Intranet/Extranet 中的 Web 服务器安全机制

杨乔林 （中国科学院计算所 100080）

摘要：本文主要讨论在 Windows NT Server 4.0 上，通过安装 Internet Information Server，建立的、用于 Internet/Intranet/Extranet 的 Web 服务器、FTP 服务器和 Gopher 服务器的三个层次的安全防护机制：

宿主操作系统 Windows NT 提供的安全防护机制；安全套接字层（SSL）的数据加密、服务器身份验证和保护数据传输完整性等安全机制。

一、引言

将计算机与 Intranet / Internet 连接时，您便可以与世界各地的人和计算机通信，这种较大的灵活性也增加了冒险性－不仅您可与其他网络上的人通信，而且其他网络上的用户也可与您的网络进行通信。尽管与您的服务器的连接通常是好意的，但也有心存不良的人企图侵入您的内部网络。因此，保护您的服务器的安全性是建立网点考虑的重点之一。

在 Windows NT Server 4.0 上，通过安装 Internet Information Server，便可建立用于 Internet/Intranet/Extranet 的 Web 服务器、FTP 服务器和 Gopher 服务器。除了外加的防火墙提供的安全防护机制外，还有如下三个层次安全防护机制：

1. **宿主操作系统 Windows NT 提供的安全防护机制**

·Windows NT 用户帐号和密码的安全保障机制

·Windows NT 文件系统（NTFS）设置文件夹和文件的访问权限的安全机制

·审核与监视 NTFS 文件和文件夹的未授权访问（入侵）

2. **Internet Information Server 服务管理器的安全防护机制**

·Web 服务器的虚拟目录的访问权限的安全设置。

·Web 服务器的用户访问的控制和监视机制

·Web 服务器的特定 IP 地址访问许可的安全机制

3. **Web 服务器利用安全套接字层（SSL）保护数据传输，为 TCP/IP 连接提供数据加密、服务器身份验证和保护数据传输完整性。**

在下面的几节中，我们分别对这三方面的安全机制，作进一步讨论。

二、Windows NT 提供的安全防护机制

任何软件都需要从其宿主操作系统取得安全庇护，Web 服务器也不例外，宿主操作系统 Windows NT 为 Web 服务器提供如下多项安全防护手段：

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，也保护 IIS 不受侵入。限制无关用户的 Web 服务器资源的使用权力，来保护 Web 服务器的安全。系统管理员可以重新分配系统资源的使用权力，所以系统管理员的帐号和密码的安全，尤其重要，是保护网络系统和 Web 服务器安全的根本保证。要确保系统上具有管理权力（特别是，系统管理员）的那些帐号，拥有难于猜测的密码（长的、大小写的字母混合密码是最好的），并设置合适的帐号规则，迫使用户不断地更改帐号密码（并使得用户不能重复使用有限几个密码）。

2. 使用 Windows NT 文件系统 NTFS，可以配置 Web 服务器的文件夹和文件的访问权限。禁止无关用户向文件夹中或从文件夹中复制、修改、删除文件；禁止无关用户执行文件，即通过 NTFS 对文件夹和文件访问权力的控制，来保护 Web 服务器文件的安全。Windows NT 中的 FAT 文件系统分区不支持文件访问权力的控制，不提供相应的保护措施，所以应该将 Web 服务器文件和文件夹放在 NTFS 文件系统分区中。

3. 审核与监视 Web 服务器 文件和文件夹的未授权访问（入侵）。判定某个 Web 服务器敏感文件是否已经受到未授权访问（入侵），可以通过审核 Web 服务器文件和文件夹（应使用 NTFS 文件系统）的未授权访问。例如，可检测任何用户或特定用户组的成员是否有过读/写/操作文件的非法企图。要对某个文件或文件上设置审核，首先使用域用户管理器的审核规则，选择审核下列事件（图 1），然后使用 Windows NT 资源管理器指定要审核 Web 服务器那些相关文件以及要审核哪类文件访问

