

LogicSQL 多级安全数据库的研究与实现

马新强¹, 王保华¹, 李丹宁², 黄 羿¹

(1. 贵州大学 信息工程学院, 贵州 贵阳 550003;

2. 贵州科学院, 贵州 贵阳 550001)

摘 要:结合数据库的用户身份认证与自主访问控制研究,设计了 LogicSQL 多级安全模型。该模型把安全级分为分层密级和非分层的范围组成的二元组形式,主要从安全标签、强制访问控制和审计方面进行讨论。该模型在企业搜索与公安系统中得到应用。

关键词:LogicSQL;强制访问控制;多级安全模型

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2007)03-0156-03

Research and Implementation of LogicSQL Multilevel Security Database

MA Xin-qiang¹, WANG Bao-hua¹, LI Dan-ning², HUANG Yi¹

(1. School of Information Engineering, Guizhou University, Guiyang 550003, China;

2. Guizhou Academy of Sciences, Guiyang 550001, China)

Abstract: A multilevel security model of LogicSQL database, which is based on user identifier, discretionary access control (DAC) of database, is designed. Multilevel security model requires that all users and resources are classified and assigned a security label, which is a combination of a hierarchical security level and non-hierarchical security categories. Discussed a few aspects of LogicSQL multilevel security model, including LogicSQL label, mandatory access control (MAC), and audit. The model is applied in enterprise search and police system.

Key words: LogicSQL; mandatory access control; multilevel security model

0 引言

数据库作为信息的载体其安全性越来越受到重视,尤其是网络环境下的数据库安全成了重中之重。目前,国内大部分企事业单位,包括国家的一些关键部门,大都使用国外进口的数据库产品,如 ORACLE, SYBASE, DB2 等。而这些国外数据库产品的最高安全等级为 C2 级,更高级别的数据库产品是限制对我国出口的。要使用 B1^[1]以上级别的安全数据库只有基于拥有全部源代码和自有知识产权的数据库管理系统进行开发。大型通用数据库系统 LogicSQL^[2]由于其创新的核心技术——formula lock 和逻辑并发控制,使得按照国际公认的测试标准 (TPC-C benchmark tests) 测试指标 (在中小型服务器上) 达到或超过美国

的主流产品。正如 2002 年 11 月,科技部 863 数据库重大专项总体专家组评语所说:“这是近几年内中国能与美国主流数据库产品抗衡的唯一希望”。在此基础上开发和加强 B1 级别以上的安全数据库尤为重要。

文中在 LogicSQL 的用户身份认证与自主访问控制基础上定义多级安全模型,给每一数据对象定义以安全级,表示它所包含的信息的敏感性,同时给每一用户定义安全级,表示他能对什么样的数据进行访问。

1 LogicSQL 的用户认证与自主控制

1.1 用户安全策略

数据库用户是连接数据库、存取数据库对象(表和记录等)的通道,通过对数据库用户账户的管理达到实现数据库系统的安全目的。LogicSQL 数据库提供两种认证机制:数据库认证和操作系统认证。若采用数据库认证方式,则每个数据库用户都必须有唯一的数据库用户名和密码,在连接数据库时输入。每个 SQL-session 都有一个 SQL-session 用户认证,这个用户认证是参考当前的活动用户和会话用户;它也能被

收稿日期:2006-06-02

基金项目:贵州省优秀科技教育人才省长专项基金项目(黔省专合字(2005)88号)

作者简介:马新强(1979-),男,山东济宁人,硕士研究生,研究方向为数据库安全与人工智能;李丹宁,副研究员,硕士生导师,博士,研究方向为数字地球。

SELECT CURRENT_USER FROM INFORMATION-SCHEMA.dual 所查询。若采用操作系统认证,则不需要数据库用户名和密码,只需将操作系统中该用户的用户名传给数据库服务器,数据库服务器在连接完成之前判断此用户是否被授权访问数据库。权限的管理除了用户身份认证以外,还通过角色(Roles)进行权限的设置和更改等。角色权限划分为两种:(1)角色直接被授予;(2)角色通过其它角色进行授予其角色控制,命令有:CREATE ROLE, DROP ROLE, SET ROLE, REVOKE ROLE 等。

