构筑安全可靠的 Web 数据库应用系统

徐永晋 朱铁峰 （上海大学自动化学院 200435）

摘要：Web 技术和数据库技术的结合是 WWW 信息服务技术发展的大势所趋，由此产生了一系列的安全性问题，本文就如何构筑安全可靠的 Web 数据库应用系统，对从工作环境到程序应用的安全性问题进行了研究。

关键词：Web 数据库 安全防护 加密 SSL ISAPI Windows NT SQL IIS

一、Web 数据库应用程序的安全防护措施

构筑安全可靠的 Web 数据库应用系统要从两个方面考虑。首先要对构筑 Web 数据库的工作环境进行合理系统的安全配置，防止非法人员攻击 Web 站点。这方面包括操作系统的安全问题、数据库服务器的安全性、Web 服务器的安全性以及如何有效的配置防火墙。只有将它们有机的结合起来，才能使 Web 数据库建立在安全的工作环境中。

其次要在编制 Web 数据库应用程序时，充分考虑安全性和容错性能，以及在不同情况下应付不同行为的能力。这方面包括设置登录 Web 数据库站点的用户名和口令；为不同级别的用户设定不同的操作权限，访问各自的数据库；一旦受到攻击，能有效地记录是哪个用户什么时候侵入的；在服务器和客户器端建立安全有效的传输通道；在传输过程中对数据进行加密；通过数字签名来验证用户的真实性等。

以上几方面不是孤立的，而是相互联系的，所以必须结合起来从多方面多层次考虑才能更好地构筑安全可靠的 Web 数据库应用系统。

二、在一个实际 Web 应用系统环境中实施的安全机制

以目前常见的系统配置为例，通过采用 Windows NT Server 作为网络操作系统、MSSQL Server 作为数据库服务器和 Internet Information Server(IIS)作为 Web 服务器来开发 Web 数据库应用系统能取得较为理想的结果。下面将介绍其安全性实现的方法和策略。

1. 操作系统 Windows NT 提供的安全防护机制

Windows NT Server 是目前流行且应用广泛的一种操作系统，它提供了完整的存取控制、内存保护、保护网络资源、强制登录等安全性措施，建立起较完整的一个安全性模型。它通过用户帐号、用户权力及资源权限的结合，为每个用户提供合适的资源访问和限制。

(1)Windows NT 安全机制通过分配用户帐号和密码来保护系统资源和网络系统，保护 IIS 不受侵入，禁止无关用户使用 Web 服务器资源，从而保护 Web 服务器的安全。

(2)Windows NT File Systems(NTFS)，通过它可以配置 Web 服务器的文件夹和文件的访问权限。它利用 Access Control List(ACL) 技术实现用户权限控制。ACL 中含有用户和组对文件和目录的权限信息，可禁止无关用户访问、复制、修改、删除和执行文件。即通过 NTFS 对文件夹和文件访问权力的控制，来保护 Web 服务器文件安全。

(3)Windows NT 通过域用户管理器的审核规则来设置审核事件，从而在受用户攻击时能及时找出记录，把安全损失降低到最低限度。使用事件查看器，查看安全日志可以审核和监视对服务器的访问情况，有效提高安全防预。

2. 数据库服务器 SQL Server 的安全机制。

每个 SQL 服务器必须配置三种有效的安全模式之一来保护数据库的安全：

(1)标准安全：对所有连接采用 SQL 服务器本身的登录证实过程，通过使用登录 ID 和口令来访问数据库服务器；

(2)集成安全：允许一个 SQL 服务器用 Windows NT 的认证机制来证实 SQL 服务器的所有连接的登录。只有可信的连接(多协议或命令管理)才允许连接；

(3)混合安全：允许 SQL 服务器的登录请求或者采用集成安全或者采用标准安全来认证，可信的连接(由集成安全使用)和不可信连接(由标准安全使用)都可支持；

一般采用集成的登录安全性设置，这样使得数据库服务器和 NT 有机结合，在用户连接完成后，对每个用户

可以设置其对数据库中每个表的访问权限，如对不同表按用户权限来设置 select、delete、update、insert 等 SQL 操作。同样可以设置日志记录来查看对数据库操作的记录事件。

3. Web 服务器 IIS 的安全性

IIS 是集成于 Windows NT4.0 内部的 Web 服务器。IIS 的安全机制建立在 Windows NT 安全机制模型之上，另外提供了附加监视和安全性特征。

(1)IP 地址控制：通过对 IIS 的配置可以允许或拒绝某些特定 IP 地址对本 Web 服务器的访问。IP 地址控制首先对服务器接收到的每个数据包的源 IP 地址(发送数据的地址)进行检查，然后将它与包含有数据包预定义操作的一系列 IP 地址进行比较。随后按照源地址内预先定义的操作对数据包进行处理。IP 地址控制适用于对大型用户组(例如公司内部的所有职员或特定的某些机构)进行访问控制的情况。这种机制也是防火墙采用的基本机制。IP 地址控制最主要的局限在于它不能识别可被某个给定 IP 地址访问的特定目录。

