普通高等教育“十一五”国家级规划教材

# 计算机网络安全技术

潘　瑜　主编

科学出版社

北　京

## 内 容 简 介

本书共10章，主要内容有计算机网络安全概述、计算机网络安全协议基础、计算机网络安全编程基础、计算机网络操作系统安全基础、计算机网络攻击与入侵技术、计算机网络病毒及反病毒技术、计算机网络站点的安全、数据加密技术基础、防火墙与入侵检测技术、网络信息安全方案设计等。本书面向应用，在强调掌握基础知识的同时，给出了各种网络安全技术和使用方法。每章都附有典型例题、习题和实验。

本书可作为应用型本科院校计算机专业、通信专业、信息专业的本科生教材，也可以供从事计算机网络安全及相关工作的工程技术人员学习参考。

**图书在版编目(CIP)数据**

计算机网络安全技术/潘瑜主编.—北京：科学出版社，2007
普通高等教育"十一五"国家级规划教材
ISBN 978-7-03-019403-9

Ⅰ.计… Ⅱ.潘… 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(2007)第108979号

责任编辑：苏 鹏 毛 莹 宛 楠 / 责任校对：郑金红
责任印制：张克忠 / 封面设计：耕者设计工作室

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com

中国科学院印刷厂印刷
科学出版社发行 各地新华书店经销
*
2007年8月第 一 版 开本：B5(720×1000)
2007年8月第一次印刷 印张：23 3/4
印数：1—4 000 字数：448 000

**定价：29.00元**

(如有印装质量问题，我社负责调换〈科印〉)

# 前　言

目前各应用型本科高等院校“计算机网络安全技术”课程教学已经基本展开。在因特网飞速发展的信息时代，计算机网络安全技术越来越重要。本书重点介绍了计算机网络安全基础、计算机网络安全协议基础、计算机网络安全编程基础、计算机网络操作系统安全基础、计算机网络攻击与入侵技术、计算机网络病毒及反病毒技术、计算机网络站点的安全、数据加密技术基础、防火墙与入侵检测技术、网络信息安全方案设计等内容。本书的基本内容是围绕提高读者“计算机网络安全能力”这个主题展开的。

在选取本书内容时，我们充分考虑了计算机网络安全技术的实际情况，将计算机网络安全领域中相对比较繁杂的部分舍去，而保留了计算机网络安全技术中最常用、最基本的部分。本书典型实例、实验和习题丰富，力求使读者通过学习能够达到“举一反三、融会贯通”的目的。

本书由江苏技术师范学院潘瑜任主编，臧海娟、何胜任副主编，蒋益峰参编。其中第1、2、4、7章由潘瑜编写，第9章的9.1～9.4节、9.6节、第10章由臧海娟编写，第3、5、8章由何胜编写，第6章、第9章的9.5节由蒋益锋编写，由潘瑜最终统稿成书。

本书在编写过程中得到江苏技术师范学院史国栋、施步洲和周丽琴的大力支持，江苏技术师范学院韩君为本书做了大量文字录入和排版工作，在此向他们表示衷心的感谢！

本书的出版还得到江苏省六大人才高峰项目06-E-040、江苏技术师范学院自然科学研究项目KYY06003和江苏技术师范学院教学改革与研究项目JG06010的资助，在此也表示衷心的感谢！

由于编者水平有限，书中难免有疏漏，错误之处，欢迎广大读者批评指正。

编　者

2007年3月

# 目　　录

# 第 1 章　计算机网络安全概述

**学习目标**

计算机网络中的安全问题与现实社会中的安全问题一样，是一个永恒的问题，也是一个很难解决的问题。本章从介绍网络安全现状、网络安全面对的威胁和网络安全面临的困难入手，引出对网络安全体系结构的描述，讨论了网络安全法规和网络安全评价标准，以助读者全面理解网络安全概念。

