摘　要

网络平安的本质是网络信息的平安性，包括信息的保密性、完整性、可用性、真实性、可控性等几个方面，它通过网络信息的存储、传输和使用过程表达。校园网络平安管理是在防病毒软件、防火墙或智能网关等构成的防御体系下，对于防止来自校园网外的攻击。防火墙，那么是内外网之间一道牢固的平安屏障。平安管理是保证网络平安的根底，平安技术是配合平安管理的辅助措施。学校建立了一套校园网络平安系统是必要的。

本文从对校园网的现状分析了可能面临的威胁，从计算机的平安策略找出解决方案既用校园网络平安管理加防火墙加设计的校园网络平安系统。通过以下三个步骤来完成校园网络平安系统：1、 建设规划；2、 技术支持；3、 组建方案。

关键词：网络； 平安； 设计

ABSTRACT

Network security is the essence of the safety of network information, including information of confidentiality, integrity, and availability, authenticity and controllable etc, it is through the network information storage, transport and use process. Campus network security management is in anti-virus software, a firewall or intelligence gateway, etc, the defense system to prevent from outside the campus. A firewall is a firm between inner and outer net security barrier. Safety management is the basis of network security and safety technology is the auxiliary measures with safety management. The school has established a set of campus network security system is necessary.

Based on the analysis of the status of the network could face threats, from the computer security strategy to find solutions in the campus network security management is designed with the campus network firewall security system. Through three steps to complete the campus network security system: 1, the construction plan. 2 and technical support. 3 and construction scheme.

Keyword: Network, Safe ； Design

目　录

绪　论 1

1. 校园网络平安 2

1.1 校园网概述 2
1.2 校园网络平安概述 3
1.3 校园网络平安现状分析 3
1.4 校园网络平安威胁 5

2. 校园网络平安措施 8

2.1 校园网络平安管理 8
2.2 校园网络平安措施 9

3.校园网络平安系统设计 11

3.1 校园网建设需求分析 11
3.1.1 需求分析 11
3.1.2 关键设备 12
校园网络拓扑 13
3.2 技术方案 13
校园网的建设规划 13
组网技术 16
网络操作系统 18
3.2.4 INTERNET 接入技术 18
3.2.5 防火墙技术 19
3.2.6 建网方案 19
3.3 校园网的运行 23
校园网的应用 23
3.3.2 校园网的管理 23

总　结 25

参考文献 26

致　谢 27

绪　论

随着网络的高速开展，网络的平安问题日益突出，近年来，黑客攻击、网络病毒等屡屡曝光，国家相关部门也一再三令五申要求切实做好网络平安建设和管理工作。但是在高校网络建设的过程中，由于对技术的偏好和运营意识的缺乏，普遍都存在“重技术、轻平安、轻管理”的倾向，随着网络规模的急剧膨胀，网络用户的快速增长，关键性应用的普及和深入，校园网从早先教育、科研的试验网的角色已经转变成教育、科研和效劳并重的带有运营性质的网络，校园网在学校的信息化建设中已经在扮演了至关重要的角色，作为数字化信息的最重要传输载体，如何保证校园网络能正常的运行不受各种网络黑客的侵害就成为各个高校不可回避的一个紧迫问题。

随着教育信息化的不断推进，各高等院校都相继建成了自己的校园网络并连入互联网，校园网在学校的信息化建设中扮演了至关重要的角色。但必须看到，随着校园网络规模的急剧膨胀,网络用户的快速增长，尤其是校园网络所面对的使用群体的特殊性〔拥有一定的网络知识、具备强烈的好奇心和求知欲、法律纪律意识却相对冷淡〕，如何保证校园网络能正常的运行不受各种网络黑客的侵害就成为各个高校不可回避的一个紧迫问题，解决网络平安问题刻不容缓。

1. 校园网络平安

网络平安是一门涉及计算机科学、网络技术、通信技术、密码技术、信息平安技术、应用数学、数论、信息论等多种学科的综合性学科。网络的生命在于其平安性。因此，在现有的技术条件下，如何构建相对可靠的校园网络平安体系，就成了校园网络管理人员的一个重要课题。

