ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.4, April 2009, pp.985−996
doi: 10.3724/SP.J.1001.2009.03246

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

短消息指标新定义及在事务信道限制中的应用*

曾海涛[1,4,5], 王永吉[1,2,5+], 祖 伟[3], 蔡嘉勇[4,5], 阮 利[1,4]

[1](中国科学院 软件研究所 互联网软件技术实验室,北京 100190)

[2](中国科学院 软件研究所 计算机科学国家重点实验室,北京 100190)

[3](哈尔滨工程大学 自动化学院,黑龙江 哈尔滨 150001)

[4](中国科学院 研究生院,北京 100049)

[5](中国科学院 软件研究所 基础软件国家工程中心,北京 100190)

New Definition of Small Message Criterion and Its Application in Transaction Covert Channel Mitigating

ZENG Hai-Tao[1,4,5], WANG Yong-Ji[1,2,5+], ZU Wei[3], CAI Jia-Yong[4,5], RUAN Li[1,4]

[1](Laboratory for Internet Software Technologies, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[2](State Key Laboratory of Computer Science, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

[3](Automation College, Harbin Engineering University, Harbin 150001, China)

[4](Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

[5](National Engineering Research Center for Fundamental Software, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: ywang@itechs.iscas.ac.cn

Zeng HT, Wang YJ, Zu W, Cai JY, Ruan L. New definition of small message criterion and its application in transaction covert channel mitigating. *Journal of Software*, 2009,20(4):985−996. http://www.jos.org.cn/1000-9825/3246.htm

Abstract: Small Message Criterion (SMC) can measure the capability of the covert channel on transmitting small messages and is a necessary complement to the capacity criterion. However, SMC's present definition has deficiencies. The acquirement of message length proved to be hard in the common information system. Mitigating mechanism can not simultaneously satisfy the two restrictions of message transfer time and fidelity. The criterion does not cover information of message's sensitivity. At first, the value function of message is introduced to represent the danger of small message transmission. Based on the value function, a new definition of SMC is presented where the threat tolerance standard of system is represented by a threshold of message value. The value function also takes message's sensitivity into account. A mechanism for secure real-time database scenario, which combines SMC with the channel capacity, is presented to measure and mitigate the threat of transaction covert

* Supported by the National Natural Science Foundation of China under Grant No.60673022 (国家自然科学基金); the Hundred Talents of the Chinese Academy of Sciences (中国科学院"百人计划"); the Key Technology Research and Development Program of China under Grant No.2005BA113A02 (国家科技攻关计划)

Received 2007-06-19; Accepted 2007-12-28

channel. Theoretical analysis and experimental results show that with the proposed new SMC, the secure system can perform comprehensive measurement and adjustable mitigation to the threat of covert channel.

Key words: small message criterion; channel capacity; transaction covert channel; secure real-time database

摘 要: 短消息指标可以度量隐蔽信道的短消息传输能力,是信道容量的必要补充.但指标现有定义中还存在着以下问题:消息长度参数在普通信息系统中不能定量分析;信道限制机制难以同时满足传输时间和保真度两个约束;没有包含消息的敏感度信息.针对这些问题,首先通过引入短消息传输价值的概念,给出了短消息指标的新定义.在该定义中,利用价值阈值统一表示系统对信道短消息传输能力的容忍程度,并且在所采用的价值函数中引入了消息的敏感度因素.其后,基于安全实时数据库应用场景给出了结合短消息指标和信道容量的事务隐蔽信道度量和限制机制.理论分析和模拟结果表明,基于短消息指标的新定义,系统可以对隐蔽信道威胁实施全面的度量和可调节的限制.

关键词: 短消息指标;信道容量;事务隐蔽信道;安全实时数据库

中图法分类号: TP393 **文献标识码**: A

军事、经济等领域的安全信息系统通常采用基于 Bell LaPudula(BLP)模型的强制访问控制机制来满足关键应用对数据安全的较高要求.但是恶意主体仍然可以利用某些手段绕过强制访问控制,实现违反安全策略的通信,这种允许主体以危害系统安全策略的方式传输信息的通道即是隐蔽信道[1].隐蔽信道分析主要包括 4 个方面:建模、定位、度量和限制[2].其中,度量是对信道传输能力和威胁程度的评价,度量结果可以用来指导限制措施的实施,因此,信道度量是整个信道分析过程中的关键环节.在 TCSEC 安全标准中以信道容量作为度量信道能力,定义信道威胁容忍标准的指标[1].但是,单一使用容量指标并不能全面反映信道的威胁程度:首先,信道容量只反映了信道的数据传输能力,并没有体现出信道所传输数据的敏感性.例如,在两个容量相同的信道中,较高安全级别的数据泄露比较低安全级别的数据泄露对系统安全的威胁更大,但是容量指标无法反映该因素[3];其次,信道容量作为一种渐进的估计方法,给出的是利用信道经过较长时间传递长文件的能力,而对信道传递短消息的能力描述不足[4].

为了度量和限制信道的短消息传输能力,Moskowitz 在文献[4]中提出了短消息指标 SMC(small message criterion)的定义.其定义中给出了评价信道传输短消息能力的要素,也同时表达了安全系统对短消息传输的容忍程度.短消息指标被认为是信道容量的必要补充[2,4,5],但是,Moskowitz 的定义只列举了短消息指标的参数,并没有对这些参数进行深入分析,定义中存在以下几个问题:1) 在一般的安全信息系统,如安全操作系统中,用户所掌握的数据类型多样,数据长度跨度较大,无法确定指标中的参数 n;2) 对短消息传输能力的容忍程度表示为 τ和ρ两个参数,二者缺乏关联,系统难以利用信道限制机制同时满足定义中这两个约束;3) 该指标的定义只能描述信道的传输能力,无法反映传输信息的敏感程度.

在安全数据库系统中,用户所能访问的数据字段类型固定,不存在消息长度 n 难以确定的问题,适合采用短消息指标.在安全数据库隐蔽信道研究中,由于事务隐蔽信道具有传输速度快、安全威胁大等特点,因此一直是研究的难点和热点.对事务隐蔽信道的研究主要关注于度量和削弱领域,特别是在安全实时数据库环境下,系统需要均衡实时和安全需求,动态确定信道限制措施力度,尤其重视对事务隐蔽信道威胁的在线度量[6].Son 在文献[5]中,在给出该种数据库环境下事务隐蔽信道容量计算方法的同时,也期望利用短消息指标来完善对信道威胁的度量.因此,我们选择安全实时数据库下的事务隐蔽信道度量场景展开对短消息指标的研究,期望解决现有定义中存在的缺点,实际应用该指标来度量事务隐蔽信道威胁.

