21世纪全国高校应用人才培养网络技术类规划教材

WANGLUO ANQUAN JISHU JI YINGYONG

# 网络安全技术及应用

马国富 主编

Network
Tech

北京大学出版社
PEKING UNIVERSITY PRESS

21 世纪全国高校应用人才培养网络技术类规划教材

# 网络安全技术及应用

主　编：马国富
副主编：齐　林　王子贤
黄仁书　姜伯东

北京大学出版社
PEKING UNIVERSITY PRESS

# 内 容 简 介

本书以网络安全技术为主线，以实际网络安全应用为重点，将近年来国内外的网络安全技术研究成果应用于解决日常生活、工作中遇到的网络安全问题。全面介绍了网络安全的保障体系及相关法规、网络安全中常用的操作系统命令、网络安全体系及协议基础、密码学基础与 PKI、网络安全协议、网络攻击技术、恶意软件、防火墙技术、入侵检测与入侵防御技术、Windows 安全技术、网络站点安全、网络设备安全及网络安全管理技术等。重点介绍了数据安全、内容安全、行为安全、设备安全，从而实现网络中的数据存储安全和传输安全，保证网络安全的保密性、完整性、可用性、不可抵赖性、可控性 5 个特征的实现。

本书在编写过程中，参考了教育部高等学校信息安全类专业教学指导委员会编写的《信息安全类专业指导性专业规范》（第三次征求意见稿），同时，以网络安全技术技能训练为目标确定了具有典型性的技能实验、案例分析、练习测试等项目，较好地处理了理论教学与技能训练的关系；力求做到：教学内容任务化，教学方法案例化、实战化；教学活动学生主体化。

本书既可以作为信息安全、计算机、信息类、电子商务和管理类专业网络安全课程的教材，也可以供网络安全、计算机网络管理人员阅读参考学习。

**图书在版编目（CIP）数据**

网络安全技术及应用/马国富主编. —北京：北京大学出版社，2010.11
（21 世纪全国高校应用人才培养网络技术类规划教材）
ISBN 978-7-301-17659-7

Ⅰ. ①网… Ⅱ. ①马… Ⅲ. ①计算机网络—安全技术—高等学校—教材 Ⅳ. ①TP393.08
中国版本图书馆 CIP 数据核字（2010）第 161241 号

**书　　名**：网络安全技术及应用
**著作责任者**：马国富　主编
**策 划 编 辑**：吴坤娟
**责 任 编 辑**：吴坤娟
**标 准 书 号**：ISBN 978-7-301-17659-7/TP · 1125
**出 版 者**：北京大学出版社
**地　　址**：北京市海淀区成府路 205 号　100871
**网　　址**：http://www.pup.cn
**电　　话**：邮购部 62752015　发行部 62750672　编辑部 62756923　出版部 62754962
**电 子 信 箱**：zyjy@pup.cn
**印 刷 者**：河北滦县鑫华书刊印刷厂
**发 行 者**：北京大学出版社
**经 销 者**：新华书店
787 毫米 × 1092 毫米　16 开本　25.5 印张　557 千字
2010 年 11 月第 1 版　2010 年 11 月第 1 次印刷
**定　　价**：45.00 元

# 前　言

进入21世纪，随着互联网的普及与应用，政府部门、军事部门、金融机构、企事业单位和商业组织对网络的依赖程度日益加深，计算机网络几乎渗透到人们日常工作与生活的方方面面。与此同时，黑客利用网络漏洞进行攻击破坏网络的正常运行、传播病毒和木马等恶意软件、控制他人计算机和网络、篡改网页、窃取和破坏计算机上的重要信息，计算机网络安全已成为国家安全、经济发展、社会稳定的重大战略课题，也越来越引起世界各国的关注，出现强劲发展态势。

网络安全技术及应用是一门理论与实际操作紧密结合、知识与技能并重的课程。本教材的编写，以培养应用型人才为目标，把网络安全技术与实际应用相结合，从实用角度对网络安全技术进行了介绍。以网络安全技术技能训练为目标确定具有典型性的技能实验、案例分析、练习测试等项目，较好地处理了理论教学与技能训练的关系；力求做到：教学内容任务化，教学方法案例化、实战化；教学活动学生主体化。具体有以下几个特点。