网络的开展极大地改变了人们的生活和工作方式，Internet 更是给人们带来了无尽的便捷。我们的教育也正朝着信息化、网络化开展，随着‘校校通”工程的深入开展，许多学校都投资建设了校园网络并投入使用。校园网络在我们的校园管理、日常教学等方面正扮演着越来越重要的角色。但是，在我们惊叹于网络的强大功能时，还应当清醒地看到，网络世界并不是一方净土。“网络天空〔Worm.Netsky〕”、“高波〔Worm.Agobot〕”、“爱情后门〔Worm.Lovgate〕”及“震荡波〔Worm.Sasser〕”等病毒，使人们更加深刻的认识到了网络平安的重要性。因此，在现有的技术条件下，如何构建相对可靠的校园网络平安体系，就成了校园网络管理人员的一个重要课题。

网络平安是一门涉及计算机科学、网络技术、通信技术、密码技术、信息平安技术、应用数学、数论、信息论等多种学科的综合性学科。网络平安是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络效劳不中断。

1.1 校园网概述

信息技术已引起了全面而深刻的社会变革，为此，世界各国政府都对教育的开展给予了前所未有的关注，把信息化教育放到重要的位置上，纷纷提出了本国的信息化教育规划。是否在学校采用最先进的信息和传播技术是一个有决定性意义的问题,而且十分重要的是,学校应该处于影响整个社会深刻变革的中心地位。 因此校园网信息系统的建设，是非常必要的，也是可行的。主要表现在：

1、当前校园网信息系统已经开展到了与校际互联、国际互联、静态资源共享、动态信息发布、远程教学和协作工作的阶段，开展对学校教育现代化的建设提出了越来越高的要求。

2、教育信息量的不断增多,使各级各类学校、家庭和教育管理部门对教育信息计算机管理和教育信息效劳的要求越来越强烈。

3、我国各级教育研究部门、软件开发单位、教学设备供给商和各级学校不断开发提供了各种在网络上运行的软件及多媒体系统，并且越来越形象化、实用化，迫切需要网络环境。

4、现代教育改革的需要。

5、计算机技术的飞速开展，使相应产品价格不断下降；同时人们的认识水平和经济实力不断提高。大量计算机进入学校和家庭，使得计算机用于教育信息管理和信息效劳是完全可行的。[1]

1.2 校园网络平安概述

自信息系统开始运行以来就存在信息系统平安问题，通过网络远程访问而构成的平安威胁成为日益受到严重关注的问题。根据美国 FBI 的调查，美国每年因为网络平安造成的经济损失超过 170 亿美元。

由于校园网络内运行的主要是多种网络协议，而这些网络协议并非专为平安通讯而设计。所以，校园网络可能存在的平安威胁来自以下方面：

1. 操作系统的平安性，目前流行的许多操作系统均存在网络平安漏洞，如 UNIX 效劳器，NT 效劳器及 Windows 桌面 PC；

2. 防火墙的平安性，防火墙产品自身是否平安，是否设置错误，需要经过检验；

3. 来自内部网用户的平安威胁；

4. 缺乏有效的手段监视、评估网络系统的平安性；

5. 采用的 TCP/IP 协议族软件，本身缺乏平安性；

6. 应用效劳的平安，许多应用效劳系统在访问控制及平安通讯方面考虑较少，并且，如果系统设置错误，很容易造成损失。

1.3 校园网络平安现状分析

随着网络技术的开展，可以说现在的大局部学校都建立了校园网络并投入使用，这对加快信息处理、提高工作效率、实现资源共享都起大了无法估量的作用，但在积极开展办公自动化、信息电子化、实现资源共享的同时，网络的平安问题越来越成为一个非常严惩的隐患，就好似一颗定时炸弹一样，深深的埋在教育现代化的进程中，如果这一个隐患不除，那么也许有一天，学校信息平台效劳器遭到攻击而停止工作、整个校园网络被迫停止、学校积累的各种数据和信息被删除了，导致辛苦积累的大量教育资源被破坏。比方 2003 年爆发的“震荡波、冲击波、FORM.A”等病毒，虽没有造成很大的损失，但足以使认识到网络平安的重要性。因此，如何在现有的条件下防止这样事件发生，搞好网络的平安工作已成了一个重要课题。

