学校编码：10384　　分类号_____密级_____

学号：X2013230351　　UDC_____

工 程 硕 士 学 位 论 文

某办公网准入控制系统的分析与设计

Analysis and Design of Access Control System for an Office Network

陈爱章

指 导 教 师：　陈海山　教授

专 业 名 称：　软 件 工 程

论文提交日期：　2015 年　　月

论文答辩日期：　2015 年　　月

学位授予日期：　　年　　月

指 导 教 师：_____

答辩委员会主席：_____

2015 年　　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

计算机互联网技术的迅速发展给人们的日常工作和生活带来了极大便利。但是在计算机互联网技术的发展过程中，网络信息安全问题已经成为了不可避免的难关。在计算机网络环境下，黑客、病毒、木马等各种安全威胁都是利用应用软件和操作系统中的相关漏洞来攻击计算机网络中的接入主机终端，并且迅速地在网络中进行传播。

针对目前这种网络安全的现状，本文应用 802.1X 的认证技术与网关认证实施联动，设计并实现了一套办公网络的安全准入控制系统。在本文实现的安全准入控制系统中，接入控制系统应用 802.1X 技术来实现，网关控制系统则采用 Linux 网关来实现。通过 802.1X 与 Linux 系统联动实现准入控制的目标，通过针对网关系统进行配置特定目的的网络访问，并通过 ulog 来记录用户的访问日志。尽管互联网已经遍布在社会的各个角落之上，但事实上，有很大一部分使用互联网的组织、机构等都没有网络安全意识或者缺乏有效的保证网络终端安全管理的技术。

通过针对终端安全准入技术进行论述以及针对相关实验结果的说明，本文得出如下结论：在办公网络应用中，将 802.1X 接入认证技术与网关认证控制技术进行联动来构建办公网络准入控制系统，帮助确保所有的用户网络设备都符合安全策略来提高办公网络的安全性，使其不受到规模动态变化和系统复杂性变化的影响，实验表明本文给出的安全准入控制系统是行之有效的。

关键词：办公网；网络准入；网关控制

Abstract

The rapid development of computer Internet technology has brought great convenience to people's daily work and life. But in the development of computer Internet technology, the problem of network information security has become the inevitable difficulty. Under the computer network environment, hackers, viruses, Trojans and other various security threats are the application software and operating system vulnerabilities to attack the computer network access a host terminal, and quickly in the network spread.

In view of the present situation of network security, this thesis is based on 802.1X authentication technology and gateway authentication linkage, and realizes a set of office network security access control system. In the security admission control system, the access control system is implemented by 802.1X technology, and the gateway is implemented by Linux gateway. Through the linkage between 802.1X and Linux system, the access control is achieved, and the access to the gateway is configured for a specific purpose, and the access log is recorded by ulog. Although the Internet has spread in every corner of the society, but in fact, a large part of the use of the Internet organizations, etc. are not network security awareness or lack of effective guarantee network terminal security management technology.

Through on terminal security access technology are discussed and according to the related experimental results, this dissertation draws the following conclusions: in the office network applications, 802.1x access authentication technologies and authentication gateway control technology for linkage to construct the office network access control system, to help ensure that all users of the network equipment is in accordance with the security policy to improve the office network security, which is

not affected by the dynamic changes of the scale and complexity of system changes. The experiments show that this security access control system is feasible and effective.