本文提出了安全数据库环境下短消息指标的度量和约束以及限制策略的一系列定义.这些定义解决了现有 SMC 定义的后两个缺陷:将对消息传输时间和保真度的约束归结为对传输消息价值的单一限制;通过将消息价值的初值设定为信道两端的安全级别差别,在指标中引入了消息的敏感程度因素.在分析短消息指标的实施要素之后,本文将其与容量指标相结合,应用于安全实时数据库,给出了事务隐蔽信道威胁的全面度量,并提出

了基于该度量的事务并发控制机制.

本文首先介绍事务隐蔽信道领域的相关研究,并在第 2 节中对事务隐蔽信道场景进行分析和建模.第 3 节给出短消息指标的新定义系列和指标参数的获取细节.第 4 节提出综合考虑短消息指标和容量指标的事务并发控制机制.第 5 节通过实验分析该限制机制的执行效果.最后对本文方法进行总结,并介绍未来的研究方向.

1 相关研究

数据库系统中的隐蔽信道主要包括 3 种:事务隐蔽信道、推理信道和安全机制引入的信道.事务隐蔽信道是由于不同安全级别的事务之间并发执行时的事务竞争而产生的[5].推理信道是恶意用户利用历史访问或相互交换查询信息,实现对敏感信息的间接访问的信道[7].在安全数据库中还需要考察安全机制的实施是否会引入新的信道[8].对后两种信道的研究主要关注于信道的定位和建模方法,而由于事务隐蔽信道在并发事务处理中的普遍存在性,它更多地关注于信道威胁的度量和限制方法.Keefe 最早提出了并发控制安全(data-conflict-security)的充分和必要条件:事务不能被更高安全级别事务所延迟或取消,即,在写访问数据时,低安全级事务具有更高优先级[9].在基于此条件开发的控制协议中,高安全级别事务受到“不公平”对待[5].根据解决并发控制中安全性和公平性之间矛盾的原则,后续研究可以分为两个方向:1) 基于绝对安全目标的安全协议和调度框架研究;2) 基于相对安全目标的度量和限制机制研究.

绝对安全目标下不允许系统中出现违背安全策略的行为,要求安全机制提供绝对的安全保障.为了避免事务间的不公平性,Son 等人提出了 Secure 2PL 协议[10],通过多重数据副本方法,实现了不同安全级别事务之间的无干扰,避免事务隐蔽信道.另外,Secure 2PL 协议中高安全级别事务不必被低安全级事务推迟或取消,类似的安全控制协议还有 SRT-OPT[11],FREEZE[12]等.但是这些协议中多重数据副本和缓存的使用,需要消耗大量的事务执行时间和存储空间,无法应用于军事信息处理等对数据操作的实时性要求较高的场合.这些领域中在保障数据安全的同时,数据操作必须及时准确,还需要满足实时需求,一般采用安全实时数据库[5].在绝对安全目标下的安全实时数据库,如 STAR 和 GUARD 数据库中,都完全使用安全并发控制协议,禁止事务隐蔽信道,从而保障安全策略的实施.但是,这些系统存在实时需求保障不足的问题[13,14].

相对安全目标则允许系统中存在一部分或一定程度地违反安全策略的行为,并利用可量化的指标,指导系统将恶意行为威胁限制在安全目标容忍范围内.在相对安全的条件下,安全实时数据库系统可以在安全需求和实时需求之间求得平衡.Son 提出数据库系统的相对安全策略,在执行过程中根据信道威胁度量结果动态选择并发控制协议:对威胁高于一定阈值的信道采用安全控制协议,降低信道威胁;而其他同步操作中,则利用实时控制协议,保障系统实时性能[6].事务隐蔽信道的威胁可以从多个角度进行衡量.Ahmed[3]利用冲突事务的安全级别差作为信道威胁的度量,双方安全级别差别越大,信息传输对系统的威胁就越大.而其他研究工作中更多地利用信道传输数据的能力来度量信道的威胁,例如事务冲突速率[15]和信道容量[5].其中,Son 在文献[5]中利用 9 个概率参数描述信道受到的干扰,给出了干扰下事务隐蔽信道容量的计算方法.

由于完全消除事务隐蔽信道的性能代价过大,为了谋求系统中多种需求的均衡,相对安全目标下的威胁度量和限制机制研究逐渐成为事务隐蔽信道分析领域的研究热点.本文也将根据相对安全目标来设计对事务隐蔽信道的度量和限制措施.

2 事务隐蔽信道分析

首先给出对安全实时数据库系统的形式化定义:

定义 1(安全实时数据库,secure real-time database,简称 SRTDB). 安全实时数据库由五元组表示:$SRTDB=(D,TR,U,L,P)$,其中,$D=\{d_1,d_2,d_3,\ldots\}$是数据库中数据元素的集合,$TR=\{tr_1,tr_2,tr_3,\ldots\}$是数据库实时事务的集合,$U=\{u_1,u_2,u_3,\ldots\}$是用户的集合.$L$ 为数据库中安全标签的集合,表示数据和用户的安全级别,并且不同的安全级别之间存在着偏序关系.P 为数据库中的事务优先级集合,L 和 P 在系统实现中一般为离散数值集合.

数据库定义中还包括以下对应关系:$DLabel:D\rightarrow L$,数据元素到安全标签的对应关系;$ULabel:U\rightarrow L$,用户到

安全标签的对应关系;$TLabel$:$TR\rightarrow L$,事务到安全标签的对应关系;UD:$U\rightarrow D$,数据库中用户到其所能访问数据的对应关系;TRU:$TR\rightarrow U$,数据库中事务与其发起用户的对应关系;TRP:$TR\rightarrow P$,数据库中事务与其实时优先级的对应关系.其中,事务的安全标签等于事务发起用户的安全标签,即 $TLabel(tr_i)=ULabel(TRU(tr_i))$.

安全数据库中通常采用基于 BLP 模型的强制访问控制机制来保障信息的机密性.在该机制中,每个主体(事务)和客体(数据)都有一个安全标签,说明其安全级别.系统根据事务操作的主、客体标签实施访问控制.在 BLP 模型中,要求访问操作遵守“不上读,不下写”的约束,从而阻止低安全级别用户直接获得更高安全级别的信息.在 SRTDB 中,系统通常依据实时调度策略来确定事务执行的优先级.在事务的并发控制协议,例如 2PL-Priority 协议[5]中,需要照顾优先级较高的事务:当两个事务发生冲突时,将停止或重启优先级较低的事务.这样的并发控制协议能够较好地保障事务的实时性,但是在该种协议下,恶意用户可以通过设计一定的事务竞争场景来构造隐蔽信道,绕过强制访问控制机制传递信息,场景如下:

两个不同安全级别的用户发出的事务 tr_1,tr_2,共同访问同一数据项 d_x,其安全级别关系为 $TLabel(tr_2)\geq DLabel(d_x)\geq TLabel(tr_1)$,其中,低安全级别事务 tr_1 写访问 d_x,高安全级别事务 tr_2 读访问 d_x.