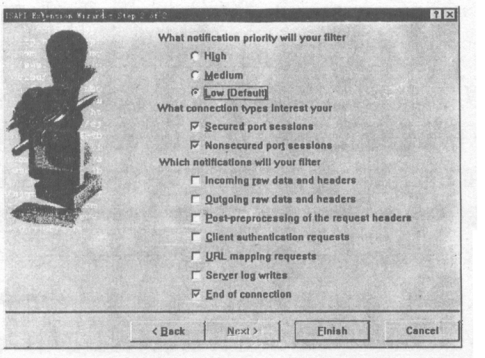
(2)Web 服务器虚拟目录控制：用户可以利用 IIS 给服务器上的某个目录路径定义一个别名，之后就可以在 URL 里使用这个路径了。这个别名称为“虚拟路径”(Virtual Directory)。例如，假设一个名为“work”的 Web 站点，服务器名为 ZTF，那么它的缺省路径应为 c:\intesvr\wwwroot\work，如果把这个路径的别名定义为/work，那么该 Web 站点的 URL 就应该是 http://ztf/work。

在定义别名的同时，用户还可以给路径及其中的所有文件和文件夹赋予一个访问权限。可选的访问权限有两个，它们分别是 Read 和 Execute。Read 权限允许用户读取和下载路径中的内容，而 Execute 权限只允许用户运行路径下的程序，不准读取或下载它们。如一般的 HTML 文本可赋予 Read 权限，而 ASP，DLL，EXE 等运行脚本赋予 Execute 权限。

(3)Web 服务器的用户访问帐号控制：由于 IIS 集成在 Windows NT 里，每个用户帐号可以是一个或多个组的成员。你可以把 Web 访问权限指定到组而不是个人的用户帐号。你可以赋予组文件和目录权限以及其他权限，组中的用户自动拥有该级别的访问权限。通过 IIS 中的 WWW Service Properties for NT Server 中 Service 标签 Allow Anonymous 允许任何人与站点连接。如果一个用户试图访问站点，IIS 使用 Anonymous login 框架中的用户名和密码。在安装 IIS 的过程中自动产生 Anonymous User 帐号。用户帐号放在表单 IUSE-servername 中，IUSER 代表 Internet User，servername 是安装 IIS 的服务器名称。密码用伪随机方式产生。如选了 Windows NT challenge/Response，访问权限定于 Windows95 和 Windows NT 客户，因其协议一部分由只包含在操作系统中的代码实现。这是一个非常安全地选择，因为密码从不会在网络上传送。服务器只在客户知道密码的情况下向客户发送信息请求。使用密码，客户考虑服务器问题的答案，只传回答案而不是密码(甚至答案也是加密的)。Basic 选项允许你在任何操作系统上的浏览者向 IIS 发送用户名称和密码。不使用 Windows95 和 NT 独特的 Challenge/Response 机制，信息在没有加密的情况下传送，这样做的安全性最差，因为某个人可以轻易地从网络上获取计划文本用户名称和密码。

4. 编制的 Web 数据库应用程序对安全的考虑

首先，在软件编制中设置访问该 Web 数据库的用户名和口令，最好有次数限制，如 3 次输错将拒绝访问 Web 数据库。当正确输入的用户名和口令则进入站点，根据数据库管理员对不同用户的授权，入网的用户只能按其操作权限对数据库操作。有的只能查询浏览数据库，有的可进行交互操作，对数据库进行添加、删除、更新记录。例如一个网上购物应用系统，对访问其站点的用户，可分为注册用户和非注册用户，注册用户可以按自己的要求浏览商品，购买商品，提交订单，支付钱款，而非注册用户只能对商品进行查询、浏览。在一个企业内部网(Intranet)内，同样要为用户设置数据表的操作权限，如一个企业中的会计部、仓储部、销售部、用户管理部等不同部门，按他们的用户口令进入后会显示其相应的 Web 页面，从而使其只能从事其相关的操作，对相应的表有其相应的权限，这样能有效地对数据库进行管理。



其次,可以编制相应的 ISAPI 过滤器应用程序,如图所示,是在 Visual C++ 中对 MFC Appwizard 的过滤器设置。在 Web 服务器运行时,按要求可对不同过程进行日志记录,如进出网站的源数据,请求提交进程,用户认证请求,URL 映射请求,服务器日志写,中止连接时进行记录,这样可允许你通过监测服务器上的事件将安全性提高,在受到攻击后,通过对日志记录监视能及时采取相应措施,从而将损失降低到最低限度。