Keywords： Office Network; Network Access; Gateway Control

目录

第 1 章 绪论 1

1.1 研究背景 1

1.2 研究目的与意义 2

1.3 国内外研究现状 3

1.4 研究内容 5

1.5 本文结构 6

第 2 章 系统需求分析 8

2.1 相关概念介绍 8

2.2 信息安全与网络准入 9

2.3 信息终端保护手段 10

2.3.1 操作系统更新 11

2.3.2 网络保护措施 11

2.3.3 终端入侵检测与防护 12

2.4 安全保护手段 15

2.4.1 可信准入 16

2.4.2 网络准入措施 16

2.4.3 接入与网关联动 18

2.5 功能需求分析 18

2.6 系统用例分析 19

2.7 本章小结 21

第 3 章 系统总体设计 23

3.1 系统设计目标 23

3.2 系统设计原则 24

3.3 系统架构设计 25

3.4 系统功能设计 25

3.5 数据库设计 26

3.6 准入系统局部设计状态属性 28

3.7 本章小结 32

第 4 章 系统详细设计 33

4.1 远程管理与控制模块 33

4.2 内网管理控制模块 34

4.3 网络准入控制模块 36

4.3.1 准入控制的模型与措施 37

4.3.2 准入控制系统结构 38

4.3.3 准入控制的原理与流程 41

4.4 准入控制系统配置模块 43

4.4.1 基本配置 43

4.4.2 终端服务器配置 44

4.4.3 VLAN 创建 44

4.4.4 网关联动与 802.1X 45

4.5 系统测试 48

4.6 本章小结 50

第 5 章 总结与展望 51

5.1 总结 51

5.2 展望 51

参考文献 53

致谢 55

Contents

Chapter 1 Introduction 1

1.1 Research Background 1

1.2 Research Purpose and Significance 2

1.3 Research Status at Home and Abroad 3

1.4 Research Contents 5

1.5 Outline of the Dissertation 6

Chapter 2 System Requirement Analysis 8

2.1 Overview of Related Concepts 8

2.2 Information Security and Network Access 9

2.3 Information Terminal Protection Measures 10

2.3.1 Operatio System Update 11

2.3.2 Network Protection Measures 11

2.3.3 Terminal Intrusion Detection and Protection 12

2.4 Security Protection Measures 15

2.4.1 Trusted Access Measures 16

2.4.2 Network Access Measures 16

2.4.3 Access and Gateway Linkages 18

2.5 Function Requirement Analysis 18

2.6 System Cases Analysis 19

2.7 Summary 21

Chapter 3 System Overall Design 23

3.1 System Design Objectives 23

3.2 System Design Principles 24

3.3 System Framework Design 25

3.4 System Function Design 25

3.5 Database Design 26

3.6 State Attribute of Access System Local Design 28

3.7 Summary 32

Chapter 4 System Detailed Design 33

4.1 Remote Management and Control Module 33

4.2 Internal Network Managemen and t Control Module 34

4.3 Network Access Control Module 36

4.3.1 Model and Measure of Access Control 37

4.3.2 System Structure of Access Control 38

4.3.3 Principle and Process of Access Control 41

4.4 Access Control System Configuration Module 43

4.4.1 Basic Configuration 43

4.4.2 Terminal Server Configuration 44

4.4.3 VLAN Creating 44

4.4.4 Gateway Linkage and 802.1X 45

4.5 System Testing 48

4.6 Summary 50

Chapter 5 Conclusions and Future Work 51

5.1 Conclusions 51

5.2 Future Work 51

References 53

Acknowledgements 55

第 1 章 绪论

1.1 研究背景

时至今日，信息技术已经历了日新月异的变化，互联网已经成为不可缺少的交流途径，是重要的信息载体，各种组织和机构的高效运转都离不开互联网。然而，网络技术的发展，一方面给网络使用者带来了方便，另一方面应用环境也面临着日益严峻的威胁和考验，如各种计算机病毒等不断出现并升级，轻者使计算机运行速度减慢、严重消耗系统资源从而导致系统崩溃，重者则导致数据丢失、窃取机密信息、泄露国家机密。这些危险意味着提供网上服务和应用的组织或机构也在面临着严重挑战，保证用户接入时自身系统安全和保证接入主机的安全成为了一个很重要的任务。办公网络是互联网环境下相对独立的局域网络环境，是一种普遍的网络应用模式。办公网络的信息传输包括办公内网用户与外部网络交互的数据、中心服务器与办公网络内节点的信息传输、一些特定应用要求的业务所定义的各种安全级别的信息传输。网络应用产品就是建立在以上信息传输之上的，由于信息传输广泛而深入的应用，网络应用产品遇到了更加艰巨的挑战，如兼容性、继承性、网络安全性等。

