以上的不正确命令,以验证在域 1 的干预下域 2 或域 3 功能的正确性及安全性. 实验表明,当采用数据 Data1 和数据 Data3 时,TCS 都得到了安全保障. 此外我们通过在 SK 中设置错误语句,验证了 SK 冗余机制的正确性. 综上所述,实验结果证明本文提出的安全体系 SADS 及防危核机制的实现方案是有效的.

(2)实验数据

为分析安全机制的加入对系统效率的影响,实验以域 2 为测试对象,收集了表 1 中的数据(时间单位是微秒),令:

T_{NET}表示 SC 的执行时间(包括了安全检查时间),ΔT_{NET} 是均值;T_C 表示 COMM 的执行时间,ΔT_C 是均值;T_S 表示 SK 的执行时间(包括了安全检查时间),ΔT_S 是均值;T_{WD}表示 WD 的执行时间,ΔT_{WD}是均值;T_1,T_2,T_3 分别为 P 中三个线程的执行时间,ΔT_1,ΔT_2,ΔT_3 是均值;I 是序号.

经过计算得:ΔT_{NET} = 3276μs,ΔT_C = 77μs,ΔT_S = 75μs,ΔT_{WD} = 26μs,ΔT_1 = 11120μs,ΔT_2 = 391μs,ΔT_3 = 541μs.

(3)安全机制对系统效率的影响

实验中每当防危核连续处理了五个有错的交通灯访问命令(实验中,概率为 0.2)时,SC 就与 PC1 通信一次. 域 2 内采用安全机制前后系统效率之比 η 为 98%. 即采用安全机制后,域 2 系统的效率是原系统效率的 98%,用于安全的系统开销并不大,安全机制在本原型实验中是可行的.

表 1　实验所测数据表

I	T_1	T_2	T_3	T_{NET}	T_c	T_s	T_{WD}	I	T_c	T_s	T_{WD}
1	11124	392	541	3364	78	74 73 75	29	14	76	74 75	29
2	11117	391	539	3315	77	74 75	28	15	77	74 74 77	24
3	11115	391	545	3297	77	75 73 76	24	16	77	74 75	23
4	11123	394	545	3290	77	74 75	26	17	77	74 74 74	29
5	11116	387	543	3233	77	74 73 75	29	18	76	74 76	25
6	11121	390	544	3249	77	74 75	24	19	77	74 74 74	29
7	11120	389	536	3217	77	74 74 74	25	20	76	74 76	24
8	11119	389	539	3236	76	76 76	23	21	77	74 74 74	30
9	11122	392	541	3292	76	74 73 76	31	22	77	74 75	24
10	11119	395	542	3259	77	74 75	25	23	77	74 76 75	26
11	11115	393	541	3280	77	74 74 74	27	24	78	74 75	25
12	11123	391	539	3309	77	74 75	24	25	77	74 74 74	26

6　结束语

Safety 和 security 是系统安全涉及的两个不可分割的方面,本文首次提出了建立集两者为一体的系统安全保障新体系 SADS. 作者一方面研究了 SADS 的设计目标、结构和具体功能等;另一方面还针对防危核这种新 safety 保障技术直接应用于大型分布式系统存在的可重用性、移植性和实时性差等不足,提出了由 RTOS 提供防危核机制的实施方案及重用算法. 并通过实验验证了 SADS 及防危核机制实施方案的有效性,还用实验数据分析了防危机制对系统效率的影响. 需说明的是,原型实验中,SK 在系统每次启动后都有一个加载过程,而在实际工程中,SK 将由 RTOS 自动提供,用户应当感觉不到 SK 的加载过程,这项工作必然要涉及到对 RTOS 内核的修改,我们下一步将对此进行研究.

参考文献:

[1] Butler R W, Finelli G B. The infeasibility of quantifying the reliability of life-critical real-time software [J]. IEEE Tran On software engineering, 1993, 19(1): 3 - 12.

[2] Benveniste A, Astrom K J. Meeting the Challenge of Computer Science in the Industrial Applications [J]. IEEE Trans Automatic Control, 1993, 38(7): 1004 - 1009.

[3] Leveson N G. System Safety in Computer-Controlled Automotive Systems [R]. SAE Congress, 2000.

[4] President's information technology advisory committee reports to the

president [R]. Information Technology research: investing in our future. 1999.
[5] Kevin R. Safety kernel enforcement of software safety policies: [D]. USA: University of Virginia, 1995.
[6] Rushby J. Kernels for safety [A]. Safe and Secure Computing Systems Sympoium [C]. London: Blackwell Scientific Publications, 1989. 210-220.
[7] 黎忠文,熊光泽. 防危(safety)内核机制的研究与实现 [J]. 计算机科学, 2001, 28(4): 87-90.
[8] Knignt J C. Achieving Software Quality Through Reuse [D]. USA: University of Virginia, 2000.
[9] 黎忠文. 分布式控制系统中新安全技术的研究-safety kernel [D]. 成都:电子科技大学, 2001.

作者简介:

黎忠文 女,1970 年 5 月出生于四川江津,分别于 1991 年毕业于四川师范大学,1998 年和 2001 年分别获得电子科技大学工学硕士和博士学位,并于 2001 年进入电子科技大学通信与信息系统博士后流动站工作,主要研究方向:大型系统的高可靠、高防危技术和主动网技术.

熊光泽 男,1938 年 7 月出生于四川丹棱,教授,博士导师,主要研究领域为实时计算机系统及其软件开发支持.

李乐民 男,1932 年 5 月出生浙江吴兴,中国工程院院士,博士导师,博士后导师,主要研究领域为通信技术.

2003'全国微波毫米波会议征文通知

由中国电子学会主办,微波分会、国家"十五"863 计划信息获取与处理主题、上海交通大学、上海航天局等单位联合承办的 2003 年全国微波毫米波会议将于 2003 年 9、10 月份在上海地区召开,届时将举行全国微波毫米波科技、教育与产业界的学术成果和技术产品交流,热忱欢迎广大学者、专家、技术人员踊跃投稿,欢迎研究所、院校、厂商等单位参展.

一、征文内容:

所有与微波理论、技术有关的内容,具体见《微波学报》2002 年第 4 期的广告.

二、征文要求:

论文应有所创新,尚未在其它专业会议和刊物上发表过. 全文包括图表参考文献在内限 4 页篇幅,采用 A4 纸,用激光打印,版芯尺寸为 140 ×215mm^2. 论文一式 2 份.

三、论文投寄截止日:2003 年 6 月 30 日

四、大会论文投寄处:

上海市华山路 1954 号上海交通大学电子工程系(邮政编码:200030)

联系人:沈一彬,毛军发;

联系电话:(021) 62933309, 62933722

Email: ybshen@mail.sjtu.edu.cn jfmao@sjtu.edu.cn

中国电子学会微波分会

上海交通大学电子工程系