教育部师资实践基地系列教材——信息与网络安全

神州数码网络安全岗位&认证系列

网络安全高级工程师

WANGLUO ANQUAN GAOJI GONGCHENGSHI

程庆梅　徐雪鹏　主编

全国职业技能大赛推荐参考书

神州数码网络安全岗位&认证指定教材

校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

配电子课件

教育部师资实践基地系列教材——信息与网络安全

网络安全高级工程师

主　编　程庆梅　徐雪鹏

副主编　杜婉琛

参　编　李东方　王　岳　王　博　郭　薇　田　弦

机械工业出版社

本书是神州数码技能教室项目的配套指导教材，也是信息安全实践基地的指定训练教材。全书共设 7 章，分别为信息与网络安全概述、安全威胁分析、安全防御技术分析、安全防御解决方案、局域网安全攻防解决方案、网络边界流量控制及入侵防御技术和安全协议分析。内容涉及现代网络安全项目实施过程中遇到的各种典型问题的主流解决方案及实施步骤。

本书可作为职业技术院校的教材，也可作为网络从业人员的参考用书。

本书配有授课用电子课件，可到机械工业出版社教材服务网 www.cmpedu.com 免费注册下载，或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

网络安全高级工程师/程庆梅，徐雪鹏主编．—北京：机械工业出版社，2012.6
教育部师资实践基地系列教材．信息与网络安全
ISBN 978-7-111-38482-3

Ⅰ．①网… Ⅱ．①程… ②徐… Ⅲ．①计算机网络—安全技术—教材
Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2012）第 106467 号

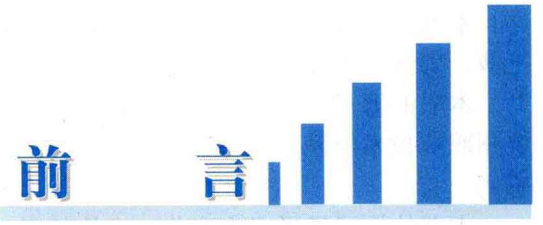
机械工业出版社（北京市百万庄大街 22 号 邮政编码 100037）
策划编辑：梁 伟 责任编辑：梁 伟 牟桂玲 责任校对：陈立辉
封面设计：鞠 杨 责任印制：杨 曦

北京双青印刷厂印刷
2012 年 6 月第 1 版第 1 次印刷
184mm×260mm · 11.25 印张 · 266 千字
标准书号：ISBN 978-7-111-38482-3
定价：32.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
社服务中心：（010）88361066
销售一部：（010）68326294
销售二部：（010）88379649
读者购书热线：（010）88379203

网络服务
门户网：http://www.cmpbook.com
教材网：http://www.cmpedu.com



前　言

本书是神州数码技能教室项目的配套指导教材，也是信息、安全实践基地的指定训练教材。

本书共分 7 章 29 节，分别针对常用的现代网络安全设备的应用场合进行介绍和深入分析，内容涵盖安全理念、安全方案、安全技术和安全网络实施等。本书与以往的安全类教材不同之处在于：理论、方案与实践三位一体；方案与技术并重；更贴近岗位实际。

教学建议：

章	节	参考理论学时	参考实践课时
第 1 章　信息与网络安全概述	1.1　信息安全	1	0
	1.2　网络安全	1	0
	1.3　安全目标	1	0
第 2 章　安全威胁分析	2.1　网络与信息安全威胁	2	1
	2.2　漏洞简介		
	2.3　网络服务威胁	2	1
	2.4　数据威胁	2	1
第 3 章　安全防御技术分析	3.1　补丁技术	2	1
	3.2　病毒防护技术	2	2
	3.3　加密技术与加密算法	2	1
	3.4　数字签名与数字证书	2	2
第 4 章　安全防御解决方案	4.1　神州数码 DCFS 流量整形解决方案	1	2
	4.2　DCSM-A 安全接入运营解决方案	1	1
	4.3　DCSM 网络准入控制与网络行为管理系统安全联动技术	1	1
	4.4　基于 802.1x 的可信网络连接技术	1	2
第 5 章　局域网安全攻防解决方案	5.1　扫描器	1	2
	5.2　欺骗攻击及防御	1	2
	5.3　Flooding 攻击及防御	1	2
	5.4　协议攻击	1	2
	5.5　监听攻击及其防御	1	2
	5.6　木马	1	2
第 6 章　网络边界流量控制及入侵防御技术	6.1　过滤 IP 网络流量	2	2
	6.2　过滤 Web 和应用流量	1	2
	6.3　流量控制理论及控制方法	2	2
	6.4　边界入侵防御技术	2	2
第 7 章　安全协议分析	7.1　IPSec 协议分析	2	2
	7.2　SSL 协议分析	2	2
	7.3　SSH 协议	2	2
	7.4　HTTPS	2	1
总　计		42	42

