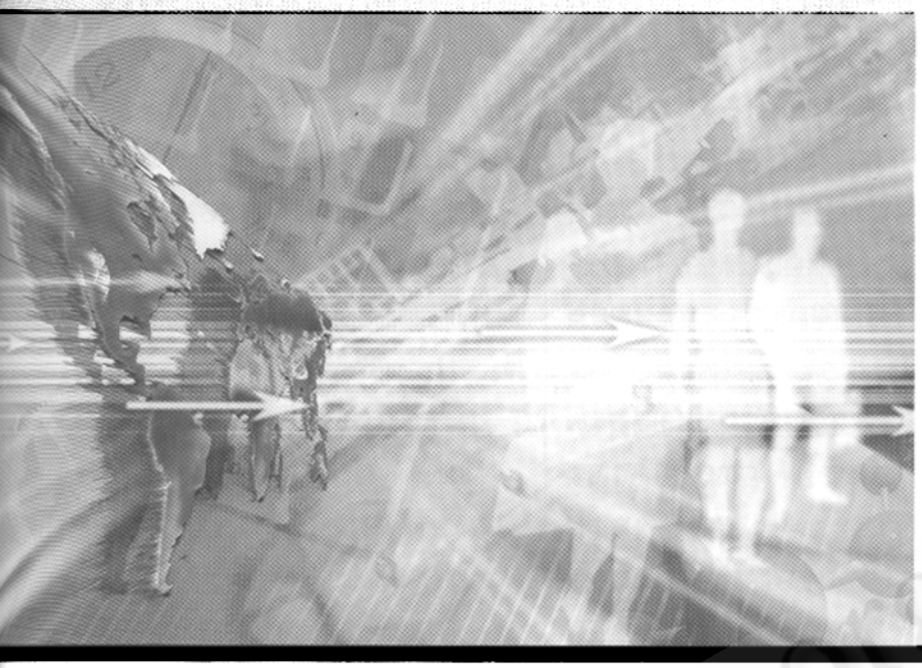


李书振 （武汉大学信息管理学院 430072）

摘要：互联网的高速发展，给人们带来了极大的便利。人们通过互联网来传输、获取、交流信息。但如何保证信息安全和如何保护自己的合法权益不受侵犯是影响互联网发展的主要问题。本文介绍了一些加强信息安全的措施，也着重阐述了如何建立安全的Web服务器和数据库系统来加强信息安全。

关键词：信息安全 Web服务器 访问 数据库系统

网络环境下的信息安全措施

The Information Security Measures in Network

1 引言

在信息时代，越来越多的企事业单位、个人在互联网(Internet)上建立自己的信息系统(主要以Web页面访问数据库的形式建立)，人们通过互联网来发布、获取、交流信息。现在我国正在大力提倡无纸化办公，即各级政府之间的信函、文件等信息都要通过网络实现电子化传输，互联网给社会经济、人类生活的各个方面带来了新的发展动力，推动了整个社会的信息化进程。但由于传输信息的主要载体——网络具有广域性、开放性、资源共享性等特点，自然灾害、人为因素、硬件设施等都会使信息的安全受到威胁，使人们的合法权益受到侵犯。信息安全是指信息的保密性、完整性、可用性不被破坏。所以为了保证信息安全，就必须了解影响信息安全的因素，建立安全的网络、安全的Web服务器及安全的数据库系统。

2 影响信息安全的因素

由于电子信息是通过网络传输的，网络是由硬件（计算机、传输介质等）和软件（操作系统、Web服务器、数据库等）构成，同时网络具有广域性、开放性、资源共享性等特点，因此影响信息安全的因素是多方面的，但概括起来分为两大方面。

2.1 自然因素

(1) 自然灾害：地震、水灾、火灾、雷电等不以人们意志为转移的灾害，会破坏硬件设施，从而使存储的信息受到毁灭性打击。

(2) 自然环境：组成网络的硬件设施所处的环境如温度、湿度、灰尘等也会影响硬件设施的安全；电磁波会引起信息的泄露。

2.2 人为因素

(1) 管理水平：管理落后、管理人员素质低、工作失误等引起的操作不当，会损坏硬件设施以及使系统不能正常运行，甚至使系统崩溃；操作系统、服务器和数据库安装设置不当，会留下安全漏洞，给他人以可乘之机，非法窃取、修改、毁坏信息。

