高等学校计算机专业“十一五”规划教材

网络安全实践

马传龙　谭建明　主编
谢晓燕　主审

西安电子科技大学出版社
http://www.xduph.com

高等学校计算机专业“十一五”规划教材

网络安全实践

主编　马传龙　谭建明
参编　黄　旭　罗　萱　路　亚　梁雪梅
主审　谢晓燕

西安电子科技大学出版社
2009

内 容 简 介

本书介绍了计算机系统及网络系统的安全知识，并配以大量实际可行的实验。本书共分 7 章，图文并茂地介绍了目前先进的网络安全实践的理论和实验，包括网络安全现状及发展趋势、虚拟机、Windows 系统安全加固技术、系统漏洞扫描与修复、入侵检测技术、密码使用及破解和数据备份与灾难恢复技术。

本书可作为高等院校网络工程及信息安全相关专业学生的教材，也可供从事计算机及网络安全技术的科研人员、工程技术人员、网络系统管理员、网络安全爱好者及其他相关人员参考。

☆ 本书配有电子教案，需要者可登录出版社网站，免费下载。

图书在版编目（CIP）数据

网络安全实践/马传龙，谭建明主编. —西安：西安电子科技大学出版社，2009.9

高等学校计算机专业“十一五”规划教材

ISBN 978-7-5606-2336-8

Ⅰ. 网… Ⅱ. ① 马… ② 谭… Ⅲ. 计算机网络—安全技术—高等学校—教材 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 133600 号

策　　划　陈　婷

责任编辑　陈　婷

出版发行　西安电子科技大学出版社（西安市太白南路 2 号）

电　　话　(029)88242885　88201467　　邮　　编　710071

网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com

经　　销　新华书店

印刷单位　陕西华沐印刷科技有限责任公司

版　　次　2009 年 9 月第 1 版　2009 年 9 月第 1 次印刷

开　　本　787 毫米×1092 毫米　1/16　印张 14

字　　数　325 千字

印　　数　1～4000 册

定　　价　20.00 元

ISBN 978 – 7 – 5606 – 2336 – 8 / TP • 1180

XDUP 2628001-1

高等学校计算机专业“十一五”规划教材

编审专家委员会

前　言

自 2001 年武汉大学创建了全国第一个信息安全本科专业以来，我国信息安全专业的本科毕业生踏上工作岗位才数年。随着我国网民人数的激增和网络安全问题日益严峻，社会各行业对信息安全人才的需求也大大增加。因此，为促进我国的信息化安全建设和提高广大网民的网络安全意识，学习信息安全基础知识和掌握基本的网络安全防范技术，已成为当前计算机用户面临的紧迫任务。

本书根据一般读者的思维习惯，以“计算机系统安全→网络系统安全→数据灾难恢复”为主线来展开全书内容，向读者深入浅出地介绍了网络安全的基础知识和网络安全工具的使用。全书共分 7 章，分别介绍了网络安全背景、网络安全实验平台、操作系统安全、计算机系统漏洞扫描、入侵检测技术、密码使用及破解、数据备份与恢复等。

第 1 章“网络安全概述”介绍了目前的网络安全现状及发展趋势，使读者对网络安全有一个整体的认识，然后介绍了网络面临的常见威胁，并给出了黑客入侵的步骤。

学习网络安全知识，仅有理论是不够的，实验是一个必不可少的关键环节。但众所周知，网络安全实验一般要在一个网络的环境中才能进行，而大部分读者不具备网络环境，况且有一些实验会对个人计算机或网络造成一定的影响，甚至会破坏网络性能。鉴于此，第 2 章“虚拟机”就向读者介绍了网络安全实验平台——虚拟机，包括虚拟机的概念，基础知识，软件介绍，虚拟机的安装、配置和使用等。通过第 2 章的学习，读者就可以创建自己的网络环境，进行以下章节所涉及的各种网络安全实验了。