1997 年开始，我国校园网络建设悄然兴起。全国各省市都把建设校园网作为现代教育的头等大事来抓。

1999 年 9 月，教育部决定正式启动国家现代远程教育工程，清华大学、浙江大学、北京邮电大学、湖南大学等高校获准进行试点。目前，这几所院校已初步形成了开办现代远程教育的技术手段。

各校在实践中逐渐意识到：一所学校教育质量的好坏，学术水平层次的上下，与教学手段的先进程度有一定关系，教学手段对学校整体的开展有着直接影响。

在世界各兴旺国家，校园网的建设速度似乎不亚于其他如政府网的兴建速度。现代教育的实施程度也与校园网络建设直接相关联。如美国要求所有中小学生都能上网，都能使用电子邮件，并方案将全国 122 所一流大学与社会广泛连接，构筑一个教育与研究的专用网络；英国提出要在 2000 年成立网上工业大学，到 2002 年所有中小学、图书馆、学院和大学全部介入全国的学习网；新加坡提出八岁儿童能阅读，十二岁儿童能上网。

1996 年，教育部提出要以全国 1000 所中小学校作为试点，建立起各自的校园网络。截止 2000 年年初，教育部宣布有 500 多家已建立。可以说，在国家政策扶持下，我国校园网建设取得了飞速开展。但现实中，各地在建立学校校园网的过程中又存在这样那样的问题，如有的学校建网初期就缺乏整体规划，从而导致主干网和各子网通路不畅，或是导致后期整体效率不高；有的学校缺乏必要的网络建设监督人员，将工程交给一些实力较弱或是责任心较差的公司全权负责，结果导致建网质量偏低，后期维护费用偏大；还有的学校认为校园网就是"一揽子"方案，无视了后期维护和配套建设工作，从而导致后期预算偏紧，校园网难以正常运作为了解决上述问题，在建网时应注意：

1. 校园网建设没有通用方案，每个学校应根据自身实际情况〔资金和技术能力〕，设计自身的校园网络；

2. 校园网建设是一个周期较长，规模庞大的系统工程，不能"一蹴而就"，更不能只考虑局部建设，而缺乏整体规划；

3. 重视对教师的培训，防止因教师素质原因导致网络应用效率不高，从而导致资源的浪费。

随着计算机网络的广泛使用和网络之间信息传输量的急剧增长，一些机构和部门在得益于网络加快业务运作的同时，其上网的数据也遭到了不同程度的破坏,或被删除或被复制，数据的平安性和自身的利益受到了严重的威胁。

校园网也同样不能幸免。黑客入侵校园网的新闻也时有发生，非更改考试成绩；更改英语全国四、六级统考成绩；更改考研成绩；非法盗取学校招生、分配机密等。

综上所述，网络必须有足够强的平安措施。无论是公众网还是校园网中，网络的平安措施应是能全方位地针对各种不同的威胁和脆弱性，这样才能确保网络信息的保密性、完整性和可用性。[7]

1.4 校园网络平安威胁

1 计算机病毒

计算机病毒是一组通过复制自身来感染其它软件的程序。当程序运行时，嵌入的病毒也随之运行并感染其它程序。计算机病毒种类繁多，形形色色，但就已经发现的计算机病毒而言，其危害性主要表现为破坏性、传染性、寄生性、潜伏性和激发性几大特征。

破坏性是指计算机病毒可能会干扰软件的运行，或者无限制地侵占系统资源使系统无法运行，又或者毁掉局部数据或程序，使之无法恢复，甚至可以毁坏整个系统，导致系统崩溃。传染性那么是计算机病毒能通过自我复制传染到内存、硬盘甚至文件中。寄生性表现为病毒程序一般不独立存在．而是寄生在磁盘系统区或文件中。潜伏性那么是指计算机病毒可以长时间地潜伏在文件中，在相应的触发机制出现前并不影响计算机，但当被触发后，那么后果严重。激发性是指病毒程序可以按照没计者的要求，例如指定的日期、时间或特定的条件出现在某个点激活并发起攻击。