(2) 电脑病毒：电脑病毒是由所谓的“电脑奇才”编制的小程序，最初用来恶作剧，现在演变成用来攻击目标。如CIH病毒定期发作，会损坏电脑硬件；特洛伊木马病毒会在用户毫无察觉的情况下复制文件或窃取信息。还有电子邮件“炸弹”，使电子邮件服务器不断收到容量大且充满乱码的垃圾邮件，占用大量的存储空间，降低系统性能，最终导致电子邮件服务器瘫痪，系统崩溃。电脑病毒现在主要是以电子邮件的形式在互联网上传播的，这种传播方式比以前的通过软磁盘传播病毒的方式具有速度更快、影响更广、损失更大等特点。

(3) 电脑黑客：有些人编制一些小程序，来搜寻且利用互联网、操作系统、数据库系统等的安全漏洞，未经许可强行进入他人的电脑系统，肆意破坏、修改、窃取别人的数据信息。这些人就是电脑黑客。

3 加强信息安全的措施

从上述因素可以看出，信息安全是一项长期、复杂的系统工程。加强信息安全要从方方面面入手，要根据系统的安全等级，采取相应措施。

3.1 安全管理

安全管理是指要建立信息安全的管理制度，健全法制法规，使信息安全走上规范化、法制化的道路。加强工作人员的安全意识教育，提高保

密观念。对工作人员进行业务培训，提高操作水平，从而建立和维护相对安全的信息系统。

3.2 设备管理

硬件设施(计算机、传输介质等)是电子信息存储、传输的载体。除一些不可抗拒的自然因素(地震、水灾、战争等)能对硬件设施造成不可挽回的损失外，但可以采取一些措施，改善硬件设施所处的环境。如服务器室尽量不用易燃材料装修且配有灭火器材，以防火灾发生；服务器室要安装空调且密封性要好，以保持室内恒温、干燥、清洁卫生；供电系统要有接地装置，以防雷电。

3.3 安全通信

电子信息如果以明文的方式在网上传输，就很有可能被黑客截获甚至篡改后再发出，这会造成商业机密、国家机密等的泄露。所以通信安全就是要确保信息数据的完整性和保密性。数据的完整性是指信息在网上的传输过程中不被篡改，即保证信息的正确性、有效性和一致性，数字签名和数据谪压技术常被用来实现这一目的。数据的保密性是通过对数据加密实现的，数据加密技术就是为了提高信息的安全性和保密性，即使数据被第三者窃取也无法破译其中的内容，现在常用的加密技术有对称密钥加密技术、非对称密钥加密技术以及综合密钥加密技术等。

3.4 防火墙技术

防火墙技术是在内部网(Intranet)和外部网(Internet)之间实施的一种访问控制机制。通过专门的软件可以对跨越网络边界的信息进行监控，一方面可以防止非法用户访问企业内部网，另一方面可以允许授权用户访问内部网信息。目前常用的防火墙技术有数据包过滤技术、应用网关技术、代理服务器技术等。

3.5 安全的 Web 服务器

在互联网上，信息的发布主要是以Web页面的形式进行，Web页面是由Web服务器支持。因此，建立安全的Web服务器是加强信息安全的重要措施之一。目前世界上拥有最多用户的Web服务器软件是Apache，对运行在Linux系统上的Web服务器，有下列基本的安全预防措施：

(1) 限制Web服务器可登录帐号的数量。若登录人数过多，一方面会降低系统效率；另一方面会留下安全漏洞，电脑黑客会反复地试图登录你的网站，达到攻击服务器的目的。

(2) 确认有权登录的用户使用了不易被他人破解的密码。选择口令时，应该仔细推敲。不要用一些明显的口令，如名字、生日、办公室电话号码、或者自己喜欢的宠物的名字。这些口令很容易被猜测出来。

(3) 关闭不用的服务。如删除FTP、Gopher等任何可能不用的功能。Apache服务器提供的自动目录列表功能确实方便，但也可能留下漏洞。如果你不是绝对需要的话，关掉它们。在Apache中要关闭自动目录列表功能，可以在/etc/http/conf/httpd.conf文件的相应目录标示<Directory 目录>…</Directory>中的Options标示后面去掉Indexes项。

