中山大学学报（自然科学版）
第40卷 增刊 ACTA SCIENTIARUM NATURALIUM Vol.40 Suppl.
2001年 3月 UNIVERSITATIS SUNYATSENI Mar. 2001

文章编号：0529-6579（2001）S-0125-05

校园网络安全解决方案*

赵敬中，曹明存
（北京理工大学网络中心，北京 100081）

摘 要： 描述了校园网络运行中普遍存在的安全缺陷，并对问题进行了分析，提出了相应的解决方案。

关键词： 防火墙；入侵检测；过滤；扫描；攻击
中图分类号： TP393.08 **文献标识码：** A

1 校园网简介

目前全国各地的学校校园网大多采用交换式以太网结构。网络拓扑结构采用三层设计，即核心层、分布层和访问层。网络主干核心层一般采用能够快速处理大量流量的高性能的交换机，处理来自所有 VLAN 的、从访问层到中心服务器的各种流量，称为网络主干线一级节点。分布层要求在 VLAN 间慎重地分配资源和安置用户，将在 VLAN 之间传送的非服务器相关流量降至最低。分布层的主要任务是从核心设备将连接“扇出”到单个的访问交换机，分布层为二级节点。访问层的设计是最简单的，要求通过交换机接口而不是共享集线器接口，访问层为三级节点。至于国际互连网的接入设备一般采用 CISCO 边缘路由器，如 CISCO 2600 系列。如果要求提供拨号访问的话，可以在上面安装异步通讯模块，提供校内分散用户或没有铺设光缆的单位上网。提供的服务主要有校内、外 Web 浏览服务，电子邮件（E-mail）服务，文件传输（FTP）服务，电子公告板（BBS）系统，图书检索，公共信息发布，网络教学资源库等。

2 校园网安全技术分析

2.1 防火墙技术

在很多学校都采用了防火墙技术，即在校园网和国际互连网之间架设了防火墙。这样做的确可以把校园网严密地保护起来，免受外部世界的侵扰。防火墙一般具有如下特性及优点：自适应安全算法、直通代理、安全实时内置代理系统、防止拒绝服务攻击、支持大量的同时连接、支持 IETF IPSec 、管理报告、URL 记帐及过滤、Java Applet 过滤器、邮件监视、多媒体应用支持、地址转换（NAT）、认证/审核。

2.2 远程访问服务

为了提供部分用户上网，可以采用的方法很多，如基于 Windows NT 的 RAS（远程访问服务）、边缘访问服务器等等。远程访问一般采用 RADIUS（远程认证拨号用户服务）或

* 收稿日期：2000-11-15；E-mail：jzhao@bit.edu.cn

TACACS+（终端访问控制器访问控制系统）授权、认证机制。

2.3 VLAN技术

为了防止网上的广播风暴，校园网大多采用VLAN技术。即将各部门或关系相近的各部门划分在一个VLAN中，不同VLAN的用户相互通信必须通过中心路由器路由，也可以采用第三层的交换机完成不同VLAN之间的通信功能。VLAN技术的采用不仅提高网络性能，同时便于综合有效的管理网络，也提高了校园网络内部安全。

2.4 全面的网络管理

根据IDG报告统计，CISCO公司网络产品的市场占有率为80%。如果采用CISCO的网络产品，网管系统主要是基于SUN Manager2.3网管平台的Cisco Works 4.0和CWSI两组网管软件。前者主要用于路由器的监控和管理，后者包括CiscoView、Traffic Director和VLAN软件，主要用于管理交换机，监控设备之间信息流量和划分VLAN。

2.5 代理服务器

目前很多学校对于国际网络站点的访问可以采用代理服务器的方式，相应的代理软件也很多，如Netscape公司的Proxy 3.5、Microsoft公司的WinProxy等。

3 校园网络不安全的主要隐患

3.1 IP盗用问题

这个问题的出现可能与很多大学通过校园网访问国际互连网的收费规则有关。这些学校的收费规则是国内站点的访问是免费的，而出国访问则要申请代理并根据流量计费的，当然上网的前提是用户必须申请合法的IP地址。可是有些用户却不申请IP地址，而使用他人的合法IP地址，从而造成网络内部地址冲突，严重妨碍了合法用户的正常使用。（注：在地址冲突时，如果两个都是Windows用户则先开机的用户占有优势。在两个用户有一个是Unix用户时，则Unix用户占有优势。）

3.2 Proxy问题

另一种情况是有些用户只申请一个IP地址，通过安装代理服务器使同一个教研室内的几个人同时上网。倘若是经过学校网络中心同意的，为了保护该教研室的某些重要信息而设置的，这属于合理使用。倘若是其它非合理原因，这种做法是违反校园网络使用的基本条例的行为。

