校园网的安全问题及对策

樊淳宁

TP393 B

摘　要： 指出了校园网安全问题的表现形式，分析了安全问题产生的原因，提出了解决办法。

关键词： 校园网　建设　安全　对策

Problems of Security and Solution on School Computer Network

FAN Chunning

(Party School of Railway Administration Huhhot , Huhhot , 010050)

Abstract: It was described security problems in school computer network, analyzed main reasons and provided solutions to them.

keyword: school computer network , construction , security , solution

1 引言

校园网作为学校基础设施重要的组成部分，在学校教学、科研、管理和对外交流等方面担当着越来越重要的角色。校园网的安全状况直接影响着学校的教学活动。由于计算机网络具有联结形式多样性，终端分布不均匀性和网络的开放性，互连性等特征，使网络容易受到来自各方面的攻击，从而使网上信息安全成为令人头痛的问题，因此，确保网络信息的保密性、完整性和可用性成为网络管理人员的重要工作。

樊淳宁　呼和浩特铁路局党校　工程师　010050　内蒙古呼和浩特市

2 校园网中安全问题的表现形式

2.1 垃圾信息

网上教学活动是校园网最主要的任务之一，师生

3.3 更严重故障

因为供电、雷击、误操作、黑客攻击等的各种意外，有可能使双机的系统盘损坏。此时，只要有1台上机硬件系统和RAID系统完好，即可启用平时冷备的备用系统盘。其上已预装完整系统，IP地址为Cluster浮动IP。然后，采用3.2所讲的步骤，手动启动。

4 磁盘文件系统可靠性分析

4.1 RAID系统

对包头西站RAID的选择，综合考虑I/O性能、使用率，以及易维护性，采取5级容错方式，用5块盘构成RAID5，外加1块热备盘，1块冷备盘，共7块盘。既保证当1块RAID5数据盘报错，热备盘变为RAID5数据盘，冷备变为热备时，还允许1块RAID5数据盘报错，同时尽快放入1块冷备盘。

5级容错，它没有单独的校验盘，用于纠错的奇偶数据直接存放在数据盘中。其优点是：I/O性能较高，尤其适合数据库这种大量却分散的小文件；使用率较高，为85%；容错性能较高，虽不及1、2、3级，也能满足数据库应用。

4.2 RAID故障与ORACLE数据库系统恢复

因RAID系统可靠性很高，故ORACLE等各种服务及应用程序都建立在其上，但RAID系统也有发生故障的可能，所以，必须考虑ORACLE数据库系统恢复的问题。

ORACLE系统主要分2部分：RDBMS和库表文件，分别建立为/oracle和/dbf文件系统。库表文件恢复主要有2种：（1）转储备份恢复，即export/import；（2）日志文件恢复。

考虑到数据实时性，以上2种方法意义不大。综合考虑RDBMS恢复，可以采用如下方案：用文件系统方式，把建立好的/oracle、/dbf文件系统复制到冷备盘的/ora_bak、/dbf_bak文件系统中；编制程序，对实时性强的表初始化；RAID故障时，利用AdvFS命令，把冷备盘的/ora_bak、/dbf_bak文件系统设置为/oracle、/dbf文件系统；运行各服务启动脚本；运行(2)的程序，初始化实时性强的表。

通过上述方法，可较好地完成ORACLE数据库系统的恢复。

5 结束语

目前，硬、软件系统针对不同的应用，有多种避错与容错的解决方案。可以针对不同的应用要求、采取成本最小的解决方案。

（收稿日期：2002-08-20）

可以通过校园网上网进入Internet。如果管理措施不健全，一些垃圾信息就会进入校园网站。

2.2 网络病毒

校园网在接入Internet后，为病毒入侵校园网大开方便之门。下载的程序和电子邮件都可能带有病毒，对计算机系统软、硬件造成损坏。

2.3 信息泄密

学校涉及的机密不是很多，但是一些学生可能会通过非法访问网站获得习题的答案，影响正常的教学活动。

2.4 网络设备受损

网络设备通常包括服务器、交换机、集线器、路由器、通信媒体和工作站等，它们分布在整个校园内，管理起来非常困难，有些人员可能出于某种目的，有意或无意地将它们损坏，造成校园网络全部或部分瘫痪。还有一些是利用黑客技术对校园网络系统进行破坏，如对校园网站的主页进行修改，破坏学校的形象；向服务器发送大量信息，使整个网络陷入瘫痪。

3 安全问题产生的原因

3.1 疏忽造成的失误

由于疏忽造成失误给网络安全带来影响的不仅仅是网络管理员，一些普通用户的疏忽是网络安全的主要问题。

（1）网络管理员的失误主要表现在对操作系统，应用软件或网络设备的配置不当而造成安全漏洞。如用户权限过大，服务端口打开得太多，未及时删除已离职用户，未进行路由器IP安全设置等。

（2）网络普通用户或者低级用户甚至是临时用户的失误，往往是由于安全意识不强、口令选择不慎、将自己的账号随意转借他人，与别人共享资源等原因造成，这些都给网络安全带来了致命的威胁。

