学校编码：10384　　分类号＿＿＿密级＿＿＿
学号：X2008230049　　UDC＿＿＿

硕　士　学　位　论　文

# 突破主动防御的网络远程监控系统的研究与设计

# Research and Design for Breaking Active Defense of Remote Controling System

王　龙

指导教师姓名：史　亮　副教授
专　业　名　称：软　件　工　程
论文提交日期：2010 年　月
论文答辩时间：2010 年　月
学位授予日期：2010 年　月

答辩委员会主席：＿＿＿＿＿＿
评　　阅　　人：＿＿＿＿＿＿

2010 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

近年来，网络成为国家间你争我夺的新战场。网络攻防战时时都在发生。远程监控软件是网络战争中不可或缺的杀手锏武器，既可以获取敌方重要的军事、政治、经济等情报，也能够对敌方的网络发起攻击，瘫痪或者摧毁其网络系统。但是伴随着网络技术的不断进步和操作系统的不断升级，特别是带有主动防御功能的杀毒软件的推出，对传统的远程监控软件提出了挑战。开发可以突破主动防御功能的远程监控系统已经迫在眉睫，对此项技术的研究也具有非常重要的现实意义。

本文分析了网络远程监控系统及木马的发展趋势，重点阐述木马开发过程中隐藏技术的实现，并根据实际需要，完成了网络远程监控系统的开发。

论文的主要内容包括：

1、简述网络攻击技术的发展趋势和遇到的瓶颈；

2、介绍基于木马的网络攻击技术和主动防御技术；

3、着重分析了网络远程监控系统木马部分的隐藏技术，主要是进程隐藏和端口复用的详细设计实现；

4、研究和设计网络远程监控系统。

**关键词：木马；远程监控；主动防御；**

## Abstract

In recent years, Internet has become a new scrambling battlefield between countries; all kinds, all levels of network battle took place all the time. Network remote control software is an integral killer war weapons, not only it can get important military, political and economic intelligence, but also it can attack the paralysis or destruction of its network system. But along with the update of the network technology and the operating system, especially with active defense capabilities of the antivirus software release, challenges the traditional remote control software. Development of breakthrough active defense remote control system has been imminent, the research on this technology also has important practical significance.

This article analyzes the network remote control system and the development trend of Trojan, focuses on the realization of hiding, and complete the remote control system occur to the actual needs.

The article includes:

1、Brief introduce the development trend of network attack techniques and bottlenecks encountered;

2、Introduce Trojan attack techniques and active defense technology;

3、Highlighting analyse the hidden technology used in the Trojan part of remote control system .Especially the detailed design of the hidden of process and the reuse of port;

4、Research and design of network remote control system .

**Key words**:Trojan Horse;Remote Control System;Active defense technology;

# 目 录

# CONTENTS

# 第一章　引　言

## 1.1 研究背景和研究意义

当今世界信息技术迅猛发展，人类社会正进入一个信息社会，信息已成为国家的主要财富和一种重要战略资源，国家综合实力的竞争越来越集中在信息优势的争夺上，而信息优势的夺取，直接地表现为信息安全与对抗。信息安全已逐步 成为国家政治、经济、科技、文化，特别是军事等安全领域的一个重要方面[1]。近年来，特洛伊木马、蠕虫、分布式拒绝服务攻击、垃圾邮件、网络仿冒、陷门、rootkit 和间谍软件等恶意代码已经成为网络安全领域面临的重要威胁并在世界各地引起了高度重视。因而及时的研究网络攻击和防御技术已经迫在眉睫。

从网络信息战的角度来看，信息是战略资源，信息是决策之源，是控制战场的灵魂，信息决定火力和机动力。信息战将以覆盖全球的计算机网络为主战场，以攻击对方的信息系统为主要手段，运用高精尖的计算机技术，不仅破坏军事指挥和武器控制系统，而且会使其金融、交通、商业、医疗、电力等涉及国民经济命脉的诸多系统遭到破坏，从而达到攻城略地的目的[2]。

网络战必将成为未来信息战场新的作战样式。首先，网络技术的广泛应用，使得网络成为新的争夺空间。在信息时代里，网络正在成为联结个人和社会，现在和未来的纽带，各种各样的计算机网络都将成为一个国家的战略资源和战略命脉，一旦重要的网络陷入瘫痪，整个国家安全就面临着崩溃的危险，使“制网络权”的争夺与对抗不可避免。同时，随着网络技术在军事领域的快速发展，军队对计算机网络的依赖越来越大，网络与作战的联系也愈来愈紧密，网络成为新的战场空间。其次，网络的特殊战略作用，促使网络对抗与争夺向网络信息对抗方向发展。和常规作战中选择打击对象一样，网络攻击也是把对敌方的战略目标作为首要进攻对象。能否有效地摧毁敌方重要网络系统，以便迅速达成一定的战略目的，就成为敌对双方进行全面网络争夺和对抗的焦点，这种对抗与争夺，必然促使网络战成为新的作战样式登上战争舞台。

