隐蔽通道在 SQL 缓存中的分析研究

李顺新,杨 鑫
(武汉科技大学 计算机学院,湖北 武汉 430081)

摘 要:在 ASP.NET 网络程序开发中,由数据库驱动的 Web 应用程序,为使从数据库读取的数据能及时、准确、快速地提供给访问客户,通常采用 SQL 缓存技术。但将数据库表的内容以缓存技术存储到内存中时,存在着由数据缓存等待而产生的隐蔽通道问题。针对内存缓存等待中的隐蔽通道问题进行分析研究,以此提高 Web 应用程序的系统安全和信息存取安全。

关键词:Web 应用程序;SQL 缓存技术;隐蔽通道;系统安全

中图分类号:TP301 **文献标识码**:A

Analysis and research of covert channel in SQL cache

LI Shun Xin, YANG Xin
(Computer College, Wuhan University of Science and Technology, Wuhan 430081, China)

Abstract: In the network software development of ASPNET, the Web application program drived database generally uses SQL cache technology, in order to improve the efficiency of accessing the datum from database, timely, accurately, swift serve clients. But when the contents of datum stored in the cache, the covert channel problem inevitably occurs, due to the existence of data cache waiting. The paper analyzes and researches the covert channel problems in the memory cache waiting, to improve the sysytem safety of the Web application program and the safety of information access.

Key words: Web application program; SQL cache technology; covert channel; system security

随着 ASP.NET2.0 与 SQL Server 网络应用程序开发的快速发展,在由数据库驱动的 Web 应用程序中,为从数据库读取的数据能及时、准确、快速地提供给访问客户,通常采用缓存技术。但在使用 SQL 缓存[1-2]提高效率的过程中,内存中缓存的数据等待时间较长,存在数据信息安全的隐蔽通道问题。

1 Web 应用程序中的 SQL 缓存

随着 ASP.NET 技术的不断完善,在 ASP.NET2.0 中增加一组新的 DataSource 控件,通过使用 DataSource 控件,使在 ASP.NET 页面上访问数据库数据的访问方式得到优化和改变,以此创建可以显示数据库数据的 ASP.NET 页面,避免编写多余的访问数据库的代码。

在使用 DataSource 控件时,不仅可以有效连接数据库,同时还可以通过设置 SqlDataSource 控件上的属性,自动在内存中缓存有 DataSource 控件表示的数据[1-2],以此在 Web 应用程序中,对数据库数据能及时、准确、快速地访问。

在使用 DataSource 控件时,通过设置 SqlDataSource 控件上的属性,将那些大量由服务器资源获取到的数据集存储在内存中,可以提高客户端快捷地获取服务的效率。但由于客户端用户的实际操作,会存在内存中缓存的数据存储等待时间过长,甚至数据过期。例如,当服务器基础数据库中的数据发生变化时,而使用 SqlDataSource 控件属性设置在客户端内存中存储的数据库表的内容没有得到及时更新,则在 Web 应用程序中会显示旧的、过期的、不准确的数据信息。

为改变因缓存技术带来的不足,在 ASP.NET2.0 新增加了 SQL 缓存无效功能,利用 SqlCacheDependency 类实现 SQL 缓存无效功能。即:在 SQL Server 数据库对象和 Web 应用程序缓存对象之间,建立 SQL 缓存依赖关系,由 SqlCacheDependency 对象监控 Web 应用程序中建立的相关缓存依赖关系的数据对象的相关行为。如果修改依赖关系对应的数据对象发生变化时,SqlCacheDependency 对象会自动移除存储在缓存中的对应对象。当客户端 Web 应用程序再次访问请求该缓存对象时,如果该对象不在缓存中,SqlCacheDependency 对象会向缓存

中填充更新的最新版本，并保证具有最新的数据。

2 隐蔽通道

在操作系统安全方面，通常存在如下5个主要操作系统安全威胁：病毒和蠕虫、逻辑炸弹、特洛伊木马、天窗、隐蔽通道[3]。本文重点分析研究ASP.NET与SQL Server应用程序开发中SQL缓存中的隐蔽通道问题。