## 1.1　网络安全概述

### 1.1.1　网络安全现状

随着计算机网络的普及和计算机网络应用的发展，人类社会对计算机网络的依赖程度日渐加深。计算机网络安全不仅对每个人都有现实意义，而且对一个国家的政治、经济和国防安全也十分重要。计算机网络安全的问题，曾经给某些生产企业、金融公司甚至政府部门造成过重大损失。

事实上计算机网络安全问题是现实社会中的各种安全问题在计算机网络这个虚拟社会中的一个映射。现实生活中可能存在的各类问题在计算机网络这个虚拟社会中也会存在。例如，在真实社会中进行商业活动时可能会遇到商业欺诈，农民可能会买到假种子、假化肥；企业和个人可能会遇到假钞等。同样，基于计算机网络技术的电子商务活动也可能会遇到各种类型的攻击，如计算机病毒、商业信息窃取、拒绝服务、虚假身份等。但有所不同的是，由于计算机网络的开放性、匿名性和计算机网络技术的复杂性，通过计算机网络进行攻击和破坏比在真实社会中容易得多。例如，在计算机网络中要隐藏身份或冒名顶替要比在真实社会中容易。在计算机网络刚刚流行的时候，很多人都以拥有电子邮件信箱为荣，纷纷把电子邮件地址印在名片上，然而，人们很快就发现，这样做会带来很大的麻烦——每天都会收到大量的无法拒绝的垃圾邮件。因为在计算机网络中发信人可以根据需要不断变更自己的邮件地址、邮件标题使电子邮件用户上当。

计算机网络安全问题涉及数学、计算机技术、通信技术、管理和法律等多个领域。从不同学科的角度出发，会有不同的解决办法，但上述任何一种方法都不可能完全解决计算机网络安全问题，因此必须综合运用上述方法才能解决问题。

在计算机网络安全领域中有一个出现频率很高的词，那就是“黑客”（hacker），本意是指一些计算机水平很高的程序员，他们可以发现系统中潜在的漏洞，彼此之间经常在计算机网络中相互交换安全信息和安全技术，但从来不对别人的计算机系统进行蓄意破坏。而那些未经授权就进入别人的系统，具有恶意并非法获取信息，对系统进行破坏或对数据进行修改、删除等操作的人，则被称为破坏者（cracker），这种攻击和破坏活动可能会对系统造成很大损失。

由于因特网的日益普及，各种网络攻击工具很容易从网站上下载，计算机网络安全所面临的形势与因特网发展初期有很大的不同。现在，即使是一个初学者，利用各种工具软件也能够很容易地对计算机系统进行攻击。虽然目前采取了安全防护措施的机器比以前多了，但是，随着计算机的普及，越来越多的家庭用户、非专业用户在使用计算机，因特网上不设防的、具有安全漏洞的计算机也越来越多。

如今，“黑客”已经失去其早期“技术高手”的含义，而成为任何进行攻击活动者的代名词。在本书中，把那些进行非授权访问、修改数据，或使系统不可靠、不可用的活动称为攻击活动，而从事这种攻击活动的人统一称为“黑客”。

利用“黑客”手段对计算机网络进行攻击的人有下面几种：

（1）第一种人

这种人只是为了提高知名度，他们拥有很多的资源（时间、计算资源和金钱等），不断地寻找目标，进行各种尝试性攻击。

（2）第二种人

这种人没有明确的目的，可能会入侵不同的系统，修改服务器的主页，发送大量的垃圾信息。

（3）第三种人

计算机网络安全技术的研究人员为了证明一个计算机系统是不安全的，需要进行模拟攻击，以便找到系统的安全隐患。

（4）第四种人

这种人有计划、有目的地对特定系统进行破坏和攻击。

### 1.1.2 网络安全面临的威胁

网络的互联拓展了计算机应用的空间，但互联技术本身以及计算机系统存在的弱点，也使得所有网络用户因为彼此互联而更容易被攻击。因为我们通过网络已经与现实社会中形形色色的人联结到一起。