大多数用户使用的操作系统是 Windows，那么如何在现有的条件下加固自己的操作系统安全呢？第 3 章“Windows 系统安全加固技术”的内容属于“计算机系统安全”的范畴，主要介绍了个人防火墙的设置、IE 的安全设置、系统帐号和口令的安全设置、文件系统的安全设置和加密等。

第 4 章“系统漏洞扫描与修复”的内容也属于“计算机系统安全”的范畴，主要介绍了端口的基础知识、端口扫描的原理、目前流行的扫描工具(如 SuperScan、流光、SSS 等)的安装和使用，最后介绍了微软公司的微软基准安全分析器 MBSA。通过 MBSA 的学习，可以检查出自己的系统存在哪些漏洞或隐患以及如何解决这些问题。

第 5 章“入侵检测技术”属于“网络系统安全”方面的内容。首先向读者介绍了入侵检测系统的基本原理，接着介绍了数据包捕获工具 Ethereal 的使用、嗅探器的原理、Sniffer 的使用、Snort 的使用以及基于 Snort 的入侵检测系统的安装过程。通过本章的学习，读者就可以在局域网内捕获和分析数据包了。如果有兴趣的话，也可以安装 IDS，检测一下自己的计算机或网络是不是存在入侵。

第 6 章“密码使用及破解”的内容有的属于“计算机系统安全”，也有一部分属于“网络系统安全”。这一章主要介绍了常用的加密和解密方法，包括 BIOS 的密码设置与清除、Windows 的密码设置与破解、Office 办公软件密码的设置与破解、用压缩软件加密文件及

破解密码、PGP 加密技术、邮箱密码的破解、QQ 密码的破解等。大家在生活中会用到很多密码，但密码多了就不容易记住，不要着急，本章最后提供的“密码工具箱”会为您解决这个问题。

虽然我们对计算机系统和网络系统安全都做了一定的防范，但大家都知道，在网络攻防技术中，病毒、木马、黑客等防不胜防。因此，重要的数据包括系统数据和个人资料一定要备份，在最坏的情况下我们可以使用这些副本将系统恢复，把个人资料还原。本书第 7 章“数据备份与灾难恢复技术”就介绍了这方面的知识，包括数据存储技术、数据备份技术、灾难恢复技术、Windows 自带的系统备份工具、常用的系统备份工具 Norton Ghost、流行的数据恢复工具 EasyRecovery 和 FinalData 等。

本书具有如下几大特点：

(1) 理论与实践相结合。

本书每一章都是先讲理论知识，然后配以实验相辅。这样既克服了只有理论知识的枯燥，又避免了仅有实验而导致深度不够的缺点。理论指导实践，实践验证理论，二者相辅相成，相互促进。

(2) 实验由浅入深，图文并茂。

本书的实验内容采用 Step-by-Step 的教学模式，实用性强，直观易懂。每章中的实验，都是先介绍背景，然后从安装、配置到使用一步步地介绍，同时配有截图。因此，根据图示读者就可以很容易地完成各个实验了。

(3) 紧密追踪网络安全最新发展。

本书内容不仅介绍了网络安全技术的基础知识，而且紧密追踪网络安全的最新发展，使读者对网络安全有一个全面和最新的了解。

(4) 教与学结合。

本书配套有教学用 PPT，可供使用本书的教师参考。相关资料可在出版社网站(www.xduph.com)上下载。

本书第 1、7 章由马传龙编写，第 2 章由谭建明编写，第 3 章由黄旭编写，第 4 章由梁雪梅编写，第 5 章由罗萱编写，第 6 章由路亚编写，感谢刘燕老师对第 5 章提出了不少宝贵意见。全书由马传龙和谭建明统稿。感谢西安邮电大学的谢晓燕老师给本书提出了宝贵的建议。

由于编者水平有限且时间仓促，尽管我们花了大量时间和精力校验，但书中疏漏之处在所难免，敬请各位读者批评指正，万分感谢。

编　者

2009 年 5 月

目　录

第 1 章

网络安全概述

1.1　网络安全的现状及发展

随着以计算机和网络为代表的信息技术的迅猛发展，政府部门、金融机构、企事业单位和商业组织对信息系统的依赖日益加深，信息技术几乎渗透到了世界各地和社会生活的方方面面，随之所带来的安全性问题也越来越多。