在该场景下,高安全级用户通过图 1 所示方式向低安全级用户发送信息:

(1) 低安全级用户发起事务 tr_1,高安全级用户根据预先定义的信号规则确定是否发起优先级更高的事务 tr_2.

(2) 如果高安全级用户希望发出符号“1”,则其将发起事务 tr_2.由于两个事务间存在冲突,因而系统放弃事务 tr_1.

(3) 如果高安全级用户希望发出符号“0”,则其不发起事务 tr_2,tr_1 可以顺利完成执行.

如上所述,处于不同安全级别的事务通过并发控制机制相互干扰,从而传递信息,该种信道就是事务隐蔽信道.在该场景下,发送 1 所需的时间为 $T=t_1$,而发送 0 所需的时间为 $T=t_2$.由于上面场景中信道传输的是 0 和 1 两种信号,因此,该信道属于二元隐蔽信道.这种结构简单的隐蔽信道受到的干扰最少,传输时间最小,因此可以获得最大的容量[5].同理,该种信道传递短消息的能力也最强.对隐蔽信道的限制措施首先要限制威胁最大的信道,因此,本文中事务隐蔽信道的讨论将针对该场景.

为了能够在提供对系统安全性保障的同时将对数据库的实时性能影响控制在可控的范围内,在相对安全目标的系统中往往采用安全调度和实时调度两者的结合方案[3,5,6].例如,在文献[5]中,系统按照一定的概率 p 执行实时控制协议,确保数据库事务的实时性,以 $q=1-p$ 的概率执行安全控制协议,保障系统的数据机密性,系统权衡两种需求来确定概率值.该类型的并发控制策略叫做相对安全策略 PSP(partial security policy).概率 q 作为系统中安全控制协议的概率,反映了系统安全措施的力度以及信道受到的干扰程度,因此将该概率称为干扰概率.在本文中也采用该策略限制隐蔽信道传输能力,利用容量和短消息指标以及系统的实时指标共同确定 q 值.

为了方便对信道性质的分析,首先对 PSP 下事务隐蔽信道的传输特性进行建模.由于系统中其他事务对信道的影响只会干扰信道的传输,造成实际的信道传输能力低于计算结果.而 TCSEC 标准中要求度量信道最大威胁,因此,信道建模过程中不需要考虑其他事务对信道的干扰[16,17].而与其他事务造成的干扰所不同,PSP 中系统按照干扰概率选择安全并发协议,其对信道的干扰作用明确,是限制方法作用下事务隐蔽信道的固有属性.基于以上原因,本文在分析信道传输特性时只考虑信道限制操作的干扰作用.另外,入侵者利用事务隐蔽信道通信时往往刻意选择访问次数很少的中间数据对象,或在数据库负载低、事务稀少的时段进行操作,这样的传输受到其他事务干扰的可能性不大.因此,在信道建模过程中忽略其他事务对信道的干扰作用,不会夸大信道的实际威胁.具体的建模结果如下:

数据库系统采用安全控制协议限制隐蔽信道的传输能力.对于冲突事务,系统执行非安全协议(如 2PL-priority)的概率为 p,而有 $q=1-p$ 的概率下会使用隐蔽信道安全的控制协议,如 Secure 2PL.在安全控制协议下,高安全级用户发起事务 tr_2 对低安全级事务 tr_1 没有影响,tr_1 可以成功提交,低安全级别用户识别的传输符号为 0.也就是说,在有 q 的概率下,高安全级用户发送符号 1,但是低安全级用户收到符号 0.此时,信道传输特性如图 2 所示,图中清楚地显示,在相对安全策略 PSP 下的事务隐蔽信道将呈现 Z 信道的特性.

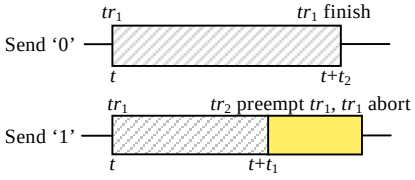


Fig.1 Transaction covert channel

图 1 事务隐蔽信道

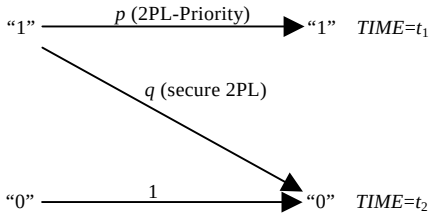


Fig.2 Transaction channel under restriction of PSP

图 2 相对安全策略限制下的事务隐蔽信道

3 短消息指标度量和约束定义

通信信道的容量为通过信道单位时间内可传输的互信息量的极值,在隐蔽信道分析中,通常利用容量作为信道威胁程度的度量.但信道容量是一种渐进的估计方法,它给出的是利用信道经较长时间传输长文件的能力,其对信道传递短消息的能力描述不足.例如文献[4]中所指出的,当信道容量为 0 时,恶意用户仍然可以在有限的时间内完成对短消息的传输,信道容量不能用来度量该情况下的安全性.为了限制这种隐蔽通信,Moskowitz[4]提出了短消息指标,用来描述系统对信道传递敏感短消息的能力的容忍程度,其给出的指标定义如下:

定义 2(短消息指标,SMC). 短消息指标包括 3 个要素(n,τ,ρ),分别是短消息的长度、信道传输该短消息的时间、消息传递的保真度.短消息指标表述为安全系统所容忍的隐蔽信道短消息传输能力为在长度τ的时间内传递长度为 n 位的消息,而消息的保真度为ρ.

以上定义给出了描述短消息传输能力的 3 个参数,但是并没有深入分析这些参数间的关系,无法从中获得短消息传输能力的度量和限制方法.该定义中,参数 n 指出了指标的适用消息长度,与消息的传输时间 t 结合可以描述信道的传输能力,但是信道的威胁还与消息的敏感程度相关,而该定义中无法直接反映该因素,对信道威胁的描述不够全面.另外,为了确保相对安全目标,系统需要利用安全机制将信道威胁限制在允许的范围内.指标定义中,参数τ和ρ是系统对信道威胁的容忍标准,但是这两个参数之间缺乏关联,无法唯一地表示系统的容忍程度,因此难以从中直接确定信道限制措施的力度.

3.1 短消息指标要素分析

首先结合数据库系统的特点,对短消息指标各要素进行分析,以便在其基础上提出指标的新定义形式.