第一，系统性。

本书以网络安全技术为主线，全面介绍了网络安全常用的网络命令、网络安全所需要的基础知识、网络攻击与防范、网络设备安全和网络安全管理，在内容安排上将理论知识和实际应用有机结合。

第二，注重先进性和实用性。

介绍目前国内外先进的、通用的网络安全新技术，并对主流的操作系统和常用的硬件设备安全进行了介绍，注重科学性、先进性、操作性。坚持“实用、特色、规范”的原则，突出实用及学生素质能力的培养。

第三，实践性。

本书介绍了网络安全中用到网络命令，并给出了具体的操作步骤和应用场景；通过在主流操作系统上部署PKI使学生掌握公钥加密技术和认证技术；同时将经常遇到的恶意软件、网络攻击与防范技术、Windows安全问题、网络设备安全问题进行了案例分析。

第四，注重实验环节。

为了加强学生的实践动手能力，根据章节内容，适当安排了学生实验、实践操作内容。同时还增加了大量的案例分析及有关研究成果，每章课后都有练习题，供学生练习测试。

第五，注重创新能力培养。

本教材根据用人单位及信息安全专业对网络信息安全人才的能力要求，注重启发学生创新思维，为学生快速适应用人单位需求做好准备。

第六，专业性。

教材编写组成员全部来自高等院校的信息安全专职老师，有丰富的专业知识和教学经验。全书由马国富担任主编，并负责拟定编写提纲、通稿、定稿和主审，齐林、王子贤、黄仁书、姜伯东担任副主编。具体分工是：马国富（第1、2、4、8、10章），齐林（第5、6章），王子贤（第9、11、12章），黄仁书（第7、13章），姜伯东（第3章）。

本教材在编写过程中，参阅了大量中外有关网络安全方面的教材和文献资料，在此谨向这些教材和文献资料的著者、译者、编者表示衷心的感谢。

由于编写时间仓促，编者水平有限，书中疏漏之处在所难免，恳请同行专家批评指正！

为方便教师教学，本书还配有电子教案。

中央司法警官学院　马国富

2010 年 10 月

# 目 录

# 第 1 章　网络安全概述

自 20 世纪 90 年代以来，以因特网（Internet）为代表的计算机网络在全球呈爆炸式增长，计算机网络已经逐步渗透到各行各业，并与人们日常生活越来越贴近。随着技术的发展，电信网络、有线电视网络逐渐融入计算机网络中，正在实现“三网融合”。21 世纪的一些重要特征就是数字化、网络化和信息化，而计算机网络是基础，处于核心地位。计算机网络已经成为一个国家社会发展的命脉和重要基础。

随着计算机网络应用的广泛普及，所承载的业务和信息逐步多样化，计算机网络在国家政治、经济、文化领域以及社会生活的各个方面发挥着愈加重要的作用，已经成为国家、社会、民众交互的重要平台。与此同时，计算机网络面临的安全威胁也随着计算机网络及其应用的发展而不断演化，呈现日益复杂的局面，网络与信息安全问题已成为计算机网络不可避免的问题。国家计算机网络应急技术处理协调中心于 2009 年 4 月 26 日发布了《2008 年中国互联网网络安全报告》，统计显示垃圾邮件、网络仿冒、网页篡改、网页恶意代码、拒绝服务攻击、病毒、蠕虫和木马等事件出现较大幅度的增长，由此造成的后果和影响也较为严重，如遭遇网络欺骗或讹诈、感染恶意代码、泄露重要信息等。网络信息系统安全漏洞的频发是引发重大网络安全事件并造成大范围影响的主要原因之一，是影响网络安全的重要因素，而罕见的“0day”漏洞攻击使得网络安全形势进一步恶化。