互联网技术的高速发展，使得网络安全问题越发受到重视。黑客攻击、系统漏洞、病毒泛滥等诸多问题，已经对办公的正常运营造成直接影响。如何防御网络安全威胁，保证企业或其他组织机构的网络安全，为企业或其他组织机构的运营提供有力可靠的网络保障，已经是办公决策者必须面对和关注的问题，也是网络维护者必须面对的挑战。由于大多数的网络安全事故都是由相对脆弱的终端和失控的用户网络使用行为所引起。在办公网中，用户的终端不进行实时病毒库升级和系统补丁的现象普遍存在；滥用办公禁止的软件，擅自访问外部网络、私设代理服务器等行为也常常出现。受到感染的终端用户一旦被接入办公网络，就使得整个网络面临着潜在安全威胁，并且这种威胁会在网络内部

达到快速扩散。因此，保证网络接入用户的终端设备的安全，防止终端用户对网络的潜在威胁，对办公网络接入用户的行为进行有效控制是建设办公网络、保证信息安全必须解决的关键问题。伴随着科学技术的不断发展，移动存储介质呈现多样化、袖珍化，如 SD 卡、便携 U 盘、移动硬盘等在人们的学习和工作中的发挥了巨大作用，移动存储介质的存在，在一定程度上比传统的纸质存储更加便捷和节省资源。移动存储介质的诸多优势相信已经人尽皆知了，但它带来的涉密信息外漏隐患也是我们不容小觑的，如何确保移动介质中涉密信息不外漏就是一个现阶段必须考虑和解决的问题了。

据调查研究，当前企业或其他组织机构在网络接入控制方面的实际需求都不是简单的拒绝访问，而是希望尽可能保持基础设施的开放性的前提下，控制访问者对网络信息的访问。另外，企业或其他组织机构还不希望影响网络应用的便捷性，若添置过多的硬件设备，或在用户终端上安装过多软件，都会影响网络资源的访问率和用户终端的可用率。值得一提的是大多数企业或其他组织机构都会基于对成本的考虑，而不去选择改变原有网架结构。在保持原有网架结构不变的基础上来解决目前遇到的网络安全问题不仅是企业或其他组织机构的迫切愿望，也是网络安全产商面对的巨大考验。在企业和其他组织机构对接入支持迫切需求基础上，出现了终端安全准入理念。

1.2 研究目的与意义

从信息网络诞生到现在，网络安全建设一直伴随着信息技术持续快速的发展，在这过程中，网络安全产品为信息网络安全、稳定运行保驾护航。但是目前网络安全问题并未呈现递减趋势，随之而来的终端安全问题迅速突显。之前，为了确保网络环境和企业资源的安全性，常把企业涉密信息放在办公内网，外部用户无法访问企业机密。也就是说为了实现网络安全，企业需要投入大量资金、技术去组建自己的内网。然而随着网络应用的快速发展和业务的纵横交错，企业或其他组织机构不能单纯的依赖单一模式去实现网络的安全，随着业务重要性的提升，网络环境的稳定和安全是必不可少的前提，不但企业内部员工，

包括供应厂商和客户等都需要访问各类办公系统，核心业务的通畅程度直接影响企业的效益。因此，企业业务延伸的同时，网络访问范围也在逐渐增大，企业对网络安全性要求也会愈加严格。办公网络中的接入元素包括核心网络设备（如路由器、防火墙、交换机）、完成不同业务的多个应用服务器以及大量的终端计算机节点。传统的信息安全管理中，终端设备安全的重要性往往低于核心网络设备和应用服务器。然而在互联网环境下，终端计算机涉及的人员众多、面对的应用情况复杂，已经成为了日常业务的重要载体，如果终端设备出现了安全问题，可能将安全威胁传染到其他机器甚至核心设备，导致整个网络的运行受到影响，甚至造成更严重的安全问题，如系统瘫痪、机密泄露等。建设一个高效的终端安全管理体系，不但可以确保终端信息安全，还能提升网络的整体安全防御能力。