本书由程庆梅、徐雪鹏任主编，杜婉琛任副主编，参与编写的还有：李东方、王岳、王博、郭薇和田弦。

本书的编写得到了神州数码技术团队的大力支持，同时在审核校对的过程中，得到了杭州职业技术学院、北京信息职业技术学院等多家院校师生的大力协助，在此表示由衷的感谢。

本书的编写虽经多方合作，多次校对，但由于编者水平所限，疏漏之处在所难免，敬请广大读者批评指正，编者邮箱：dcnu_2007@163.com。

编　者

目　录

第 1 章
信息与网络安全概述

学习目标

1. 了解信息安全的目标。
2. 了解网络安全体系的构成。
3. 了解影响网络安全的因素。

重点及难点

1. 信息安全和网络安全的真正意义。
2. 引发网络安全的原因，以及如何避免此类现象的产生。

1.1 信息安全

1.1.1 信息安全概述

信息是信息论中的一个术语，常常把消息中有意义的内容称为信息。1948 年，美国数学家、信息论的创始人仙农在《通讯的数学理论》的论文中指出：“信息是用来消除随机不定性的东西。”1948 年，美国著名数学家、控制论的创始人维纳在《控制论》一书中指出：“信息就是信息，既非物质，也非能量。”

安全是指不受威胁，没有危险、危害和损失。人类的整体与生存环境资源的和谐相处，互相不伤害，不存在危险的、危害的隐患，是免除了不可接受的损害风险的状态。安全是在人类生产过程中，将系统的运行状态对人类的生命、财产、环境可能产生的损害控制在人类能接受的水平以下的状态。

信息安全是指信息网络的硬件、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、更改和泄露，系统连续、可靠、正常地运行，信息服务不中断。信息安全主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权复制和所寄生系统的安全性。

信息安全的根本目的就是使内部信息不受外部威胁，因此信息通常要加密。为保障信息安全，要求有信息源认证和访问控制，不能有非法软件驻留，不能有非法操作。

信息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。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于人类具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织（ISO）的定义，信息安全性主要是指信息的完整性、可用性、保密性和可靠性。信息安全是任何国家、政府、部门、行业都必须十分重视的问题，是一个不容忽视的国家安全战略。但是，对于不同的部门和行业来说，其对信息安全的要求和侧重点却是有区别的。

我国的改革开放带来了各方面信息量的急剧增加，并要求大容量、高效率地传输这些信息。为了适应这一形势，通信技术发生了前所未有的爆炸性发展。目前，除有线通信外，短波、超短波、微波、卫星等无线电通信的应用也越来越广泛。与此同时，国外敌对势力为了窃取我国的政治、军事、经济、科学技术等方面的信息，运用侦察台、侦察船、侦察机、卫星等手段，形成固定与移动、远距离与近距离、空中与地面相结合的立体侦察网，截取我国通信传输中的信息。在 20 世纪后 50 年中，从社会所属计算机中了解一个社会的内幕，正变得越来越容易。

日益繁多的事情托付给计算机来完成，敏感信息正经过脆弱的通信线路在计算机系统之间传送，专用信息在计算机内存储或在计算机之间传送。电子银行业务使财务账目可通过通信线路查阅，执法部门可从计算机中了解罪犯的前科，医生们用计算机管理病历，等等。所有这一切，最重要的问题是不能在对非法（非授权）获取（访问）不加防范的条件下传输信息。

传输信息的方式很多，有局域网、互联网和分布式数据库，还有蜂窝式无线、分组交换式无线、卫星电视会议、电子邮件及其他各种传输技术。信息在存储、处理和交换的过程中，都存在泄密或被截收、窃听、篡改和伪造的可能性。不难看出，单一的保密措施已很难保证通信和信息的安全，必须综合应用各种保密措施，即通过技术的、管理的、行政的手段，实现信源、信号、信息 3 个环节的保护，借以达到秘密信息安全的目的。