事件。要审核与监视 Web 服务器 文件和文件夹的未授权访问，要使用事件查看器，查看安全日志。应定期地考察审核报告，以便检查是否有未授权读/写/操作等行为。

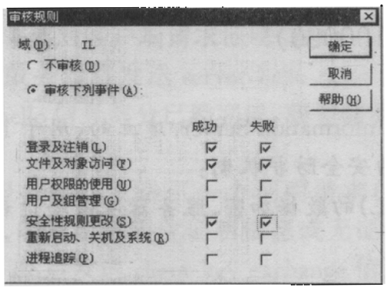

图 1 使用域用户管理器的审核规则，设置审核事件

三、IIS 服务管理器”安全设置

当 Web 服务器接收浏览器请求信息时，它判定请求是否有效。下面以算法的形式，简单地概括说明对每个访问请求，所使用的安全验证过程：

```
对每个访问请求
if (不允许该 IP 地址访问) then 拒绝访问
    else if (用户帐号和密码不允许)then 拒绝访问
        else if (IIS 访问权限不允许)then 拒绝访问
            else if (NTFS 访问权限不允许)then 拒绝访问
                else if (SSL 安全验证通不过)then 拒绝访问
                else 接受访问
```

1. Web 服务器的虚拟目录的访问权限设置

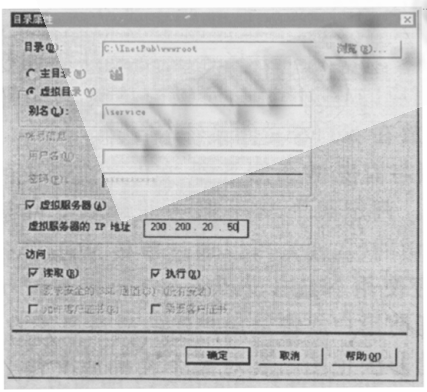

图 2 Web 服务器的虚拟目录的访问权限设置

图 2 是 Web 服务器的虚拟目录的访问权限设置的选择菜单，可设置虚拟目录的访问权限为读和执行的组合。例如，只读或只执行或可读和可执行。

2. Web 服务器的用户访问的控制和监视安全机制

控制匿名访问：在 Internet 的许多 Web 服务器上，其 WWW、FTP、和 gopher 的访问是匿名的，即客户请求不包含用户名和密码。例如，FTP 客户以用户名”匿名”登录；Web 浏览器在 HTTP 请求中不包含用户名和密码。

是否允许匿名登录访问您的 Web 服务器，由图 3 的框中选择来决定。如果允许匿名登录，则该用户所有的权限(例如访问信息权限)，将是 IUSR-WWW.IL.ORG 帐号权限。IUSR-WWW.IL.ORG 帐号的权限由系统管理员使用域用户管理器和资源管理器进行分配。

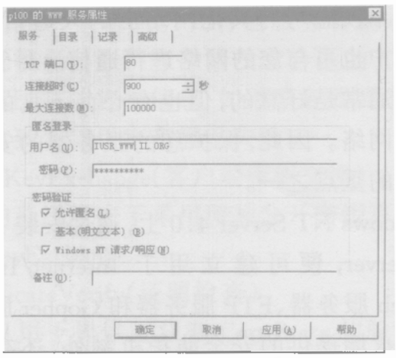

图 3 匿名登录访问 Web 服务器的选择框

如果禁止匿名访问，对远程客户请求需要进行验证，则要指定使用的验证程序。”基本”验证是不用安全套接字层(SSL)连接，验证用明文(不加密)发送密码。选用”Windows NT 请求/响应”验证时，使用安全套接字层(SSL)，自动加密用户名和密码。

3. 特定 IP 地址访问的安全机制

通过指定 IP 地址范围，控制对本 Web 服务器的访问。可以配置 IIS，以允许或拒绝某些特定 IP 地址对本 Web 服务器的访问。例如，可以通过拒绝从某特定 IP 地址来的访问，以排除某些个人的入侵，也可以拒绝某整个网络对本 Web 服务器的访问(图 4)。相反，可以有选择地允许某些特定网络或节点访问您的服务器，而拒绝其他网络对本 Web 服务器的访问(图 5)。在 Internet 上排除未知用户的访问的 IP 地址安全机制可能是最有用。