据国家互联网应急中心（CNCERT）自主监测结果显示，2006—2008 年，恶意代码捕获次数和恶意代码新样本捕获次数呈不断上升趋势。恶意代码成为黑客推进攻击活动的主要武器和弹药，并可通过垃圾邮件、网页挂马、即时聊天工具、系统漏洞等多种方式传播和扩散。恶意代码已经不仅仅是黑客手中的玩具，目前，围绕恶意代码，尤其是网络病毒的生产、销售、传播等环节，已经形成了规模庞大、收益巨大的黑色地下产业链。相关统计数据显示，2008 年我国网络安全服务市场规模已经超过 80 亿元人民币，这也从侧面凸显出社会各界为对抗黑色地下产业而不得不付出的巨大投入。但从实际效果看，由于缺乏必要的以及联合一致的行动，防护方仍然处在被动和不利的地位。这些情况的出现对网络安全提出了更高的要求，而如何保障网络安全已成为一个急需解决的问题。

## 1.1　网络安全的基本概念

### 1.1.1　网络安全的定义

网络安全是一门涉及计算机科学、网络技术、通信技术、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。国际标准化组织（ISO）对计算机系统安全的定义是：为数据处理系统建立和采用的技术和管理的安全保护，保护计算机硬件、软件和数据不因偶然和恶意的原因遭到破坏、更改和泄露。网络安全的具体含义会随着“角度”的变化而变化。比如：从用户（个人、企业等）的角度来说，他们希望涉及

个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，同时也避免其他用户的非授权访问和破坏；从网络运行和管理者角度来说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击；对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害、对国家造成巨大损失；从社会教育和意识形态角度来说；网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

网络安全是指网络系统的硬件、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，系统连续可靠正常地运行，网络服务不中断。从本质上来说，网络安全就是网络上的信息安全；从广义上来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题，也有管理方面的问题，两方面相互补充，缺一不可。技术方面主要侧重于防范非法的攻击，管理方面则侧重于人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性已经成为所有计算机网络应用必须考虑和必须解决的一个重要问题。

1. 不同环境和应用中的网络安全

（1）运行系统安全。

运行系统安全即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电磁泄漏而产生信息泄露、干扰他人、受他人干扰。

（2）网络上系统信息的安全。

网络上系统信息的安全包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密。

（3）网络上信息传播安全。

网络上信息传播安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播后的后果。避免公用网络上大量自由传输的信息失控。

（4）网络上信息内容的安全。

网络上信息内容的安全侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

2. 不同位置上的网络安全

（1）外网安全。

外网安全主要防范外部入侵或者外部非法流量访问，技术上也以防火墙、入侵检测等防御角度出发的技术为主。

（2）内网安全。

内网在安全管理上比外网要细得多，同时技术上内网安全通常采用的是加固技术，比

如设置访问控制、身份管理等。从调查情况看，在所有的安全事件中，有超过70%是发生在内网上的，随着网络的庞大化和复杂化，这一比例仍有增长趋势，内网安全面临着前所未有的挑战。与外网安全的被动防御不同，内网安全应该从人、技术、流程三个方面主动加固，才能有效地保护内网上运行的核心业务的安全。

### 1.1.2 网络安全的属性

美国国家信息基础设施（NII）提出了5个属性：保密性、完整性、可靠性、可用性、不可抵赖性。在美国信息保障技术框架（IATF）基础上我们把网络安全特性分为6个属性。

（1）可靠性。

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是网络安全的最基本要求之一，是所有网络信息系统的建设和运行目标。网络信息系统的可靠性测度主要有三种：抗毁性、生存性和有效性。

抗毁性是指系统在人为破坏下的可靠性。比如，部分线路或节点失效后，系统是否仍然能够提供一定程度的服务。增强抗毁性可以有效地避免因各种灾害（战争、地震等）造成的大面积瘫痪事件。

生存性是在随机破坏下系统的可靠性。生存性主要反映随机性破坏和网络拓扑结构对系统可靠性的影响。这里，随机性破坏是指系统部件因为自然老化等造成的自然失效。

有效性是一种基于业务性能的可靠性。有效性主要反映在网络信息系统的部件失效情况下，满足业务性能要求的程度。比如，网络部件失效虽然没有引起连接性故障，但是却造成质量指标下降、平均延时增加、线路阻塞等现象。