信息安全本身包括的范围很广。大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范青少年对不良信息的浏览、个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证和数据加密等），直至安全系统，其中任何一个安全漏洞都可能威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

1.1.2 信息安全的目标

1. 机密性

机密性（Confidentiality），又称保密性（Secrecy），是指个人或团体的信息不为其他不应获得者获得。在计算机中，许多软件包括邮件软件、网络浏览器等，都有保密性相关的

设定，用以维护用户资讯的保密性。另外，间谍档案或攻击者有可能会造成保密性的问题。

2．完整性

数据完整性（Integrity）是信息安全的 3 个基本要点之一，指在传输、存储信息或数据的过程中，确保信息或数据不被未授权的用户篡改或在篡改后能够被迅速发现。在信息安全领域的使用过程中，完整性常常和保密性边界混淆。以普通 RSA 对数值信息加密为例，攻击者或恶意用户在没有获得密钥破解密文的情况下，可以通过对密文进行线性运算，相应改变数值信息的值。例如，交易金额为 X 元，通过对密文乘以 2，可以使交易金额成为 2X。为解决以上问题，通常使用数字签名或散列函数对密文进行保护。

3．可用性

数据可用性（Availability）是一种以使用者为中心的设计概念，可用性设计的重点在于让产品的设计能够符合使用者的习惯与需求。以互联网网站的设计为例，希望让使用者在浏览的过程中不会产生压力或有挫折感，并能让使用者在使用网站功能时，能用最少的努力发挥最大的效能。基于这个原因，任何有违信息的“可用性”都算是违反信息安全的规定。因此，世界上不少国家，如中国、美国都要求举行保持信息可以不受规限地流通的运动。

对信息安全的认识经历了数据安全阶段（强调保密通信）、网络信息安全阶段（强调网络环境）和信息保障阶段（强调不能被动地保护，需要有保护—检测—反应—恢复 4 个环节）。

1.2　网络安全

1.2.1　网络安全概述

在计算机领域中，网络就是用物理链路将各个孤立的工作站或主机连接在一起，组成数据链路，从而达到资源共享和通信的目的。凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现网络资源共享的系统，称为计算机网络。

网络安全是指通过采用各种技术和管理措施，使网络系统正常运行，从而确保网络数据的可用性、完整性和机密性。国际标准化组织对网络安全的定义是：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。

网络安全从其本质上来讲就是网络上的信息安全。从广义来讲，凡是涉及网络中信息的机密性、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的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。例如从用户（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。

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，避免受到“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，制止和防御网络攻击者的攻击。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，给国家造成巨大损失。从社会教育和意识形态角度来讲，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，因此必须对其进行控制。

随着计算机技术的迅速发展，在计算机上处理的业务也由基于单机的数学运算、文件处理，基于简单连接的内部网络的内部业务处理、办公自动化等，发展到基于复杂的内部网（Intranet）、企业外部网（Extranet）、全球互联网（Internet）的企业级计算机处理系统和世界范围内的信息共享和业务处理。在系统处理能力提高的同时，系统的连接能力也在不断地提高。但在连接能力、信息流通能力提高的同时，基于网络连接的安全问题也日益突出，整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、网络系统安全、应用系统安全和网络管理的安全等。因此，计算机安全问题，应该像每家每户的防火、防盗问题一样，做到防患于未然。

通常，系统安全与系统性能（功能）是一对矛盾体。如果某个系统不向外界提供任何服务（断开），外界是不可能对其构成安全威胁的。但是，企业接入国际互联网络，可提供网上商店和电子商务等服务，等于将一个内部封闭的网络建成了一个开放的网络环境，而各种安全包括系统级的安全问题也随之产生了。

构建网络安全系统，一方面由于要进行认证、加密、监听、分析、记录等工作，由此影响了网络效率，并且降低了客户应用的灵活性；另一方面也增加了管理费用。但是，来自网络的安全威胁是实际存在的，特别是在网络上运行关键业务时，网络安全是首先要解决的问题。

