学校编码：10384　　分类号_____密级_____

学号：X2009221037　　UDC_____

厦门大学

工　程　硕　士　学　位　论　文

基于 NS2 的校园网安全模型设计及实现

Design and Implementation of Campus Network Security Model based on NS2

曾伟渊

指导教师姓名：　杨晨晖教授

专　业　名　称：　计算机技术

论文提交日期：　2014 年 6 月

论文答辩时间：　2014 年 8 月

学位授予日期：　　年　　月

答辩委员会主席：_____

评　　阅　　人：_____

2014　年　8　月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘　要

近年来，我国校园网络在科学研究中的重要性不断增加，校园网的功能已经覆盖到对高校的管理，教学，和许多其他的任务。同时，随着校园网复杂性的提升，校园网的攻击防护以及安全保证等工作，已经逐渐成为了一个系统工程，需要从全方位进行建设和维护。因此，校园网络安全系统的构建逐渐成为了学术界工业界是一个重点探讨的问题。

校园网作为一个面向学生和老师的开放系统，近年来网络上运载的各种数据成爆发式增长，同时，也面临着各式各样已存在的和潜在的威胁和攻击。校园网安全状况直接关系到我国高校师生生活和工作，直接影响着我国高校的教学科研工作的正常开展。

VPN 是一种组网技术(即在公网中建立虚拟专网)，拓展了各类应用在网络环境中存在的宽度和广度，有效地解决网络中信息交互中存在的信息权限问题。VPN 技术有效地提高了互联网访问的安全性，这使得 VPN 获得了广泛的应用。

PKI(Public Key Infrastructure)技术是一种密钥管理技术和规范，它遵循既定标准，同时能够为所有互联网应用提供完整的证书管理体系、解密、密码服务、数字签名、加密、和所必需的密钥。

本课题的研究以笔者多年实施校园网管理的相关项目为背景， 将校园网内部的安全应用研究和安全模型的构建是研究重点。本文的研究出发点是认为校园网的网络环境中存在不安全因素，将校园网络当作一个不安全的公共网络来对待。针对校园网中的不安全因素，本文利用 VPN、IPSec、PKI 技术构建一个校园网安全模型，并通过 NS2 实现。这个安全模型的目标是解决校园网中存在的安全问题。本文分析了现有的高职院校校园网络安全技术以及校园网概况，结合 VPN、PKI、IPSec 和 NS2 的主要技术和特点，通过在 VPN 技术中加入 PKI 技术，设计了一个基于 NS2 实现的校园网安全网络架构模型。该模型在校园网中设置了一个带 PKI 认证服务的 IPSec-VPN 网关来解决网络中常见的安全攻击问题，尤其是从校园内网来攻击校园网内部来的攻击安全问题。

关键词：校园网； NS2；安全

Abstract

In recent years, the importance of the campus network in scientific research in our country continue to increase. The function of the campus network has already covered the management of colleges and universities, teaching, and many other tasks. At the same time, along with the campus network, the complexity of campus network attack protection and security work, has become an engineering task, which need to be done from the comprehensive construction and maintenance. Therefore, the construction of campus network security system has gradually become a key academic problem.

Campus network always be treated as an open system for students and teachers, which carries on the network of all kinds of data in recent years into explosive growth, at the same time, also faces the format of the existing and potential threats and attacks. Campus network security situation is directly related to the teachers and students' lives and work in colleges and universities, and directly affects the normal work of teaching and research.

VPN is a kind of networking technology (that is, in the public network to establish a virtual private network), which expands the various width and breadth of the application in the network environment, effectively solves the network information interaction problems in information access. VPN technology effectively improved the security of the Internet access, this makes the VPN gained widespread application.

PKI (Public Key Infrastructure) technology is a Key management technique and the specification, it follows the established standards, at the same time to provide a complete certificate for all Internet applications management system, digital signature, encryption, decryption and password service, and the necessary Key.

As the background, this topic research basing on years of implementing the management of campus network related project, the inside of the campus network security application research and the construction of a security model is the key. The starting point of this paper is that, the campus network as an insecure public network, the unsafe factors exist in the network environment of campus net. For the unsafe factors in the campus network, this paper use VPN, IPSec, PKI technology to build a network security model, and implement the model base on NS2.The goal of the security model is to solve the problem existing in the campus network security. This paper analyzes the current general situation of the higher vocational college campus network security technology and campus network, combined with the VPN, PKI, IPSec and

main technology and characteristic of NS2, through adding PKI technology in VPN technology, designed a model of campus network security network architecture based on NS2 to achieve. The model set up a band in the campus network PKI authentication services of IPSec VPN gateway to solve the problem of common security attacks in the network, especially the attacks from the campus Intranet to attack inside the campus network security issues.