如图 1-1 所示，假设主机 A 和主机 B 是计算机网络中的两个用户，主机 C 是连接在计算机网络上的第三个用户，主机 A 和主机 B 之间正在通过计算机网络进行正常的通信，在这种情况下面临的主要安全问题是：

1）主机 C 对主机 A 或主机 B 的非授权访问。

2）主机 C 冒用主机 A 或者主机 B 的身份对网络上的其他主机进行访问。

3）主机 C 使主机 A 或主机 B 无法使用网络等。

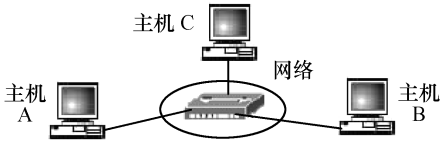

图 1-1　网络安全示意图

归纳起来，计算机网络安全面临的风险主要有以下几种。

1. 保密性（confidentiality）

在计算机网络中通信双方的信息有可能被网络中的第三方获得。

在如图 1-1 中，当主机 A 和主机 B 通信时，在不安全的计算机网络环境中，他们的通信内容有可能被第三方主机 C 截取，这可以通过下面几种典型的情况实现：

（1）电磁辐射监听

数据信号的传输通常是一定频率的电信号在金属导体或者无线的环境下传输，或者是通过光脉冲在光纤中传输。而对于前者，总会产生一定的电磁辐射，通过灵敏的仪器获取、分析这些电磁辐射，就可以了解传输的内容。

（2）线路中搭线窃听

这是一种经典的信息获取方法，在通信线路上搭接一根线和一部电话机，就可以知道这根线上通话的内容。如果将电话机换成一个协议分析设备，就可以对传输的信息进行分析、窃听。

（3）共享网络中的信息监听

对于共享以太网、无线网络等，任意一台连接到网络中的计算机，都可以通过运行数据包监听程序（如 Sniffer Pro 数据包抓包软件），捕获数据包并进行分析。

（4）其他方式

光纤通信虽然不会产生电磁辐射，但攻击者如果可以物理接触到光纤，也可以通过诸如分光器之类的设备监听数据。

“黑客”还可以利用一些伪装技术，设法获得用户的网络数据流量并加以分析。如果“黑客”能够控制计算机网络中的重要设备（如交换机和路由器）时，就可以很容易地得到各种用户数据流量，进行分析。为了确保计算机网络中的通信内容的安全，防止网络中的第三方窃取，必须在发送方对所要传输的信息加密，在接收方进行解密。

2. 认证（authentication）

所谓认证是指在计算机网络中，进行通信的双方在通信之前需要彼此确认对

方就是要通信的对象，而不是假冒的通信对象。

在现实社会中，当对话双方面对面说话时，人们通过识别对方的面孔，能够很清楚地知道要通信的对象是谁；当对话双方通过电话交谈时，人们也基本可以通过识别对方的声音，知道要通信的对象是谁。但是，在计算机网络这个虚拟社会中，当通信的双方无法真正“看”到或“听”到对方，不能根据传统的特征识别对方时，如何确保通信的双方不是假冒的对象就成了一个必须严肃对待的问题。

例如，当你在家中的计算机上通过因特网收到一封来自远方的电子邮件，这封邮件说他是你自大学毕业后就没有见过面的老同学，你是相信还是不相信呢？当你收到来自电子银行的邮件，请你填写银行账号和密码，你该怎样做呢？给大家的忠告是在没有进行必要的认证之前，上述的电子邮件都不是 100% 可信的。

如图 1-1 所示，如果主机 A 只允许主机 B 访问，主机 A 应该如何确认主机 B 的身份？如果主机 C 模仿成主机 B 与主机 A 通信，主机 A 应该怎样识别？是通过 IP 地址、用户名和口令还是其他信息？对于这些问题，都是需要通过适当的认证来解决的。