为了缓解网络安全与网络性能之间的矛盾关系，可采用如下方案。

1）采用适当的安全体系设计和管理计划，能够有效降低网络安全对网络性能的影响并降低管理费用。

2）选择适当的技术和产品，制定灵活的网络安全策略，在保证网络安全的前提下，提供灵活的网络服务通道。

网络安全的实施离不开安全产品的部署，通常在部署中需要考虑如下问题：第一，网络安全来源于安全策略与技术的多样化，如果采用一种统一的技术和策略也就不安全了；第二，网络的安全机制与技术要不断地变化；第三，随着网络在社会各方面的延伸，进入网络的手段也越来越多，因此，网络安全技术是一个十分复杂的系统工程。因此，建立有中国特色的网络安全体系，需要国家政策和法规的支持以及集团联合研究开发。安全与反安全就像矛盾的两个方面，总是不断地向上攀升，所以安全产业将来也是一个随着新技术发展而不断发展的产业。

网络安全产品的自身安全的防护技术是网络安全设备安全防护的关键，一个自身不安全的设备不仅不能保护被保护的网络，而且一旦被入侵，反而会成为入侵者进一步入侵的平台。网络安全是国家发展所面临的一个重要问题。对于这个问题，以前并没有从系统的规划层面上去考虑它。我们不仅应该看到网络安全的发展是我国高科技产业的一部分，而且应该看到，发展安全产业的政策是网络安全保障系统的一个重要组成部分，甚至应该看到它对我国未来电子化、信息化的发展将起到非常重要的作用。

1.2.2　网络安全典型问题

影响网络不安全的因素有很多，归纳起来，主要有以下几种典型因素。

1．未进行操作系统相关安全配置

无论采用什么操作系统，在默认安装的条件下都会存在一些安全问题。只有专门针对操作系统安全性进行相关的和严格的安全配置，才能达到一定的安全程度。千万不要以为操作系统默认安装后，再配上很强的密码系统就安全了。网络软件的漏洞和“后门”是网络攻击的首选目标。

2．未进行 CGI 程序代码审计

如果是通用的 CGI（Common Gateway Interface，通用网关接口）问题，防范起来还稍微容易一些，但是对于网站或软件供应商专门开发的一些 CGI 程序，很多都存在严重的 CGI 问题，这对电子商务网站来说，会出现攻击者恶意冒用他人账户进行网上购物等严重后果。

3．有目的的攻击

随着电子商务的兴起，对网站的实时性要求越来越高，DoS 或 DDoS 对网站的威胁越来越大。以网络瘫痪为目标的攻击效果比任何传统的恐怖主义和战争方式都来得更猛烈，破坏性更大，造成危害的速度更快，范围也更广，而攻击者本身的风险却非常小，甚至在攻击开始前就已经消失得无影无踪，不给对方报复、打击的机会。2000 年 2 月美国“雅虎”、“亚马逊”受攻击事件就证明了这一点。

4．安全产品使用不当

虽然不少网站采用了一些网络安全设备，但由于安全产品本身的问题或使用问题，这些产品并没有起到应有的作用。很多安全厂商的产品对配置人员的技术背景要求很高，超出对普通网管人员的技术要求，就算是厂商在最初给用户做了正确的安装、配置，但一旦系统改动，需要改动相关安全产品的设置时，很容易产生许多安全问题。

5．缺少严格的网络安全管理制度

网络安全最重要的还是要在思想上高度重视，网站或局域网内部的安全需要完备的安全制度来保障。建立和实施严密的计算机网络安全制度与策略是真正实现网络安全的基础。

1.2.3　安全体系构成

与其他安全体系（如保安系统）类似，企业应用系统的安全体系应包含如下内容。

1）访问控制：通过对特定网段、服务建立的访问控制体系，将绝大多数攻击阻止在到达攻击目标之前。

2）检查安全漏洞：通过对安全漏洞的周期检查，即使攻击可到达攻击目标，也可使绝大多数攻击无效。

3）攻击监控：通过对特定网段、服务建立的攻击监控体系，可实时检测出绝大多数攻

击，并采取相应的行动（如断开网络连接、记录攻击过程、跟踪攻击源等）。

4）加密通信：主动地加密通信，可使攻击者不能了解、修改敏感信息。

5）认证：良好的认证体系可防止攻击者假冒合法用户。

6）备份和恢复：良好的备份和恢复机制，可在攻击造成损失时，尽快地恢复数据和系统服务。

7）多层防御：攻击者在突破第一道防线后，延缓或阻断其到达攻击目标。

8）隐藏内部信息：使攻击者不能了解系统内的基本情况。

9）设立安全监控中心：为信息系统提供安全体系管理、监控、渠护及紧急情况服务。

1.3 安全目标

所有的信息安全技术都是为了达到一定的安全目标，其核心包括保密性（Confidentiality）、完整性（Integrity）、可用性（Usability）、可控性（Controllability）和不可否认性（Non—repudiation）5 个安全目标。