(4) 定期检查系统和Web的日志记录，看有无可疑动作。查看URL请求中特别长的行，同时要检查重复的失败，这可能意味着有人试图猜测口令，试图存取受口令保护的文档。

(5) SSI(Server side includes)的"exec"指令是安全上的主要漏洞。在Apache中，只要在httpd.conf文件的相应目录控制部分加上如下标示，就可以关掉该目录的exec功能：

```
<Direcrory 目录的完全路径>
    Options IncludesNoExec
</Directory>
```

(6) 确认系统文件的权限设置正确。对Web服务器的根目录，要建立严格的访问约束机制。在Apache中，可以在httpd.conf文件中加入以下内容，拒绝所有用户访问根目录。

```
<Direcrory />
    Options FollowSymLinks
    AllowOverride None
    Order Deny,Allow
    Deny from All
</Directory>
```

(7) 限定IP地址、子网或域名的访问。这种方式保护的个别文档或整个目录，只有特定的IP地址，IP子网或域名的主机可以访问。在Apache中，可以在httpd.conf文件中加入以下目录控制标示段：

```
<Directory 目录的完全路径>
order mutual-failure
    deny from all
    allow from 10.1.0.0/255.255.0.0 (特定的IP地址)
    allow from 192.198.2 (IP子网)
    allow from .ncsa.uiuc.edu (特定的域名)
</Directory>
```

这将会禁止除了指定主机(10.1.0.0/255.255.0.0)、子网(192.198.2)和域名(.ncsa.uinc.edu)外的其他任何主机访问该目录。

(8) 限定用户名和口令的访问。通过IP地址来限制访问，对偶然的好奇能起到一定的防范作用，但对有目的的黑客则不然。为了安全起见，IP地址限制必须与其他检查用户身份的手段相结合，如检查用户名和口令。用这种方式保护的文档或目录，用户要访问时必须提供用户名和口令。在Apache中，用户名和口令的限制是这样实现的，在httpd.conf配置文件中，给相应的目录加上以下内容：

```
<Directory "/usr/local/apache/phpMyAdmin">
    Options FollowSymLinks
    AllowOverride None
    AuthName 我的网站
    AuthType Basic
    AuthUserFile "/usr/local/apache/user.txt"
    Require valid-user
</Directory>
```

这样，目录phpMyAdmin就置于保护之下，只有文件user.txt中的合法用户才可以访问。当有人试图访问phpMyAdmin目录下的页面时，就

会弹出一个认证窗口，如果用户输入了无效的用户名和口令，该窗口将一直显示，直到输入正确。

用户口令文件user.txt是在Apache目录下，用Apache的htpasswd命令创建的，格式是：htpasswd -c user.txt username，该命令执行后会提示你输入两次密码，两次输入相同时将该密码经过MD5加密后写入user.txt文件中。

3.6 安全的数据库

在互联网上，数据信息的存储、添加、修改、删除等主要是通过数据库来实现。MySQL是一个真正的多用户、多线程的SQL数据库服务器，越来越多的人们把它作为网络开发数据库，所以它的安全与否就直接关系到存储在其中的信息的安全。下面就介绍MySQL数据库的权限系统即安全机制是如何控制用户访问数据库，从而实现信息安全。

MySQL的数据库文件一般安装在…/mysql/目录下，该目录下有个子目录mysql，这个子目录代表一个数据库，子目录名也就是数据库名(mysql)。数据库子目录mysql下存放的是mysql数据库的数据表文件，这些数据表文件就是MySQL的权限表。mysql数据库是MySQL权限系统的核心，包含表：user、db、host、tables_priv和columns_privuser，这些表中的字段可分为范围字段和权限字段。范围字段是指哪些主机、用户可以访问数据表、表列。权限字段是指用户是否有读取、插入、更新、删除记录的权限。

当连接一个MySQL服务器时，用户身份由用户连接的主机和指定的用户名来决定，系统将根据用户的身份来授予权限。MySQL在确定用户身份时考虑了主机名和用户名，这样做允许用相同的用户名从不同的主机连接同一个MySQL服务器，同名用户属于不同的身份。例如，从whitehouse.com连接的用户bill与从microsoft.com连接的用户bill是不同的身份，而且具有不同的权限。

