河北大学计算中心　罗朝晖　边小凡　刘铁英　李天柱

三层模式下信息系统的安全

基于Internet/Intranet的三层模式(B/S)是近年来非常流行的信息系统运行模式，本文从分析三层模式的特点出发，探讨了各个层次的安全措施，并给出了这种模式下的整体安全设计方案。

目前市场上有很多标准化浏览器和Web服务器产品可供用户选择。浏览器的主要工作是解释和展现HTML文件(网页)的内容，Web服务器的作用是存储和发送浏览器需要的HTML文件。由于用户经常需要访问存储在数据库中的动态变化的数据，并对其进行必要的计算或其他处理，许多厂商对浏览器和Web服务器进行了不同形式的扩展，使得用户通过WWW平台不但可以进行静态信息浏览而且可以进行数据库访问和数据处理，使WWW的运行模式扩展为浏览器／Web服务器／数据库服务器(B/WS/DBS)三层体系结构。因为用户的业务处理应用程序主要以某种形式驻留于Web服务器或专门的应用服务器，所以也可称其为B／A／S模式（Browser/Application/Server)。由于它具有很多传统模式不具备的优点，尤其非常适合在Internet/Intranet环境下运行，目前它已成为信息系统的最流行的运行模式。

无论在哪种模式下，系统的安全性都是一个非常重要的问题，是信息系统成功与否的重要保障。由于三层模式的网络环境和自身的特点，使系统的安全设置更加重要。

信息系统的安全包括很多方面，例如：防止病毒的侵入、系统故障时不破坏系统关键数据、用户操作失误不造成数据丢失或损坏等。这里讨论的系统安全主要指防止非法用户入侵而造成系统破坏或窃取数据。

三层模式的特点

1. 功能分布灵活，但需要安全防范的层次增多

三层模式是传统C/S模式的扩展，可以将其看作两个C/S模式的结合。浏览器向应用服务器发送请求，应用服务器响应请求并进行相应的处理，然后把处理结果以HTML文件的方式返回浏览器，这是第一层C/S模式；应用服务器运行业务处理程序时，如需访问数据库则向数据库服务器发出请求，数据库服务器把数据处理结果返回应用服务器，这是第二层C/S模式。因此三层模式具有传统C/S模式的全部优点，且用户接口、业务处理和数据管理的分布更加灵活。但由于网络环境复杂，系统资源分散，给系统的安全带来许多不利因素，需要在多个层次上考虑系统的安全问题。

2.操作界面统一，使用灵活，但为非法入侵提供了有利条件

任何地方的计算机只要联网并安装浏览器就可以进入系统进行操作，标准友好的图形界面的浏览器软件作为信息系统最终用户的操作界面，用户端的配置十分简单、灵活，用户操作方法标准、统一，易学易用。但正是由于这种方便性，也为非法入侵大开方便之门，Internet“黑

客”猖獗便是一例。

3. 更新维护方便，系统的安全防范主要针对各种服务器

三层模式信息系统的数据存放在数据库服务器中，大部分的业务处理程序在应用服务器中存放和运行，另一小部分程序存放在应用服务器的网页和控件中，需要时以浏览器端扩展（Java、ActiveX等）的形式下载到浏览器端运行。应用程序更新、升级时，只需更新应用服务器中的程序。这可使应用程序的维护对用户是透明的，大大降低维护成本，提高系统可维护性。由于客户端（浏览器）不存放应用程序和数据，只要保证传到浏览器的HTML源码不包含关键程序代码，操作人员就不能看到更不能修改应用程序，只要各类服务器安全设计合理，就可以保证应用程序和数据不被破坏。

4. 信息系统的安全设计与网络安全设计密切相关。

三层模式的信息系统运行环境一般是开放性的网络环境，系统信息要在网络上传输，系统的功能全部基于网络实现。要保证信息不被窃取，不仅要保证服务器中数据和程序的安全，还应保证信息传输过程中的安全。因此，网络安全是整个信息系统安全的一部分，整个信息系统的安全设计与网络安全设计密切相关。

三层模式下信息系统的安全层次

由于三层模式的运行环境较复杂，设计系统安全的环节较多，所以在此模式下信息系统的安全设计格外重要。应从以下多个层次进行系统安全设计：

1. 网络安全层次

当企业内部网（Intranet）与Internet相连时，应考虑隔离措施，避免将Intranet上的资源毫无防范的暴露在Internet环境中，隔离的方式有多种，可以采用路由器的IP过滤功能、网关、防火墙、代理服务器等。

通过交换机或路由器将Intranet划分成多个子网，可以有效减少网络频带压力，使大部分信息在子网范围之内传输，减少信息外泄的机会，还可同时实现IP地址身份验证机制，防止持有非法IP地址的人访问本子网的资源。