1.2 自主访问控制机制

自主访问控制^[3](DAC, Discretionary Access Control)就是根据用户持有的特权限制其对数据库客体的访问,用来 need-to-know 访问控制。在 LogicSQL 数据库中的客体指:数据库、表、视图、触发器、存储过程、函数、包、索引等数据库中的对象。有两种类型的特权:系统特权和客体特权。系统特权指允许执行数据库内的特定操作,LogicSQL 数据库中的系统特权命令有:CREATE USER, DROP USER, ALTER USER, SET SESSION USER, GRANT PRIVILEGE, REVOKE PRIVILEGE 等。客体特权指在一个数据库客体上执行特定操作,LogicSQL 数据库对客体的访问控制有以下命令:SELECT, INSERT, UPDATE, DELETE, REFERENCES, EXECUTE, CONNECT, CREATE TABLE, CREATE VIEW, CREATE INDEX, CREATE TRIGGER 等。

2 LogicSQL 的多级安全模型

2.1 多级安全模型的形式化定义

定义1 客体。 $O = \{Da, D, T, V, F, A, Tp\}$; Da (数据库), D (数据), T (表), V (视图), F (存储过程/函数), A (列属性), Tp (元组)。模型中的客体是多级安全数据库中的载体,客体是受保护的對象,模型中的客体分为三层,第一层为数据库,第二层为表、视图、存储过程/函数,第三层为属性和元组,这样客体集合形成了一个三层的隶属层次关系树,隶属关系记为: \in 。对于任意两个客体 O_1, O_2 , $O_1 \in O_2$ 表示 O_2 在隶属层次关系中是 O_1 父节点,例如客体 O_2 代表一个数据库,客体 O_1 代表一张表, $O_1 \in O_2$ 表示表 O_1 是数据库 O_2 中的一张表。

定义2 主体。 $Sub = \{DU, SSO, AT\}$; DU (数据库用户), SSO (数据库安全管理员), AT (数据库审计员)。系统实现基于角色的管理^[4], LogicSQL 采用“三权分立”的安全机制,把系统管理员分为数据库管理员(DBA)、数据库安全管理员(SSO)、数据库审计员(AU-

DITOR)三类。DBA 负责系统维护与日常管理和自主存取控制,SSO 负责强制存取控制,AUDITOR 负责系统的审计。这种管理体制真正做到三权分立,各行其责,相互制约,从而更为可靠地保证数据库的安全性。

定义3 分层密级。 $L = \{L_1, L_2, L_3, \dots, L_n\}$ 表示分层密级,设 $L_i (1 \leq i \leq n)$ 表示 n 个名称,且 $L_1 \leq L_2 \leq L_3 \dots \leq L_n$ 。分层密级是一系列按密级高低的升序的名称序列,也称为敏感度或密级,有的文章用密级区间来表示分层密级: $[LOW \dots HIGH]$ ^[3]。LOW 表示最低密级, HIGH 表示最高密级,且 $LOW \leq HIGH$ 。若 $LOW = HIGH$, 表示系统没有划分级别。如在 LogicSQL 数据库中:公开 U、秘密 C、机密 S、绝密 TS 等名称构成分层密级 $L = \{U, C, S, TS\}$ 且有: $U < C < S < TS$ 。

定义4 多范围。 $C = \{C_1, C_2, C_3, \dots, C_m\}$ 表示数据在各个方面的特性,设 $C_i (1 \leq i \leq m)$ 表示 m 组类别,每一个类别是一部门范围, $C_1, C_2, C_3, \dots, C_m$ 间彼此独立无序。如: $C = \{\text{财务部, 技术部, 销售部, 市场部}\}$ 作为一个多范围集合,财务部、技术部、销售部、市场部是范围元素。

定义5 数据安全级。 $S = \{S_1, S_2, S_3, \dots, S_q\}$ 表示由 $S_i (1 \leq i \leq q)$ 组成的安全级集合, $S_i = (L_i, C_i)$ 是由分层密级和多范围组成的二元组, $L_i \in L, C_i \subseteq C$ 。安全级集合形成一个满足偏序关系的格,此偏序关系成为支配(\geq)关系。由以上定义可得出以下引理:

引理 设任意两个安全级 $S_1 = (L_1, C_1), S_2 = (L_2, C_2)$ 。

$S_1 \geq S_2 \Leftrightarrow \textcircled{1} L_1 \geq L_2, \textcircled{2} C_1 \supseteq C_2$ (S_1 支配 S_2 成立);