计算机病毒的传染性证明其具有传播性，防止病毒传播，首先必须认识其传播途径和传播机理。计算机病毒最初传播主要是通过被病毒感染的软件的相互拷贝、携带病毒的盗版光盘的使用等传播。这时候的病毒传播还是线下传播。随着计算机网络的开展，计算机病毒传播主要是通过磁盘拷贝、互联网上的文件传输、硬件设备中的固化病毒程序等方式实现。

病毒还可以利用网络的薄弱环节攻击计算机网络。在现有的各计算机系统中都存在着一定的缺陷，尤其是网络系统软件方面存在着漏洞。因此．网络病毒利用软件的破绽和研制时因疏忽而留下的“后门”大肆发起攻击。

2 网络攻击校园网面临的另一个平安威胁就是网络攻击。

广义的网络攻击包括很多方面。这里结合校园网络平安的特点，重点介绍拒绝效劳(DoS，Daniel of Service)攻击。之所以介绍拒绝效劳攻击，因为拒绝效劳攻击在校园网发牛的更为普遍。这是因为校园网用户集中度高、密度大．为拒绝效劳攻击提供了天然条件。加之学生的好奇心的因素，导致拒绝效劳攻击发生频率较高，是危害校园网平安的重要类型之一。

拒绝效劳攻击是通过攻击主机、效劳器、路由器等网络设备，导致被攻击网络无法提供效劳的一种攻击方式。典型的拒绝效劳攻击表现为攻击者向被攻击网络大陆发送数据从而消耗其资源、使得用户无法访问所需信息。

拒绝效劳攻击的方法多样。攻击者在发起攻击时，可能采取单一手段的攻击模式，也可能采取多种攻击手段联合使用的模式。就其攻击手段来说．主要有以下几种：

1〕死亡之 Ping。早期的网络不支持大包，攻击者通过网络发送大母的大数据包到被攻击者网络，造成网络堵塞以致瘫痪。目前的网络已经能够支持大包，这种方式已经不再出现。

2〕泪滴攻击。攻击者采用修改包片段字头的方式，使得包无法正确组装．导致网络访问失败的方式。

3 〕UDP 洪水攻击。攻击利用如 chargen 和 echo 等简单的 TCP／IP 效劳．相互发送大量数据以沾满带宽，从而瘫痪网络的方式。

4) SYN 洪水攻击。攻击者通过想效劳器发送连续的 SYN 握手信息来瘫痪效劳器的攻击方式。

5) LAND 攻击 该攻击是让效劳器自己向自己发送 SYN 握手信息．已到达瘫痪主机的目的。

6) Smurf 攻击。攻击者将报文地址设为 Echo 地址，这样 Echo78 地址就必须不问断的响应该报文，使得网络带宽被侵占，从而到达瘫痪网络的目的。

7) Fraggle 攻击。Fraggle 攻击对 Smurf 攻击做了修改。

8)电子邮件炸弹。通过向一台效劳器大量的不间断的发送电子邮件，起到瘫痪效劳器的作用。

9)急性消息攻击。借助机器对某些消息为进行错误校验来攻击效劳器。

10)分布式拒绝效劳攻击。它是威力最强大的拒绝效劳攻击方式，其主要采用多台效劳器对同一网络同时发起攻击，导致该网络瞬间瘫痪。

常见的拒绝效劳攻击主要有以上几种，攻击者攻击目的和攻击水平不同，选用的方式不同。无论哪种方式，都对网络平安造成很大的危害。[5]

3　存在的平安隐患,以我校为例，校园网络存在的平安隐患和漏洞有:

1) 计算机与 Internet 相连，却没有安装相应的杀毒软件及防火墙。

2) 使用的操作系统存在平安漏洞，网络木马、病毒和黑客攻击影响到系统的平安。校内大局部计算机系统或多或少都存在着各种的漏洞，校园网络又对社会开放，这样一来只要接入 INTERNET 的用户就可以对校园的网络效劳器进行攻击，而流行于网络上的很多病毒如“震荡波、冲击波、尼姆达”

