郑州铁路职业技术学院毕业论文

论文题目：校园网网络平安问题及其解决方案

作者姓名：

班级学号：

系　　部：软件学院/信息工程系

专　　业：计算机网络

指导教师：

2013 年 5 月 20 日

摘　要

随着 Internet 的飞速开展，校园网作为高校重要的根底设施，担当着高校教学、科研、管理和对外宣传交流等许多角色。在我们享受着网络给教学管理带来便捷的同时，网络中的种种不平安因素也在无时无刻不在威胁校园网的健康开展，例如，病毒侵犯、保密资料外泄、黑客的非法入侵，有害信息等等。所以，对于校园网这个特殊而又重要的局域网来说，必须建立完备的校园网平安防护体系，不断加强校园网络的平安管理体制，保证校园网络能正常的运行以及校园内部的信息资源不受各种网络黑客的侵害，确保学生的身心健康，使学生尽可能少地接触网络上的不良信息，使他们具备一个积极向上的意识形态，并确保网络教学等活动得以正常运转。因此，如何在开放网络的环境中保证校园网的平安性已经成为一个及其重要并且必须要解决的问题。

本文通过分析当今校园网网络平安问题的现状，找出校园网面临的各种威胁，列出解决校园网平安问题的关键技术，校园网平安管理和维护的措施与建议。

关键词：

校园网； 网络平安； 防火墙；入侵检测

目录

参考文献：43

一、校园网网络概述

1.1 互联网的开展与平安

计算机与通信技术推动了因特网的快速开展。截至2010年1月底，我国网民数量已跃居世界第一。互联网的普及为我们的工作和生活带来了根本性变化，人们可以通过互联网来浏览新闻、获取资料、电子邮件、存储信息、进行实时通讯；可以足不出户进行网上购物、网上股票交易，利用网上银行进行转账业务等；电子政务的推广也使得政府部门和企业进行网上办公成为可能。计算机网络已经渗透到了教育、文化、经济、政治、军事等各个方面。可以说，今天的互联网已经成为了人们生活和工作中必不可少的一局部。但同时近几年网络信息平安问题表现异常突出：网上病毒感染事件逐年增多；网络入侵攻击大幅上升，据统计说明，平均每20秒就有一个网络遭到入侵；网上经济诈骗成倍增长。网络平安是一个多层面的平安问题，它不仅涉及到黑客、漏洞、入侵、病毒等外来攻击平安问题，而且还涉及到保密、授权、抵赖等内部平安问题。目前世界上的各国正在通过采用各种技术和管理措施来保障互联网的平安，保证互联网系统的正常运行，确保网络传输和交换的数据不会发生修改、丧失和泄漏等。互联网网络的平安性同网络的性能、可靠性和可用性一起成为组建和运行网络不可无视的问题。

1.2 国内网络平安现状

计算机网络的广泛应用已经对经济、文化、教育与科学的开展产生了重要的影响，同时也不可防止地带来了一系列新的社会道德、法律问题。网络的快速开展使得网上资源越来越丰富，诸如电子商务、电子政务、电子税务、电子海关、网上银行、网络防伪等许多新兴业务也迅速兴起，因此，加强网络信息平安保障已成为当前的迫切任务。网络平安的保障能力是一个国家综合国力、经济竞争实力和生存能力的重要组成局部。网络平安问题解决不好将会全面地危及国家的政治、经济、文化、社会生活的各方面。

目前我国网络平安的现状和面临的威胁主要有：

1、计算机网络系统使用的软、硬件产品很大一局部依赖于国外产品，引进的信息技术和设备对信息平安的保护缺乏有效管理和技术改造。

2、国内信息平安人才培养体系虽已初步形成，但随着信息化进程的加快和计算机的广泛应用，目前我国信息平安人才培养还远远不能满足国内需要。

3、目前关于网络犯罪的法律还不健全，因特网上的犯罪对传统的法律提出了挑战。

4、公民对信息平安意识虽然有所提高，但将实际应用中依然很少注意防范，计算机病毒、木马、黑客攻击泛滥成灾。

1.3 校园网的特点

近几年来因 CERNET

网的开展，我国校园网的建设得到了快速的开展。全国绝大多数的高校建成了自己的校园网络，随着高校校园网建设工程的实施，全面提高了校园网网络通信的水平和规模，扩大了校园网的应用范围，为高校教师的教学和科研以及大学生对网络系统的应用提供了根本保障。