1.1.1　网络安全的内涵

首先我们了解一下什么是信息安全、网络安全以及二者之间的关系。

信息安全(Information Security，InfoSec)自古以来就是人们关注的问题，但在不同时期，信息安全的侧重点和控制方式有所不同。信息安全是指信息的硬件、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、正常、可靠地运行，信息服务不中断。信息安全是一门涉及计算机技术、网络技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

在网络技术飞速发展的信息时代，网络是信息传输的载体，信息依靠网络进行传输。信息安全、网络安全、计算机安全等已没有明确的界限。本书所讨论的信息安全侧重指网络安全。

信息安全通常强调所谓 CIA 三元组的目标，即保密性、完整性和可用性。CIA 概念的阐述源自信息技术安全评估标准(Information Technology Security Evaluation Criteria，ITSEC)，它也是信息安全的基本要素和安全建设所应遵循的基本原则。后来，人们对 CIA 进行了扩展，加入了可控性、不可否认性等。

(1) 保密性(Confidentiality)——确保信息在存储、使用、传输过程中不会泄露给非授权用户或实体。

(2) 完整性(Integrity)——确保信息在存储、使用、传输过程中不会被非授权用户篡改，防止授权用户或实体不恰当地修改信息，保持信息内部和外部的一致性。

(3) 可用性(Availability)——确保授权用户或实体对信息及资源的正常使用不会被异常拒绝，允许其可靠而及时地访问信息及资源。

(4) 可控性(Controllability)——是否能够监控管理信息和系统，保证信息和信息系统的授权认证和监控管理。

(5) 不可否认性(Non-Repudiation)——为信息行为承担责任，保证信息行为人不能否认其信息行为。

1.1.2　网络安全的现状

伴随着网络的发展，也产生了各种各样的问题，其中安全问题尤为突出。了解网络面临的各种威胁，防范和消除这些威胁，实现真正的网络安全已经成为网络发展中最重要的事情。网络安全现状主要包括以下几方面。

1．黑客的攻击

黑客对于大家来说，已经不再高深莫测，黑客技术正逐渐被越来越多的人所掌握。目前，世界上有20多万个黑客网站，这些站点都介绍一些攻击方法和攻击软件的使用，并公布系统的一些漏洞，这就导致系统、站点遭受攻击的可能性变大了。尤其是现在还缺乏针对网络犯罪卓有成效的反击和跟踪手段，使得黑客攻击的隐蔽性好，“杀伤力”强，成为网络安全的主要威胁。

2．管理的欠缺

网络系统的严格管理是企业、机构及用户免受攻击的重要措施。事实上，很多企业、机构及用户的网站或系统都疏于这方面的管理。据IT界企业团体ITAA的调查显示，美国90%的IT企业对黑客攻击准备不足。目前，美国75%～85%的网站都抵挡不住黑客的攻击，约有75%的企业网上信息失窃，其中25%的企业因受黑客攻击而造成的损失每年在25万美元以上。

3．网络的缺陷

因特网的共享性和开放性使网上信息安全存在先天不足，因为其赖以生存的TCP/IP协议族缺乏相应的安全机制，而且因特网最初的设计考虑是该网站不会因局部故障而影响信息的传输，基本没有考虑安全问题。因此它在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

4．软件的漏洞或“后门”

随着软件系统规模的不断增大，更多的系统中的安全漏洞或“后门”被曝光，比如我们常用的操作系统，无论是Windows还是UNIX几乎都存在或多或少的安全漏洞，众多的各类服务器、浏览器、一些桌面软件等都被发现过存在安全隐患，大家熟悉的尼姆达、中国黑客等病毒都是利用微软系统的漏洞给企业造成了巨大损失。可以说任何一个软件系统都可能会因为程序员的一个疏忽、设计中的一个缺陷等原因而存在漏洞，这也是网络安全的主要威胁之一。