1．保密性

保密性是指阻止非授权的主体阅读信息。它是信息安全一诞生就具有的特性，也是信息安全主要的研究内容之一。更通俗地讲，就是说未授权的用户不能够获取敏感信息。对纸质文档信息，我们只需要保护好文件，不被非授权者接触即可。而对计算机及网络环境中的信息，不仅要制止非授权者对信息的阅读，而且要阻止授权者将其访问的信息传递给非授权者，以免信息泄露。

2．完整性

完整性是指防止信息被未经授权者篡改。它保护信息保持原始的状态，使信息保持其真实性。如果这些信息被蓄意地修改、插入或删除等，形成的虚假信息将带来严重的后果。

3．可用性

可用性是指授权主体在需要信息时能及时得到服务的能力。可用性是在信息安全保护阶段对信息安全提出的新要求，也是在网络化空间中必须满足的一项信息安全要求。

4．可控性

可控性是指对信息和信息系统实施安全监控管理，防止非法利用信息和信息系统。

5．不可否认性

不可否认性是指在网络环境中，信息交换的双方不能否认其在交换过程中发送信息或接收信息的行为。

信息安全的保密性、完整性和可用性主要强调对非授权主体的控制，而对授权主体的不正当行为如何控制呢？信息安全的可控性和不可否认性恰恰是通过对授权主体的控制，实现对保密性、完整性和可用性的有效补充，主要强调授权用户只能在授权范围内进行合法的访问，并对其行为进行监督和审查。

除了上述 5 个信息安全性外，还有信息安全的可审计性（Auditability）、可鉴别性

（Authenticity）等。信息安全的可审计性是指信息系统的行为人不能否认自己的信息处理行为。与不可否认性的信息交换过程中行为可认定性相比，可审计性的含义更宽泛一些。信息安全的可鉴别性是指信息的接收者能对信息的发送者的身份进行判定。它也是一个与不可否认性相关的概念。

为了达到信息安全的目标，各种信息安全技术的使用必须遵守一些基本的原则。

（1）最小化原则

受保护的敏感信息只能在一定范围内被共享，履行工作职责和职能的安全主体，在法律和相关安全策略允许的前提下，为满足工作需要，仅被授予其访问信息的适当权限，这称为最小化原则。敏感信息的“知情权”一定要加以限制，是在“满足工作需要”的前提下的一种限制性开放。可以将最小化原则细分为知所必须（Need to Know）和用所必须（Need to Use）的原则。

（2）分权制衡原则

在信息系统中，对所有权限应该进行适当的划分，使每个授权主体只能拥有其中的一部分权限，使他们之间相互制约、相互监督，共同保证信息系统的安全，这称为分权制衡原则。如果一个授权主体分配的权限过大，无人监督和制约，就隐含了“滥用权力”、“一言九鼎”的安全隐患。

（3）安全隔离原则

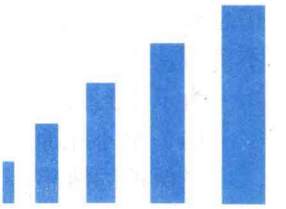
隔离和控制是实现信息安全的基本方法，而隔离是进行控制的基础。安全隔离原则就是将信息的主体与客体分离，按照一定的安全策略，在可控和安全的前提下实施主体对客体的访问。

在这些基本原则的基础上，人们在生产实践过程中还总结出一些实施原则，它们是基本原则的具体体现和扩展。包括：整体保护原则、谁主管谁负责原则、适度保护的等级化原则、分域保护原则、动态保护原则、多级保护原则、深度保护原则和信息流向原则等。