MySQL存取控制包含两个步骤：首先MySQL服务器检查是否允许连接；若允许连接，服务器检查用户的每个请求，看看是否有足够的权限实施它。

3.6.1 连接确认

当用户试图连接一个MySQL服务器时，服务器根据用户身份来确定是接受或拒绝连接。用户身份基于以下信息：从哪个主机连接(主机名)、用户名、用户密码。

身份验证使用user表的范围字段(Host，User和Password)。只有在user表中找到相匹配的主机名和用户名，并且口令正确时，服务器才接受连接。

一个到来的连接可以匹配user表中的多个记录。如果超过一个匹配，服务器怎么选择使用哪个匹配呢?一般是服务器在启动时读入user表后通过排序来解决这个问题的。当一个用户试图连接时，以排序的顺序浏览user表的记录，第一个匹配的记录将被使用。

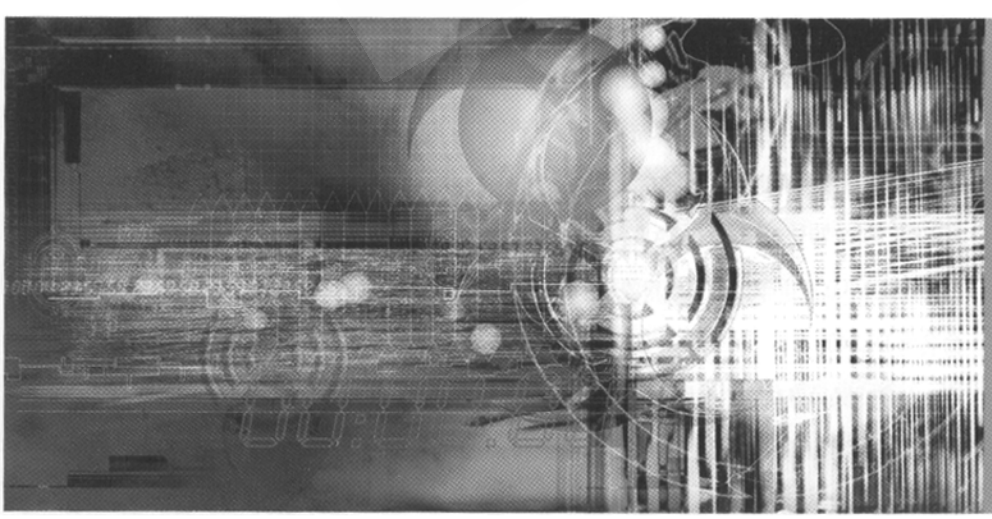
3.6.2 请求确认

通过身份认证之后，就与服务器建立了连接，对在此连接上进来的每个请求，服务器检查用户是否有权限来执行它。这些权限可以是user、db、host、tables_priv或columns_priv表中的任何一个。

user表在一个全局基础上授予用户权限，该权限不管当前使用的数据库是什么。例如，如果user表授予一个用户delete权限，则他可以从任何数据库中删除记录!换句话说，user表权限就是超级用户(superuser)权限。为了安全考虑，user表中的权限最好不要授予普通用户，而是使用db和host表，在一个特定数据库上授予用户权限。

4 结束语

在网络环境下，加强信息安全的前提就是确保网络的安全。只有网络安全了，信息的存储、传输才有安全可言。而网络安全问题是一个涉及多方面的问题，对于一个网络的安全性来说，不仅要看它所采取的防范措施，而且还要看它的管理措施。随着Internet的发展，网络的安全性日益受到人们的重视，但安全只是相对而言，绝对安全的网络是不存在的。提供的服务越多，系统的漏洞就越大，安全性就越差。网络在不断地发展，解决了旧的问题，随着新功能的出现，新的安全问题随之而来。网络提供的服务功能是否强大与网络是否安全总是一对矛盾，互联网正是在不断解决这对矛盾中向前发展的。



参考文献

1 1 MySQL Reference Manual for version 3.23.30-gamma，电子文档。

2 Apache 1.3.17 documentation 电子文档。

3 方义等，Apache Server的配置与管理，人民邮电出版社，2001。

4 黄前聪，网络安全基础知识，清华大学出版社，1999。