$S_1 = S_2 \Leftrightarrow \textcircled{1} L_1 = L_2, \textcircled{2} C_1 = C_2$;

$S_1 > S_2 \Leftrightarrow \textcircled{1} L_1 > L_2, \textcircled{2} C_1 \supset C_2$;

$S_1 < S_2 \Leftrightarrow \textcircled{1} L_1 < L_2, \textcircled{2} C_1 \subset C_2$;

$S_1 \leq S_2 \Leftrightarrow \textcircled{1} L_1 \leq L_2, \textcircled{2} C_1 \subseteq C_2$ (S_2 支配 S_1 成立);

如果 S_1, S_2 既不满足 $S_1 \geq S_2$, 也不满足 $S_1 \leq S_2$, 认为 S_1, S_2 不可比。

定义6 多级关系模式^[5]。用 $R(A_1, C_1, A_2, C_2, \dots, A_n, C_n, TC)$ 表示,其中 A_i 是域 D_i 上的数据属性, C_i 是元组的分层密级属性, TC 是元组的多范围安全级; (C_n, TC) 构成的二元组是系统安全员在定义基表的安全级集合中的元素。

2.2 LogicSQL 标签

LogicSQL 标签安全是 LogicSQL 的一个重要的安全选项,它是以虚拟专用数据库(VPD)^[6]记述为依据,

支持行粒度级安全标签。允许不同敏感度的数据存储在单一数据库中,通过安全身份来限制对敏感信息的访问。标签安全中的敏感标签包括三部分: Levels, Compartments, and Groups。每一个策略都规定了相应的 Levels, Compartments, and Groups, 数据可以被赋予由此三者任意的组合形成的标签。对于每一个策略, 用户都有一个最大和最小的敏感 Levels、零个或者更多的 Groups, 也就是用户的标签授权。用标签策略访问数据, 是看三个内容的关系: Data Labels, User Labels, Policy Privileges; 用户标签在拥有授权的前提下, 看是否与数据标签一致或大于其标签组合才能执行行级动作。如图 1 所示: LogicSQL 标签实例。