5．企业网络内部的安全攻击

网络内部用户的误操作、资源滥用和恶意行为等，使得再完善的防火墙也无法抵御来自网络内部的攻击，也无法对网络内部的滥用做出反应。

1.1.3　网络安全的发展趋势

2008年对网络安全行业而言并不是平静的一年。在这一年里，病毒的互联网化导致其数量剧增，网页挂马大行其道，种种漏洞层出不穷，各种Web 2.0应用和社交网站的兴起也带来了新的威胁。与此同时，“云安全”成为安全厂商们津津乐道的名词。

在未来几年内，可以预见这些趋势将持续下去，网络威胁形势并不会得到多少改善。此外，金融危机影响的进一步加深及一些新技术的应用，也给网络安全行业带来了变数。那么，网络安全行业将会呈现一些什么趋势呢?

1.“云安全”大势所趋

“云安全”无疑是 2008 年网络安全行业最热的关键词。安全威胁的演变直接推动了安全技术的发展，病毒的互联网化使得安全形势发生了根本性的改变，而“云安全”正是为了应对这一改变，安全软件互联网化的表现。

1) 什么是“云安全”

“云安全(Cloud Security)”计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常监测，获取互联网上木马、恶意程序的最新信息，推送到 Server 端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。

用一句话描述，“云安全”就是一个巨大的系统，它是杀毒软件互联网化的实际体现。互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。这样可以做到全民防御，绝杀木马。每个用户都为“云安全”计划贡献一份力量，同时分享其他所有用户的安全成果。

2) 瑞星“云安全”计划

瑞星“云安全”系统主要包括三个部分：超过一亿的客户端、智能型云安全服务器、数百家互联网重量级公司(瑞星的合作伙伴)，如图 1-1 所示。

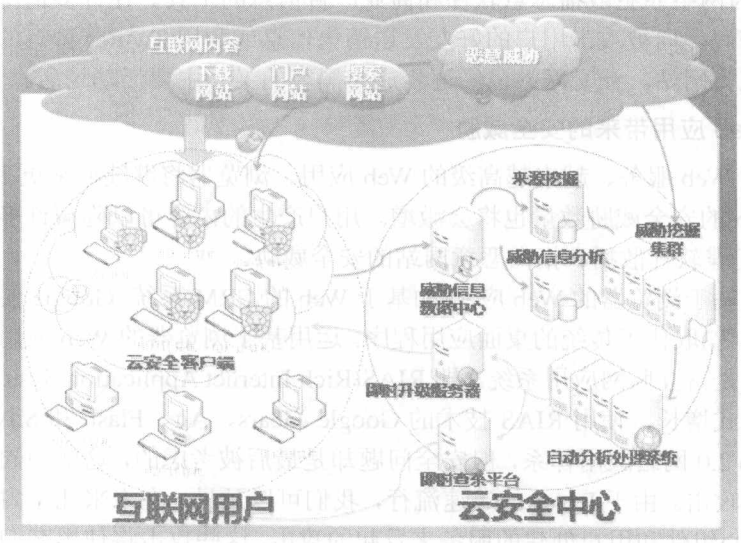

图 1-1　瑞星“云安全”系统

瑞星 2009、瑞星卡卡上网安全助手等软件中集成了“云安全探针”，用户电脑安装这些软件后就成为“云安全”的客户端。随着“云安全”的发展，包括迅雷、快车、巨人、久游等一批重量级厂商加入了瑞星“云安全”计划，他们旗下的软件中也加入了“云安全探针”功能，成为客户端。

用户安装的“云安全探针”能够感知电脑上的非安全信息，如异常的木马文件开始运行、木马对系统注册表关键位置的修改、用户访问的网页带病毒等，“探针”会把这些信息上传到“云安全”服务器，进行深入分析。