可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面；硬件可靠性最为直观和常见；软件可靠性是指在规定的时间内，程序成功运行的概率；人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色，因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响，受到其技术熟练程度、责任心和品德等素质方面的影响。因此，人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内，保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

（2）可用性。

可用性是网络信息可被授权实体访问并按需求使用的特性，即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。网络信息系统最基本的功能是向用户提供服务，而用户的需求是随机的、多方面的，有时还有时间要求。可用性是网络信息系统面向用户的安全性能，一般用系统正常使用时间和整个工作时间之比来度量。

可用性还应该满足以下要求：身份识别与确认；访问控制（对用户的权限进行控制，只能访问相应权限的资源，防止或限制经隐蔽通道的非法访问，包括自主访问控制和强制访问控制）；业务流控制（利用均分负荷方法，防止业务流量过度集中而引起网络阻塞）；路由选择控制（选择那些稳定可靠的子网、中继线或链路等）；审计跟踪（把网络信息系统中发生的所有安全事件情况存储在安全审计跟踪之中，以便分析原因，分清责任，及时

采取相应的措施。审计跟踪的信息主要包括事件类型、被管客体等级、事件时间、事件信息、事件回答以及事件统计等方面的信息）。

（3）保密性。

保密性是网络信息不被泄露给非授权的用户、实体或进程，不被其利用的特性，即防止信息泄漏给非授权个人或实体，信息只为授权用户使用的特性。网络的保密性包括网络传输过程中的保密性和在网络系统存储时的保密性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

常用的保密技术包括：防监听（使对手监听不到有用的信息）；防辐射（防止有用信息以各种途径辐射出去）；信息加密（在密钥的控制下，用加密算法对信息进行加密处理，即使对手得到了加密后的信息也会因为没有密钥而无法读懂有效信息）；物理保密（利用各种物理方法，如限制、隔离、掩蔽、控制等措施，保护信息不被泄露）。

（4）完整性。

完整性是网络信息未经授权不能进行改变的特性，即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障；误码（传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码）；人为攻击；计算机病毒等。

保障网络信息完整性的主要方法有以下几种。

- 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。
- 纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。
- 密码校验和方法：它是抗篡改和传输失败的重要手段。
- 数字签名：保障信息的真实性。
- 公证：请求网络管理或中介机构证明信息的真实性。

（5）不可抵赖性。

不可抵赖性也称作不可否认性，在网络信息系统的信息交互过程中，确信通信双方的真实同一性，即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息，利用递交接收证据可以防止收信方事后否认已经接收的信息。

（6）可控性。

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说，网络信息安全的核心是通过计算机、网络、密码技术和安全技术，保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、可控性、可靠性、可用性、不可抵赖性等。

## 1.2 网络安全面临的威胁

### 1.2.1 网络安全威胁的定义及分类

网络安全威胁是指某个实体对某一网络资源的可靠性、可用性、保密性、完整性、可控性、不可抵赖性等造成的破坏。网络安全威胁来自多方面，从攻击对象来看，网络安全威胁分为人为威胁和非人为威胁。例如黑客攻击、非授权访问、信息监听等属于人为威胁，而来自水灾、火灾、地震、意外事故、电磁辐射等属于非人为威胁等。从攻击的方式来看，分为被动威胁和主动威胁，被动威胁只对信息进行监听，而不对其进行修改和破坏，攻击者截获、窃取通信信息，损害信息的保密性；主动威胁则对信息进行篡改和破坏，使授权用户得不到可用信息，破坏信息的完整性和可用性，即造成网络通信中断、通信内容破坏甚至系统无法正常运行等较严重后果的攻击行为。

### 1.2.2 物理威胁

物理安全是指用于保护计算机硬件、网络设备、存储介质及其信息的硬件装置和工作程序。常见的物理威胁有偷窃、废物搜寻、间谍等。

（1）偷窃。

网络信息安全中的偷窃包括设备偷窃、信息偷窃和服务偷窃等。偷窃攻击比网络攻击更直接，造成的损失往往可能数倍于被偷设备的价值，必须采取严格的防范措施以确保不被入侵者偷窃。最近几年内部员工偷窃敏感信息，出售给商业竞争对手的网络安全事件呈上升趋势。