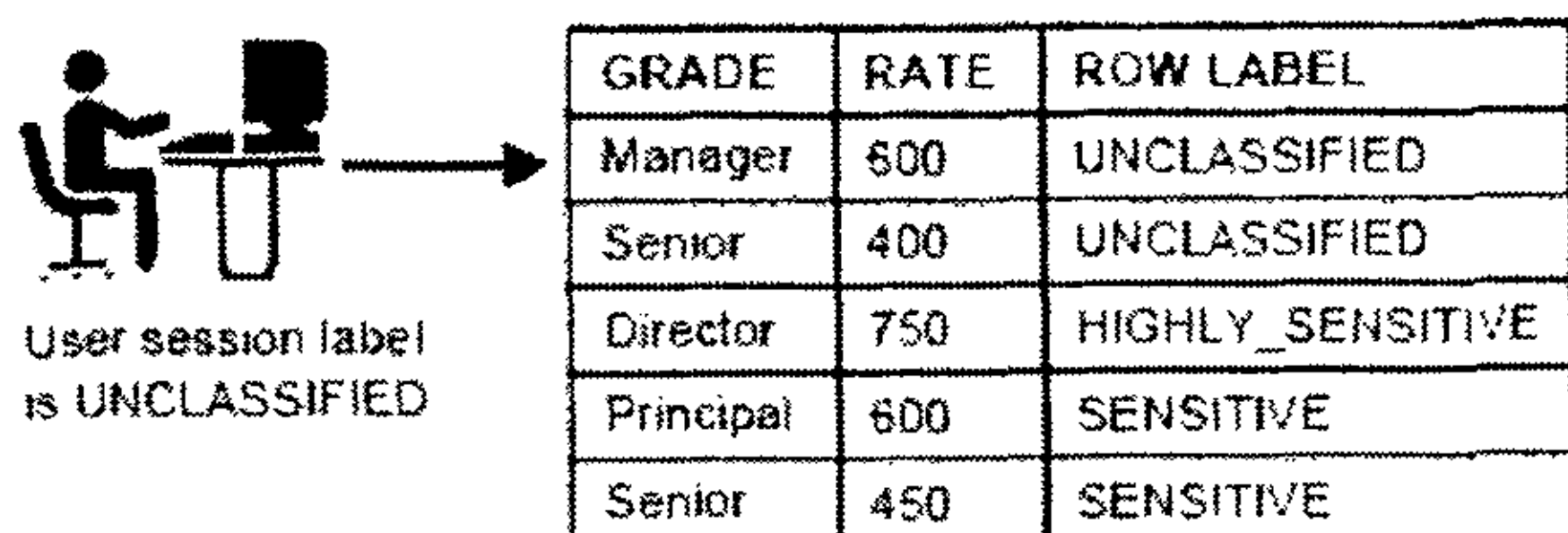


图 1 LogicSQL Label 实例

LogicSQL 中用下列过程实现标签:

SA_SESSION.SET_LABEL,
SA_SESSION.SET_ROW_LABEL,
SA_SESSION.RESTORE_DEFAULT_LABELS,
SA_SESSION.SAVE_DEFAULT_LABELS 等。

2.3 强制访问控制

LogicSQL 中自主存取控制是必需的, 数据库主体(用户、角色)只有获得了某对象的存取权限后, 才能存取该对象。强制访问控制^[3](MAC, Mandatory Access Control)是可选的, 这是从系统的灵活性和效率方面考虑的。当选择强制存取控制时, SSO 为系统的每个主体和对象定义密级, 只有当主体的安全级和对象的安全级相匹配, 且具有该对象的存取权限时, 才能存取此对象。在 LogicSQL 中, 表中的每一行的标签存储在“ROW LABEL”列中, 作为表的一部分自动生成, 对于每个数据和索引行都存储一个标签。每个用户也有一个安全级标签, 用户只能写和他安全级相同的数据, 读和他安全级相同或更小的数据。如图 2: User Session Label 与 Data Label 匹配读写运用。用户标签为 C: FIN[, OP]WR, 在表中的元组级数据标签符合的只有: U: FIN, C: OP: WR, 而其它的标签不是 Levels 就是 Compartments、Groups 与用户标签不匹配。

因此, 对于一个安全级高的用户写的的数据, 安全级低的用户肯定是无权访问的。

在 LogicSQL 中的建表举例:

CREATE TABLE student (

```
data label VARCHAR(32),
sid INT,
name VARCHAR(64) NOT NULL,
major VARCHAR(10),
PRIMARY KEY(sid)
);
```