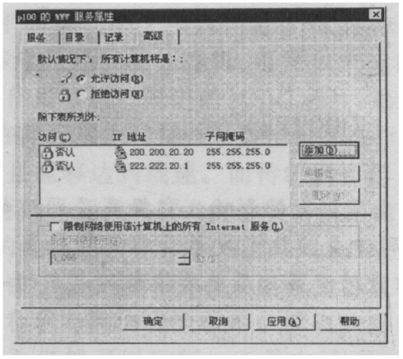

图 4 拒绝某些特定 IP 地址的访问

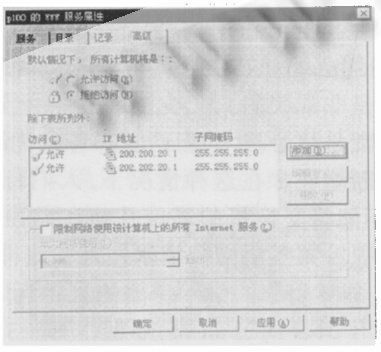

图 5 允许某些特定网络或节点访问 Web 服务器

四、安全套接字层 (SSL)提供的功能

SSL 是 Internet 在其服务协议 (HTTP) 和 TCP/IP 之间提供分层数据安全性的协议。SSL 是提交给 W3C 工作组关于安全性的协议,它被视为 Internet 上 Web 浏览器和服务器的标准安全性措施。SSL 提供了用于启动 TCP/IP 安全连接的"信号交换"。这种信号交换导致客户和服务器同意将使用的安全性级别,并履行连接的身份验证要求。在此之后,SSL 的唯一作用是加密和解密应用程序协议的字节流(例如 HTTP)。这意味着 HTTP 请求和 HTTP 响应中的所有信息将完全被加密,包括客户正请求的 URL,任何形式提交内容(例如信用卡号)、任何 HTTP 访问身份验证信息(用户名和密码)以及从服务器返回到客户的所有信息。

在 Web 服务器上实现 SSL 安全措施,要求完成下列步骤:

1. 生成密钥对文件和请求文件
2. 从身份验证权限中请求一个证书
3. 在服务器上安装证书
4. 激活 WWW 服务文件夹上的 SSL 安全性

生成密钥对文件和请求文件,要使用密钥管理器(图 6)和密钥对文件和请求文件生成框(图 7)。

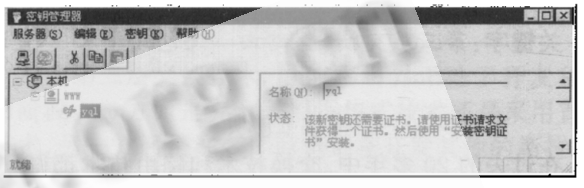

图 6 密钥管理器

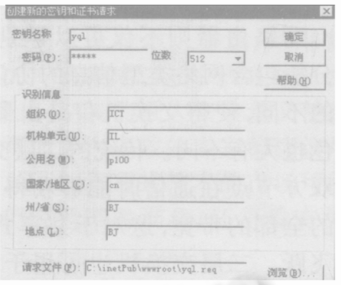

图 7 密钥对和请求文件生成

一旦已经生成密钥对,还必须获得证书,只有安装证书后,才能在 Internet/Intranet/Extranet 上使用。要获得证书需要向证书授权中心(例如 VeriSign ,其网址为 http://www.verisign.com/),发出获得证书的请求,在收到授权中心签名的证书后,还要在密钥管理器中,用密钥对安装证书。

如果在 Web 服务器上要进行商业和金融活动(作为电子商务服务器),为保障交易能安全地顺利进行,必须安全问题更要严加控制,还要补充一些有效的保障交易安全的协议标准。例如,安全超文本传输协议(S-HTTP)、安全交易技术协议(STT - Secure Transaction Technology)、安全电子交易协议(SET - Secure Electronic Transaction)和安全多成分邮件编码(S/MIME)等。

(下转第 3 页)

(上接第 21 页)

在 Web 服务器的电子商务中,收、发文都要进行数据加密,发信方和收信方分别使用的数据加密步骤如下:

A. 发信方的加密过程

1. 将信息(明文)通过安全 HASH 算法(SHA),生成数字摘要。

2. 利用发信方私有密钥进行加密,得到数字签名。

3. 发信方使用 64bit 的 DES 生成对称密钥。

4. 利用产生对称密钥,加密信息(明文)使其变成密文(电子信封)。

5. 利用收信方的公开密钥,对数字签名、密文和对称密钥加密,然后给收方发出。

B.收信方

1. 使用收信方的私有密钥,对收件进行解密,分别解出数字签名、发信方对称密钥和发送信息的密文。

2. 使用发信方对称密钥,对信息密文解密,得到信息明文。

3. 用 RHA 算法处理信息明文,得到新的数字摘要。

4. 用发信方公开密钥对数字签名解密,得到发信方发过来的原数字摘要。

5. 两个数字摘要要进行比较,若相同说明报文可信,没有人修改过;否则说明报文有问题,不可信。

参考文献

[1] 杨乔林等:"Intranet 的规划及设计" 计算机系统应用 1998 NO.2

[2] 杨乔林:"电子 Internet 上的电子商务 " 计算机系统应用 1998 NO.11

[3] Microsoft:"Windows NT 4.0 网络系统管理" 1997 Microsoft Press

(来稿时间:1998 年 9 月)