Key Words: Campus network; NS2; Security

目　录

Table of Contents

第一章　绪论

1.1 引言

随着近年来我国计算机网络技术、电子技术、移动通信技术、以及多媒体技术的飞速发展，校园网已经成为高校日常教学和科研工作中不可或缺的一部分。在各高职院校加强信息化建设的背景下，校园网相关的研究和建设已经成为一个研究热点[1]。同时，随着我国互联网技术的发展，互联网上各类应用越来越丰富，无论是从数量上还是功能上来看，互联网上的应用都在呈爆发式增长。

在此背景之下，校园网作为互联网的一个重要分支，得到了蓬勃发展，在高职院校的日常办公和科研教学中，凸显出了越来越重要的作用。校园网应用于高职院校中很多方面，从教学过程到师生的日常生活再到各类研究所实验室的日常科研工作。校园网正在改变较为陈旧的教学方法、教学模式、以及教学手段，同时，通过较为广泛的互联网资源，进一步提高了教学质量，而进一步促进了教育教学思想的提升、教学观念的转变。在这样的背景下，互联网提供的开放，自由，丰富的教育资源为教师的教学和学生的学习以及相关的科研工作提供了极好的支撑[1]。作为高职院校基础公共服务，校园网在很多高职院校的办公中已经成了重要的基础平台，院校的办公，学生的生活，老师的教学，以及常规的资源获取分配管理等，几乎都离不开校园网的支持。众所周知，其中，数据共享，学籍管理、图书管理、教学信息发布、教室使用情况管理、教学的质量评估、学生学籍和成绩的管理、网上选课以及考试报名和许多申请的提交，表格下载等共工作都是基于校园网提供的基本功能获得的支撑。

当前，各种在线管理软件和各类基于虚拟系统，基于分布式系统，基于云端的办公软件的应用在高校的日常管理和工作的作用体现越来越明显，各高校的日常运作也越来越离不开校园网的支持[2]。但是，随着用户群的逐渐增加、流量的增加、网络应用功能的多样性的增加，以及软件操作逻辑的复杂性增强，网络安全在校园网中的重要性日趋明显，同时，随着我国教育事业的蓬勃发展，多校区现象的出现，校区之间的联网和内网的构建需求，也给我国校园网的安全性和稳定性带来了更大的挑战。

VPN(Virtual Private Network，虚拟专用网络)是一种在公共网络上构建专

有的虚拟私网的网络技术，其技术包含传输数据的封装技术和数据加密技术，这些技术的综合使用，可以为用户在公共网络设备上建立一个安全的传输隧道，从而达到私有专用网络的安全级别[2]。在 VPN 的帮助下，使用者通过启动终端上的 VPN 可以建立一个虚拟的网络传输隧道用以加密传输数据。同时，完全加密封装的相关技术，在整个数据的传输过程中被引入，在接收端，通过采用相应的认证技术和解密技术，可以保证发起的请求的合法性。在这个模式之下，整个传输过程中的安全在 VPN 中得到了保证[3][9]。

在我们的模型以及实现当中，我们的一个基本假设就是把校园网作为一个相对开放的网络环境对待。实际上，我国大多数高职院校的校园网都已经做到了网络入户（学生、老师宿舍）中，有的高校已经做到了全校无线网络覆盖。在这种情况之下，如果入侵者在校园内，绕过防火墙，对数据库服务器进行入侵攻击，如果获得成功，学生的个人信息，校园中的一些重要资料，甚至与一些具有保密级别的科研资料可能被修改或窃取，因此，如何保障校园网中的数据信息安全，已成为我们研究中的一个十分重要的问题，同时，各方面广泛的关注和重视也逐渐聚焦到针对校园内的网络犯罪上。

本文的研究以校园网改造项目为背景，结合笔者多年管理、改造、维护校园网项目经验，将研究的重点放在校园网内部的安全应用研究上，以校园网络是一个不安全的公共网络作为基本出发点，以 NS2 模拟器为技术基础，利用 PKI 和 IPSec 协议将加密认证服务植入 VPN 当中，针对校园网中的不安全因素构建一个校园网安全应用模型，并希望通过这个安全模型及其实现来解决校园网中存在的安全隐患。

1.2 研究背景及意义

1.2.1 研究背景

现今，互联网技术，通信技术，移动互联网技术在规模上，复杂性上，用户群体上都正在高速发展，计算机网络在工作和生活中的重要性越来越凸显出来。教育信息化，教育资源电子化的需求，使得高校在各方面对校园网的依赖程度越来越大[4][21][32]。由于开放和自由是互联网固有的特点，因此，公共网络中的应用，信息、设备的安全性并不能得到保证。数据在互联网上传递，设备连入公共网络，

很容易受到威胁和攻击，数据很容易受到窃取，监听等，数据安全性并不能得到保证[5]。同时，随着我国教育的现代化，校园网的普及和应用管理在我国国内高职院校中展现出了它越来越重要的地位，在此背景之下，学校各方领导和管理人员对于信息系统安全的重视也在逐步加深。

