第32卷 第18期 计 算 机 工 程 2006年9月
Vol.32 № 18 Computer Engineering September 2006
·安全技术· 文章编号：1000—3428(2006)18—0133—02 文献标识码：A 中图分类号：TP309.2

数据库系统隐蔽通道分析的设计

张世明，何守才
(上海第二工业大学数据库研究所，上海 201209)

摘 要：从隐蔽通道概念入手，阐述了隐蔽通道分析在Oracle中的设计思想，讨论了隐蔽通道分析的内容与层次、隐蔽通道的标识方法、隐蔽通道带宽的计算与测量、隐蔽通道的处理，就如何提高Oracle 9i安全性能提供了一种途径。
关键词：数据库安全；B2级安全；隐蔽通道标识；隐蔽通道处理

Design of Database System Covert Channel Analysis

ZHANG Shiming, HE Shoucai
(Database Research Institute, Shanghai Second Polytechnic University, Shanghai 201209)

【Abstract】 This paper elaborates a way of thinking about covert channel analysis in Oracle from the concept of covert channel, discusses contents and levels of covert channel analysis, the mark method of covert channel, the calculation and measurement of covert channel band width and the processing of covert channel, which provides a new way of improving Oracle 9i's security performance.
【Key words】 Database security; B2 level security; Covert channel mark; Covert channel processing

一直以来，欧美国家在高端技术上对我国实行禁运，在操作系统和数据库管理系统等方面，安全级别限制在C2级以下，所以目前我国市场上的Oracle、SyBase、DB2等DBMS的版本一般只提供身份鉴别、自主存取控制、数据完整性和审计等安全性保护功能，其安全级别只达到C2级，远远不能满足众多大中型企业及政务、商务网站对数据库安全的需要，因此必须提升我国现有关系DBMS的安全性能至B1级甚至B2级，以满足我国计算机信息系统对数据库安全的需要。

隐蔽通道分析是B2级安全的重要部分，2002年公安部颁布的“计算机信息系统安全等级保护DBMS技术要求”[1]和1985年美国国防部发布的“计算机安全产品评估标准”的橘皮书TCSEC[2]都明确规定，在对第4级(B2级)以上的高等级安全进行评估时，必须分析隐蔽通道，并且随着安全级别的提高，对隐蔽通道分析的要求越来越严格。

1 隐蔽通道的基本概念

正确理解隐蔽通道的定义，熟悉隐蔽通道的本质与内涵，是隐蔽通道分析的第1步。多年来，随着研究的不断深入，人们对隐蔽通道的认识也逐渐加深。

1977年，Schaefer[3]将隐蔽通道定义为：“如果一个通道从存储单元向描述资源状态的变量传输信息，则称该通道为隐蔽通道”。

1978年，Huskamp[4]为隐蔽通道下了一个新定义：“如果一个通道是通过资源分配策略和资源管理实现产生的，则称该通道为隐蔽通道”。

1983年，Kemmerer[5]将隐蔽通道定义为：“如果一个通道使用非数据客体项从一个主体向另一个主体传输信息，则称该通道为隐蔽通道”。

1990年，Tsai [6]等人提出了一种新的观点。他们认为，隐蔽通道与强制访问控制策略有密切联系，“给定一个强制安全策略模型M和它在一个系统中的解释I(M)，I(M)中两个主体I(Si)和I(Sj)之间的任何潜在通信都是隐蔽的，当且仅当模型M中的相应主体Si和Sj之间的任何通信在M中都是非法的”。

Schaefer、Huskamp和Kemmerer的定义，都是从某一个侧面描述隐蔽通道。Tsai等人的定义则较为全面地叙述了隐蔽通道的内涵，这是因为：

(1)指出隐蔽通道分析仅与强制安全策略模型有关，而与自主安全策略模型无关；

(2)指出隐蔽通道分析不仅与安全性模型相关，而且与完整性模型相关；

(3)指出隐蔽通道分析与TCB规范有关。

本文以我国国内现有的Oracle DBMS为基础，设计隐蔽通道分析。

2 设计思想

由于Oracle DBMS是一个封闭系统，且没有源程序代码，因此无法从Oracle DBMS内部来实现隐蔽通道分析，只有通过在Oracle与应用程序之间添加一个保护层(以下简称“安全构件”)来实现。