（2）废物搜寻。

废物搜寻是指在被扔掉的打印材料、废弃的光盘和硬盘等存储介质中搜寻所需要的信息。目前大部分单位都已开始使用粉碎机来处理打印材料，而存储介质由于数据恢复技术发展，是物理威胁中需要重点关注的内容。

（3）间谍。

间谍行为是为了获取有价值的保密信息，采用不道德的手段获取信息的一种行为。一些商业机构为了击败对手采取任何不道德的手段，有时政府也有可能卷入这种间谍活动中。职场心理谍战小说《监控》中的一些行为可能就是现实的真实写照。

### 1.2.3 漏洞威胁

（1）不安全的服务。

系统漏洞也称为陷阱，它通常是由操作系统或应用程序的开发者有意或无意造成的，这些问题可能导致一些服务程序绕过安全系统，从而对网络系统造成损失。

（2）配置和初始化错误。

由于网络系统的默认配置及初始化造成的系统漏洞往往被人们所忽略，同时服务器的关闭或重新启动使得如果没有正确的初始化，就会留下安全漏洞而被人利用。类似的问题

在恶意软件修改了安全程序后及系统的安全配置文件时也会发生。

### 1.2.4 身份鉴别威胁

（1）口令圈套。

口令圈套是网络安全的一种诡计，通过编写一个代码模块模拟正常的系统登录界面，并把它插入到正常的登录过程之前，当最终用户输入了用户名和密码后，该口令圈套模块就会写入到数据文件中以备使用，而后显示登录失败，用户被迫再次输入登录信息，这样用户就不容易发现该圈套。

（2）口令破解。

口令破解是通过使用密码字典或其他工具软件来破解口令，有时由于口令设定的过于简单或口令验证系统所使用的算法考虑不周也会被利用。

### 1.2.5 恶意软件威胁

（1）计算机病毒。

1994 年 2 月 18 日，我国正式颁布实施了《中华人民共和国计算机信息系统安全保护条例》。在该条例的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。"

这个定义具有法律性、权威性。根据这个定义，计算机病毒是一种计算机程序，它不仅能破坏计算机系统，而且还能够传染到其他系统。计算机病毒通常隐藏在其他正常程序中，能生成自身的拷贝并将其插入其他的程序中，对计算机系统进行恶意的破坏。

计算机病毒不是天然存在的，是某些人利用计算机软、硬件所固有的脆弱性，编制的具有破坏功能的程序。计算机病毒能通过某种途径潜伏在计算机存储介质（或程序）里，当达到某种条件时即被激活，它用修改其他程序的方法将自己的精确拷贝或者可能演化的形式放入其他程序中，从而感染它们，对计算机资源进行破坏的这样一组程序或指令集合。

（2）蠕虫。

蠕虫（Worm）也可以算是病毒中的一种，但是它与普通病毒之间有着很大的区别。一般认为蠕虫是一种通过网络传播的恶性病毒，它具有病毒的一些共性，如传播性、隐蔽性、破坏性等，同时具有自己的一些特征，如不利用文件寄生（有的只存在于内存中），对网络造成拒绝服务，以及和黑客技术相结合等。普通病毒需要传播受感染的驻留文件来进行复制，而蠕虫不使用驻留文件即可在系统之间进行自我复制，普通病毒的传染能力主要是针对计算机内的文件系统而言，而蠕虫病毒的传染目标是互联网内的所有计算机。它能控制计算机上可以传输文件或信息的功能，一旦系统感染蠕虫，蠕虫即可自行传播，将自己从一台计算机复制到另一台计算机，更危险的是，它还可大量复制。因而在破坏性上，蠕虫病毒也不是普通病毒所能比拟的，网络的发展使得蠕虫可以在短短的时间内蔓延整个网络，造成网络瘫痪。局域网条件下的共享文件夹、电子邮件 E-mail、网络中的恶意网页、大量存在着漏洞的服务器等，都成为蠕虫传播的良好途径，蠕虫病毒可以在几个小