(1) 在一般的信息系统,如操作系统中,难以确定信道中可能传输的消息长度:一个用户所掌握的数据类型是多样的,信道利用者既可能希望通过隐蔽信道传递机密文件的内容,也可能只是利用信道来传递较短的秘密数据,如用户的登陆数据等.前者将花费较长时间,而后者的传输时间则较短.在这样的系统中,对于复杂、多样的秘密信息将无法直接应用短消息指标来衡量和限制.而数据库系统却具有以下特点:

- 用户所能访问的数据字段类型固定,数据的长度确定;
- 数据库系统的数据访问控制集中,便于进行数据的监控和统计.

这些特性决定数据库系统更加适合利用短消息指标来度量其中隐蔽信道的传输能力.

(2) 短消息指标需要确定系统中对短消息长度 n 的界定.由于无法提前预知用户可能利用隐蔽信道传输他所拥有的何种类型的信息,因此,在度量用户可利用的信道短消息传输能力时,需要考察其所拥有的最短长度的信息类型,这种方法同样符合隐蔽信道分析中度量信道最大传输能力的原则.

(3) 在短消息指标中,传输时间τ和保真度ρ是对信道传输短消息能力的限定.为了准确地定义和实施限制标准,需要将τ和ρ归结为单一限定值.本文将对二者的限定归结为对被传输的短消息的价值的考察.在 SRTDB 中,数据具有较强的时效性,数据所包含信息的价值将随时间而衰减,要求入侵者在有限的时间内通过信道完成数据传递,否则,即使传输成功,数据价值也将受损,因此,短消息价值可以表示成时间为参数的函数.另一方面,信息的保真程度也决定了盗取的信息的可利用性,从而制约着信息的价值.结合这两个因素,可以给出以下的短消

息价值的函数形式:

定义 3(短消息传输价值及其函数). 短消息传输价值 V_i 是恶意用户利用隐蔽信道在时间τ内以保真度ρ完成对数据项 d_i 的传输所能获得的价值.V_i 与变量τ和ρ的关系用短消息传输价值函数 $V_i(\rho,\tau)$表示.

由于无法确知恶意用户将利用事务隐蔽信道传输何种信息,因此,数据项 d_i 考察信道中较高安全级别用户所拥有的最短长度的信息,本文根据 SRTDB 的数据特点,给出短消息传输价值函数的具体形式为

$$V_i(\rho,\tau)=\rho^{\omega}U_i(\tau) \tag{1}$$

其中,$U_i(\tau)$为数据项d_i的准确信息的价值随时间变化的函数,由两部分确定:消息的初始价值U_0以及消息价值随时间变化的趋势.短消息的价值 V 同时还受到数据传输的保真度ρ的制约,参数ω反映了保真度对消息价值的影响方式.当ω=0 时,数据价值不受保真度影响.参数ω越大,数据的价值随传输的保真度下降而衰减得越快.

信息的价值可以有许多种度量方法,而在安全系统中,信息的敏感度是其价值的直接体现.另外,在前面的讨论中已经指出,为了全面反映信道威胁,短消息指标需要反映消息的敏感程度,因此,本文中利用冲突事务的敏感度差别,即安全级别差别,作为信息价值的初始值 U_0.文献[3]中认为,隐蔽通信对系统安全的威胁由通信双方的安全级别差来决定,双方安全级别差别越大,信息传输对系统的威胁也越大.举例来说,假设系统中存在 3 个安全级别 $L=\{UN(Unclassified),CL(Classified),SE(Secret)\}$,级别间偏序关系为 $SE\geq CL\geq UN$,则 UN 与 CL 之间的隐蔽信道威胁小于 UN 与 SE 之间的隐蔽信道威胁.这种信道威胁度量结果被称作隐蔽信道因素 CCF(covert channel factor)[3].为了便于推导,本文中采用'–'符号来表示安全级别差距的度量,即将两个事务的安全级别差别表示为公式(2).

定义 4(事务安全级别差别度量). 事务之间的安全级别差别定义为

$$\exists tr_{high},tr_{low}\in TR,TLabel(tr_{high})\geq TLabel(tr_{low}),diff(tr_{high},tr_{low})=TLabel(tr_{high})-TLabel(tr_{low}) \tag{2}$$

隐蔽信道因素 CCF 定义为安全级别差别与最大差距的比值:

$$CCF=\frac{diff(tr_{high},tr_{low})}{\#L-1} \tag{3}$$

其中,$\#L$ 为系统中最大的安全级别差,即两个极端安全级别之间的差距.

隐蔽信道传输的数据的原始价值用冲突事务的隐蔽信道因素表示,记为 $U_0=CCF$.不同类型数据的价值 U 随时间 t 变化的规律不同,其函数关系由数据的特性决定,数据库安全管理员需要根据数据的不同特征提供数据的价值时间函数的定义.图 3 为数据项价值时间函数的示例.

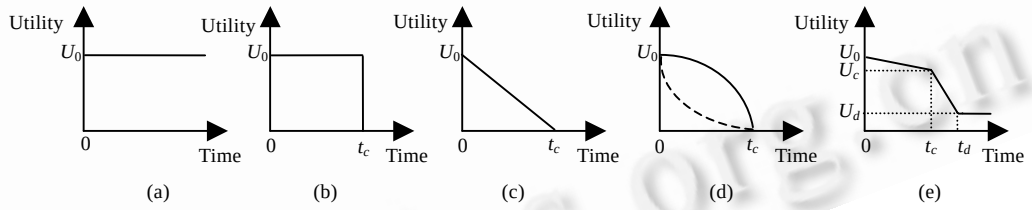


Fig.3 Examples of utility function of data items

图 3 数据项价值函数示例

图 3(a)类型的数据价值在秘密期内恒定不变,只有在解密公开后才丧失机密价值,数据实例包括关键事件的事实等.图 3(b)是一种脉冲型的价值函数,这种数据在有效时间 t_c 内价值保持不变,当超出有效时间时价值将即刻消失.例如,定时修改的密码数据,当密码修改后,原有的密码即完全失去价值.图 3(c)、图 3(d)所示的信息价值将随时间逐渐衰减,并在一定时间 t_c 之后完全丧失,数据库中的数据主要呈现该种形式.例如,商业信息越早被获取,其价值就越大.价值函数可能具有更加复杂的形式,在不同的时间段呈现不同的变化趋势.例如,军事目标的位置信息,在一次采样后,随着动态物体位置的变化,原有数据对分析目标现有位置的指导作用逐渐降低.在 t_c 时刻产生新的采样数据后,原有数据虽不准确,但价值不会即刻消失,只是下降速度加快.在时间 t_d 之后,该信息已经无法表示目标的位置,但是作为目标的轨迹信息仍然保留一定价值,其价值时间曲线如图 3(e)所示.