2. 服务器安全层次

三层模式的信息系统的资源都在各类服务器上，对这些资源的使用，应根据具体情况，通过给不同的用户赋予相应的权限，来对系统资源的访问加以限制。

①在用户使用服务器资源之前，首先应检查其合法性----身份验证。身份验证的方式很多。可以采用在网络中设一登录验证服务器的方法。凡是要使用信息系统的用户计算机，必须要经过登录验证服务器的检验，才能成为网络的合法用户进入系统操作，未通过检验的用户为非法用户，拒绝其使用系统资源。

②三层模式信息系统都是通过网页来访问业务处理程序，可以在Web服务器上设计相应的权限限制，只有合法用户才能根据自己的权限访问信息系统的网页。

③数据库服务器上保存有整个信息系统的所有数据，它的安全性格外重要。理 论上，网络上的计算机既可以通过Web页面调用业务处理程序来访问数据库，也可以绕过业务处理程序，使用一些数据库客户端工具直接登录数据库服务器，存取其中的数据。所以，应在数据库服务器中对允许访问的用户授予合适的权限，未经授权的用户禁止访问。

3. 应用程序安全层次

在业务处理程序中，应对各层次中的用户名及其口令加以屏蔽，绝不能使它们以任何形式出现在操作人员可以察看的地方，以免给非法侵入者以可乘之机。例如，传送到浏览器端的HTML文件源代码中不能出现各类服务器的用户名及其口令。

4. 信息传输安全层次

如果关键信息（例如用户口令、商业密码等）需要通过Internet / Intranet进行远程传输，应该有防窃听的措施，防止在传输过程中被窃取。防窃听一般采用信息加密的方式，信息加密的技术发展比较早，也有很多现成的设备和软件工具可以使用。这里不具体讨论信息加密技术。

Windows NT环境下的安全设计

网络隔离、划分子网属于网络设计的范畴，信息加密是一门相对独立的技术，我们都不在这里作详细讨论。仅从用户身份验证、资源访问控制和权限设置的角度讨论如下。

我们以Windows NT + MS IIS 4.0 + MS SQL Server为例来讨论具体的安全解决方案。因为Windows NT是常用的网络操作系统，在此之上的各种服务器和应用软件的集成性和一致性都较好，MS的ASP三层模式解决方案也是现在比较先进和流行的。

1. 服务器登录检验

Microsoft三层模式的基础是ASP（Active Server Page）技术，在这种技术中，业务处理程序嵌在扩展名为.asp的网页中，所以Web服务器也是系统的应用服务器，此服务器保存着业务处理的全部程序。Microsoft的Web

服务器为IIS（Internet Information Server），它与NT紧密的集成在一起，应充分利用系统平台（NT）所提供的安全机制。

我们可以在信息系统所在的网络中设一主域控制器，主域控制器可设在Web服务器上，凡是允许使用信息系统的用户必须是此域的域用户，并应在使用信息系统之前首先登录此域，非域用户禁止使用服务器的任何资源。

2.Web服务器权限设定

可以利用IIS提供的如下安全防护机制:

① Web服务器的虚拟目录访问权限的安全设置。

② Web服务器的用户访问控制和监视。将用户的访问控制设置为禁止匿名访问。IIS提供了三种类型的请求认证：基本认证（用户名和口令的传输、验证用明文，不加密）、Windows NT请求／响应（用户名和口令的验证用密文）、安全套接字层SSL（对通过Web链路的所有会话信息加密），可以选择使用。

③ Web服务器的特定IP地址访问许可。通过配置IIS，可以允许或禁止某些特定的IP地址对本Web服务器的访问。

④ NT文件系统（NTFS）对文件的访问控制。配置Web服务器的文件夹和文件的访问权限，禁止无关用户在文件夹中复制、修改、删除文件，来保护Web服务器文件的安全。

3.数据库服务器权限设定

SQL Server的登录验证有两种方式:

① Windows NT认证方式。在此方式中，SQL Server数据库应与域登录验证服务器在同一域中，数据库服务器与NT域建立一种信任关系，把对用户的验证工作交给NT域验证服务器。客户用某一用户名登录到NT域，在与数据库连接时，数据库服务器检查此用户是否在数据库用户表中，如果在，则不再要求输入口令，允许登录数据库服务器。

② SQL Server认证方式。在这种方式中，SQL Server不一定要与域登录验证服务器在同一域，SQL Server数据库服务器可在与Internet/Intranet相连的任何一台服务器上。客户要想登录到数据库服务器，必须在数据库服务器上建立用户，此用户与NT域的域用户无关。当客户从网络上访问SQL Server数据库时，客户必须提供数据库登记的合法的用户名和口令才能登录。如果是通过应用程序访问数据库，则应在应用程序中提供数据库的用户名和口令。