校园网作为高校重要的根底设施，担当着高校教学、科研、管理和对外宣传交流等许多角色。因此校园网平安状况直接影响着高校的教学等活动。随着网络应用的深入，校园网上各种传输的数据信息量急剧增加，网络的攻击越来越多，各种各样的平安问题影响校园网的正常运行。同时，随着网络规模的不断扩大，网络复杂性不断增加，用户对网络性能要求的不断提高，网络平安正逐步成为网络技术开展中一个极为关键的任务，对网络的开展产生了很大的影响，成为现代网络应用中最重要的问题之一。因此，如何确保校园网正常、平安和高效地运行是所有高校目前面临的问题。高校校园网建设中面临的问题概括起来主要有以下几个方面：

〔1〕网络日常管理维护的困境。随着课堂教学逐步走向网络化，学生在线学习、娱乐时间的增加必然造成校园网网络大、业务多、故障产生问题复杂，网络的平安性差、管理难度较大。

〔2〕滥用网络资源。在校园网内，用户滥用网络资源的情况严重，有私自开设代理效劳器非法获取网络效劳的，也有校园网用户非法下载或上载的，甚至有的用户每天都不断网，其流量每天都到达几十个G，占用了大量的网络带宽，影响了校园网的其它应用[4]。

〔3〕网络平安、计费等运营问题。校园网中的计算机系统管理比拟复杂，缺乏用户认证、授权、计费体系，平安认证存在有意无意的攻击。

〔4〕互联网上的非法内容也形成了对网络的另一大威胁。不良信息的传播对正在形成世界观和人生观的大学生而言，危害是非常大的。要确保高校学生健康成长、积极向上，就必须采取措施对校园网络信息进行过滤和处理，使他们尽可能少地接触网络上的不良信息。对校园网来说，如不具有过滤和识别作用，不但会造成大量非法内容及邮件进入，占用大量流量资源，造成网络流量堵塞、上网速度变慢等问题。

许多校园网是从局域网开展而来的，由于平安管理意识与资金方面的原因，它们在平安方面往往没有作太多的设置，一般往往直接面向互联网，这就给病毒、黑客提供了充分施展身手的空间，这些平安隐患发生任何一次，都会对整个网络产生致命的危害。因此，校园网的网络平安需求是全方位的。

1．4 校园网的网络构成

校园网的网络组成可以按照不同的标准来区分，通常可以分为按照网络的拓扑分为校园网的体系机构以及按网络的功能分为校园网的功能结构。

1.4.1　校园网网络体系结构概述

校园网平安策略的制定和实施是以各高校校园网的根底体系结构和网络应用具体情况为依据和实施根底的。因此在制定各高校的网络平安策略和实施具体的平安策略之前，透彻分析本校的校园网体系结构,网络

拓扑结构，网络的路由策略，网络的区域划分，IP 及 VLAN

的规划，网络访问策略，各应用系统的功能效劳对象，访问限制等等是非常必要的，其性能直接影响到网络平安策略的实施效果。

网络体系结构是关于如何构建网络的技术，它包括两个层次的内涵。一是要标识出网络系统由哪些局部组成，清晰地描述出各个局部的功能、目的和特点。二是要描述网络各个组成局部之间的关系，如何将各个局部有机地结合在一起，形成完整的网络系统，从而保证网络有效地运转，也就是将各个局部进行集成的方式或方法。根据教育部《教育管理信息化标准》的要求，校园网的总体建设目标包括：

校园网根底设施建设是我们数字化校园的根底，它的建设水平和效果直接影响到我们运行在校园网上的效劳，影响到全校的教学、科研甚至影响到师生的日常生活。校园网的建设包括根据自身的应用需求和特点进行校园网的体系结构的设计，相关技术设备的选择，网络出口包括带宽的选择，设备之间拓扑关系确实定，集成、调试，应用建设等关键环节，在这些环节当中也包含着对校园网络平安的考虑与设计。