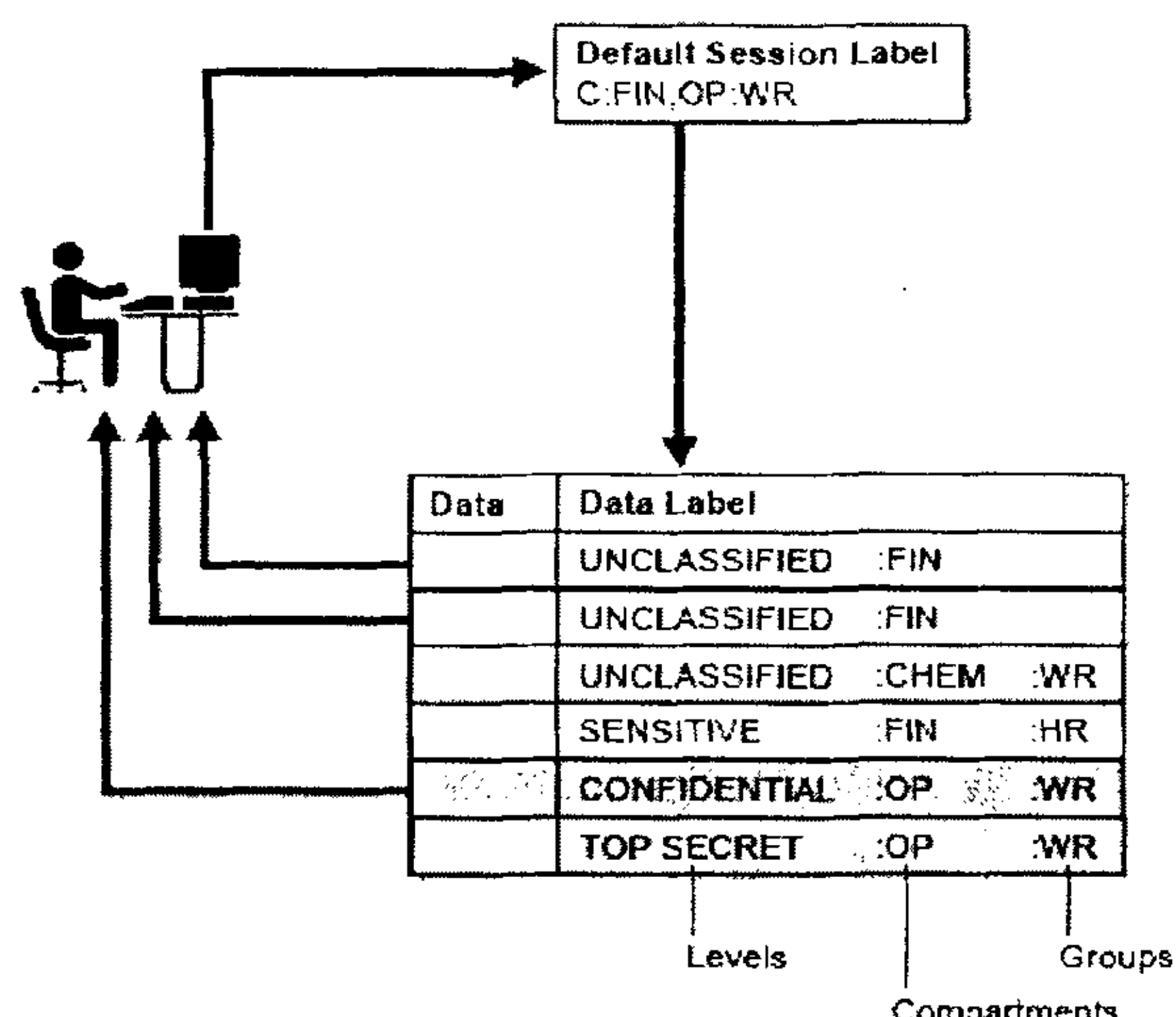


图 2 User Session Label 与 Data Label 匹配读写

在 LogicSQL 中的读操作举例:

```
LogicSQL> select * from student;
data label sid name major
.....
SENSITIVE 5500 Susan Law
UNCLASSIFIED 12001 Sarah Math
CONFIDENTIAL 12345 Peter
TOP SECRET 54321 Bob Business
```

在 LogicSQL 中“ROW LABEL”列中都存储标签, 只有使用户标签匹配或大于数据标签, 才能访问, 从而达到标签级的安全控制(即强制存取控制)。

2.4 审计

审计是对选定的用户动作的监控和记录, 通过审计, 可以把用户对数据库的所有操作自动记录下来放入审计日志中, 这样数据库系统可以利用审计跟踪的信息, 重现导致数据库现有状况的一系列事件, 找出非法存取数据的人、时间和内容等, 以便于追查有关责任; 同时审计也有助于发现系统安全方面的弱点和漏洞。按照 TDI/TCSEC^[1]标准中安全策略的要求, 审计功能也是 DBMS 达到 B1 安全级别必不可少的一项指标。LogicSQL 在一开始启动运行就有 LogicSQL log 进行监视跟踪; LogicSQL 可以根据用户、数据库行为、客体和系统特权进行审计配置。也可以根据行为成功与否来进行审计选择。审计记录被正确地赋予一个标签(Auditing Label), 表示了被审计的行为的安全级别, 以及防止未授权用户读取审计记录信息。LogicSQL

(下转第 162 页)

STM。然后 STM 发送一条查询请求给相应的 SCAR。SCAR 收集本区内每个路由器的日志信息,并分析攻击包是否通过本区。如果是的话,SCAR 判定攻击包经过的路由器并在本区内重构攻击路径。所有相关的 SCAR 把重构好的它们那部分的路径递交给 STM,然后 STM 通过分析这些结果来重构每条路径。

每个路由器分类收集下面的信息:IP 头的固定位、包有效负载的前八个字节。路由器中的分类表是用过滤器实现的,这种过滤器是一种有效节省空间的数据结构。只要一个过滤器达到七成满,就把它存档用于将来的查询,同时使用一个新的过滤器。借助 TLT(转换查找表),SPIE 可以追踪每个数据包。