2.1 隐蔽通道概念及分类

随着计算机技术的迅速发展，人们对信息安全问题的认识逐渐深刻。通常对系统或应用程序进行的各种入侵攻击多是通过分析操作系统和应用程序的弱点或缺陷来实现的。

在操作系统安全威胁中，隐蔽通道是指系统中不受安全策略控制的、违反安全策略的信息泄露路径。按信息传递的方式和方法区分，可把隐蔽通道分为：隐蔽存储通道和隐蔽定时通道。隐蔽存储通道在系统中通过2个进程利用不受安全策略控制的存储单元传递信息，2个进程中的前1个进程通过改变存储单元的内容发送信息，后1个进程通过观察存储单元的变换来接收信息。隐蔽定时存储通道在系统中通过2个进程利用其中1个不受安全策略控制的广义存储单元传递信息，其前1个进程通过改变广义存储单元的内容发送信息；后1个进程通过观察广义存储单元的变换接收信息，并用实时时钟这样的坐标进行测量。广义存储单元只能在短时间内保留前1个进程发送的信息，后1个进程必须迅速地接收广义存储单元的信息，否则信息将消失，如图1所示的隐蔽定时通道[3-4]。

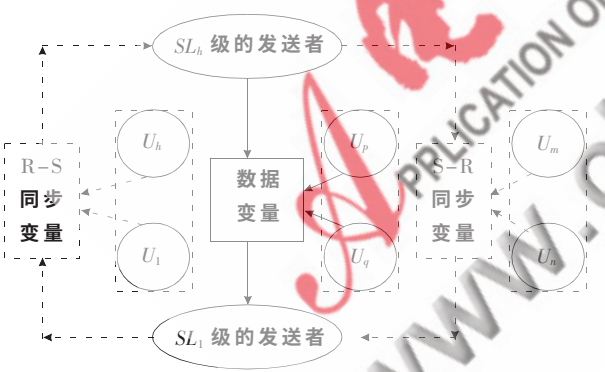

图1 发送者S与接收者R之间的隐蔽通道

2.2 常用隐蔽通道标识技术

随着信息安全技术的不断完善和发展，在20世纪80年代前期，隐蔽通道分析的对象大体上为特定的系统机制或者特定的系统功能(如多级目录机制)。目前常用的隐蔽通道标识技术有[3-4]：

(1)句法信息流分析法(Syntactic Information flow Analysis)：是一个比较系统的隐蔽通道分析方法，但此方法不宜分析类似操作系统内核的大规模程序，故在实际的系统分析中较少应用。但此方法对后来出现的SRM等方法奠定了相关概念基础。

(2)无干扰分析法(Noninterference Analysis)：此方法能把可信计算(TCB)视为一个抽象机。通常1个进程的1个请求操作会得到1个相应的响应，如1个有效响应、1个数据值、或者1个错误消息，因此该抽象机将把1个进程的请求作为输入，把对它的响应作为1个输出，任意给定时刻抽象机内部变量和数据结构的内容就是抽象机的当前状态。分析系统的时候，源代码或者更抽象一些的形式化/描述性规范都可以使用这些变量和数据结构。

(3)共享资源矩阵分析法SRM(Shared Resource Matrix)：在该分析法中，首先要统计主体可以读或写的所有共享资源(系统变量)，然后检查每个共享资源，确定它是否可能被用来在各个主体之间隐蔽地址传递信息，要完成这一步需要仔细研究每个TCB原语的貌似。此外，由于两个进程可能读写同一个共享资源的不同属性，因此需要进一步精化，指出共享资源的每个属性。

(4)语义信息流分析法(Information-flow Analysis with Semantic Component)：此分析法是借鉴了Denning信息流分析和Kemmerer共享资源矩阵法的优点设计而成，并在安全Xenix项目中用这种方法进行隐蔽通道分析工作的。

(5)隐蔽流树分析法CFT(Covert Flow Tree Analysis)：该分析法采用树结构将信息从一个共享资源向另外一个共享资源的流动过程建模，实现对通过共享变量属性发送、能被监听进程接收的通信系统化搜索，从而提供查找隐蔽通道场景的方法。

2.3 隐蔽通道处理技术

隐蔽通道的常用处理技术有消除法和宽带限制法等[3]。

(1)消除法：是指消除隐蔽通道。消除隐蔽通道需要改变系统的设计和实现，改变通常包括：消除系统潜在的隐蔽通信参与者的共享资源和消除导致隐蔽通道的接口和机制。

(2)带宽限制法：通过设法降低通道的最大或者平均带宽，使之降低到一个事先预定的可以接受的带宽程度的一种带宽限制策略，以此实现处理隐蔽通道问题。限制带宽的方法有：故意引入噪音，即用随机分配算法分配诸如共享表、磁盘分区、PID等共享资源的索引或者引入额外的进程随机修改隐蔽通道的变量；其次是故意引入延时。