近年的信息化建设，通过科研需求、教学应用、网络办公、网上娱乐等应用建设和使用，网络应用逐渐渗透到了校园生活的方方面面。上网备课，接收邮件，网络聊天，游戏购物，校园用户联网的时间一天天延长。教育部科技开展中心公布的相关数据显示，98.4%的高校教学、科研、行政办公已经全部联入校园网，90.5%高校的教室已提供了校园网接入环境，74.35%的学校在学生宿舍已经接入网络，校园网覆盖范围正在逐步地扩大。同时各个高校的网络应用建设也是搞得风风火火，从原来的只提供局部特殊用户的上网接入，只提供根本的 Web 和 Mail

效劳开展到了增加网络出口，增加带宽，建设各部门和学院的二级站点乃至个人站点，Video 视频点播系统、IPTV 网络电视系统、各学科知识数据库系统、教学、人事等业务系统，精品课程、网上录播、监控等多种应用系统的建设。现在各高校正制定各自的数字化校园的规划，新一轮的校园网应用建设和信息系统集成将展开，这对我们的校园网根底设施建设和网络平安提出了新的挑战。

1.4.2 校园网系统功能构成

校园网作为校园网络信息平台应该由一个平台和三个系统构成，即系统管理平台、校园公共信息系统、校园管理信息及办公自动化系统、校园教-学资源库系统。

具体系统功能构成见下列图

1.4.3 校园应用管理平台

校园应用系统管理平台是一个可靠性高、平安性好、易管理的操作平台。在此平台上可轻松的实现用户注册、系统的备份和恢复、用户权限的设置以及资源的调整、初始化等管理工作。通过使用 Intranet/Internet 技术以及先进的 XML 技术和 B/S 结构，实现了与 Internet 的无缝连接。

校园公共信息系统〔Internet 效劳系统〕主要用于校园公共信息的管理，是学校师生进行交流的场所，老师和学生通过公共信息系统将大大拓展信息交流的空间。作为大学的信息门户，该系统为全校师生提供校园讨论区〔BBS

〕、校园聊天室、校园大事记、通知公告、信息发布等根底信息效劳。通过权限设置，实现角色化管理，年级、班级、兴趣小组等各类角色都可以根据自己定制的需求去查询、发布信息。

校园管理信息系统用于支持学校日常管理的各项工作。用户通过使用人事管理、教育教学管理、后勤管理、教学资源与应用平台、图书馆管理、生活管理、医疗管理等多个功能子系统可以方便快捷地处理各种复杂数据操作和文字录入，完成各种校园信息数据的有效管理。校园办公自动化针对校园办公需求不仅实现了便捷保密的公文管理、档案管理、信息交流，而且使每位老师、每个学生都拥有自己的信箱。

教学资源库系统提供一致的资源管理和使用方式，实现简便精确的资源获取与检索，全面支持教学应用，包括对各类教学软件库、教学网络平台、电子阅览室等资源的分类、检索和管理、多媒体教学、远程教育等功能。

1.4.4　典型校园网拓扑结构

校园网的网络体系结构包括校园网的网络边界设备，核心及骨干设备，网络接入层设备，网络效劳提供设备和这些设备的连接方式以及该结构采用的协议及技术。

当前的校园网多采用 1000M 以太网主干技术，1000M 或 100M 到楼，100M 或 10M 到桌面，局部区域采用无线接入技术〔〕实现无线接入。校园网络一般有边界路由器，高性能的核心路由交换机，各分布层的三层路由交换机，大量的二层可网管接入交换机，以及防火墙，IDS〔或 IPS

〕，内容过滤系统，流量分析系统，网络设备管理系统等网络硬件设备。

校园网多采用星形拓扑结构，常见的校园网拓扑结构如图 1-2

图 1-2　校园网拓扑结构

1.4.5　校园网的建设目标

网络平安〔NetworkSecurity〕是抵御内部和外部各种形式的威胁，以确保网络的平安的过程。为了深入彻底地理解什么是网络平安，必须理解网络平安旨在保护的网络上所面临的威胁，理解一个能够用于阻止这些攻击的主要机制也是非常重要的。通常，在网络上实现最终的平安目标可通过下面的一系列步骤完成，每一都是为了澄清攻击和阻止攻击的保护方法之间的关系。下面的步骤是在一个站上建立和实现平安的方法：