2.4.2 算法分析

SPIE 是一种确定日志记录方法。它需要额外的组成部分,比如说 STM 和 SCAR。它支持更加高级的功能,比如单个包追踪。

SPIE 有三个主要缺点,它导致高计算负载、管理负载和存储负载。针对这些缺点,Li 等^[7]提出了一种基于采样的小说日志算法来优化 SPIE。通过关联采样,这种算法可以成功地重构攻击路径,他们通过仿真模拟展示了改进后的 SPIE 可以有效追踪到超过 5000 的攻击源。然而,由于现有网络的分散性,SPIE 还是很难在整个网络中推广,实际上没有一个网络的 STM 可以超出边境来使用它的管理权限,这些缺点阻碍了 SPIE 的应用。

3 结 语

文中总结和分析了可能能够实际应用的几种 IP

追踪技术。很明显,现今的 IP 追踪技术只是应对 DDoS 攻击的第一步,以后还有很多的工作要做,一个完美的 IP 追踪技术必须能够协调现实网络中的各种因素。为了更好地分析 IP 追踪技术,文中从几个方面把现有的绝大多数 IP 追踪技术进行分类,并从实用性和可行性的观点出发,深入分析和探究了这些技术的优缺点,重点突出了每个技术的改进方法。

参考文献:

- [1] Baba T, Matsuda S. Tracing Network Attacks to Their Sources[J]. IEEE Internet Computing, 2002, 16(2): 20 - 26.
- [2] Gao Zhiqiang, Ansari N. Tracing Cyber Attacks from the Practical Perspective[J]. IEEE Communications Magazine, 2005, 43(5): 123 - 131.
- [3] Savage S. Network Support for IP Traceback[J]. IEEE/ACM transactions on networking, 2001, 9: 226 - 237.
- [4] Belenky A. IP Traceback with Deterministic Packet Marking[J]. IEEE Communications Letters, 2003, 7(4): 162 - 164.
- [5] Vrizlynn. Enhanced ICMP Traceback with Cumulative Path[J]. IEEE Communications Magazine, 2005, 4: 2415 - 2419.
- [6] Snoeren A C. Single Packet Ip Traceback[J]. IEEE/ACM transactions on networking, 2002, 10: 721 - 734.
- [7] Li Jun. Large - Scale Ip Traceback in High - Speed Internet [C]//IEEE Symposium on Security and Privacy. [s. l.]: [s. n.], 2004: 115 - 129.
- [8] Stone R. CenterTrack: An Ip Overlay Network for Tracking DoS Floods[C]//USENIX Sec. Symp. [s. l.]: [s. n.], 2000: 199 - 212.
- [9] Min Fan. An IP Traceback Scheme Integrating DPM and PPM[J]. ACNS, 2003, 2846: 76 - 85.

(上接第 158 页)

利用触发器可以实现特定的、定制的审计策略。

论文的研究成果被应用于新一代企业信息搜索工具的研究课题中, LogicSQL 数据库的多级安全性为确保企业信息的完整性和保密性提供了有利条件;本数据库能够很好地应用于贵州省公安厅信息系统,再次证明其可靠性。

3 结束语

重点研究了 LogicSQL 数据库安全模型使其基本达到 B1 级别以上安全级别。但模型中隐蔽信道问题,即如何通过信息流控制和推理控制等其他安全控制机制来彻底检测与消除,还需要做进一步的研究。尤其是如何达到更细的客体粒度而不影响系统效率,形成 B2 级别的形式化模型将成为下一步研究的重点。

参考文献:

- [1] Department of Defense (DOD). Trusted Computer System Evaluation Criteria (TCSEC)[M]. Fort Meade, MD: Department of Defense, 1985.
- [2] Yuan Li - Yan. The Documentation of LogicSQL[D]. Canada: Alberta University, 2005.
- [3] 袁晓东, 冯 颖. B1 级数据库管理系统强制存取控制模型研究[J]. 计算机学报, 2000, 23(10): 1096 - 1101.
- [4] Sandhu R S, Coyne E J, Feinstein H L, et al. Role - based access control models[J]. IEEE Computer, 1996, 29(2): 38 - 47.
- [5] Sandhu R S, Chen F. The Multilevel Relational (MLR) Data Mode[J]. ACM Transactions on Information and System Security, 1998, 1(1): 1 - 26.
- [6] Levinger J. Oracle Label Security Administrator's Guide[M]. Release 2(9.2). [s. l.]: [s. n.], 2002.