3. 完整性（integrity）

所谓完整性是指信息在传输的过程中无法被篡改，或者即使被篡改了，也可以被接受方发现。在计算机网络中进行数据通信过程中，通信双方在网络上传输的信息有可能被监听，也有可能被篡改。如图 1-1 所示，即使主机 A 和主机 B 之间的数据通信是保密的，主机 C 虽然无法理解其内容，但主机 C 仍然可以通过某些方法和工具篡改或破坏主机 A 和主机 B 之间的通信的内容。因此，在计算机网络中不仅通信的双方要彼此认证，对双方的通信内容的完整性和不可篡改性也要保证。

4. 不可否认性（non-repudiation）

所谓不可否认性是指在电子交易过程中，发出信息的一方无法否认其行为。如图 1-1 所示，在基于计算机网络的电子商务中，如果主机 A 向主机 B 发出了一个订单，或者主机 A 收到了主机 B 的一笔汇款，如何确保主机 A 或主机 B 无法否认在计算机网络上做过上述操作？因此，在基于计算机网络的电子商务活动中确保信息的不可否认性是十分重要的。

5. 可用性（availability）

所谓可用性是指计算机网络的基础设施、硬件和软件系统等在任何时候都能够可靠运行，并且随时能被所有用户正常使用。由于对国家、企业和个人来说计算机网络的作用越来越重要，人们要利用计算机网络来做各种各样的事情，如可

以利用计算机网络进行人员招聘、广告发布、商业信件收发、合同签订和商品销售等工作。这些商业企业对网络的依存度很高，如果计算机网络服务中断（哪怕只是几个小时），企业的业务也会受到很大的影响。因此，计算机网络的可用性直接关系到企业的生存。

事实上，所有连接在计算机网络上的计算机都同时扮演着两个角色：即网络服务的提供者和网络服务的使用者。当一台计算机通过网络对外提供服务时，自己就处于被攻击的危险中；而当一台计算机通过网络使用外面的服务时，也同样处于被攻击的网络中。来自网络的攻击可能会破坏系统，也可能会使原先提供的网络服务不可用。目前在计算机网络中可能出现的攻击和破坏活动，归纳起来有下面几种：

（1）扫描（scan）

利用特定的工具和专用的软件，向目标（如指定的网络或指定的主机）发出一些特定的数据包，根据响应的结果进行分析，了解目标网络或目标主机的相关特征，为进一步的攻击做准备。

（2）入侵（intrusion）

在计算机网络中，利用不同的方法和工具，进行诸如口令猜测、漏洞攻击等活动，一旦侵入目标系统，并获取相应的权限，则可以对目标系统的资源进行非授权访问和其他破坏活动。

（3）拒绝服务（denial of service）

在计算机网络中利用专用的工具软件或自己编写的程序，向目标系统发送大量的无用数据包，将目标系统的带宽占满，使得目标系统的服务无法被合法的用户所使用。

（4）滥用（misuse）

在计算机网络中传播计算机病毒、发布垃圾邮件、扩散有害信息等活动都是对网络的滥用。这些活动也有可能导致目标系统不能够使用。

要解决这些网络安全问题，需要综合运用多种技术手段、管理手段和法律手段。其中，保密性、认证、完整性、不可否认性等问题，主要基于密码算法及其应用。而可用性涉及更多的因素，如访问控制、管理等。因此，我们将在介绍有关攻击的基础上，介绍加密技术及其应用，以及各种常见安全防护手段，说明如何发挥人的作用，通过有效的安全管理，综合各种技术手段，从而达到比较安全的防护效果。

另外，从信息系统面临的威胁来看，最具破坏性的主要来自内部。在内部威胁中，危害性最大的就是内部关键人员为了某种利益从事的攻击、破坏活动。对工作不满、遭到辞退或者与外部勾结的工作人员，往往更容易获取和破坏内部的关键信息。工作中的漫不经心，也经常会导致各种漏洞。