服务器进行分析后，把分析结果加入“云安全”系统，使“云安全”的所有客户端能够立刻防御这些威胁。对不同类型的威胁，有不同的处理方式。如果是新发现的木马病毒，则“云安全”服务器会将病毒的特征码送回中毒客户端，使用户能够及时查杀该病毒；如果发现的是“带毒网页”，则“云安全”系统会将网址发送给所有的合作伙伴，使搜索引擎、下载软件这样的公司能够在第一时间屏蔽这些网站，这样能够在最短时间内保证用户的安全。

3) 建立“云安全”系统的难点

要想建立“云安全”系统，并使之正常运行，需要解决四大问题：需要海量的客户端(云安全探针)、需要专业的反病毒技术和经验、需要大量的资金和技术投入、必须是开放的系统，而且需要大量合作伙伴的加入。

2. 社交网站成黑客关注焦点

随着社交网站的流行，这些网站已成为黑客关注的焦点。人们利用社交网站结识朋友，扩张人脉，而黑客则企图透过这些人脉散布恶意程序。目前，以窃取用户帐号信息为目的的钓鱼邮件，以及使用社交网站内容作为攻击载体的行为越来越多，黑客通过仿冒网页获取用户帐号或假借社交之名提高在线威胁的“成功率”。

2008 年 8 月，Facebook 有多达 1800 名用户的档案遭到秘密安装的木马程序的篡改。Twitter 同样成为网络罪犯散播恶意软件和商业广告信息的工具。在许多情况下，黑客盗取用户的帐号和密码，向被攻击用户的好友发送销售信息或利用 Twitter 特有的缩址服务，欺骗网友进入第三方网站。社交网站已经逐步成为黑客的又一主要活动场所。

3. 高级 Web 应用带来的安全威胁

越来越多的 Web 服务、越来越高级的 Web 应用、浏览器将继续迎来更多的脚本语言，而新的基于 Web 的安全威胁数量也将会激增。用户产生的内容可以隐藏许多来自浏览器漏洞、恶意软件/间谍软件散播和指向恶意网站的安全威胁。

越来越多的基于浏览器的 Web 应用(如基于 Web 的 CRM 系统、Google 文档和其他基于 Web 的办公工具等)取代了传统的桌面应用程序。运用基于浏览器的 Web 应用来丰富互联网使用体验的程序是富互联网应用系统，即 RIAS(Rich Internet Application System)。伴随这些应用需求的爆炸式增长，使用 RIAS 技术的 Google Gears、Air、Flash 和 Silverlight 构建了一个大型的 Web 2.0 网络应用体系，但安全问题却是最后被考虑的，这就如同敞开大门让网络犯罪分子肆意攻击。由于 RIAS 的迅速流行，我们可以预见，在未来几年内将会有大规模的利用 RIAS 核心组件和用户创建的服务来发起的攻击，这些攻击将使黑客们能够窃取用户的机密信息或者远程操控用户的电脑。

4. 虚拟机安全

随着服务器和台式机虚拟技术的日益普及，虚拟化技术对人们已不再陌生，它能帮助企业的数据中心大大提高利用率，节省大量的资源。在 2008 年，虚拟化战略已经被许多大

型企业和小型企业所接受并应用。在目前全球金融危机的形势下，高效节能的虚拟化技术将得到更广泛的应用。

可以预见，在网络安全方面，虚拟化技术将会整合到安全解决方案中，为用户提供独立于环境的解决方案，并且面对通用操作系统环境可能造成的混乱，可避免受到其所产生的影响。虚拟化技术将为银行业等敏感交易行业提供安全的环境，并保护安全组件等关键基础架构，从而实现通用操作系统的全面防护。

同时，虚拟化技术的应用将给人们带来另一个问题：如何保障虚拟机本身的安全。我们在基于角色的访问控制、虚拟服务器身份管理、虚拟网络安全、报告/审计等方面需要更好的安全工具。而黑客们要考虑的则是如何突破虚拟机的界限，至少当他们散布一个恶意程序时，这个恶意程序需要能够弄明白自己究竟是运行在一个虚拟的环境还是一个实际的环境中。