3.2 短消息指标定义系列

利用以上分析结果,本文将给出基于消息价值的短消息指标相关定义.不同于 Moskowitz 的 SMC 中同时包含短消息传输能力的度量和限制条件的定义方式,我们将分别给出短消息指标度量和约束的定义.

定义 5(短消息指标度量). 用户 u_{high} 与较低安全级别用户 u_{low} 之间隐蔽信道的短消息指标度量 SMM(small message measurement)记为

$$SMM=(ULabel(u_{high}),ULabel(u_{low}),ml,\tau,\rho,V_{high}) \tag{4}$$

$ml=minlen(UD(u_{high}))$:较高安全级别用户 u_{high} 所拥有的长度最短的数据类型的数据长度;

V_{high}:用户 u_{high} 所拥有的长度最短的数据类型的价值时间函数.

定义 6(短消息指标约束). 短消息指标约束 SMR(small message restriction):

$$SMR=(N,V_{thres}) \tag{5}$$

$N=\{n_1,n_2,...,n_i,...\}$:当处于安全级别 i 的用户拥有长度小于 n_i 的数据时适用该约束.N 是这些长度限制的集合;V_{thres}:对用户利用信道传递短消息可以获取的价值的限制阈值.

SMM 中包含了描述信道传输短消息能力所需的参量.SMR 表示系统所容忍的信道威胁.基于 SMM 和 SMR 的定义,本文给出短消息传输能力的限制策略,旨在将信道的短消息传输能力和安全威胁限制在容忍的范围内.

定义 7(短消息指标限制策略). 短消息指标限制策略 SMMP(small message mitigation policy).

利用 SMM 度量用户 u_{high} 与用户 u_{low} 之间隐蔽信道的短消息传输能力.根据 SMR 要求,当 $ml<N_{high}$ 时,系统需要采取隐蔽信道限制措施,将信道可能传输的短消息价值限制在容忍的范围内,即要求确保:

$$V_{high}(\tau,\rho)\le V_{thres} \tag{6}$$

3.3 短消息指标参数分析

以下具体分析相对安全策略 PSP 下事务隐蔽信道的 SMM 的参数 τ 和 ρ 的获取方式及其与概率 q 的关系.

保真度 ρ 表示消息传播的准确率.本文第 2 节中指出,在 PSP 下,事务隐蔽信道呈现 Z 信道形态,其中一种信号按照概率 q 被误认为另一种信号.按照第 2 节的结论,在信道传输特性分析中不考虑其他事务对信道的干扰,因此,q 取值为系统中采取安全控制协议的概率.我们规定,PSP 下数据传输的保真度计算公式为 $\rho=1-q$,该式反映了信号的可准确辨识程度.保真度 ρ 与 q 呈线性关系,q 越大,数据传输受到的干扰越大,保真度越低.当 $q=0$ 时,信号无干扰传输,保真度 ρ 为 1.当 $q=1$ 时,信号无法辨识,保真度 ρ 为 0.

短消息传输时间 τ 由消息的长度和信道的传输速度共同决定.基于衡量信道最大威胁的目标,只考察用户利用信道以最大速度传送其所拥有的最短敏感信息的能力.SMM 中,该信息的长度为 ml,而用户可以利用的最快传输方式是使用第 2 节中介绍的场景连续传输符号.在该场景下,传输长度为 ml 的消息所需要的时间 τ 为

$$\tau = ml\cdot\overline{t} \tag{7}$$

其中,$\overline{t}$ 为每个符号的平均传输时间.如图 2 所示,信道传输符号分别需要时间 t_1 和 t_2,当数据中两种符号的比例相等时,信道传输一个符号的平均时间为

$$\overline{t}=\frac{(1-q)t_1+qt_2+t_2}{2}=\frac{t_1+t_2}{2}+\frac{q}{2}(t_2-t_1)=\frac{\Sigma t}{2}+\Delta t\frac{q}{2} \tag{8}$$

其中,$\Delta t=t_2-t_1$,$\Sigma t=t_2+t_1$.将公式(8)代入公式(7)可得:

$$\tau = ml\cdot\overline{t}=ml\cdot\left(\frac{\Sigma t}{2}+\Delta t\frac{q}{2}\right) \tag{9}$$

安全实时数据库事务的执行时间基本确定,可以方便地获取信道时间参数 t_1 和 t_2.在图 1 的场景中,低安全级事务希望察觉高安全级事务操作,t_2 必须大于 t_1,则 $\Delta t>0$.从公式(9)可知,信道传输短消息的时间 τ 将随着 q 的增大而增大,即相对安全策略施加的干扰越大,信道传输短消息花费的时间越长.

由以上分析可知,信道传输短消息能力指标 τ 和 ρ 会随着 PSP 的干扰概率 q 的变化而变化.当 q 增大时,ρ 减小,τ 增大.由 V 的函数定义,消息的价值将减少,系统的安全性将提高.同时,由于实时控制协议概率 $p=1-q$ 的减小,系统实时性将会下降.当 q 减小时,ρ 随之增大,τ 减小,价值 V 增大,系统安全性将有所下降,而实时性将有所提高.

4 短消息指标和信道容量的融合

在 SRTDB 中,需要兼顾系统的安全和实时需求,根据两种需求的满足程度,动态调节系统安全限制措施的力度.系统的实时性能通常利用事务的截止期错失率 DMP(deadline miss percentage)来表示,而单独利用短消息指标或容量度量安全性能,都不能全面地反映隐蔽信道威胁程度,因此需要将二者结合起来,给出信道威胁的更全面的度量.

本文第 2 节中将相对安全策略下的事务隐蔽信道归结为 Z 信道的形式,可以利用 Z 信道领域的研究成果来分析概率 q 对信道容量的影响.在文献[18]中,Moskowitz 得出 Z 信道容量的计算公式为

$$C=\log\kappa\gamma_q \tag{10}$$

其中,γ_q 是信道的干扰概率为 q 时方程(11)的正根,并有 $\kappa=(pq^{q/p})^{1/t_1}$, $\varepsilon=t_2-t_1=\Delta t$.

$$1-[(\kappa\gamma)^{-(t_1+\varepsilon)}+\gamma^{-t_1}]=0 \tag{11}$$

图 4 显示了不同干扰概率 q 下信道容量的计算结果.由图 4 可见,信道容量 C 将随着 q 的增大而减小.因此,q 同时影响事务隐蔽信道的短消息指标和容量,q 越大,信道的威胁越小.另外,q 还同时影响着系统的安全性和实时性指标,且对二者的影响趋势相反.因此,PSP 中参数 q 可以作为均衡系统安全性和实时性需求的参量.