5. 传输过程中对数据进行加密技术及安全套接字层(SSL)的使用

为保证数据在网上传输的安全性,常采用加密技术。常用的加密方法有私有密钥加密和公有密钥加密。私有密钥加密也称对称加密法。是美国国家标准局 1977 年正式宣布的数据加密标准 DES。其加密密钥与解密密钥相同,加密过程中所用的全部步骤的逆过程就是解密过程。一旦泄漏了加密密钥即可破译密文。虽然 DES 方式具有处理速度快实现方便的优点,但它的密钥传递和分配是一个致命弱点。在网络环境下,当参与者数目增加时表现得尤为突出。为克服这个缺点,一个新的"公共密钥"被设计出来。公共密钥公开,它们允许任何系统以公开密钥将其信息加密后传给另一个系统,而接收者要用自己的私有密钥对这个信息加密。由于加密和解密遵循着两条不同的途径,这样在只掌握加密密钥的情况下,无法从加密过程中来推断解密变换,即不能对加密结果进行解密。公开密钥密码系统解决了网络环境下密钥的管理和分配问题。RSA 作为其代表算法具有许多优点。能很方便地引入数字签名,以实现身份确认。但是其算法保密强度建立在计算复杂性基础上,计算工作量远远大于 DES 算法,对于许多应用不适合。

为克服 DES,RSA 各自弱点,实行 DES 和 RSA 综合起来的混合方式,这种混合体制使用 DES 方式对通信数据进行加/解密,其 DES 方式的密钥用 RSA 方式加密后传递。网上大多数是两者组合使用,最常用是由 Netscape 开发的运行于 HTTP 和 TCP/IP 之间的"安全套接字层"(SSL),它除了可以提供快速的加密和验证之外还具有很高的安全性。

私钥加密的速度非常快,但存在着传送密钥的问题。公钥加密的保密性很好但速度慢。如果在开始进行保密传输时先用公密加密传送一把私有密钥,那么用户就可以很安全地使用私有密钥来快速传输任意数据了。这就是 SSL 工作原理,它首先使用一把 RSA 公共密钥来传送一把任选的私有密钥以实行 DES 或 RSA 加密。

SSL 具有双重功能。除提供一种安全传输数据方式外,还可以对数据和服务器进行验证。

(1) 可确认信息发送者真实身份以防止他人冒名顶替。这是对客户或发送者的验证;

(2) 可确认接收者的真实身份,这样可保证发出的信息能够安全到达真实的接收者手里,这是对服务器或接收者的验证;

(3) 可保证传送的数据在被接收前不被他人修改,这是对数据验证。

SSL 可通过下面的步骤来实现这些验证:

①首先,发送者采用一种极为复杂的运算规则为传送的数据建立一个信息摘要,这种运算法则对于数据的变化是非常敏感的。该过程与计算校验总数或进行循环冗余校验(CRC)相似;

②发送者使用自己的个人密钥给信息摘要加密后产生一个数字签名;

③ 接收到数据后,接收者使用发送者的公共密钥对数字签名进行解密,然后利用解密得到的数据就可以打开信息摘要了。如果公共密钥能够解密数字签名,那么说明发送者的身份是真实的;

④ 随后,接收者利用接收到的数据重新计算出一个新的信息摘要。如果这两个信息摘要是相同的,那么就说明数据在传输过程中未被修改;

⑤ 接收者使用自己的个人 RSA 密钥给新的信息摘要加密以建立一个新的数字签名,然后把它传送给信息发送者。

⑥ 接收到这个新的数字签名后,发送者再使用接收者的公共密钥对它进行解密,那么就说明接收者的身份是真实的,这两份信息摘要相同,则表明数据已被接收者成功接收到了。

冒名顶替者完全可以利用与这些公共密钥相匹配的个人密钥来解密及盗用数据。解决这个问题的方法是把公共密钥放在一份证书里。证书利用某个鉴定权威机构提供的个人密钥,对包含有发送者用户名的信息摘要和公共密钥进行加密。然后,通过鉴定权威机构的公共密钥,就可以获得发送者的用户名及公共密钥了。当然这样做的前提是大家都必须承认鉴定权威机构公共密钥的合法性。

(下转第 44 页)

(上接第 15 页)

访问 SSL 允许的 WWW 目录 URL,必须使用 URL 中的"https://",这样就建立了安全通道。在使用 SSL 前先要建立密钥系统。生成密钥对的方法是采用在"Microsoft Internet 服务器"中的"密钥管理器"。一旦生成密钥,必须获得证书,然后再以密钥对安装此证书,在相应的 WWW 目录 URL 网页设置建立 SSL 通道,这样在客户机和服务器之间建立了安全通道,其中传输的数据都是加密的。

6. 其他安全技术

除了上述安全技术外,在企业内部网(Intranet)和外部网(Internet)间常采用防火墙技术,它大致分为三大类:数据包过滤、应用级网关、代理服务器。通过对它们的合理配置可以有效地保护内部数据免受外部攻击。

参考文献

[1] Internet 网络安全专业参考手册(美)Derek Atkins 等著 严伟 刘晓丹 王千群等译 机械工业出版社

[2] Microsoft Internet Information Server 4 使用指南 N. 豪厄尔等著 希望电脑公司

[3] World Wide Web 数据库开发人员指南 (美)Mark Swank Drew Krittel 著 王建华 高杏生等译机械工业出版社

(来稿时间:1999 年 8 月)