3.3 拨号服务器问题

有些用户为了方便或者其它原因，自己在实验室内设定拨号访问服务器，甚至还向外提供拨号上网服务。这样做其实是在校园网络内部开设了一个后门，这样做将会给网络带来了严重的安全隐患。

3.4 E-mail（电子邮件）问题

由于用户的安全观念的淡漠，在上网浏览的过程中很随意的将自己的信箱交给了不该信任的他人，致使造成邮件垃圾和安全后患。如近期较为流行的爱虫病毒就是通过电子邮件来传播的，该病毒的破坏是十分严重的。

3.5 拨号上网问题

有一种比较特殊的情况是无法接入校园主干网的分散用户和个人用户通过电话拨号方式接入校园网。目前采取的措施是拨号用户的拨号连接、身份认证和授权全部在防火墙外

部，分配的IP地址范围也是必须通过防火墙才能访问学校内部的网络信息。当然这样做会很大的程度上限制了这些用户的访问。可是如何有效地加以控制拨号上网帐号的传播又是个相当令人头疼的问题，因为倘若某个帐号落在非法分子手中，后果也的确让人担心不已。

3.6 防火墙攻击

防火墙系统的确很坚固，但只是对外的防护，而对内的防护可以说是极为脆弱。大量的事实已经证明，70%以上的攻击来自企业或单位内部人员，而不是网上的黑客。

3.7 各种服务器和网络设备的扫描和攻击

总是有很多用户对这些设备进行各种各样的攻击，造成网络负载过重，致使重要服务器拒绝服务。当然这种攻击有时是无意的，例如：有些人为了获得免费的出国代理服务器的网络地址，使用代理猎手或其它代理搜索软件进行大范围的搜索，给本来带宽就比较紧张的网络带来了更大的负担，使很多用户就根本无法上网。不管攻击情况属于哪一种，在校园网内部都是应该禁止的。

3.8 非法URL访问问题

主要是一些反动或不健康的站点的访问，危害了公民的身心健康，与学校这个大的学习环境极为不相称。

3.9 BBS站点非法言论问题

某些不法分子利用电脑网络手段进行反动宣传，特别是在政治敏感期间，这些过激的言论都严重威胁着社会的安定团结。

4 网络安全的解决方案

4.1 IP盗用问题解决方法

(1) 使公共机房的计算机与各单独用户的计算机分别占用交换机的不同端口，然后在交换机的各端口上只允许经过登记的合法用户进入校园网。

(2) 在路由器上捆绑IP和MAC地址。IP地址与MAC地址的绑定指的是规定某一IP只对应某一特定的网卡（MAC)。当某个IP通过路由器访问Internet时，路由器要检查发出这个IP广播包的工作站的MAC是否与路由器上的MAC地址表相符，如果相符就放行。否则不允许通过路由器，同时给发出这个IP广播包的工作站返回一个警告信息。

(3) 对于公共机房的另一种管理办法是，只给它分配一个合法的IP地址，让他们自己建立双网卡的NT路由和服务器。机房内部用Internet的私有局域网地址，内部用户也可以由自己的NT服务器管理。这样就可以彻底解决公共机房人为造成的IP与其它单位的IP发生冲突问题。

(4) 鉴于目前MAC地址可以通过特别手段更改的问题，可再将IP地址与用户帐号绑定起来，用户可以根据自己的使用情况来灵活设定IP地址是否有效，即是否可以通过防火墙来访问Internet。这样使得非法IP用户上网也就受到了极大的限制，打击了某些非法用户的嚣张气焰。另一种办法是访问层交换机上在每个端口增加固定硬件地址表，使得只是具有这些物理地址的用户数据包才能从这里通过，即使产生冲突也只是在这个端口内的几台机器的范围内，很容易定位到各部门的具体机器上。

4.2 Proxy（代理服务器）问题解决方法

编制代理服务器查找工具，不定期的对校园网内部进行扫描，根据网络安全管理员的任务设定，对无权使用代理服务器的用户加以限制。不过问题的难度不是FTP、HTTP等代理，而是使用SOCK代理，由于这种代理的特点是具有权限限制，在一定意义上讲，起到了防火墙的作用。通常的方法无法获知自行设置的小局域网内部的情况，这可以通过流量、目标主机发出的数据报的特征来识别。

4.3 拨号服务器问题解决方法

编制拨号服务器的搜索工具，不定期的对各部门的电话进行扫描，判别对方是否在使用拨号服务器。倘若在使用拨号服务器，则根据各部门注册的电话号码找到响应的部门，并给予警告。

4.4 拨号上网问题解决方法

采用RADIUS（远程认证拨号用户服务）或TACACS（终端访问控制器访问控制系统）认证，提供远程拨号的安全访问。方法是：在建立拨号用户帐户的时候除去设定用户帐号、口令外，再设定回拨功能、回拨号码和设定固定IP地址等。这样使得仅校内的某些用户可以拨入校园网络内部，控制其它校外的用户访问，提高校园网的安全。