3.2 人为恶意的攻击

（1）以各种方式有选择地破坏信息的有效性和完整性，或者造成网络服务器瘫痪，停止提供各类服务。如死亡之Ping，UDP洪水，SYN洪水和电子邮件炸弹等等，都是利用畸形的或大量的TCP/IP包而将服务器摧垮。

（2）在不影响网络正常工作的情况下，进行截获、窃取和破译以获得重要机密信息。如特洛伊木马、缓冲区溢出等，都是通过一小段程序夺取服务器的控制权，实现对服务器的远程控制。

这2种攻击均可对计算机网络造成极大的危害，并导致机密数据的泄漏。

3.3 软件的漏洞

几乎没有一个操作系统或应用软件是百分之百安全的。从Windows NT到Windows2000，从UNIX到Linux，以及Internet Information Server和Exchange，都或多或少地存在着安全漏洞和安全缺陷，另外，程序员为了方便自己而设置的软件“后门”，危害更是极大。

4 网络安全策略

完全杜绝网络安全漏洞几乎是不可能的事情，因为漏洞不可能在被发现和被利用之前得到弥补。网络安全策略主要包括2大部分，即访问控制策略和信息加密策略。访问控制策略是网络安全防范和保护的主要策略，也是维护网络系统安全、保护网络资源的重要手段，用以保证网络资源不被非法使用和非常访问。信息加密策略主要是一种补救手段，也就是说，即使信息在传输过程中被截获，也将由于不能解密而无法读取，从而保证数据的安全。虽然各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心之一。

4.1 登录控制

用户的入网访问控制分为3个步骤：用户名的识别与验证，用户口令的识别与验证，用户帐号的缺省限制检查。

（1）口令

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户在注册网络时，必须输入用户名和口令，服务器将验证其合法性。

（2）账号

网络管理员应当控制普通用户的账号使用、访问时间和访问方式。用户名或用户账号是所有计算机系统中最基本的安全措施，用户账号只有系统管理员才能建立。在管理账号时，应当遵循下列规则：

安装某些系统服务功能模块时，应及时修改操作系统内部账号口令的缺省设置。

网络管理员在建立新账户时应对用户口令作出以下几个方面的限制：最小口令长度，强制修改口令的时间间隔，口令的唯一性和口令过期失效后允许入网的宽限次数。

（3）缺省限制

用户名和口令验证有效之后，再进一步履行用户账号的缺省限制检查。网络对所有用户的访问进行审核，如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

4.2 权限控制

权限控制是针对网络非法操作所提出的一种安全保护措施，网络管理员可以为用户指定适当的访问权

限，并通过访问权限控制用户对服务器的访问。

（1）目录级安全控制

网络管理员可以控制用户对目录、文件和设备的访问。对目录和文件的访问权限一般有8种：系统管理员权限（Supervisor），读权限（Read），写权限（Write），创建权限（Create），删除权限（Erase），修改权限（Modify），文件查找权限（File Scan）和存取控制权限（Access Control）。

（2）属性安全控制

当用户被允许访问文件、目录和网络设备时，网络系统管理员还应当为这些文件、目录和设备指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据，拷贝一个文件，删除目录或文件，查看目录和文件，执行文件，隐含文件，共享和系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的删除、修改和读取。

4.3 服务器安全控制

许多服务器允许远程用户通过Telnet等方式登录，并可在控制台上执行一系列操作，如装载和卸载模块，安装和删除软件等等。虽然在网络管理员进入服务器管理时会便利一些，但无疑也给非法用户访问和控制服务器带来了可乘之机。服务器安全控制包括设置口令锁定服务器控制台，防止非法用户修改、删除重要信息或破坏数据；设定服务器登录时间，限制非法访问者检测和关闭的时间间隔。

4.4 路由器和交换机安全控制

（1）控制会话超时

当网络管理员在特权模式下登录到控制台后，因事外出，使控制台处于无人看管状态，此时任何用户都可以乘机修改网络设备的配置。因此，对空闲状态必须进行超时设置，使得控制台在一段时间的空闲后自动断开与网络设备的连接，从而提供安全保障。

（2）控制虚拟终端访问

（3）控制HTTP访问

（4）端口安全

当端口接收到一个数据帧时，它将这个帧的源地址与端口原来所记录的“安全”源地址进行比较。如果MAC地址不匹配，那么该端口将被关闭，同时端口的指示灯变成橙色；

（5）用过滤器控制信息

（6）MAC地址绑定

4.5 防火墙控制

防火墙是目前最为流行的一种网络安全技术。防火墙（Firewall）是指设置在不同网络（如可信任的企业网和不可信的公共网）或网络安全域之间的一系列部件的组合。它是不同网络或网络安全域之间信息的唯一出入口，能根据企业的安全政策控制（允许、拒绝、监测）出入网络的信息流，且本身具有较强的抗攻击能力。

