现代计算机技术与应用
2022 年 8 月第 4 卷第 3 期

浅析校园网的安全管理

张青芸

江汉大学，武汉

摘　要 | 随着校园网应用的深入，其安全问题越来越突出，数据的安全性和学校教学管理活动受到了严重威胁。从校园网总体规划建设及校园网的安全隐患的角度出发，介绍了建设安全校园网络的重要性，通过理论与实践相结合研究如何落实校园网络安全防范体系，并重点研究网络安全策略在校园网中的实际应用。

关键词 | 校园网；规划建设；安全隐患

1　校园网规划设计的关键特点

（1）系统可靠性与安全性

在系统设计中，很重要的一点就是在尽量短的时间内恢复正常工作，是校园网系统这样的重点工程所必须考虑的。在设计时对可靠性的考虑，可以充分减少或消除因意外或事故造成的损失。随着计算机技术的发展，尤其是网络和网络间互联的规模的扩大，信息和网络的安全性日益受到重视，面临着是网络的可靠性。在外界环境或内部条件发生突变时，怎样使系统保持正常工十分严肃的安全性挑战。在网络设计时，要从内部访问控制和外部防火墙两方面保证

作者简介：张青芸，江汉大学助教。
文章引用：张青芸．浅析校园网的安全管理［J］．现代计算机技术与应用，2022，4（3）：89-96.
https://doi.org/10.35534/mcta.0403013c

校园网系统的安全。

（2）系统的先进性

校园网系统处理的信息量是十分庞大的，要求计算机网络有很高的工作效率。而且随着教学科研任务的迅速发展，系统面临的任务也愈来愈艰巨。所以，设计的网络在技术上必须体现高度的先进性，技术上的先进性将保证处理数据的高效率，技术上的先进性将保证系统工作的灵活性，技术上的先进性将保证网络的可靠性，技术上的先进性也使系统的扩展和维护变得简单。要在网络架构、硬件设备、传输速率、协议选择、内外安全控制和虚拟网划分等各个方面充分体现校园网系统的先进性。

（3）容易管理和升级

校园网系统的节点数目大，分布范围广，通信介质多种多样，采用的网络技术也较先进，尤其引入交换式网络和虚拟网之后，网络的管理任务会加重，如何有效地管理好网络，是否充分有效地利用网络的系统资源等问题显得至关重要。要尽量使用图形化的管理界面和简洁的操作方式，提供强大的网络管理功能，使网络日常的维护和操作变得直观、简便和高效。

随着教学科研的快速发展，校园网系统面临的任务将愈来愈艰巨，愈来愈复杂。为了适应变化和日新月异的计算机技术的发展，校园网的建设要十分注重可扩充性。无论是网络硬件还是系统软件，都应可以方便扩充和升级。

2　校园网的安全隐患

随着校园网络应用的深入，校园网络的安全问题也逐渐突出，直接影响着学校的教学、管理、科研等活动。下文将对目前校园网络的安全隐患进行分析。

2.1　网络部件的安全隐患

（1）系统的易被监控性、薄弱的认证环节、局域网服务的缺陷和系统主机复杂的设置与控制，使得计算机网络容易遭受威胁和攻击。

（2）网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄漏。目前，大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易

出现信息泄露。

（3）非法分子通过技术渗透侵入网络，非法使用、破坏或获取数据及系统资源。目前的网络系统大都采用口令来防止非法访问，一旦口令被窃，网络很容易被侵入。

（4）随着信息传递量的不断增加，传递数据的密级也不断提高，犯罪分子为了获取大量情报，采用监听通信线路的手段，非法接收信息。

2.2 软件的安全隐患

（1）网络软件的漏洞及缺陷被利用，能对网络进行入侵和损坏。如网络软件安全功能不健全；应加以安全措施的软件未予标识和保护，要害的软件没有安全措施；错误地进行路由选择，为一个用户与另一个用户之间通信选择不合适的路径；拒绝服务、中断或妨碍通信，延误对时间要求较高的操作和信息重播。

（2）黑客采用种种手段，对网络及其计算机系统进行攻击，侵占系统资源或对网络和计算机设备进行破坏、窃取或破坏数据和信息等。

（3）校园网内部用户的计算机技术素质较低，管理维护技术滞后，导致计算机网络病毒木马泛滥，病毒木马以多种方式侵入网络并不断繁殖，然后传播到网上的其它计算机来攻击和破坏系统，甚至可能导致网络瘫痪。