时内蔓延全球，而且蠕虫的主动攻击性和突然爆发性会使人们手足无措。此外，蠕虫会消耗内存或网络带宽，从而可能导致计算机崩溃，而且它的传播不必通过“宿主”程序或文件，因此可潜入系统并允许其他人远程控制计算机，这也使它的危害远较普通病毒更大。典型的蠕虫病毒有尼姆达、震荡波等。

（3）特洛伊木马

特洛伊木马（Trojan Horse），是指一种隐藏了一些恶意代码的程序，它可在用户不知情的情况下实现对用户计算机的远程控制、窃取用户密码和信息。特洛伊木马同病毒和蠕虫是不同的概念，因为特洛伊木马一般不复制自身，它是一种攻击计算机系统的方法，典型的方法是提供一个包含具有攻击性隐含代码的有用程序给用户，在用户执行该程序的时候，其隐含的代码对系统进行非法访问，并可能产生破坏。

特洛伊木马是一种恶意程序，它们悄悄地在宿主机器上运行，在用户毫无察觉的情况下，让攻击者获得了远程访问和控制系统的权限。一般而言，大多数特洛伊木马都模仿一些正规的远程控制软件的功能，如 Symantec 的 PC Anywhere，但特洛伊木马也有一些明显的特点，例如它的安装和操作都是在隐蔽之中完成的。攻击者经常把特洛伊木马隐藏在一些游戏或小软件之中，诱使粗心的用户在自己的机器上运行。最常见的情况是，上当的用户要么从不正规的网站下载和运行了带恶意代码的软件，要么不小心点击了带恶意代码的邮件附件。

### 1.2.6 网络威胁

（1）网络监听。

网络监听是指在网络通信过程中对传输的网络信息进行截获，然后进行数据分析、获取信息的过程。在网络上，监听效果最好的地方是在网关、路由器、防火墙一类的设备处。能不能监听不在同一个网段计算机传输的信息？答案是否定的，一台计算机只能监听经过自己网络接口的那些信息包。现实生活中黑客往往潜入一台不引人注意的计算机中，悄悄地运行一个监听程序来监听同一个网络中的信息。

（2）网络冒充。

网络冒充是通过使用非授权的密码和账号访问网络及其数据、程序的使用能力。一般需要内部人员配合才能完成。

（3）网络钓鱼。

网络钓鱼（Phishing）是指攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息。

网络威胁是相对于环境和事件而言的，它们可以通过对数据进行泄露、更改和破坏来对一个机构造成危害。威胁可能是无意的，如人为失误、软硬件失效和自然灾害等，也可能是恶意的。但威胁的存在并不意味着造成真正的危害，威胁是机会主义的，及时发现并采取措施是可以避免危害的。

## 1.3 网络安全现状及发展趋势

### 1.3.1 网络安全现状

随着计算机和通信技术的发展，网络信息的安全和保密已成为一个至关重要且亟需解决的问题。计算机网络所具有的开放性、互连性和共享性等特征使网上信息安全存在着先天不足，再加上系统软件中的安全漏洞以及所欠缺的严格管理，致使网络易受攻击，因此网络安全所采取的措施应能全方位地针对各种不同的威胁，保障网络信息的保密性、完整性、可靠性、可用性和不可抵赖性。

我国内地感染木马和僵尸网络的主机数量巨大，造成木马和僵尸网络产生和扩散的一大途径是恶意代码的肆虐传播。另外，信息系统软件的安全漏洞仍是各种安全威胁的主要根源，但层出不穷的应用软件安全漏洞的威胁也越来越大。同时，针对漏洞出现的攻击程序、代码也呈现出目的性强、时效性高的趋势。

综合分析以上情况，当前网络安全形势严峻的原因主要有以下几个：一是由于近年来中国互联网持续快速发展，我国网民数量、宽带用户数量、.cn 域名数量都已经跃居全球第一位，而我国网络安全基础设施建设、民众的网络安全意识培养还跟不上互联网发展的步伐，庞大的用户群、信息系统群加之粗放式网络安全管理埋下了安全隐患；二是随着技术的不断提高，攻击工具日益专业化、易用化，攻击方法也越来越复杂、隐蔽，防护难度较大；三是互联网业务与现实社会中诸如货币、交易、信息交互等活动不断融合，为网络世界的虚拟要素附加了实际价值，越来越多的承载这类业务的信息系统成为黑客攻击的目标。