防火墙作为一个分离器、限制器和分析器，能有效监控局域网和Internet之间的任何活动，对于联接到Internet的局域网而言，选用防火墙是非常必要的。

4.6 代理服务器控制

代理服务器（Proxy Server）是运行特定服务器程序的计算机。代理服务器拥有2个网络接口，一个接口用于联接Internet，另一个接口则用于联接局域网，从而使得局域网从物理上隔离了Internet上可能的非法侵入者。代理服务器能够对Internet保护内部IP地址，禁止IP转发，只有运行Proxy Server的计算机的IP地址才是Internet中可见的。从而只将最安全的计算机—代理服务器暴露在Internet上。也就是说，代理服务器作为一种双宿主主机，它直接暴露于Internet，代理局域网用户向Internet发出请求，并将接受的信息反馈给用户，为局域网用户连接Internet提供必要的屏蔽。除此之外，代理服务器还具有带宽利用、将局域网用户连接到Internet等功能。

4.7 VLAN安全

VLAN分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听。在集中式网络环境下，通常将敏感部门的所有计算机系统集中到一个VLAN里，在这个VLAN里不允许有其他任何用户节点，从而较好地保护这些主机中的资源。

4.8 VPN安全

VPN（虚拟专用网）技术的核心是采用隧道技术，将内部网络的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据被窃。

VPN技术通常采用2种加密协议，即点到点隧道协议（PPTP）和IP安全（IPSec）协议。PPTP和VPN可以实现Internet上的专用会话，将远程用户安全地链接到企业网络。Windows2000以完全基于软件的方式实现了虚拟专用网，因此成本非常低廉，这无疑是联网技术中一次具有划时代意义的革命。无论您身处何处，只要能连接到Internet（通过普通拨号上网PPP的方式），就能够与校园网络在Internet上的“虚拟专用网”网关

铁路局客运公司计算机信息网的设计与实现

赵建军 TP393 B

摘 要：阐述了呼和浩特铁路局客运公司计算机信息网的设计及组建方法，探讨了 Intranet 内联网安全问题，介绍了远程网络互联技术在内联网中的应用。

关键词：内联网 网络安全 网络设计

Design and Implementation of Intranet in Passenger Transport Corp of Railway Administration

ZHAO Jianjun

(Information Technology Department of Railway Administration Huhhot, Huhhot, 010051)

Abstract: It was expatiated on the methods of designing and building computer information network in Huhhot Railway Administration Passenger Transport Corp., introduced the security problems in Intranet and the application to the Intranet.

Keyword: Intranet, network security, network design

1 引言

呼和浩特铁路局客运公司计算机信息网的建设涉及面广，投资大。为确保网络建设成功，必须制定技术可行，安全可靠，经济实用的设计方案，系统设计遵循以下原则：

（1）先进性和标准化原则。采用现行先进的网络技术，保证系统日后的顺利扩容和维护方便，采用标准化技术，分层设计，使得网点的变更可随时发生，便于扩容和维护。

（2）实用性原则。结合公司业务要求，对传输介质，交换机间通信主干，广播网段，容量和性能等方面都作了合理的考虑和设计。

（3）安全、可靠性原则。从OSI的物理层和数据链路层采取冗余的方式，网络层采用IP过滤(FILTERING)，虚拟局域网（VLAN），服务质量(QOS)和端口监视（端口RMON）的先进技术，确保网络畅通和安全应用。

2 网络结构

公司信息网由内联网(Intranet)和票务中心网组成，平时，两者之间物理隔开，当票务中心网络发生故障时，自动切换到Intranet，使用VLAV，实现数据传输的可靠性和安全性。

2.1 路由协议的选取

广域网协议及路由协议的选取对技术要求比较高，2个客运管理中心、2个客车检修中心以2M带宽上连到总公司，路由协议有RIP、EIGRP和OSPF等几种，RIP是一种距离矢量路由协议，适用于小型简单网络；OSPF是一种链路状态路由协议，完全能够满足较大型网络的高稳定性、高性能的要求；EIGRP路由协议是CISCO公司自己开发的一套路由协议，具有很好的扩展性，采用DUAL扩散更新算法，确保无路由回路，传输路由变化可靠，支持可变长子网掩码（VLSM）和手工汇总IP，协议运行占用带宽小，较OSPF配置简单，具有快速收敛、非均衡负载的特性，因此建网采用了EIGRP协议。为进一步保证网络的可靠性，增加了浮动静态路由作为备份路由。

2.2 Intranet结构

公司用户共享网络公共资源的同时，又有着各自独立的业务，针对这一格局，我们采取了星形拓扑结构和划分不同的网段，公司内部以3COM交换机作为核心层，以HUB为接入层，建立起10/100M交换式快速

赵建军 呼和浩特铁路局信息技术处 工程师 010050 呼和浩特市

联接，登录到内部浏览或交换信息。

4.9 信息加密策略

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密，端点加密和节点加密3种。

5 结束语

校园网的安全状况直接影响着学校的教学活动。文中所述的安全策略可以有效地保障校园网的安全，提高网络信息的保密性、完整性和可用性。

（收稿日期：2002-08-20）