2.3 网络管理人员的安全隐患

（1）保密观念不强或不懂保密规则，随便向无关人员泄露机密信息。

（2）专业素质和技术水平差，业务不熟练，不能及时发现网络安全隐患并采取相应措施。

（3）缺乏责任心，没有良好的工作态度，访问权限管理混乱。

3 校园网的安全解决策略

3.1 建立良好的网络拓扑结构

合理地划分 VLAN 校园网络至少要采用两级结构：主干网和子网。校

https://doi.org/10.35534/mcta.0403013c

园网的主干采用成熟的 1000 M快速以太网，在校园网络中心机房设有一个总的出口（代理服务器）访问互联网，提供认证系统，所有进出校园网的数据都需要通过此出口检测过滤。由网络中心用光纤连到各座大楼的分节点，再经分节点的交换机连接到大楼的各个用户。这种配置结构既保证了主干网信息可靠、高速、无瓶颈地传输，又为用户计算机接入提供了灵活、方便的手段。

同时将校园网划分为若干虚拟局域网，虚拟局域网可不受设备物理位置的限制，灵活性较大。校园网按网络功能划分为：接入网部分和内部局域网部分。内部局域网又按数据交换能力分为：核心层、汇聚层和接入层。将各种主要服务器（WEB、MAIL、FTP 服务器、数据库服务器等）放在一个虚拟网内，这样便于管理、维护，同时也可以尽可能减少外部入侵及破坏系统的可能性。另外划分一个教学管理子网，方便教师进行管理和教学；其余虚拟子网可按教务管理系统、图书馆系统、办公管理系统、多媒体网上教学系统等划分。

3.2 优化网络平台，减少外部入侵

网络平台是校园网软件运行的物理平台，是整个网络安全建设的基础，因此对网络安全的第一步需要是对现有的网络平台进行改造和优化，利用防火墙控制网络内部的访问权限，由目前开放式的结构向有条件开放式的网络结构转变。具体可采取以下措施。

（1）应用防火墙技术，实现网络信息安全域的划分与隔离控制。为保护内部网络不受外部网络的干扰，对所有的外部网络接口用防火墙进行隔离，对数据包进行过滤，防止病毒和黑客的攻击；

（2）基于 VLAN 和 VPN 的信息保护和通讯保密。根据校园内部网络与信息系统的网络结构、具体的应用以及安全等级的需求，在校园网内部，在各部门的交换机上设置 VLAN，同时对连接国家教育科研网的线路采用 VPN 方式进行加密，保障数据安全；

（3）对外部网络出口进行统一管理。加强对所有的外部出口进行严格管理，

对所有出口加装防火墙，以最小权限方式控制出入的数据包，利用入侵检测系统等安全防护软件保留外部网络访问日志，并定期分析访问日志，及时掌握外网访问情况。

3.3 保证网络中硬件系统的物理安全

校园网安全首先要保证网络硬件系统的物理安全，它包括多方面的内容。

（1）防盗。主机、内存条、CPU 等被盗的事件在学校里时有发生。为此，要采取对应的措施，如在机房窗户安装防盗网、给机箱上锁、实行机房所在大楼 24 小时值班制度和举报奖励制度等。

（2）防火。机房发生火灾一般是由于电气原因、人为事故引起的。因此，机房均应采用防静电地板，通过接地泄放静电荷；禁止在机房抽烟；安装感温自动报警装置和惰性气体自动灭火装置等。