### 1.3.2 网络安全发展趋势

未来几年，更多的安全问题会逐渐涌现，越来越多的新型安全威胁将得到前所未有的快速发展。

（1）垃圾邮件和网络欺骗将立足“社交网络”。

安全专家认为，恶意软件作者将进一步拓展攻击范围，把恶意软件植入到社交网站应用内部。有了这种病毒，无论用户是否访问社交网站，黑客都能毫无限制地窃取用户的资料和登录密码。

思科在其2009年《年度安全报告》中揭示了社交媒体（尤其是社交网络）对网络安全的影响，并探讨了人（而非技术）在为网络犯罪创造机会方面所起的关键作用。社交网络已经迅速成为网络犯罪的温床，因为这些网站的成员过于信任他们社区的其他成员，没有采取阻止恶意软件和计算机病毒的预防措施。小漏洞、不良用户行为以及过期的安全软件结合在一起会具有潜在的破坏性，可能大幅增加网络安全的风险。

（2）云计算成为孕育黑客新的温床。

我们必须意识到，市场的快速发展会牺牲一定的安全性。攻击者今后将把更多的时间用于挖掘云计算服务提供商的 API（应用编程接口）漏洞。

毋庸置疑，已经开始有越来越多的 IT 功能通过云计算来提供，网络犯罪也顺应了这一趋势。安全厂商 Fortinet 预计，网络犯罪借鉴服务即安全（Security As A Service，SAAS）的理念，打造服务即网络犯罪（Cybercrime As A Service，CAAS）这一特殊品牌。网络犯罪也将效仿企业的做法使用基于云计算的工具，以便更有效率地部署远程攻击，甚至借此大幅拓展攻击范围。

对于云计算将被黑客所利用这个严峻的问题，各大安全公司和技术人员会把精力放在与云计算相关的安全服务上，提供加密、目录和管理、反垃圾邮件、恶意程序等各种解决方案。据悉，著名安全评测机构 VB100 号召安全行业应该联合起来，组成一个对抗恶意程序的共同体，分享技术和资源。

（3）大量 Mac 计算机被病毒感染或黑客入侵。

经济危机非但没有伤害到苹果的利益，反而使其业绩进一步提升。但安全专家表示，在市场份额提升的同时，Mac 也要面临更多的黑客攻击。过去几年间，苹果的 PC 市场份额已经从 10% 增长到 12%，而且没有放缓的迹象。与此同时，在售价高于 1000 美元的笔记本电脑中，苹果更是占据了 90% 的份额，但针对 iPhone（手机上网）和 MacBook 的攻击也逐步引发外界关注。安全专家预计，Mac 有可能会成为下一个最易受攻击的目标。尽管多数攻击都瞄准 Windows，但未来将会出现更多针对 Mac OS X 的攻击。

（4）智能手机安全问题愈发严重。

随着移动应用的不断增多，智能设备的受攻击面也在不断扩大，移动安全所面临的局面将会越来越严重。

卡巴斯基实验室恶意软件高级研究员罗伊尔·文伯格（Roel Schouwenberg）说："Android 手机的日益流行，加之缺乏对第三方应用安全性的有效控制，将导致诸多高调恶意软件的出现。"总体而言，安全专家认为，随着用户将智能手机作为迷你 PC 来处理银行交易、游戏、社交网站和其他的业务，黑客将越发关注这一平台。

（5）搜索引擎成为黑客全新赢利方式。

黑客会不断寻找新的方法借助钓鱼网站吸引用户上钩，利用搜索引擎优化技术展开攻击便是其中的一种方法。谷歌和必应（Bing）对实时搜索的支持也将吸引黑客进一步提升相关技术。作为一种攻击渠道，搜索引擎是非常理想的选择，因为用户通常都非常信任搜索引擎，对于排在前几位的搜索结果更是没有任何怀疑，这就给了黑客可乘之机，从而对用户发动攻击。