课后习题

1．信息安全的目标是什么？
2．引起网络不安全的主要因素有哪些？
3．企业应用系统的安全体系应包含哪些内容？
4．安全目标的核心内容是什么？

第 2 章 安全威胁分析



学习目标

1. 了解操作系统漏洞对安全的威胁。
2. 了解网络服务安全威胁的种类。
3. 了解数据安全威胁的种类。

重点及难点

1. 拒绝服务攻击的原理及防御方法。
2. 数据攻击的原理及防御方法。
3. 漏洞的威胁及防御方法。

2.1 网络与信息安全威胁

1. 信息安全的主要威胁

信息安全的威胁来自方方面面，不可一一罗列。但这些威胁根据其性质，基本上可以归结为以下几个方面。

1）信息泄露：保护的信息被泄露或透露给某个非授权的实体。

2）破坏信息的完整性：数据因被非授权地增删、修改或破坏而受到损失。

3）拒绝服务：信息使用者对信息或其他资源的合法访问被无条件地阻止。

4）非法使用（非授权访问）：某一资源被某个非授权的人，或以非授权的方式使用。

5）窃听：用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

6）业务流分析：通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，从中发现有价值的信息和规律。

7）假冒：通过欺骗通信系统（或用户）达到非法用户冒充为合法用户，或者特权小的

用户冒充为特权大的用户的目的。我们平常所说的攻击者大多采用的就是假冒攻击。

8）旁路控制：攻击者利用系统的安全缺陷或安全性上的脆弱之处获得非授权的权利或特权。例如，攻击者通过各种攻击手段发现原本应保密，却又暴露出来的一些系统“特性”，利用这些“特性”，攻击者可以绕过防线守卫者侵入系统的内部。

9）授权侵犯：被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的。这也称为“内部攻击”。

10）抵赖：这是一种来自用户的攻击，涵盖范围比较广泛。例如，否认自己曾经发布过的某条消息、伪造一份对方来信等。

11）计算机病毒：这是一种在计算机系统运行过程中能够实现传染和侵害功能的程序，行为类似病毒，故称为计算机病毒。

12）信息安全的法律、法规不完善：由于当前约束操作信息行为的法律、法规还很不完善，存在很多漏洞，很多人打法律的擦边球，这就给信息窃取者、信息破坏者以可乘之机。

无论何种安全威胁，都是在一定的前提下产生的，网络的安全威胁很大程度上是来源于网络体系的架构脆弱性。从网络终端系统到网络设备，再到数据传输的模式，以及在终端中运行的各种应用，其底层的协议架构往往存在很多的漏洞供别有用心的人利用，于是安全问题就产生了，而且随着网络的发展以及网络应用和网络技术的普及，愈发严重。

2．互联网的安全隐患

互联网的安全隐患主要体现在以下几个方面。

1）互联网是一个开放的、无控制机构的网络，攻击者（Hacker）经常会侵入网络中的计算机系统，或窃取机密数据，或盗用特权，或破坏重要数据，或使系统功能得不到充分发挥直至瘫痪。

2）互联网的数据传输是基于 TCP/IP 通信协议进行的，这些协议缺乏使传输过程中的信息不被窃取的安全措施。

3）互联网上的通信业务多数使用 UNIX 操作系统来支持，UNIX 操作系统中明显存在的安全脆弱性问题会直接影响安全服务。

4）在计算机上存储、传输和处理的电子信息，还没有像传统的邮件通信那样进行信封保护和签字盖章。信息的来源和去向是否真实，内容是否被改动以及是否泄露等，在应用层支持的服务协议中是凭着君子协定来维系的。

5）电子邮件存在着被拆看、误投和伪造的可能性。使用电子邮件来传输重要机密信息存在着很大的危险。

6）计算机病毒通过互联网的传播给上网用户带来极大的危害，病毒可以使计算机和计算机网络系统瘫痪，数据和文件丢失。在网络上病毒可以通过公共匿名 FTP 文件传播，也可以通过邮件和邮件的附加文件传播。

3．网络安全攻击的形式

网络安全攻击的形式主要有 4 种：中断、截获、修改和伪造。

1）中断是以可用性作为攻击目标，它毁坏系统资源，使网络不可用。

2）截获是以保密性作为攻击目标，非授权用户通过某种手段获得对系统资源的访问。

3）修改是以完整性作为攻击目标，非授权用户不仅获得访问，而且对数据进行修改。