终端安全管理往往非常复杂，通常一个机构中的终端分布在不同的地理位置，用户承载的业务不同，水平参差不齐，安全需求各异，这些导致了终端安全建设的多元性和复杂性，要根据终端用户的业务需要、所属部门、接入位置等条件来选择和部署合适的安全管理措施。当今终端安全面临严重挑战：系统管理问题、安全防护问题和行为监控问题。其中系统管理问题多数表现在对各种操作系统中不断涌现的漏洞的及时升级补丁管理，对网络中终端设备的资产变化信息的精确统计和管理。而安全防护问题包括木马程序不断出现给用户带来威胁，病毒蠕虫的大规模泛滥，来自外部和内部的攻击和入侵问题，网络边缘扩展出现的对于第三方合作伙伴以及移动办公用户的接入安全防护不足而导致的安全风险问题。至于网络行为监控，则是机构对于员工的行为和安全防范和监控预防措施。

1.3 国内外研究现状

终端安全准入这个词，六、七年前才开始出现在信息技术行业。终端安全准入是个容易理解的概念，准入控制系统会将所有即将入网的终端进行安全扫描和认证，也就是说终端在不满足安全准入条件下是不允许其入网的。然后根

据个人的身份和其他基本信息，例如用户是通过有线或者无线接入、端点安全的检查结果等，分配其不同的访问控制策略，但实现起来却非常复杂。传统的访问控制技术曾经在办公网络环境中得以成功部署与实施，然而，随着互联网技术的高速发展，以前对单个计算机的攻击已经发展成对网络基础设施的威胁，原有的访问控制管理技术已无法适应目前的网络发展现状。因此，准入控制需求和技术应运而生。安全准入控制是传统访问控制理论发展到一定阶段的必然结果。各研究机构和厂商都在为解决终端安全，建立全网安全体系而努力。在那之前，人们一直都使用类似扫描或者拦截的术语来防范网络中出现的各类威胁。终端安全准入的思路是，如果有终端携有计算机病毒（如木马、蠕虫等）访问办公内网，办公网准入控制系统会立马检测到该终端，并将其阻断出网络。办公网准入控制系统将重点放在为所有入网的设备做访问控制管理。这也是终端安全准入为网络安全提供解决方案的原因所在。

通过网络接入控制管理系统可以满足企业要求，将设备接入控制扩展到超出简单远程访问及路由器、专有协议和已管理设备的限定之外；能够覆盖到企业网络的每一个角落，甚至是当使用者拿着他们的移动设备离开企业网络时，仍能有效的提供设备接入控制的执行。网络接入控制管理系统针对所有的网络架构工作，并且不必进行昂贵的网络架构改造。

终端安全准入技术发展迅速，而且各种方案呈现整合趋势。一方面，业界主流厂商在突出自己技术的同时，加大了相互之间的合作力度。诸如，微软和思科互相兼容准入控制技术；另一方面，网络准入控制技术也日趋规范化和精益化。不管是基于网关，还是 DHCP、802.1x 的方案，都需要标准化工作，实现互操作的支持。可信计算组织 TCG（Trusted Computing Group）于 2004 年成立了一个可信网络连接 TNC（Trusted Network Connect）分组 TNC 准备为终端安全准入规则开发一个对业界开放的架构规范，以确保任何厂商开发的端点准入产品具有可互操作性。成立 TNC 旨在加快标准化的发展，诸多优秀的网络安全公司如 Symantec、Juniper、Zone Labs、Foundry 和 Trend Micro 等都加入了 TNC