第 1 步确定要保护的是什么；

第 2 步决定尽力保护它免于什么威胁；

第 3 步决定威胁的可能性；

第 4 步以一种划算的方法实现保护资产的目的；

第 5 步不断地检查这些步骤，每当发现一个弱点就进行改良。

校园网络系统需要实现以下平安目标：

- 保护网络系统的可用性；
- 保护网络系统效劳的连续性；
- 防范网络资源的非法访问及非授权访问；
- 防范入侵者的恶意攻击与破坏；
- 保护信息通过网上传输过程中的机密性、完整性。

二、校园网网络平安问题现状

校园网在学校的日常活动中发挥着越来越重要的作用，与此同时，校园网的平安问题也越来越突出，网络病毒，黑客入侵，管理不善等原因使得校园网络面临着严重的威胁。

2.1 网络的开放性带来的平安问题

Internet 的开放性以及其他方面因素导致了网络环境下的计算机系统存在很多平安问题。为了解决这些平安问题，各种平安机制、策略、管理和技术被研究和应用。然而，即使在使用了现有的平安工具和技术的情况下，网络的平安仍然存在很大隐患，这些平安隐患主要可以包括为以下几点:

(1)平安机制在特定环境下并非万无一失。比方防火墙，它虽然是一种有效的平安工具，可以隐蔽内部网络结构，限制外部网络到内部网络的访问。但是对于内部网络之间的访问，防火墙往往是无能为力的。因此，对于内部网络到内部网络之间的入侵行为和内外勾结的入侵行为，防火墙是很难觉察和防范的。

(2)平安工具的使用受到人为因素的影响。一个平安工具能不能实现期望的效果，在很大程度上取决于使用者，包括系统管理者和普通用户，不正当的设置就会产生不平安因素。例如，WindowsXP 在进行合理的设置后可以到达 C 级的平安性，但很少有人能够对 WindowsXP 本身的平安策略进行合理的设置。虽然在这方面，可以通过静态扫描工具来检测系统是否进行了合理的设置，但是这些扫描工具根本上也只是基于一种缺省的系统平安策略进行比拟，针对具体的应用环境和专门的应用需求就很难判断设置的正确性。

(3)系统的后门是难于考虑到的地方。防火墙很难考虑到这类平安问题，多数情况下，这类入侵行为可以堂而皇之经过防火墙而很难被觉察；比方说，众所周知的 ASP 源码问题，这个问题在 IIS 效劳器 4.0 以前一直存在，它是 IIS 效劳的设计者留下的一个后门，任何人都可以使用浏览器从网络上方便地调出 ASP 程序的源码，从而可以收集系统信息，进而对系统进行攻击。对于这类入侵行为，防火墙是无法觉察的，因为对于防火墙来说，该入侵行为的访问过程和正常的 WEB 访问是相似的，唯一区别是入侵访问在请求链接中多加了一个后缀。

2.2 校园网网络平安的主要威胁因素

(1)软件漏洞：每一个操作系统或网络软件的出现都不可能是无缺陷和漏洞的。这就使我们的计算机处于危险的境地，一旦连接入网，将成为众矢之的。

(2)配置不当：平安配置不当造成平安漏洞，例如，防火墙软件的配置不

正确，那么它根本不起作用。对特定的网络应用程序，当它启动时，就翻开了一系列的平安缺口，许多与该软件捆绑在一起的应用软件也会被启用。除非用户禁止该程序或对其进行正确配置，否那么，平安隐患始终存在。

(3)平安意识不强：用户口令选择不慎，或将自己的帐号随意转借他人或与别人共享等都会对网络平安带来威胁

(4)病毒：目前数据平安的头号大敌是计算机病毒，它是编制者在计算机程序中插入的破坏计算机功能或数据，影响计算机软件、硬件的正常运行并且能够自我复制的一组计算机指令或程序代码。计算机病毒具有传染性、寄生性、隐蔽性、触发性、破坏性等特点。因此，提高对病毒的防范刻不容缓。

2.3.1 网络自身的平安缺陷

网络是一个开放的环境,TCP/IP 是一个通用的协议,即通过 IP 地址作为网络节点的唯一标识,基于 IP 地址进行多用户的认证和授权,并根据 IP 包中源 IP 地址判断数据的真实和平安性,但该协议的最大缺点就是缺乏对 IP 地址的保护,缺乏对源 IP 地址真实性的认证机制,这就是 TCP/IP 协议不平安的根本所在。通过 TCP/IP 协议缺陷进行的常见攻击有:源地址欺骗、IP 欺骗、源路由选择欺骗、路由选择信息协议攻击、SYN 攻击等等。