因此，如果发现了一个攻击者声势很大地对系统进行入侵、破坏，实际上产生的危害并不算大。那很可能是一个业余攻击者，使用从网络上获得的攻击工具“练手”。危害最大的是那些不动声色的“专业”攻击者，他们可以长期地对信息进行窃取、修改，并使自己攻击的活动很隐蔽，不被发现。

综上所述，我们可以对网络安全防护定义如下：

拒绝未经授权的物理或电子入侵、操作，保证网络和所传信息端到端的完整性，能够抗拒各种类型的破坏，包括电子袭击、物理袭击、人为错误等。

### 1.1.3 网络安全面临的困难

计算机网络中的安全问题与现实社会中的安全问题一样，是一个永恒的问题，也是一个很难解决的问题，在可以预见的未来不会有一个“一劳永逸”的解决方案。这主要是由以下几个方面的原因造成的。

1. 网络攻击与网络防守的不对称性

“黑客”在攻击计算机网络时，通常不会遵守正常计算机网络用户所默认的一些规则，他们会利用操作系统软件或者网络协议上的漏洞达到攻击网络主机的目的。如果我们分析一个“黑客”攻击网络的全过程，可以发现他的攻击行动是经过精心准备的，用于攻击的工具也很容易从因特网上获得。因此，“黑客”攻击的风险低，也很难被追踪。对于网络系统管理员来说，则意味着必须堵住所有可能的漏洞。因特网不断增加的复杂性、协议与应用的不断增多等都使得网络系统管理员进行安全防护的难度加大。

我们也可以把安全问题看成是一根安全链条，最脆弱的一环可以使整个系统崩溃。例如，某个设计得很好的网络安全系统，就因为系统管理员使用了一个简单的“弱口令”，而使得整个网络安全设计都变得不安全。

另外，“黑客”的攻击是主动行为，他可以选择一天的任何时候进行，而系统管理员不可能做到每周 7×24 小时都处于积极的防守状态。因此，网络攻击和网络防守是极不对称的，100% 网络安全是非常难做到的。

2. 网络安全的动态性

由于计算机网络技术发展非常迅速，随着技术的发展，网络操作系统、网络硬件平台、网络应用软件和网络协议都会发生变化。当用户安装了新的服务器，升级了网络操作系统，采用了新的网络协议，安装了新的应用后，原来存在的一系列安全问题可能会消失，但新的安全问题和安全漏洞可能又会出现。因此，网络安全是动态的，不可能存一个“一劳永逸”的解决方案。对计算机网络安全的攻击与防守来讲，攻击者总是占有优势，因为防守者必须仔细检查和防守每个可

能的漏洞，一旦有所疏忽让攻击者找到一个漏洞，系统就有可能被攻破。另外如前所述，实施攻击的“黑客”往往是具有丰富专业知识和经验的计算机网络专业人员，而被攻击者大部分是普通的计算机用户，也许仅仅会操作和使用计算机，对计算机网络安全知识知道得很少，这也是“黑客”攻击能够频频得手的一个重要原因。

3. 网络安全的成本问题

所谓计算机网络安全成本，既可以是所投入的资金和人力资源成本，也可以是投入的时间成本。为了让计算机网络系统更安全，网络的管理者可能需要安装更多的网络安全设备、雇用更多的网络安全专业人员，所以拥有的资源越多，就越可能达到更好的安全程度。但是如果网络安全的成本太高，甚至高出所要保护的信息资源的价值，则网络安全投入就失去了实际的意义。同样，如果“黑客”攻击的代价超过了攻击的获益，也是没有实际意义的。

计算机网络服务的本质是开放的，如搜索引擎网站、新闻网站、门户网站、公共信息网站是面向所有用户的，而采取各种网络防范措施就意味着限制这种开放性，必然会给用户带来不便。因此，网络安全措施并不一定越多越好，既要兼顾安全，又要兼顾易用性。一套极其烦琐的安全措施是没有人愿意用的。