基于以上分析,本文提出融合短消息指标和信道容量的并发控制机制 CoCCM(comprehensive concurrency control mechanism).在 CoCCM 中,以执行安全并发控制协议的概率 q 作为限制短消息传输价值 V 和信道容量 C 的参量,如图 5 所示.该机制中,由 q 选择安全控制协议和实时控制协议,可同时兼顾系统的实时性和安全性需求.

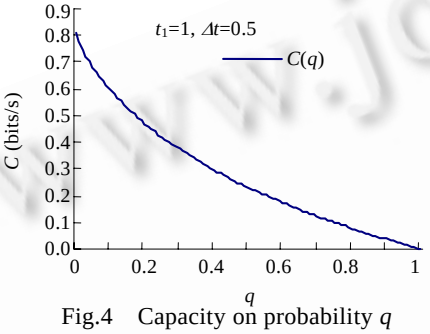


Fig.4 Capacity on probability q

图 4 信道容量 C 随概率 q 变化趋势图

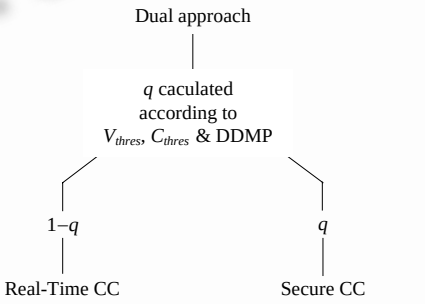


Fig.5 Illustration of how to select concurrency control protocol in CoCCM

图 5 CoCCM 中并发控制策略选择示意图

CoCCM 机制中的安全标准包括:信道容量标准 C_{thres} 以及系统短消息指标限制策略 SMMP.SMMP 策略中,SMM 指定了不同数据项 d_i 的短消息传输价值函数 $V_i(\rho,\tau)$,SMR 部分包括短消息价值的限制阈值 V_{thres} 以及约束实施条件集合 N.同步控制机制中的实时标准为期望的截止期错失率 DDMP.系统中将根据实际情况动态调节 C_{thres},V_{thres} 和 DDMP 这 3 项标准,并按照这些标准确定采用安全控制协议的概率 q.

由参考文献[5]中根据信道容量进行并发控制的方法,我们对以上机制的实现设计如下:

1. Calculate q given C_{thres};
2. Monitor conflicting transactions and collect SMM data;
3. If (tr_{high} conflict with tr_{low}) and ($ml<N_{high}$)
   calculate τ and ρ for small message of $TRU(tr_{high})$, then get small message value V;
   If ($V>V_{thres}$)
      increase q or use secure CC protocol to cut off covert channel between user $TRU(tr_{high})$ and user $TRU(tr_{low})$;
      send message to security administrator;
4. Observe resulting deadline miss *percentage*(*DMP*);

5. If ($DMP \geq DDMP$)

send message to system administrator;

adjust $DDMP$ and/or (C_{thres},V_{thres});

jump to Step 1;

Else if ($DDMP-DMP>DMP_{span}$)

increase q to 1;

6. Jump to Step 2;

在该机制中,系统优先满足安全需求,即要求系统中的信道威胁符合容量 C_{thres} 和价值 V_{thres} 的约束.系统首先根据 C_{thres} 确定干扰概率 q.在监视到系统中事务冲突时,收集冲突所代表的潜在信道的 SMM,计算出信道传输短消息的价值 V,当 V 超过阈值 V_{thres} 时,系统将提高 q 值,或者在这两个事务的所属用户之间完全采用安全控制协议切断信道.当系统实时性表现良好,即实际错失率比期望错失率还要低 DMP_{span} 时,则可以调高系统的安全保障程度,即完全采用安全控制协议(q=1).当系统的截止期错失率超出期望范围时,即 DMP 超过 $DDMP$,则需要降低系统的事务准入比率,减少系统的负载,或者降低系统对隐蔽信道的限制程度(C_{thres},V_{thres}).

然后证明该方法的正确性:该实现方法可以保证信道威胁满足(C_{thres},V_{thres})的限制.当 q 增加时,信道容量将减少,直至下降为 0.因此,给定 C_{thres},一定能够求取相应 q 值使得信道容量 $C \leq C_{thres}$.同样,当 q 增加时,短消息传输价值将下降,直至下降为 0.因此给定 V_{thres},也能够通过求取相应 q 值使得短消息传输价值 $V \leq V_{thres}$.按照两个概率中较大者执行安全并发控制协议,就能够保证同时满足(C_{thres},V_{thres}).实时性在本方法中作为性能指标,方法中只是采取措施谋求减少实时性能损失,但并不保证实时标准 DDMP 的满足.该方法运算简单,运算复杂度为 $O(1)$.

5 实验分析

5.1 实验环境设定

在基于相对安全目标的信道度量和限制机制中,旨在根据量化指标限制信道威胁,从而避免完全禁止潜在隐蔽信道的操作对系统实时性能的影响.本节利用模拟实验,分析 CoCCM 机制的执行效果.主要关注于短消息指标实施条件下 SRTDB 系统的实时性能表现.实验中采用与文献[5,13]类似的数据库模型:单机磁盘驻留数据库系统,数据库运行在共享内存的多个处理器上.模拟系统中采用 CoCCM 并发控制机制.除了数据库的基本性能参数和负载参数外,为了实现短消息限制策略,还需要设置以下参数(见表 1).

Table 1 Data parameters of database

表 1 数据库中数据的相关参数

Parameter	Meaning	Value
Min*Size*	Minimum data length	8 (bit)
Max*Size*	Maximum data length	1 024 (bit)
Min*Life*	Minimum data sampling period	100 (ms)
Max*Life*	Maximum data sampling period	2 000 (ms)
LevelNum	Number of classification levels	8
N	Length bound of SMR for different classification level (listed from high to low according to classification level)	256,128,64,32,16,16,16,16 (bit)

其他环境说明还包括:数据项的消息价值函数都为脉冲类型;数据的有效时间等于采样周期,在最短和最长采样周期之间平均分布,*LifeTime*=*Uniform*(Min*Life*,Max*Life*);用户所拥有的最短数据项长度在数据的最短和最长长度之间正态分布,*DataSize*=*Normal*(Min*Size*,Max*Size*).

实验中采用短消息指标和信道容量度量信道威胁,指导安全保障.对实时性能的评价则采用事务截止期错失率 DMP:

$$DMP = \frac{\text{Number of transactions missing deadline}}{\text{Total number of transactions}}.$$

另一个实时性能评价指标为吞吐量(throughput),其定义为:在满足一定事务截止期错失率 DMP_{thres} 条件下,

系统能够承受的最大事务到达速率.受篇幅所限,我们只给出吞吐量的简单定义:

$$Throughput=\max(transactions\ arrival\ rates),\ \text{when}\ DMP\le DMP_{thres}.$$

5.2 实验结果及分析

实验 1. 分析信道限制参数(C_{thres},V_{thres})对截止期错失率的影响.