5. 手机安全

如今智能手机和移动互联网越来越普及，一部强大的智能手机的功能，并不逊于一部小型电脑，而这为黑客提供了一条新的攻击通道。随着手机的处理能力日益强大，互联网连接带宽越来越高，黑客将能够利用手机操作系统或 Web 应用软件中的安全缺陷，使手机病毒泛滥，而病毒所带来的危害也会越来越大。据统计，目前网络安全专家发现的手机病毒已经超过 500 种。

手机安全作为一个全新的话题越来越受到产业链各方的关注。目前已有很多反病毒软件厂商进入了手机安全市场，但由于产业链条尚未完全形成，手机安全问题还只停留在讨论阶段，有关的赢利模式也不清晰，这些成为阻碍行业发展的瓶颈。手机安全市场爆发的临界点仍未来临。

但在 2009 年，随着手机用户数量的不断攀升，智能手机，如苹果的 iPhone、基于谷歌 Android 操作系统的 G1 手机等的流行，还有 3G 手机的发展，手机的安全问题变得越来越重要，手机安全市场蕴藏的巨大商机已经逐渐显现。可以预见，手机安全将成为安全行业发展的一个全新增长点。

6. 更加关注软件安全性

在过去的几年内，各种软件漏洞层出不穷，而在这些漏洞中，应用软件漏洞更是占据了多数，给网络安全带来了严重的威胁。这些漏洞主要来自计算机用户平时经常使用的搜索引擎、网络视频软件、媒体播放器软件、网络游戏、网络下载工具和浏览器等，其中很多都是被广泛使用的应用软件。这些应用软件漏洞在病毒和木马的传播过程中被大量利用，一方面是由于这些软件用户众多，使得黑客有相当大的攻击目标；另一方面由于第三方软件厂商软件更新速度不够快，使得针对该种漏洞的恶意网页长时间在网上肆虐；再者是由于用户对第三方软件的安全更新意识比较低而导致安全威胁。

今后，恶意攻击将会更多地针对应用软件而非操作系统，这也将促使软件公司在进行软件开发时更加注重保障应用软件本身的安全，采用安全的软件开发规范，例如“开放 Web 应用安全项目”或“SANS 软件安全计划”。而对用户而言，也应当学会更加关注应用软件的安全性，更谨慎地去使用应用软件。

7. UTM 受企业热捧

作为企业网络边界安全防护的一体化解决方案，UTM(Unified Threat Management，统一威胁管理)在保障企业网络安全的同时又可大幅降低运行维护成本，受到很多企业尤其是中小企业的欢迎，一直以来发展迅速。

但是由于 UTM 性能瓶颈的存在，制约了其进一步发展。不过，随着多核技术的成熟，2008 年不少 UTM 厂商已经推出了万兆级的 UTM 产品，突破了性能瓶颈的限制，这无疑将使得今后 UTM 的应用得到进一步的普及。由于受金融危机的影响，可以预想不少企业 IT 预算将会进行紧缩。这种情况下，高性价比的 UTM 产品将成为企业采购安全设备时的首选，市场对 UTM 产品的需要将大幅提升。

8. 普遍加密

加密技术已经被“嵌入”在产品中，如磁带驱动器和富士通、日立、希捷的部分硬盘已经“嵌入”有加密处理器，英特尔将发布一款支持加密的 vPro 芯片组。今后还将出现多层加密技术。

9. 授权管理

认证技术使用户能够进入一个网络内，但授权管理系统则负责管理用户能做什么或不能做什么。

10. 金融危机对安全行业的影响

随着全球金融风暴、股市低迷以及银行业调整的不断加深，当前互联网经济犯罪出现了此消彼涨的新特点：传统的针对金融机构的钓鱼、恶意软件数量大幅度下降，而针对互联网应用的欺诈与攻击行为大幅度激增。越来越严重的金融危机对信息安全的影响进一步深入，并引发更多的网络犯罪。