Oracle数据库系统提供了3种不同的网络访问接口：ODBC、JDBC和Oracle的专用网络访问接口。由于绝大多数的Oracle数据库的应用程序都是通过ODBC接口来访问Oracle数据库的，因此我们实现的“安全构件”将加在Oracle数据库的ODBC访问接口上，即应用程序通过ODBC接口首先访问到“安全构件”，再通过“安全构件”访问Oracle数据库管理系统。当应用程序通过ODBC接口来访问数据库中的数据时，为了能够在真正存取数据库中的数据之前对用户的访问操作进行强制存取控制检查，系统必须能够获取通过ODBC发送的数据库访问命令。但是，不论是数据库服务器

作者简介：张世明(1964—)，男，硕士、讲师，主研方向：数据库安全；何守才，教授
收稿日期：2006-07-31 **E-mail：**sm99@sohu.com

端的 ODBC 访问接口，还是在客户端的 ODBC 访问接口，都无法通过了解其实现细节来得到数据库的访问命令。因此必须按照最新的 ODBC 标准实现一套自己的 ODBC 访问接口 MyODBC，应用程序在使用 MyODBC 访问接口访问 Oracle 数据库时，首先进入该安全增强系统进行强制存取控制检查，只有检查通过后，才能允许执行对后台 Oracle 数据库的访问，若使用自己的 JDBC 访问接口访问 Oracle 数据库时，服务器端会通过“桥接器”再通过 MyODBC 访问 Oracle，如图 1 所示。

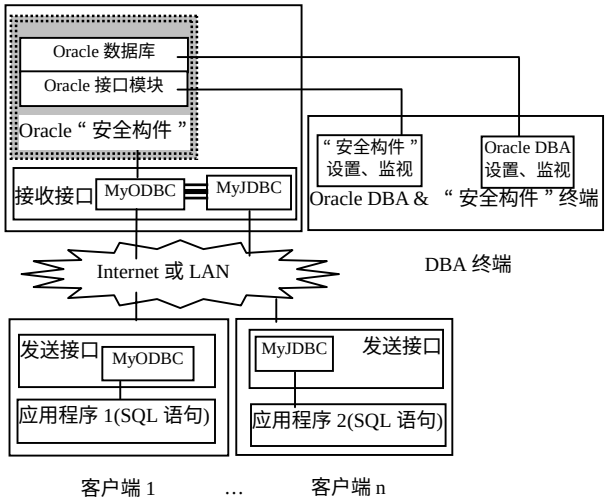

图 1 Oracle 的“安全构件”系统的体系结构

当安装“安全构件”时，系统同时将其它接口进行“封闭”，在日后访问数据库时，将拒绝通过其它的 ODBC 访问接口、JDBC 以及 Oracle 的专用网络访问接口对后台 Oracle 数据库的访问请求，以堵塞可能出现的非法访问通道。

基于上述的设计思想，本设想由 3 个部分组成：“安全构件”终端程序，MyODBC 网络访问接口，“安全构件”服务器端程序。

3 “安全构件”目标及技术

3.1 隐蔽通道分析的内容与层次

隐蔽通道的分析包含 3 个方面的内容：(1)隐蔽通道标识；(2)隐蔽通道带宽的计算与工程测量；(3)对被标识的隐蔽通道进行处理[7]。

原则上，隐蔽通道分析可以在安全数据库系统任何一个层次上进行。分析的抽象层次越高，越容易在早期发现系统开发时引入的安全漏洞。通常，根据实际需要与所采用的分析方法，在以下 3 个层次进行隐蔽通道分析：(1)描述性顶层规范(DTLS)级；(2)形式化项层规范(FTLS)级；(3)源代码级。