图 6(a)对应的实验中,系统单独根据容量指标度量和限制隐蔽信道.由图 6 可见,在两组事务到达速率不同的数据中,DMP 都会随着 C_{thres} 的放宽(即 C_{thres} 值变大)而缩小.这是因为,当系统放宽对信道容量的限制时,系统中采用安全控制协议的概率减小,系统的实时性得到更好的保护.两组数据之间,事务到达速率较高时(25trans/sec),系统的负载较大,DMP 也就较大.图 6(b)对应的实验中,系统中加入短消息限制策略 SMMP 来限制信道的威胁,即采用 CoCCM 机制,其中 C_{thres} 固定为 5bits/sec.如图 6(b)所示,两组实验结果中,事务的截止期错失率都会随着价值阈值 V_{thres} 限制的放宽(即 V_{thres} 值变大)而缩小.当 V_{thres} 取 1 时,系统已经完全放开对信道短消息传输能力的限制,此时仍存在一定的 DMP,其由信道容量限制操作以及事务集自身过载程度来决定.同样地,两组数据之间,当事务到达速率较高时,DMP 也较大.

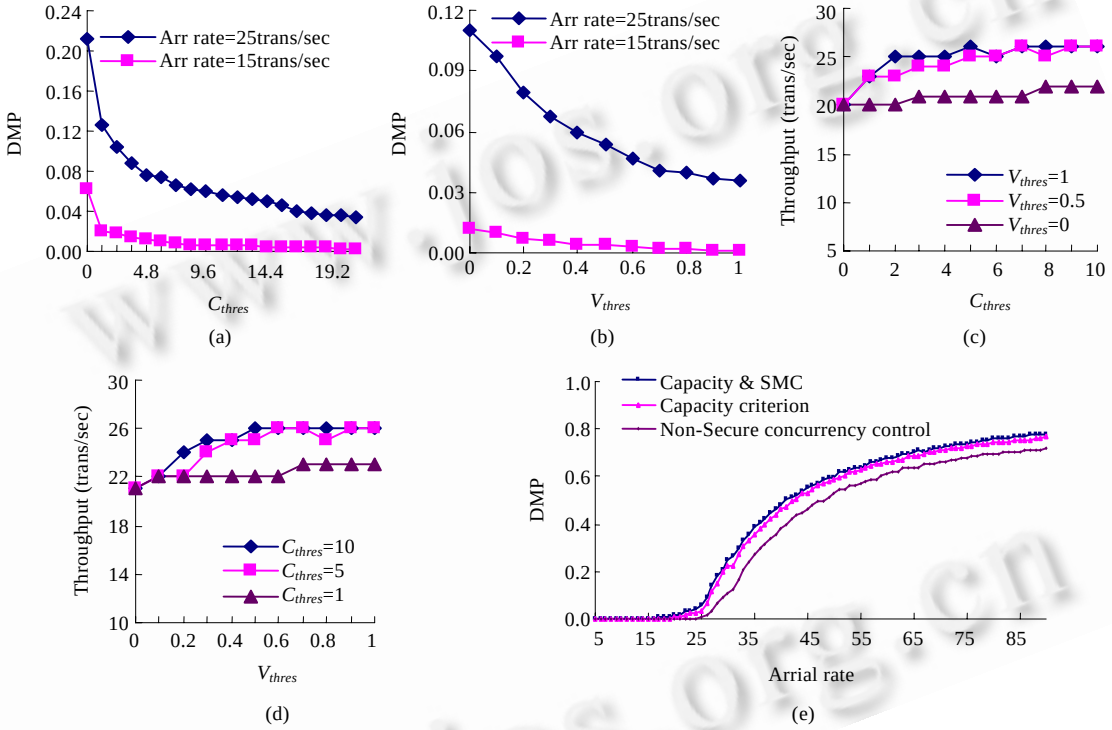


Fig.6 Illustration of experimental results

图 6 实验结果对照图

实验 2. 分析信道限制参数(C_{thres},V_{thres})对吞吐量的影响(DMP_{thres} 取 5%).

图 6(c)中各条曲线显示系统的吞吐量都将随 C_{thres} 的放宽而增大,同样,图 6(d)中各条曲线显示系统的吞吐量都将随 V_{thres} 的放宽而增大.由图 6(c)可见,当 V_{thres} 取 0 时,要求完全消除信道的短消息传输能力,此时即使 C_{thres} 放宽,冲突事务也要按照安全并发控制处理,因此,系统的吞吐量随 C_{thres} 从 0 提高到 10 时只提高了 2.而 V_{thres} 值较大的两条曲线,其吞吐量则提高了 6.在图 6(c)的各曲线之间,V_{thres} 限制越宽,吞吐量相应也就越大,这是因为系统限制信道操作越少,对系统的实时性能影响越小,系统的事务处理能力也就越强.图 6(d)中也有类似现象,各条曲线之间吞吐量随 C_{thres} 放宽而增大.另外,在图 6(c)和图 6(d)所示吞吐量随信道限制放宽而上升的曲线中,都呈现开始上升较快,后段基本稳定的特点.吞吐量在信道限制参数放宽后,将最终稳定于一个上限.该稳定值由系

统的处理能力所决定,本实验中为 26trans/sec.对照图 6(a)和图 6(b),其中 DMP 随信道限制变化的趋势同样呈现开始急、后期缓的特征.这说明,当信道限制标准较严格时,系统的实时性能对限制标准的变化更敏感.

实验 3. 系统横向比较采用不同安全策略对系统实时性能的影响.

在实验 3 中,分别研究同时采用短消息指标和信道容量的 CoCCM 机制(C_{thres}=5bits/sec,V_{thres}=0.5)和只采用信道容量以及不采用安全标准时,DMP 随系统负载(事务到达速率)变化的规律.图 6(e)中各曲线都呈两端缓和、中段陡峭的形式.这是因为,当负载较低时,系统尚有富余的处理能力,因此即使负载继续增加,也可以保证事务满足截止期.而当事务到达速率较高时,事务间时间重叠的可能性增加,冲突数量加大,使得大量事务未到截止期即被放弃,这些被放弃的事务并不记入 DMP 中,因此 DMP 增长的速度也将放缓.由图 6(e)可以看到,采用信道限制措施后,DMP 将有所升高.同时,采用两种安全标准较之采用单一标准,系统的实时性能又会有所下降.但是由于容量和短消息限制策略对隐蔽信道的限制操作有可能重叠,即潜在隐蔽信道在容量标准的限制下可能已经同时满足了短消息指标的限制,这时,短消息限制策略的实施不会带来新的实时性能损失,因此,由图 6(e)可以看到,短消息限制策略对系统实时性能的附加影响并不大.