4.应用程序安全措施

在浏览器端查看到的HTML和ASP源码及URL中不应含有任何数据处理源代码，更不应该出现安全登录和数据源的连接参数，如数据库的地址、登录口令和密码等。虽然，ASP页面允许使用客户端执行代码在客户端建立数据连接和运行应用程序，但这将使数据连接参数和程序代码暴露在网页中，应尽量避免。如果由于特殊原因应用程序必须在客户端运行，也应采用ActiveX技术，在网页中嵌入经编译的ActiveX组件，当浏览器请求页面时，先将ActiveX组件下载，然后在客户端运行，这样浏览器中不会出现源代码。由于客户端运行的Java程序可在浏览器中查看源代码时出现，在涉及到数据安全和关键业务处理程序时，应避免使用。

采用Web服务器的验证手段，使用户登录网站时必须回答用户名和口令。如果要在一个网站之内防止未经授权的用户查看某些页面，可在进入这些页面之前，由程序强制用户输入用户名和口令，经验证后，才可进入页面。必要时，甚至可以对一个网页中的某些资源加以访问限制，这些都可以通过ASP程序来实现。

信息系统安全的整体设计

在信息系统中安全防范措施不能给用户的操作带来太多的不方便。三层模式的系统，由于资源分散，需要在多个层次上进行安全防范，如果设计不当，会由于过多的用户名和口令验证操作使操作繁琐，甚至影响数据处理的自动化程度，影响系统运行效率。

1.资源访问权限的分配

安全设计原则应该是不给用户不必要的权限。信息系统中不同的用户有不同的权限，同一用户做不同的处理时所需要访问的数据也不同。有多种分配资源访问权限的方法，归纳起来可以有:

①按人分配权限：不同的人分配不同的用户ID，根据用户ID分配不同的权限。例如处长比一般办事人员能浏览到更多的信息。好处是使用计算机的人员都有一个唯一的用户ID，便于记忆和设置。

②按角色分配权限：在信息系统中以某种身份进行某一项工作就是信息系统的一个角色，不同的角色应有不同的权限。例如，进行帐务管理、某一报表的汇总打印等，对资源的需求是基本相同的。好处是系统设计时即可有系统开发人员根据处理需要决定，不涉及权力分配问题，便于设计。每一角色仅赋予必要的权限，利于安全管理。

③以上二者的结合：同一人扮演不同角色时分配不同的用户ID，赋予不同的权限。好处是权限分配可以非常灵活，且便于审计。但用户ID偏多，管理繁琐。

2. 用户验证方法

用户验证的方式也有多种，从总体上可以分为集成安全模式和分层安全模式两种。

集成安全模式：整个系统在入口处设置一个验证点，进入系统后，不管使用何处资源都由系统自动判断用户的权限。此种方法最有利于数据处理的自动化。

分层安全模式：每一类资源的入口处均进行验证。系统安全程度较高。

以下给出Windows NT + MS IIS 4.0 + MS SQL Server系统平台的三层模式下信息系统的两个安全设计方案，供参考。

3. 集成安全模式 -- 根据角色设置权限

MS SQL Server和MS IIS与NT紧密地集成在一起，可以共用NT的安全策略。IIS和SQL Server可以利用NT的用户验证机制，把对用户的确认工作交给NT来完成。以这种方式运行的信息系统，用户登录到NT域，通过了NT的用户验证，也就通过了信息系统的用户认证，从而决定了此用户在信息系统中的角色和可使用资源的权限范围。

这种方式的优点是：最大限度的方便信息系统的使用者，登录到NT域以后，在使用信息系统的整个过程中，使用者不再需要输入任何的用户名和口令，系统会根据预先设定的IIS和SQL Server的用户权限，自动地完成对用户的访问限制。当需要修改用户的口令时，只需修改NT域用户的口令即可。

这种方式的缺点是：由于信息系统各层的安全检验都依赖于NT的域用户认证，一旦域用户名和口令泄漏，整个信息系统便毫无安全性可言。

4. 分层安全模式 -- 高安全性模式

在信息系统的各层独立设置安全措施，层层设防。分层安全模式可以充分利用各层的安全机制，提高整个系统的安全性。

NT服务器用户认证及文件保护：在NT的域用户管理器设置允许访问的域用户和该用户对不同资源的访问权限。

MS IIS网站的域用户认证：将信息系统需要安全保护的网站的“允许匿名访问”一项关闭，利用网站权限设置功能赋予NT域用户“浏览”权。这样，当用户访问此网站时，必须输入用户名和口令，只有被授权的用户才能进入网站。

如果需要在网站内部的某些网页或网页中的某些内容加以保护，则在应用程序中加以限制，当用户访问这些内容时，系统会提示输入安全认证信息，通过认证之后才能访问。

数据库安全认证：在数据库管理系统中为不同用户赋予不同的用户名，并赋予不同的访问权限，当用户通过网页访问数据库时，必须回答正确的用户名和口令后才能操作数据库。

采用分层安全模式的优点是：最大限度的提高信息系统的安全性，避免非法用户从任何一个层次非法侵入系统。

采用分层安全模式的缺点是：在使用信息系统的过程中，根据访问内容的不同，需要多次输入用户名和口令，给用户带来极大的不便。当需要改变安全设置时，需要在各层分别设置，使系统的安全管理变得非常复杂。■