（3）防雷击。一般做法是在楼顶设置避雷针、避雷带以防止雷击。

（4）防停电。在机房里添加不间断电源 UPS，附设一定的直流电池组作为后备电源，即可保证供电。

3.4 制定切实可行的网络安全管理制度

这是解决网络安全问题的所有对策中最重要的一点，主要包括以下几方面的内容。

（1）建立一个高度权威的信息安全管理机构，并不断强化其权限和职能；

（2）制定统管全局的网络信息安全规章，做到有章可循、有章可依；

（3）制定网络管理员岗位工作制度和激励制度，规范他们的工作行为，并促使他们提高工作热情，加强工作责任心，专心于校园网络管理工作；

（4）加强对网络管理员的专业知识和技能培训；

（5）把网络信息安全的基本知识纳入学校各专业教育之中；

（6）对学校教师和其他人员进行信息安全知识普及教育；

（7）在学校的网站设立网络安全信息发布栏目，发布网络法令法规、网络病毒公告、系统更新、补丁公告等，并提供常用软件的下载。

https://doi.org/10.35534/mcta.0403013c

3.5 采用先进的网络安全技术

（1）运用网络入侵检测

入侵检测能力是衡量一个防御体系是否完整有效的重要因素，强大完整的入侵检测体系可以弥补防火墙相对静态防御的不足。根据校园网络的特点，可以采用相应入侵检测系统，如瑞星 RIDS-100，对来自外部网和校园网内部的各种行为进行实时检测，及时发现各种可能的攻击企图，并采取相应的措施。入侵检测系统集入侵检测、网络管理和网络监视功能于一身，能实时捕获内外网之间传输的所有数据，利用内置的攻击特征库，使用模式匹配和智能分析的方法，检测网络上发生的入侵行为和异常现象，并在数据库中记录有关事件，作为网络管理员事后分析的依据；如果情况严重，入侵检测系统可以发出实时报警，使得学校管理员能够及时采取应对措施。

（2）运用防火墙技术

它可以根据既定的安全策略允许特定的用户和数据包穿过，同时将安全策略不允许的用户和数据包隔断，达到保护高安全等级的子网、阻止墙外黑客的攻击、限制入侵蔓延等目的。根据防火墙的位置，可以分为外部防火墙和内部防火墙。外部防火墙将校园网与外部因特网隔离开来。防火墙并不是万能的，它在很多方面存在弱点。它无法防止来自防火墙内侧的攻击，对各种已识别类型的攻击的防御有赖于正确的配置，对各种最新的攻击类型的防御取决于防火墙知识库更新的速度和相应的配置更新的速度。

（3）网络杀毒软件

选择合适的网络杀毒软件可以有效地防止病毒在校园网上传播。在学校网络中心配置一台高效的 Windows 2003 服务器，安装一个网络版杀毒软件系统中心，负责管理校园网内所有主机网点的计算机。在各主机节点分别安装网络版杀毒软件的客户端。安装完杀毒软件网络版后，在管理员控制台对网络中所有客户端进行定时查杀毒的设置，保证所有客户端即使在没有联网的时候也能够定时进行对本机的查杀毒。网络中心负责整个校园网的升级工作。为了安全和管理的方便起见，由网络中心的系统中心定期地、自动地到杀毒软件网站上获

取最新的升级文件（包括病毒定义码、扫描引擎、程序文件等），然后自动将最新的升级文件分发到其它各个主机网点的客户端与服务器端，并自动对网络版杀毒软件进行更新。

（4）运用 VLAN 技术

采用交换式局域网技术（ATM 或以太交换）的校园网络，可以用 VLAN 技术来加强内部网络管理。VLAN 技术的核心是网络分段，根据不同的应用业务以及不同的安全级别，将网络分段并进行隔离，实现相互间的访问控制，可以达到限制用户非法访问的目的。

4 小结

校园网通过采用上述的网络安全策略以及网络安全技术，有了较高的安全系数，但并不能保证校园网是绝对安全的。因为影响校园网的安全因素在不断地变化，黑客与病毒的攻击方式在不断地更新。为此，要确保校园网络的安全就只有根据实际情况，在网络安全技术上采用最新的技术成果，并及时调整网络安全策略，不断地加强安全管理，才能使我们的网络具有更高的安全性和可靠性。

参考文献

[1] 谢希仁. 计算机网络 [M]. 北京：电子工业出版社，2003.

[2] 查贵庭. 校园网安全威胁及安全系统构建 [J]. 计算机应用研究，2005（3）.

[3] 袁海燕. 浅谈网络安全技术及其在校园网中的应用 [J]. 电脑知识与技术，2006（5）.

https://doi.org/10.35534/mcta.0403013c

Analysis of Campus Network Security Management

Zhang Qingyun

Jianghan University, Wuhan

Abstract: With the deepening of campus network application, its security problem is more and more prominent, the security of data and school teaching management activities have been seriously threatened. From the perspective of the overall planning and construction of the campus network and the security risks of the campus network, this paper introduces the importance of building a safe campus network, and studies how to implement the campus network security prevention system through the combination of theory and practice, and focuses on the practical application of network security strategy in the campus network.

Key words: Campus network; Planning and construction; Safety hazards