金融危机本身成为了众多新型攻击利用的主要时机，网络犯罪者可能利用这次金融危机，对用户发起大规模的网络钓鱼攻击。那些遭受金融危机沉重打击而丢失工作的人，也可能会成为恶意分子的主要攻击对象。

1.2　网络面临的常见安全威胁

网络安全伴随着网络的产生而产生，有网络的地方就存在着网络安全隐患。像病毒入侵和黑客攻击之类的网络安全事件，目前主要是通过网络进行的，而且几乎每时每刻都在发生，遍及全球。网络安全事件所带来的危害，相信每个计算机用户都或多或少地亲身体验过一些，轻则可能使电脑系统运行不正常，重则可以使整个计算机系统中的磁盘数据全盘覆灭，甚至导致磁盘、计算机等硬件的损坏。对于个人来说所带来的损失可能还不足以令人重视，但对于企业用户来说，可能会是灭顶之灾。

为了防范这些网络安全事故的发生，每个计算机用户，特别是企业网络用户，必须采取足够的安全防范措施。当然，网络安全策略的实施是一个系统工程，涉及许多方面，既

要充分考虑到那些平时我们经常提及的外部网络威胁，又要对来自内部网络的安全隐患有足够的重视。

1.2.1　计算机病毒

1．计算机病毒的定义

计算机病毒的前身只不过是程序员闲来无事而编写的趣味程序，后来才发展出了诸如破坏文件、修改系统参数、干扰计算机正常工作等的恶性病毒。病毒的定义比较多，直至1994年2月18日，我国才正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》，在《条例》第二十八条中明确指出："计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。"此定义具有法律性和权威性。

2．计算机病毒的发展历程

计算机病毒的概念其实起源相当早，在第一部商用电脑出现之前，电脑的先驱者冯·诺伊曼(John Von Neumann)在他的一篇论文《复杂自动装置的理论及组织的进行》里，已经勾勒出病毒程序的蓝图。不过在当时，绝大部分的电脑专家都无法想像会有这种能自我繁殖的程序。

1975 年，美国科普作家约翰· 布鲁勒尔(John Brunner)写了一本名为《震荡波骑士》(Shock Wave Rider)的书。该书第一次描写了在信息社会中，计算机作为正义和邪恶双方斗争的工具的故事，成为当年最佳畅销书之一。

1977 年夏天，托马斯· 捷· 瑞安(Thomas.J.Ryan)的科幻小说《P-1 的春天》(The Adolescence of P-1)成为美国的畅销书。作者在这本书中描写了一种可以在计算机中互相传染的病毒，病毒最后控制了 7 000 台计算机，造成了一场灾难。虚拟科幻小说世界中的东西，在几年后逐渐开始成为电脑使用者的噩梦。

而差不多在同一时间，美国著名的 AT&T 贝尔实验室中，三个年轻人在工作之余，很无聊地玩起一种游戏：彼此撰写出能够吃掉别人程序的程序来互相作战。这个叫做"磁芯大战"(Core War)的游戏，进一步将电脑病毒"感染性"的概念体现出来。

1983 年 11 月 3 日，一位南加州大学的学生弗雷德·科恩(Fred Cohen)在 UNIX 系统下，写了一个会引起系统死机的程序，但是这个程序并未引起一些教授的注意与认同。科恩为了证明其理论而将这些程序以论文发表，在当时引起了不小的震撼。科恩的程序让电脑病毒具备破坏性的概念具体成形。

不过，这种具备感染与破坏性的程序被真正称之为"病毒"，则是在两年后的一本《科学美国人》的月刊中，一位叫做杜特尼(A.K.Dewdney)的专栏作家在讨论"磁芯大战"与苹果 II 型电脑时，把这种程序称之为"病毒"。