3 SQL缓存中的隐蔽通道分析研究

在ASP.NET2.0与SQL Server相结合由数据库驱动的Web网络应用程序开发中，采用缓存技术可以提高从数据库读取数据的效率，能及时、准确、快速地为访问客户服务。但内存中缓存的数据可能会存储时间较长，会出现数据信息不受安全策略控制的、违反安全策略的信息泄露路径。因此，在重要的Web网络应用程序开发中，要对SQL缓存中可能存在的隐蔽通道问题进行分析研究，确保由此引发的隐蔽通道数据信息安全问题得到有效解决。

由信息传递的方式和方法对隐蔽通道的分类可知，隐蔽存储通道和隐蔽定时通道在SQL缓存中都可能存

在。特别是隐蔽存储通道在数据被存储到内存后，会在系统中通过 2 个进程利用不受安全策略控制的存储单元传递信息。2 个进程中的前 1 个进程通过改变存储单元的内容发送信息；后 1 个进程通过观察存储单元的变换来接收信息，以此对存储在内存中的信息进行读取操作。而 SqlDataSource 控件上设置的属性只能将那些大量服务器资源获取到的数据集存储在内存中，提高客户端快捷地获取服务的效率，但不能保障数据信息的信息安全不被破坏或访问。

使用 ASP.NET2.0 新增功能 SQL 缓存无效技术，利用 SqlCacheDependency 类，在 SQL Server 数据库对象与应用程序缓存对象之间建立一种缓存对象，然后在 SQL Server7.0/2000 版本中，使用轮询技术使缓存无效。同时，对缓存内容建立安全策略监控机制，对其内容的访问权限、安全策略、读取存储路径等安全因素进行监控分析，以此提高缓存中内容的数据信息安全和整个系统的安全[5-7]。SQL 缓存中的隐蔽通道分析功能设计如图 2 所示。

隐蔽通道系统安全分析技术应用在 ASP.NET 与 SQL Server 的 Web 应用程序开发中，在提高整个 Web 应用程序性能的同时，能有效保证 SQL 缓存数据信息的安全和用户数据信息的安全，这在 Web 应用程序开发中具有重要的实际应用意义。

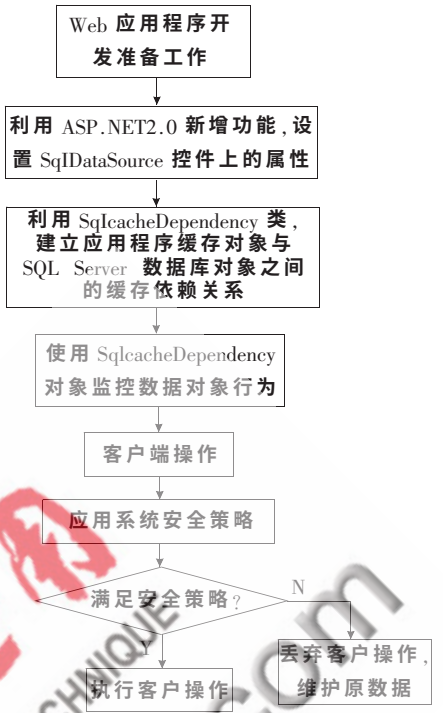

图 2 SQL 缓存中的隐蔽通道分析功能图

参考文献

[1] 贺伟，陈哲，龚涛，等.新一代 ASP.NET2.0 网络编程入门与实践[M].北京：清华大学出版社，2007:263-296.
[2] 杨云，王毅.ASP.NET2.0 程序开发详解[M].北京：人民邮电出版社，2007:83-163.
[3] 陈颂，何良生，王建华，等.安全操作系统中隐蔽通道的研究[J].信息安全与通信保密，2006(11).
[4] 卿斯汉，刘文清，温红子.操作系统安全[M].北京：清华大学出版社，2004:4-196.
[5] 赵玉伟，赵小雨，乔木.缓存技术在 B/S 架构信息系统中的应用[J].计算机工程，2008(1).
[6] 刘美华，古志民，曹元大，等.一个基于机群的可扩展的 Web 缓存服务器[J].计算机工程与应用，2003(7).
[7] 钱小军.Web 文本挖掘技术研究及其实现[D].杭州：浙江大学，2002.

(收稿日期：2009-10-08)

作者简介：
李顺新，男，1972 年生，硕士，副教授，主要研究方向：软件工程。
杨鑫，男，1984 年生，硕士，主要研究方向：计算机软件软件。