（6）虚拟化普及安全威胁适应潮流。

与云计算类似的是，虚拟化技术也将抓住快速发展的时机。业界中已经有公司开始研究传统桌面电脑的虚拟化。虚拟化不仅能提供一种极高的安全保障，还能方便协作，提高效率。

除了瘦客户机的虚拟桌面以外，企业还将会开始考察笔记本电脑虚拟机以作为创建安全企业桌面的手段之一。虚拟机可利用快照迅速恢复到已知的安全状态配置，从而为网上银行或安全的企业应用提供更高等级的安全保障。工作和休闲可以在同一硬件上共存，只要相互保持隔离就行。

（7）"僵尸网络"继续扮演攻击者角色。

2009 年是重要恶意软件和在线恶意活动年份，原因很多，而其中数个都和 Botnet 僵尸/

傀儡网络有关。一个僵尸，或一个宿主，指的是受恶意软件感染而遭犯罪分子从远程操控的个人计算机。当犯罪分子运作网络时，受操控的感染计算机有上万到上千万台不等，犯罪分子们使用这些计算机来增强现今常见的网络犯罪功能，如垃圾邮件散发、服务阻断式攻击、恐吓软件、网络钓鱼及恶意或非法的主机网站等，涉及了网络犯罪的所有项目。愈来愈多的计算机受到感染，而被感染的时间也愈来愈长了。

从现在开始对于僵尸网络而言将是新的开始，在云计算的孕育下僵尸网络将大行其道，开始“云计算僵尸时代”！

（8）Windows 7 挑战“后 XP”时代安全问题。

相对于 Windows XP 而言，Windows 7 的确更加安全，也的确可以提升整体的安全水平。但正因如此，才使得那些仍然使用 Windows XP 的用户更容易受到攻击。黑客们将会重点攻击那些仍然使用 XP 的用户。与此同时，随着 Windows 7 的市场份额增长，黑客也将对其发动更多的攻击。

安全厂商 ESET 技术教育总监兰迪·卜拉姆斯（Randy Abrams）说：“除了上网本外，多数搭配 Windows XP 的电脑都开始老化，并且逐步被预装 Windows 7 的电脑所取代。对多数黑客而言，Windows 7 较高的安全性能意味着，欺骗用户比寻找系统安全漏洞更为可行。”

（9）通过更多的法规制约“安全危机”。

安然的财务丑闻给了我们萨班斯法案（SOX）。那么数百家安然的出现会给我们带来什么？法规遵从的数学是令人震惊的，因为这是一场“信息不对称的战争”。多起司法案例可能导致数十亿美元的政府支出。

RSA，EMC 信息安全事业部全球产品管理与策略副总裁 Sam Curry 表示，“法规遵从是一种催化剂，这种催化剂是加速推动企业内部的这种变化的发生或者叫变革的发生。其实人们是不喜欢变革的，但是现在有了法规遵从，人们必须去变化，使得大家离开了以前觉得非常舒服的小角落。”

（10）传统攻击方式再度兴起。

这似乎是一个轮回，安全专家预计，今后将有很多旧的攻击方式重新开始流行。IBM X-Force 团队预计，大规模的蠕虫攻击将再度兴起，与此同时，DDoS（分布式拒绝服务攻击）也将重新成为主流攻击方式。木马仍将占据主要地位。

另外，Websense 的卢纳德预计，电子邮件攻击也有重新抬头之势。他表示，研究人员已经发现，通过 PDF 等电子邮件附件发动的攻击开始增加。

## 1.4 网络安全保障体系与相关法规

### 1.4.1 网络安全保障体系

1998 年美国国家安全局（NSA）制定了《信息保障技术框架》（IATF），提出了“深度防御策略”，确定了包括网络与基础设施防御、区域边界防御、计算环境防御和支撑性基础设施的深度防御目标。2004 年 1 月，美国成立了“全国信息保障委员会”、“全国信息保障同盟”和“关键基础设施保障办公室”等 10 多个全国性机构。“9·11”事件后，