2.3.2 网络结构、配置、物理设备不平安

最初的互联网只是用于少数可信的用户群体,因此设计时没有充分考虑平安威胁,互联网和所连接的计算机系统在实现阶段也留下了大量的平安漏洞。并且网络使用中由于所连接的计算机硬件多,一些厂商可能将未经严格测试的产品推向市场,留下大量平安隐患。同时,由于操作人员技术水平有限,所以在网络系统维护阶段会产生某些平安漏洞,尽管某些系统提供了一些平安机制,但由于种种原因使这些平安机制没有发挥其作用。

2.3.3 内部用户的平安威胁

系统内部人员存心攻击、恶作剧或无心之失等原因对网络进行破坏或攻击的行为,将会给网络信息系统带来更加难以预料的重大损失。U 盘、移动硬盘等移动介质交叉使用和在联接互联网的电脑上使用,造成病毒交叉感染等等,都会给校园网络带来较大的平安威胁。特别是近年来利用 ARP 协议漏洞进行窃听、流量分析、DNS 劫持、资源非授权使用、植入木马病毒不断增加,严重影响了网络平安。

2.3.4 软件的漏洞

一般认为,软件中的漏洞和软件的规模成正比,软件越复杂其漏洞也就越多。在网络系统运行过程中,由于操作系统自身不够完善,针对系统漏洞本身的攻击较多,且影响也较严重。目前如办公、下载、视频播放、聊天等软件的流行,让使用率较高的程序也成为被攻击的目标。

2.3.5 病毒的传播

网络的开展使资源的共享更加方便，移动设备使资源利用显著提高,但却带来病毒泛滥、网络性能急剧下降,许多重要的数据因此受到破坏或丧失,也就是说,网络在提供方便的同时，也成为了病毒传播最为便捷的途径。例如,“红色代码”、“尼姆达”、“冲击波”、“震荡波”、“欢乐时光”、“熊猫烧香”

的爆发无不使成千上万的用户受到影响。几年病毒的黑客化,使得病毒的感染和传播更加快速化、多样化,因而网络病毒的防范任务越来越严峻。

2.3.6 各种非法入侵和攻击

由于校园网接入点较多,拥有众多的公共资源,并且使用者平安意识淡薄,平安防护比拟薄弱,使得校园网成为易受攻击的目标。非法入侵者有目的的破坏信息的有效性和完整性,窃取数据,非法抢占系统控制权、占用系统资源。比方:漏洞、薄弱点扫描,口令破解;非授权访问或在非授权和不能监测的方式下对数据进行修改;通过网络传播病毒或恶意脚本,干扰用户正常使用或者占用过多的系统资源导致授权的用户不能获得应有的访问或操作被延迟产生了拒绝效劳等。

三、校园网网络平安问题解决方案

3.1　解决校园网平安问题的关键技术

3.1.1 密码加密解密技术

对称密码体制也称为私钥加密法。从一定意义上说，密码学的根本目的是保护隐私。也就是使通信双方通过某一不平安的信道传递信息时，只有对方才能破译这一信息。在过去，这一愿望是通过私钥密码体制来实现的。私钥密码体制是一种传统密码体制，在过去，最有代表性的私钥密码体制有 Caesar、Hill、Vigenere 等。而当代最有代表性的有：DES、AES、IDEA、RC5等，它们的平安性都是基于复杂的数学运算。假设以 M 表示所有的明文信息，C 表示密文信息，K 是所有的密钥。那么私钥密码体制是由这样一组函数对构成的：

Ek:M→C

Dk:C→M,k∈K

在这里，对于所有的 m∈M 及 k∈K，都有 Dk(Ek(m))=M。使用这一体制时，通信的双方 A 和 B 需要事先达成某一秘密钥 k∈K，他们可以通过直接会晤或者可以信赖的信使来互相得到对方的秘密钥。之后，假设 A 想发送一组明文给 B，他传送的是密文信息 C∈Ek(m)。根据 C，B 通过解码函数 Dk 复原信息。显而易见，解码系统应当具有的特点是：Dk 和 Ek 易于应用以及在第三方了解除选用密钥的方法之外的保密系统的信息之后，仍然不可能根据 C 得到 M〔或 k〕。