为了在未来的网络战中掌握主动权，网络攻击技术是不可或缺的武器，

发展研究网络攻击技术具有重要的战略意义。从军事应用的角度，网络攻击应当是战平结合，和平时期进行网上侦察，以获取敌方军事、经济、政治等重要信息；战争时期破坏敌方系统，瘫痪敌方网络，使其指挥系统失灵达到制约敌方的目的。因而应该构建一个网络攻击平台，即具有渗透式攻击窃取秘密信息的特点，又具有主动攻击摧毁敌方系统的特点。

综上所述，网络信息安全已与国家的安全和利益紧密的联系在一起，网络信息战已引起很多国家的普遍重视，网络攻击技术也相应的得到了长足的发展。未来战场，“无网不胜”，因而开发具有高有效性的网络攻击系统，研究最先进的网络攻击技术对于将来在网络战中争夺“制网络权”具有重要的意义。

## 1.2 研究现状

### 1.2.1 网络攻击技术的发展趋势

常见的黑客入侵基本流程，一般可以分为三个阶段：

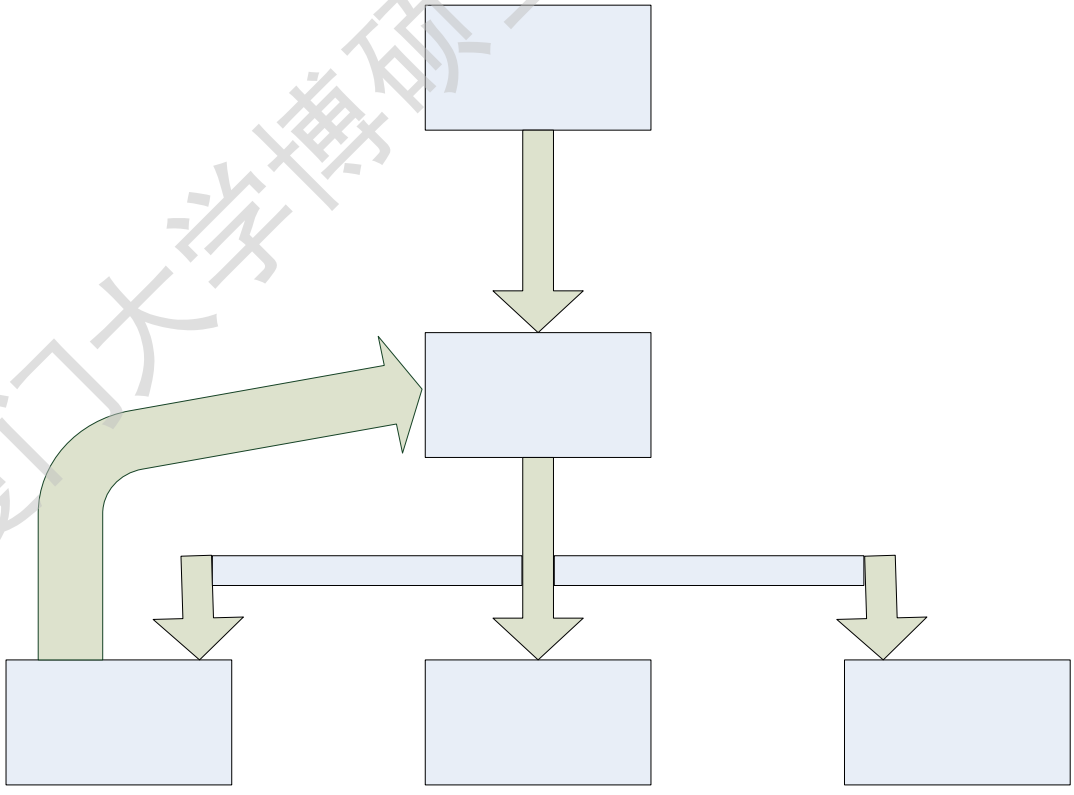

图 1.1 黑客入侵基本流程图

第一阶段，入侵前的准备，主要进行入侵目标的信息收集、对目标的进行系统扫描，获取电子邮箱地址、获取目标的网络状况、获取操作系统类型及其开放的服务、刺探目标系统可能存在的漏洞[3-5]。

第二阶段，入侵系统，取得受害主机的控制权，并安装后门程序。此阶段攻击的手法可以归纳为以下几种：一是利用第一阶段发现的漏洞直接对目标主机进行攻击，以取得系统的控制权。从网络上流行的工具可以看出大多数漏洞都是设计上的 BUG 和管理员的疏忽造成的。常见的有 WebDev、RPC、IIS、SQL 注入、默认密码等等方式。二是发送含有恶意代码的 Email 至攻击目标用户的电子邮箱，欺骗用户执行恶意代码，从而获得系统的控制权。三是发送含有某个链接的 Email 给目标用户的帐号，诱骗用户访问此链接,借此黑客可以利用 IE 的漏洞在用户端执行命令或者安装恶意程序，进而取得系统的控制权。