4.5 采用入侵检测系统

目前比较流行的入侵检测系统是ISS公司的REAL SECURY，可以很好的防备来自各方面的攻击。由于该软件的价格比较贵，用户在这方面的要求又不是极为强烈的话，自己可以定义规则，即认为哪些是属于入侵的范畴，可以自行开发小的应用程序，不断积累起来完善自己的入侵检测系统，或者称为安全服务器。安全探测器的设置一般是在防火墙的内外接口处、重要服务器所在的网段等处，由于入侵检测一般是基于日志、实时检测数据报等信息的计算机系统，自身安全的保证也尤为重要，可以通过专门网络和安装仅需要协议有限部分的方法来减少外部的攻击。

4.6 防火墙系统

采用防火墙系统之后，网络管理员并不是完事大吉了，除去配置有效的过滤规则之外，还要定期更改密码、日志要每天进行检查。大多数黑客在进行攻击之前都要进行扫描，搜集一些重要信息，找某些主机或网络设备的漏洞所在。因此用户在检查日志时，如果发现可疑日志之后就要增强防范措施，并检查在网络设备或主机系统上是否已经存在了安全漏洞等。

4.7 Web，Email，BBS安全问题解决方法

（1）Web服务：防火墙一般提供了主动过滤URL，从而控制用户可以访问哪一个站点。URL过滤功能可以通过与Web Sense服务器软件的集成实现。也可以通过编写客户端程序，利用防火墙的访问原则的修改来禁止某些站点的访问。在防火墙内部提供了大量日志，利用它可以后期查看站点访问情况，从而进行必要的管理。

（2）WEB安全包括：WEB服务器基本信息检测、WEB服务器属主检测、CGI程序检测、符号链接检测、WEB目录读写属性检测、访问日志分析、文件更新检测等。

（3）Email过滤：在邮件服务器上编写ProcMail（邮件过滤软件），用户通过邮箱设置主页来灵活编写过滤规则，完成对接受邮件的过滤。由于大部分邮件采用PGP加密，因此只是对发信Email地址、邮箱、主题，内容为明文的信件加以简单的过滤。

对于发送邮件的过滤可以采用 Blackmail 软件（代理邮件服务器软件），来完成对于发送邮件的的过滤。该软件采用一种代理机制，外发的邮件首先经过 BlackMail 软件的规则检查，在允许通过的情况下重新生成电子邮件副本向外转发。

(4) BBS 过滤：在文章中提取关键字的方法加以过滤，过滤的方法与 Email 的思想很是相似，不再详述。

4.8 安全管理解决方法

一次性密码技术；安装防病毒技术，定期进行病毒检查；安全意识的提高，如发送电子邮件进行加密传输。

4.9 陷阱和跟踪技术解决方法

为了更多的获取非法分子或黑客的信息，我们可以在自己的服务器上设置陷阱，即故意留下几个破绽给对方。在对方入侵时诱导他们留下狐狸尾巴，收集对方的信息，以便以后追究其法律责任。不过这种陷阱的设置一定要设计的巧妙，为了不让黑客或入侵者识别到是陷阱，不能过于明显又不能过于复杂。

4.10 禁止非法用户或报警措施

(1) 首先在安全服务器或网管计算机上警告进行非法活动的用户，在必要的情况下给出适当的证据（包括时间、行为与危害等），采用的方式可以是电子邮件、BBS 或 WWW，新闻等方式。

(2) 进一步禁止 IP 地址和 MAC 地址（修改路由器访问表实现），这样做可能会增加路由器或防火墙的负担，要慎重考虑。

(3) 通过 IP、MAC 和用户的对应关系，以及通过安全服务器探测到的主机名、所属分组等信息进行查找非法用户，给予罚款或取消上网资格。

(4) 在发现可疑用户的时候，还可以通过电话报警。管理员当然自己可以编制简单的拨号应用小程序来完成报警工作。

参考文献：

[1] 彭业飞译.Cisco IOS 交换服务.1997.
[2] 邸瑞华,冯国璨.Intranet 组网技术.1997.
[3] 许锦波,严望佳.网络安全结构设计.1996.
[4] 付攸,乔一林.设计与实现.1996.
[5] 马树奇,金燕.网络安全从入门到精通.1998.

Solutions to the Security Drawbacks in Campus Network

ZHAO Jing-zhong *, *CAO Ming-cun*

Abstract: This paper not only depicts the security drawbacks existing in campus network, but also analyzes these problems and provides the appropriate solution.

Keywords:

* Network & Information Center, Beijing Institute of Technology, Beijing 100081, China