4. 网络安全的本质

多年以来，网络安全更多地被作为一个技术问题来研究，关注的焦点也始终是技术，如数据加密技术、安全访问控制技术、安全监控技术等。但仔细研究计算机网络安全面临的问题，我们会发现一个有趣的现象，不论采用什么样的网络安全防护技术，最终的安全都要落实在人身上，即“决定战争胜负的是人而不是物”。网络安全问题的本质在于人性的弱点，人们要么认为自己不会成为“黑客”攻击的目标，要么认为系统已经安装了先进的网络安全设备且有网络安全管理员在管理，不存在网络安全问题。由于这种人性的弱点，以及大量没有网络安全经验的用户存在，不管网络安全技术怎样发展，网络安全问题总是存在的。因此，要确保网络安全，必须加强和普及网络安全知识的教育，改善网络安全技术的管理手段，最大限度地减少风险，增加攻击者的成本。不管网络安全技术多么的完善，必须要有人的参与和管理，才能够较好地发挥作用。因此，建立安全意识，强化安全管理更为重要。

### 1.1.4　网络安全组织与机构

计算机网络安全问题是一个全球性的问题，目前全世界有许多组织和机构正在开展网络安全方面的研究工作，作为计算机网络安全方面的专业人员应该对这

些组织和机构有所了解。

1. IETF（www.ietf.org）

IETF（Internet Engineering Task Force，因特网工程任务组）是一个大型的、开放的国际组织，它由网络设计、网络运行、网络研究和网络厂商等方面的人员组成，共同推动因特网的发展。

因特网的各项标准都是通过 IETF 制定的，IETF 的标准、草案等通过 RFC 文件来发布，并按顺序编号，RFC 越新，编号就越高。关于 RFC 格式、提交过程的详细说明，可以参看 RFC2026。每个成员都可以提出建议，发布在网络上，供其他人讨论、反馈，最后形成草案和标准。

IETF 是民间组织，在因特网发展初期，IETF 花费大量时间和精力来解决网络的互联互通问题，而对网络安全问题很少涉及。如果参考 IETF 早期的文件，就会发现这一点。当因特网广泛应用于商业领域之后，网络安全问题日益突出，IETF 也把更多的注意力放在了网络安全领域。对于因特网的许多经典协议，如 IP 协议、TCP 协议、TELNET 协议、FTP 协议和 DNS 协议等，IETF 都提出了相应的安全增强协议和改进协议，如 IPSec 协议、TLS 协议、SSH 协议和 DNSSEC 等。

2. CERT/CC（www.cert.org）

计算机安全应急响应/协同中心（CERT/CC）是由美国政府资助，位于卡耐基梅隆（Carnegie Mellon）大学软件工程研究所（SEI）的一个机构，提供各种网络安全方面的技术支持和信息。CERT 的工作范围包括，协同对网络安全事件的响应、提出针对不同网络安全问题的解决方案、研究网络入侵活动的趋势、分析发现各种产品中的漏洞和脆弱性、提供网络安全评估和培训等服务。

CERT 成立于 1988 年，目前已经成为因特网上最有名的一个安全组织。它对于提高人们的安全意识，帮助网络管理人员进行应急响应等，都起到了很好的促进作用。世界上很多国家、各网络运营商，乃至园区网的管理机构等，都开始借鉴其经验，逐步建立起自己的安全应急响应/协同中心，处理各种安全问题并对用户进行培训。

3. NSA（www.nsa.gov）和 NIST（www.nist.gov）

美国国家安全局（National Security Agency，NSA）是美国政府的一个情报机构，采用各种先进技术和设备进行信息收集、加密、解密、分析等工作。NSA 汇集了一大批工程师、物理学家、数学家、语言学家、计算机科学家、公共关系专家和项目管理专家。NSA 不仅提供网络安全产品、服务和解决方