分组。该分组迫切渴望利用构建规范和框架来确保兼容性，这些对于业界开放的规范会依托现有的工业标准，并在规范应用成熟的时候开发新的协议和标准，包括网络设备之间、网络设备和端点主机之间的通信协议和软件接口。 据 2009 CSI/FBI 安全报告称，尽管多年来已经耗资数百万美元来解决网络安全问题，但各种形式的网络威胁如计算机病毒、恶意软件等仍然是网络信息安全领域面临的主要问题。每年都有很多办公机构会遭遇由于网络信息安全事故带来的整个系统崩溃、经济损失、数据丢失或损坏等问题，严重影响到办公机构的经济效益。

办公网准入控制系统是一种结合终端安全防护、办公网访问控制和系统管理等办公网络安全解决方案，保证所有接入办公网的设备（包括核心网络设备、应用服务器，也包括终端接入用户）都符合安全策略。网络安全准入系统对所有试图接入办公网络的终端设备进行分析和控制，确保每个设备都符合本网络系统的安全策略，消除可能作为感染源的终端设备危害网络信息安全。虽然大多数企业或其他组织机构都使用身份验证、授权和记账（AAA）机制来验证和区分用户并为其分配网络访问权限，但仅靠账户信息来分析控制终端设备不符合安全策略要求的，必须通过科学的方法来评估接入设备的安全状态，避免用户在疏忽中将感染病毒的终端或未采取安全防护措施的设备接入网络，进而威胁办公网安全。终端安全准入是构建在多种技术之上的一系列解决方法。对于满足办公网准入控制系统安全策略的终端，允许其访问办公网内相关业务系统。对于不满足上述条件的终端，办公网准入控制系统会协助终端使用者完成问题整改，从而顺利访问办公网。

1.4 研究内容

本文主要基于安全准入策略和相关检测技术，研究与设计具有终端安全准入的自防御系统结构办公网络准入控制系统。它是一个由客户端检测程序、准入策略服务器、接入交换机或边界防火墙等模块一起构成的完善的分步式安全体系。文中论证了终端安全准入是网络安全的重要发展方向。目前办公网络环

境日趋复杂，许多应用分布在不同位置，可能在办公网络内部，也可能分布在办公网络的边界外。这样，对用户的管理控制靠单纯的接入控制或网关控制难以完成。针对这种现状，本文采用 802.1X 认证技术和网关认证进行联动，设计实现了一个办公网络准入控制系统。在本系统中，接入控制系统用 802.1X 技术实现，网关控制系统采用 Linux 平台。通过 802.1X 和 Linux 平台联动实现准入控制的目的，通过对网关系统进行配置特定目的的网络访问，并通过 ulog 来记录用户的访问日志。 在论文后期，通过搭建实验环境，完成讨论方案的环境测试，通过对终端安全准入的技术论述以及相关的实验结果，本文得出如下结论：在办公网应用中，将 802.1X 接入认证技术和网关认证控制技术进行联动构建办公网准入控制系统，这样一来，接入办公网的所有设备都会满足准入控制系统的安全防护策略，如果办公网准入系统检测到终端不满足上述条件，会在第一时间将异常中断阻断出网络，待终端问题解决后，办公网准入控制系统会再次检测终端是否满足安全防护策略，通过这一手段终端安全问题就会被抑制和消除，网络的安全性和稳定性也会进一步得以提升。

1.5 本文结构

本文旨在研究准入控制在办公网中的应用及潜在发展趋势，通过五章内容对现有准入控制系统的功能和应用进行总结，并结合自身工作经验分析与设计适合本企业的准入控制系统。

第 1 章 绪论，介绍终端安全准入技术的研究背景及意义，分析国内外的研究现状，并结合当前主流技术的优点来设计出适合本企业应用的准入控制系统。

第 2 章 系统需求分析，从终端安全防护手段、信息防护手段、功能需求等方面进行了分析。

第 3 章 系统总体设计，在系统需求分析的技术上，进行终端准入系统的总体设计。

第 4 章 系统详细设计，在完善总体设计的基础上，对终端准入系统进行详细设计，并对系统的配置和系统的功能进一步优化。