6 结 语

本文中对短消息指标度量和限制的定义克服了原有定义的缺点,确保了短消息限制策略的可实施性.在此基础上,结合安全实时数据库系统的特征,提出了融合短消息指标和容量的信道威胁度量和限制机制 CoCCM.与现有的单一信道威胁度量、限制方法相比较,本文的方法同时从信道传输能力以及用户利用信道传输的数据的特征两个方面考察信道威胁,融合了安全级别差别、信道容量和短消息传输能力 3 种度量方式,提高了信道威胁度量的全面性和限制标准的健壮性.实验结果表明,CoCCM 机制实施效果良好,能够提供对信道威胁的可调节的限制,并且对系统实时性能附加影响较小,可以用来在系统实时和安全需求之间求取动态均衡.

另外,文章中短消息指标的定义虽然是在安全实时数据库中事务隐蔽信道度量场景下给出的,但是其中并没有包含该场景下所特定的条件和参数.在安全数据库中,用户所拥有或能够访问的数据长度容易确定,因此只要能够确定短消息传输价值函数,则短消息指标也可以应用于安全数据库中的其他信道,如推理信道和安全机制引入的信道.对于安全操作系统、安全网络等其他信息系统,在确定用户可能传输的消息长度参数和消息价值函数的条件下,同样能够应用短消息指标的新定义对其隐蔽信道威胁进行度量和限制.

如何继续增强短消息限制策略的健壮性,避免恶意用户绕过策略盗取信息,并将短消息指标应用于其他隐蔽信道限制场景,是本文作者未来的工作重点.

致谢 在此,我们向对本文的工作给予支持和建议的老师和同学,尤其是中国科学院软件研究所基础软件国家工程中心的贺也平研究员、沈建军博士、何建波博士和刘伟博士表示感谢.

References:

[1] U. S. Department of Defense. Trusted computer system evaluation criteria. DoD 5200.28-STD, 1985.

[2] Millen J. 20 years of covert channel modeling and analysis. In: Proc. of the 1999 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1999. 113−114. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=766906

[3] Ahmed QN, Vrbsky SV. Maintaining security and timeliness in real-time database system. Journal of Systems and Software, 2002, 61(1):15−29.

[4] Moskowitz IS, Kang MK. Covert channels—Here to stay? In: Proc. of the 9th Annual Conf. on Computer Assurance. Gaithersburg: National Institute of Standards and Technology, 1994. 235−243. http://www.itd.nrl.navy.mil/ITD/5540/publications/CHACS/1994/index1994.html

[5] Son SH, Mukkamala R, David R. Integrating security and real-time requirements using covert channel capacity. IEEE Trans. on Knowledge and Data Engineering, 2000,12(6):865−879.

[6] Son SH, Chaney C, Thomlinson NP. Partial security policies to support timeliness in secure real-time databases. In: Proc. of the 1998 IEEE Symp. on Security and Privacy. 1998. 136−147. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=674830

[7] Yan HP, Wang W, Shi BL. Inference control in secure database. Journal of Software, 2006,17(4):750−758 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/17/750.htm

[8] He YZ, Li L, Feng DG. A generic audit policy model on multilevel secure DBMS. Journal of Software, 2005,16(10):1774−1783 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1774.htm

[9] Keefe TF, Tsai WT. Database concurrency control in multilevel secure database management systems. IEEE Trans. on Knowledge and Data Engineering, 1993,5(6):1039−1055.

[10] Son SH, David R. Design and analysis of a secure two-phase locking protocol. In: Proc. of the 8th Annual Int'l Computer Software and Applications Conf. Taipei: IEEE Computer Society Press, 1994. 374−379. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=342775

[11] Jeong BS, Kim D, Lee SY. Optimistic secure real-time concurrency control using multiple data version. In: Proc. of the LCTES 2000. LNCS 1985, 2001. 33−47. http://www.springerlink.com/content/9efj8yrl00yu2c91/

[12] Park C, Park S, Son SH. Multiversion locking protocol with freezing for secure real-time database systems. IEEE Trans. on Knowledge and Data Engineering, 2002,14(5):1141−1154.

[13] George B, Haritsa JR. Secure concurrency control in firm real-time database systems. Distributed and Parallel Databases, 2000,8(1):41−83.

[14] Kang KD, Son SH, Stankovic JA. STAR: Secure real-time transaction processing with timeliness guarantees. In: Proc. of the 23rd IEEE Real-Time Systems Symp. IEEE Computer Society Press, 2002. 303−314. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1181584

[15] Son SH, David R, Thuraisingham B. Improving timeliness in real-time secure database systems. ACM SIGMOD Record, 1996, 25(1):29−33.

[16] National Computer Security Center. A guide to understanding covert channel analysis. NCSC-TG-003, Version 1, 1993.

[17] Qing SH, Zhu JF. Covet channel analysis on ANSHENG secure operating system. Journal of Software, 2004,15(9):1385−1392 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/1385.htm

[18] Moskowitz IS, Greenwald SJ, Kang MH. An analysis of the timed Z-channel. In: Proc. of the 1996 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society Press, 1996. 2−11. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=502664

附中文参考文献:

[7] 严和平,汪卫,施伯乐.安全数据库的推理控制.软件学报,2006,17(4):750−758. http://www.jos.org.cn/1000-9825/17/750.htm

[8] 何永忠,李斓,冯登国.多级安全 DBMS 的通用审计策略模型.软件学报,2005,16(10):1774−1783. http://www.jos.org.cn/1000-9825/16/1774.htm

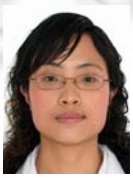
[17] 卿斯汉,朱继锋.安胜操作系统的隐蔽信道分析.软件学报,2004,15(9):1385−1392. http://www.jos.org.cn/1000-9825/15/1385.htm

曾海涛(1979－),男,山西太原人,博士生,主要研究领域为操作系统安全,数据库安全,实时系统.

王永吉(1962－),男,博士,研究员,博士生导师,主要研究领域为实时系统,网络技术,软件工程.

祖伟(1980－),女,博士生,主要研究领域为智能控制,路径规划,计算机仿真.

蔡嘉勇(1978－),男,博士生,主要研究领域为信息系统安全理论和技术.



阮利(1978－),女,博士生,主要研究领域为软件过程建模,软件过程挖掘,软件度量,数据挖掘,运筹学.