第三阶段，扩大攻击范围，持续维持所取得的控制权限，窃取重要资料和档案。至此阶段，黑客已经控制了某个内网的机器，通过后门程序可以继续对内网进行进一步蚕食，得以控制更多的机器，以备后用。黑客为了维护所取得的控制权限和掌握更多的信息，除安装后门程序外，也会安装远程监控程序等软件，取得窗口操作界面，更加方便的维持控制权限，同时进行窃取目标机器的重要资料，完成攻击的最终目的。

上述传统入侵模式在很长一段时间内一直没有很大的变革，远程监控软件和木马一直是黑客界永恒的主题和必要的技术手段之一。特别是近年来，特洛伊木马、蠕虫、分布式拒绝服务攻击、垃圾邮件、网络仿冒、陷门、Rootkit 和间谍软件等恶意代码已经成为网络安全领域面临的重要威胁并在世界各地引起了高度重视。因此及时的研究网络攻击和防御技术已经迫在眉睫[6][7]。

针对近几年网络攻击技术和攻击工具的最新发展，本文认为网络攻击技术发展趋势主要表现为以下几个方面：

1、自动化程度和攻击速度提高

攻击工具的自动化水平不断提高。自动攻击一般涉及四个阶段，从扫描受害主机，损坏脆弱系统，传播攻击，到攻击工具的协调都出现了自动

化的特征。攻击工具趋向于自动化、图形化和多线程化，提高了攻击工具的易用性、执行速度和攻击效率。

2、攻击代码的动态化和模块化

攻击代码趋向于动态化、模块化（插件化）和反制化，提高了攻击代码的生存性、对抗性以及鲁棒性。

3、攻击代码的伪装化和蠕虫化

攻击代码趋向于伪装化、隐身化和蠕虫化（深度传播），提高了攻击代码的欺骗性、隐身性和传播性。

4、漏洞发现的自动化和快速化

系统漏洞发现趋向于自动化和快速化，新发现的安全漏洞每年都成倍增加，管理人员不断用最新的补丁修补这些漏洞，而且每年都会发现安全漏洞的新类型。入侵者经常能够在厂商修补这些漏洞前攻击目标，从而利用新漏洞可以提高攻击成功率和工作效率。

5、攻击手法的融合化和多样化

攻击手法趋向于多种攻击方法相互融合和多样化，这样使得攻击工具越来越成熟，复杂。攻击工具具有三个特点：反侦察、动态行为和攻击工具的成熟性。这些特点提高了攻击成功率和效率。

6、越来越多的防火墙渗透率

防火墙是人们用来防范入侵者的主要保护措施，但是越来越多的攻击技术可以绕过防火墙，如：反向连接技术、IPP（Internet 打印技术）和 WebDAV（基于 web 的分布式创造与翻译）都可以被攻击者来利用来绕过防火墙。这样使得对内部网络的保护受到挑战。

7、对基础设施将形成越来越大的威胁

基础设施攻击是大面积影响 Internet 关键组成部分的攻击。由于用户越来越多地依赖 Internet 完成日常任务，因而对基础设施的攻击越来越引起攻击者的兴趣。基础设施面临着分布式拒绝服务攻击、蠕虫病毒及其对路由器攻击和利用路由器攻击等众多威胁。

### 1.2.2 网络攻击遇到的瓶颈

经过网络攻击技术和防范技术的不断发展，特别是近年来由于媒体宣

称等因素导致网络安全越来越多地引起广大网民的关注，网民的防范意识空前提高，各类防御软硬件和新防御技术层出不穷，直接造成黑客入侵的难度不端增加。难度的增加最明显的体现在于操作系统持续自动安装补丁、0Day 的漏洞利用稀少而且昂贵、普通网民不再轻易打开带有附件或者链接的电子邮件、企业内网的防御设备愈发健全、网管更为专业和敬业等等各个环节[8]。

## 1.3 论文的主要内容

本文在研究木马的基础上，结合实际需要，给出一种能够突破主动防御的远程监控系统。论文的主要内容如下：

1、分析了当前的网络攻击技术，特别是木马技术；

2、探讨了安全防御软件采用的主动防御技术；

3、着重介绍了突破主动防御的隐藏技术，包括进程隐藏和端口复用；

4、对远程监控系统的体系结构、功能模块进行了详细讨论，并进行了实现；

5、对该系统进行了测试，结果表明该系统运行正常，达到了设计要求。

## 1.4 论文的结构及章节安排

第一章简要陈述了本文的研究背景和主要内容，以及论文结构安排。

第二章介绍了网络远程监控的基础知识，包括木马、Windows 核心编程、缓冲区溢出、Shellcode 以及主动防御技术的基础理论。

第三章着重详细分析和设计了远程监控系统木马部分采用的隐藏技术，主要是进程隐藏和网络通信隐藏技术。

第四章给出了远程监控系统的总体设计，详述了各个组成部分的功能组成，并开发了该系统。

第五章对系统进行了测试，测试结果表明系统是可用的。

第六章是结论，总结了论文的研究成果，并展望了后续的研究工作。