我们对一些主流校园网配置方案的分析，发现大部分的大学将集中在校园网中的功能实现，即校园网络架构和硬件配置在第一位。笔者通过分析发现，校园网安全事件的主要原因在于忽视校园网网络和信息安全，使得信息安全保障不能得到足够的重视，从而发生了信息泄露、越权访问等计算机安全上较为严重的后果[5][6]。虽然我们发现，一些较为简易常规的安全解决方案在部分高校中获得使用，但是其中绝多数只是包括购买或者部署了一些开源的防火墙系统，或者是一些杀毒软件的启用。笔者并没有发现在与校园网的管理相关工作措施中，以及校园网的网络应用使用流程中，有安全流程管理措施得到强制的执行，网络设备和应用也没有采用健全和配套的安全防范体系。这样就导致我们的安全防御体系具有较大漏洞，后续可能会产生非常严重的安全问题[7][8]。

VPN是为了解决在公共网络上数据传输的安全问题而产生并快速得到广泛认可并获得应用的虚拟网络链接技术[2]。通过搭建虚拟专用数据通道，两端的终端设备可以在网络通道中稳定地传输数据，同时具有价格低廉、较好的安全性和便利性的特点，在工业界学术界，均受到了高度关注，各大名企均对研发 VPN 产品进行了一定的投入，同时学术界中对于 VPN 安全性和效率的研究，也一直是一个热点。IPV4 协议中的 IP 包并没有安全特性[40]，另外，由于网络 ISO 架构中，没有对 IP 层的安全性进行保证，也没有对 IP 层进行安全协议的规范。以上问题，导致数据在整个网络传输过程的安全性并不能得到保证。因此，IPSec 作为 VPN 的主要协议，主要功能即是在网络架构的 IP 层上为数据传输提供强大的安全支撑[9][12]。但是在 IPSec 的原始设计当中，身份认证不严成为了一个较为严重的漏洞，而且，在实际情况下，网络环境较为复杂，其身份认证不严这一问题可能导致 IPSec 协议失效，从而成为严重漏洞。

近年来兴起的 PKI(Public Key Infrastructure)技术正好从身份认证和数据加密解密方面，较好地弥补了 VPN 这方面的缺点。身份鉴别技术是 PKI 的核心技术，身份鉴别技术同时是角色访问控制的实现核心。我们将 PKI 技术嵌入到 VPN 中，在常规传输隧道之前，要求通信双方通过 CA 来确认合法身份，下一步

进行访问权限的控制会根据用户从证书中心获得的证书中的角色属性进行最终确定，在此背景之下，保证双方的通信安全才能够被保证。因此，我们的模型的基本架构，使用了多种安全措施，从各方面提升了 VPN 的通信安全性。

1.2.2 研究意义

近年来，我国高校的校园网建设已取得了较快的发展，尤其是伴随全信息化校园的建设发展，各种攻击、入侵和破坏等不法行为也随着网络技术的发展而发展。各类校园网络资源，网络服务的安全性和稳定性，已经关系到学生老师切身利益。当前，校园网为教师、学生之间的数字资源的共享，广大科研人员研究资料的快速获取查询、以及科研人员之间的信息交流、国际国内高校科研机构之间的科研合作以及科学计算等。校园网对以上工作的支撑，使得这些我们国家科研和教育事业得到了快速高效的发展，校园网已经成为了我国科教工作中最为重要的基础平台性设施。

另一方面同时，校园网在提供便捷的网络服务的同时，也面临着存在着各种非法入侵、病毒、系统漏洞等。通过笔者的研究和分析，校园网的入侵者主要来源于学校的学生以及少量的校外黑客。他们的入侵可能会带来诸如：在校园网上启动计算机病毒；伪造用户身份；窃取，篡改，复制数据库内容；修改用户的口令以及校园网内的其他信息；摧毁网络节点等攻击行为，会给我们的网络服务造成严重损害。

如何通过一个安全的网络架构将各种服务器保护起来并且不改变现有校园网整体架构，同时防御来自内外网的各种攻击，是校园网信息安全体系建设的重点工作[11]。当前，校园网已经获得了较好的普及，各院校也自主研发或应用了不少软件在校园网平台上运行，以支撑高校的日常工作，因此，要想通过更换基础应用软件，如操作系统等来增强安全性，并不能够获得用户的支持。但是，如果能够在现有基础上架构上，通过改进更新升级校园网的架构，并且同时能够实现安全性能的提升，而不需要更换已有的办公软件，网络应用，数据库系统或操作系统，这样既保证了校园网的安全，又保护了学校资源，提升了校园网络的安全性。

本文中所论述模型的研发可以提高校园网络的安全性，同时降低校园网络被攻击的可能性。本文的主要工作是依托于现在主流的校园网架构，对校园网进行