病毒都是利用系统的漏洞来进行病毒传播的，加上带毒的木马程序，一感染便驻留在你的计算机当中，在以后的计算机启动后，木马就在机器中翻开一个效劳，通过这个效劳将你计算机的信息、资料向外传递。

3) 目录共享导致信息的外泄, 在校园网络中，利用在对等网中对计算机中的某个目录设置共享进行资料的传输与共享是人们常采用的一个方法。但可以说几乎所有的人都没有充分认识到当一个目录共享后，就不光是校园网内的用户可以访问到，而是连在网络上的各台计算机都能对它进行访问。这也成了数据资料平安的一个隐患。我曾经搜索过外地机器的一个 C 类 IP 网段，发现共享的机器就有十几台，而且许多机器是将整个 C 盘、D 盘进行共享，并且在共享时将属性设置为完全共享，且不进行密码保护，这样只要将其映射成一个网络硬盘，就能对上面的资料、文档进行查看、修改、删除。因而对目录共享平安意识的薄弱，会导致了信息的外泄。

4) 网络平安意识淡薄，校园网络上的攻击、侵入他人机器，盗用他人帐号非法使用网络、非法获取未授权的文件、通过邮件等方式进行骚扰和人身攻击等事件经常发生、屡见不鲜，我校应用效劳器和普通计算机平均一个星期会经受到数千次甚至上万次的非常访问尝试，而其中一大局部的非法访问源自校内，说明校园网络上的用户平安意识淡薄; 另外，没有制定完善而严格的网络平安制度，各校园网在平安管理上也没有任何标准，这也是网络平安问题泛滥的一个重要原因.由此可见，构筑具有必要的信息平安防护体系，建立一套有效的网络平安机制显得尤其重要.

2. 校园网络平安策略

校园网的平安威胁既有来自校内的，也有来自校外的，只有将技术和管理都重视起来，才能切实构筑一个平安的校园网。

国内高校校园网的平安问题有其历史原因：在以前的网络时期，一方面因为意识与资金方面的原因，以及对技术的偏好和运营意识的缺乏，普遍都存在“重技术、轻平安、轻管理“的倾向，常常只是在内部网与互联网之间放一个防火墙就万事大吉，有些学校甚至直接连接互联网，这就给病毒、黑客提供了充分施展身手的空间。而病毒泛滥、黑客攻击、信息丧失、效劳被拒绝等等，这些平安隐患只要发生一次，对整个网络都将是致命性的。

作为高等院校，如何构筑相对可靠的校园网络平安体系问题，变得越来越突出了。一般来说，构筑校园网络平安体系，要从两个方面着手：一是采用先进的技术；二是不断改良管理方法。

2.1 校园网平安管理

针对目前高校校园网平安现状的认识与理解，在防病毒软件、防火墙或智能网关等构成的防御体系下，对于防止来自校园网外的攻击已经足够。以下五点是高校的平安策略：

1、标准出口管理，实施校园网的整体平安架构，必须解决多出口的问题。对于出口进行标准统一的管理，使校园网络平安体系能够得以实施。为校园网的平安提供最根底的保障。

2、配备完整系统的网络平安设备，在网内和网外接口处配置一定的统一网络平安控制和监管设备就可杜绝大局部的攻击和破坏，一般包括：防火墙、入侵检测系统、漏洞扫描系统、网络版的防病毒系统等。另外，通过配置平安产品可以实现对校园网络进行系统的防护、预警和监控，对大量的非法访问和不健康信息起到有效的阻断作用，对网络的故障可以迅速定位并解决。

3、解决用户上网身份问题，建立全校统一的身份认证系统 。校园网络必须要解决用户上网身份问题，而身份认证系统是整个校园网络平安体系的根底的根底，否那么即便发现了平安问题也大多只能不了了之，只有建立了基于校园网络的全校统一身份认证系统，才能彻底的解决用户上网身份问题，同时也为校园信息化的各项应用系统提供了平安可靠的保证。

4、严格标准上网场所的管理，集中进行监控和管理 。上网用户不但要通过统一的校级身份认证系统确认，而且，合法用户上网的行为也要受到统一的监控，上网行为的日志要集中保存在中心效劳器上，保证了这个记录的法律性和准确性。