到了 1987 年，第一个电脑病毒 C-BRAIN 终于诞生了(这似乎不是一件值得庆贺的事)。一般而言，业界都公认这是真正具备完整特征的电脑病毒始祖。这个病毒程序是由一对巴基斯坦兄弟巴斯特(Basit)和阿姆捷特(Amjad)编写的。他们在当地经营一家贩卖个人电脑的商店，由于当地盗拷软件的风气非常盛行，因此他们的目的主要是为了防止他们的软件被

任意盗拷。只要有人盗拷他们的软件，C-BRAIN 就会发作，将盗拷者的硬盘剩余空间吃掉。这个病毒在当时并没有太大的杀伤力，但后来一些有心人士以 C-BRAIN 为基础，制作出了一些变形的病毒。而其他新的病毒创作也纷纷出笼，不仅有个人创作，甚至出现不少创作集团(如 NuKE，Phalcon/Skism,VDV)。各类扫毒、防毒与杀毒软件以及专业公司也纷纷出现。一时间，各种病毒(如“大麻”、“IBM 圣诞树”、“黑色星期五”等)创作与反病毒程序不断推陈出新。

1988 年 3 月 2 日，一种苹果机的病毒发作，这天受感染的苹果机停止工作，只显示“向所有苹果电脑的使用者宣布和平的信息”，以庆祝苹果机生日。

1988 年冬天，正在康乃尔大学攻读的莫里斯，把一个被称为“蠕虫”的电脑病毒送进了美国最大的电脑网络——互联网。1988 年 11 月 2 日下午 5 点，互联网的管理人员首次发现网络有不明入侵者。当晚，从美国东海岸到西海岸，互联网用户陷入一片恐慌。

1989 年全世界的计算机病毒攻击十分猖獗，我国也未能幸免。

1991 年在“海湾战争”中，美军第一次将计算机病毒用于实战。

1992 年出现针对杀毒软件的“幽灵”病毒，如 One-half。

1996 年首次出现针对微软公司 Office 的“宏病毒”。

1997 年被公认为计算机反病毒界的“宏病毒”年。

1999 年 4 月 26 日，CIH 病毒在全球范围大规模爆发，造成近 6000 万台电脑瘫痪(该病毒产生于 1998 年)。

1999 年 Happy 99 等完全通过 Internet 传播的病毒的出现标志着 Internet 病毒将成为病毒新的增长点。

2001 年 7 月中旬，一种名为“红色代码”的病毒在美国大面积蔓延，这个专门攻击服务器的病毒攻击了白宫网站，造成了全世界恐慌。

2003 年，“2003 蠕虫王”病毒在亚洲、美洲、澳大利亚等地迅速传播，造成了全球性的网络灾害。

2004 年是蠕虫泛滥的一年，流行蠕虫病毒有网络天空(Worm.Netsky)、高波(Worm.Agobot)、爱情后门(Worm.Lovgate)、震荡波(Worm.Sasser)、SCO 炸弹(Worm.Novarg)、冲击波(Worm.Blaster)、恶鹰(Worm.Bbeagle)、小邮差(Worm.Mimail)、求职信(Worm.Klez)、大无极(Worm.SoBig)等。

3. 近几年计算机病毒基本情况分析

据中国电脑病毒疫情及互联网安全报告，2008 年中国新增计算机病毒、木马数量呈爆炸式增长，总数量已突破千万。病毒制造的模块化、专业化以及病毒“运营”模式的互联网化成为 2008 年中国计算机病毒发展的三大显著特征。同时，病毒制造者的“逐利性”依旧没有改变，网页挂马、漏洞攻击成为黑客获利的主要渠道。

据金山毒霸“云安全”中心监测数据显示，2008 年，全国共有 69 738 785 台计算机感染病毒，与 2007 年相比增长了 40%。新增计算机病毒、木马数量呈几何级增长，2008 年金山毒霸共截获新增病毒、木马 13 899 717 个，与 2007 年相比增长 48 倍。其中，网页脚本所占比例从 2007 年的 0.8%跃升至 5.96%，成为增长速度最快的一类病毒。90%的病毒依附网页感染用户。图 1-2 为近几年来的新增病毒、木马数量对比。