3.2 隐蔽通道的标识方法

彻底搜索隐蔽通道，即隐蔽通道标识的工作是隐蔽通道分析中最为困难的一环。其困难性体现在理论和工程实践两个方面：(1)理论上仍然不够成熟，缺乏严谨且行之有效的方法；(2)实际工作量庞大，手工分析容易出错，缺乏行之有效的自动工具。

在“安全构件”中，采用语义信息流方法[6]对隐蔽通道进行标识，语义信息流方法的分析步骤是：

(1)选择用于隐蔽通道分析的内核原语；

(2)确定内核变量的可见性/可修改性：1)通过语义分析，确定内核变量的直接可见性/可修改性；2)对每个原语生成一个“函数调用依赖关系”集合 FCD；3)通过信息流分析，确定内核变量的间接可见性；4)在每个原语中解决变量别名问题；5)标识在原语间共享的用户进程可见/可修改的变量，消除局部变量；

(3)分析共享变量，并标识隐蔽存储通道。

该方法的主要优点是：

(1)适用于源代码级的形式化分析，可以发现所有的潜在隐蔽存储通道，并确定强制安全规则是否正确地实现。

(2)可以发现大量伪非法流。

(3)可以找出内核共享变量被观察/修改的位置，有助于确定安置审计代码和时间延迟变量的位置。

3.3 隐蔽通道带宽的计算与测量

带宽是隐蔽通道传送数据的速度，单位是 bps。带宽的计算或工程测量非常重要，因为隐蔽通道的处理策略依赖于隐蔽通道带宽的确定。

计算无噪隐蔽通道最大带宽 B(0) 的公式：$B(0)=b(T_R+T_S+2T_{CS})-1$。其中，b是编码因子，在实际应用中通常假设为 1。T_R表示接收进程观察共享变量所需的时间，以及接收进程建立隐蔽通信环境所需的时间。T_S表示发送进程修改共享变量所需的时间，以及发送进程建立隐蔽通信环境所需的时间。当为一个新进程分配CPU时，内核从当前进程向新进程执行一个“上下文切换”操作。T_{CS}即表示进程切换或上下文切换所需的时间。

理论上计算或估算出的最大带宽必须符合实际。因此，实际测量隐蔽通道的带宽，即测量每个通道真实的最大带宽，是一项十分重要的任务。但是，进行准确测量是十分困难的。因为，我们很难准确测量一个原语的执行时间，而且很难刻画隐蔽通道真实应用的场景。

在测量隐蔽通道的带宽时，应当遵循如下原则：(1)在有或无出错返回这两种情形下，掌握一个原语观察一个变量所需的时间；(2)在测量时，仅选择修改和观察每一个隐蔽通道变量最快的 TCB 原语对；(3)被选择的修改原语和观察原语必须能够合作传送隐蔽信息。注意，当使用 TCB 原语进行隐蔽通道信息传输时，既可能依赖于系统状态，即环境；也可能依赖于调用参数。因此，通道中速度最快的原语不一定被用于数据传输。通常，如果一个原语使用最短的时间观察一个无出错返回的变量，那么，该原语也使用最短的时间观察一个有出错返回的变量。在其它情形，需要应用理论计算或估算的结果帮助选择原语。如果原语已经近似地选定，就可以开始测量隐蔽通道真实的最大带宽。

3.4 隐蔽通道的处理

“安全构件”使用审计法进行隐蔽通道的处理，审计法是一种威慑方法，它的目的是无二义性地检测隐蔽通道的应用，监控系统中已知隐蔽通道的使用情况。对审计机制的基本要求只有一条：不错报。首先，保证审计机制不被旁路，即不漏报；其次，保证准确审计，即不误报。事实上，这个要求很难达到。审计的固有困难性表现在：(1)很难区分 TCB 原语的正常应用与非正常应用(产生隐蔽通道)；(2)很难区分隐蔽通道中的发送进程与接收进程。甚至，有些隐蔽通道是无法进行审计的。

4 小结

我们在前期的“安全构件”中已经设计了“身份鉴别功能、自主访问控制、标记、强制访问控制、审计、数据完整性、安全构件自身保护”等 B1 级安全性能，隐蔽通道分析设计是 B1 级向 B2 级提升的新增需求。 (下转第 154 页)