5、根据相关部门的要求，配备专门的平安管理人员，出台网络平安管理制度 。网络平安的技术是多样化的，现状还是“道高一尺，魔高一丈”，因此管理的工作就愈发重要和艰巨，必须要做到及时进行漏洞修补和定期询检，保证对网络的监控和管理。[2]

2.2 校园网络平安措施

前述各种网络平安威胁，都是通过网络平安缺陷和系统软硬件漏洞来对网络发起攻击的。为杜绝网络威胁，主要手段就是完善网络病毒监管能力，堵塞网络漏洞，从而到达网络平安。

1、杀毒软件。

杀毒产品的部署. 在该网络防病毒方案中，要到达一个目的就是：要在整个局域网内杜绝病毒的感染、传播和发作。为了实现这一点，应在整个网络内可能感染和传播病毒的地方采取相应的防病毒手段；同时为了有效、快捷地实施和管理整个网络的防病毒体系，应能实现远程安装、智能升级、远程报警、集中管理、分布查杀等多种功能.。

〔1〕在学校网络中心配置一台高效的 Windows2000 效劳器安装一个杀毒软件的系统中心，负责管理校内网点的计算机。

〔2〕在各办公室分别安装杀毒软件的客户端。

〔3〕安装完杀毒软件，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。

〔4〕网络中心负责整个校园网的升级工作。

2、采用 VLAN 技术。

VLAN 技术是在局域网内将工作站逻辑的划分成多个网段，从而实现虚拟工作组的技术。VLAN 技术根据不同的应用业务以及不同的平安级别，将网络分段并进行隔离，实现相互间的访问控制，可以到达限制用户非法访问的目的。

3、内容过滤器。

内容过滤器是有效保护网络系免于误用和无意识效劳拒绝的工具。同时，可以限制外来的垃圾邮件。

4、防火墙。

在与 Internet 相连的每一台电脑上都装上防火墙，成为内外网之间一道牢固的平安屏障。在防火墙设置上按照以下原那么配置来提高网络平安性:

(1)根据校园网平安策略和平安目标，规划设置正确的平安过滤规那么，规那么审核 IP 数据包的内容包括：协议、端口、源地址、目的地址、流向等工程，严格禁止来自公网对校园内部网不必要的、非法的访问。总体上遵从“不被允许的效劳就是被禁止”的原那么.

(2〕禁止访问系统级别的效劳(如 HTTP , FTP 等)。局域网内部的机器只允许访问文件、打印机共享效劳。使用动态规那么管理，允许授权运行的程序开放的端口效劳，比方网络游戏或者视频语音　软件提供的效劳。

(3〕如果你在局域网中使用你的机器,那么你就必须正确设置你在局域网中的 IP，防火墙系统才能认识哪些数据包是从局域网来，哪些是从互联网来，从而保证你在局域网中正常使用网络效劳〔如文件、打印机共享〕功能。

(4〕定期查看防火墙访问日志，及时发现攻击行为和不良上网记录。

(5〕允许通过配置网卡对防火墙设置，提高防火墙管理平安性.

5、入侵检测。

入侵检测系统是防火墙的合理补充，帮助系统对付网络攻击。扩展系统管理员的平安管理能力．提高信息平安根底结构的完整性。入侵检测系统能实时捕获内外网之间传输的数据，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,并记录有关事件。入侵检测系统还可以发出实时报警，使网络管理员能够及时采取应对措施。

6、漏洞扫描。

随着软件规模的不断增大．系统中的平安漏洞或“后门”也不可防止地存在．因此，应采用先进的漏洞扫描系统定期对工作站、效劳器等进行平安检查，并写出详细的平安性分析报告，及时地将发现的平安漏洞打上“补丁”。

7、数据加密。

数据加密是核心的对策，是保障数据平安最根本的技术措施和理论根底。

8、加强网络平安管理。

加强网络管理主要是要做好两方面的工作。首先，加强网络平安知识的培训和普及；其次，是健全完善管理制度和相应的考核机制，以提高网络管理的效率。[6]

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

https://d.book118.com/038104032062006121