案，还从事一些网络安全方面的研究项目。如“安全建议准则”里给出了如何配置安全的 Windows XP/NT/2000 系统及 Cisco 路由器、电子邮件系统的建议；“安全增强 Linux 系统”研究在 Linux 系统的基础上，增加强制访问控制，并可根据信息机密性、完整性的要求隔离信息，从而提供一个更安全的操作系统环境。

美国国家标准局（NIST）是美国政府中制定各种领域产品的技术标准并进行测试的机构。NIST 的计算机安全资源中心（csrc. nist. gov）主要从事安全风险方面的研究，开发有关标准、测试程序，以对系统和应用的安全进行测试，并提出在安全设计、实施、管理运行等方面的指导原则。其研究主要集中在以下 5 个领域：

（1）加密算法标准和应用

研究加密算法，包括加密算法（如 DES、AES）、认证技术、安全协议和接口、公钥证书管理、智能令牌及安全体系结构等。

（2）安全测试

开发并对安全技术、服务、产品等进行测试、评估的方法和工具。

（3）安全研究

对一些安全新技术进行研究，如入侵检测、“防火墙”、安全扫描工具、漏洞分析、访问控制、安全事件响应等。

（4）安全管理和指导

研究安全管理方面的准则，如风险管理、安全培训、人员安全、管理措施等。

（5）安全培训

在更大范围内进行安全意识培训，以促进整个社会的安全意识。

4. ISO/ITU

国际标准化组织（International Standard Organization，ISO）在网络安全方面也制定了一系列标准，如 ISO 17799 是一个覆盖范围很广的安全标准，包括了 10 个部分，涉及各种安全问题，如安全策略、风险评估等。但和 ISO 的开放系统互联（open system interconnection，OSI）有关标准一样，也比较复杂，不容易实现。ISO 15408 则是在 CC（共同准则）的基础上制定的一个安全评估方面的标准。

国际电信联盟（International Telecommunication Union，ITU）在 X. 400～X. 409 建议中有一些关于信息处理的标准；对应于 ISO 10021，在安全体系结构、模型、目录服务等方面也在制定有关标准。

5. 其他民间组织

除了政府机构和著名组织外，世界上还有许多民间组织和机构在从事网络安全方面的研究，提供有关网络安全的信息。有兴趣的读者可以通过搜索引擎来了解最新的变化情况。如 Phrack（www.phrack.org）就是一个比较著名的专业“黑客”网站，可以在该网站找到一些很有深度的技术文章。

## 1.2 网络安全体系结构

计算机网络安全是一个涉及面很广的研究领域。通常人们只在这个领域中的一个小范围内从事自己的研究工作，开发出某些能够解决特殊网络安全问题的方案，有人研究数据加密和解密算法，有人研究入侵和检测技术等。为了从整体上研究计算机网络安全问题，必须研究网络安全体系结构，从系统整体的角度去理解网络安全问题的解决方案，这对网络安全研究和网络安全管理工作具有全局性的指导作用。

### 1.2.1 网络安全总体框架

虽然各人的研究领域都只涉及网络安全中一个很小的范围，但是研究者应该知道其所研究的问题在整个计算机网络安全领域内中的地位，以及与其他网络安全问题的关系。因此应该理解计算机网络安全的总体框架。

1. ISO 的 OSI 参考模型

（1）物理层（physical layer）

物理层提供通信媒体的物理连接。主要功能体现在利用传输物理介质，提供建立、维持和拆除物理连接的机械、电气、功能和规程等方面的手段，以进行比特流的透明传输。

（2）数据链路层（data link layer）

数据链路层是在物理层提供服务的基础上，面向网络层在相邻的结点间提供可靠的、无差错传输链路。主要功能有传输以帧为单位的数据包，屏蔽物理介质，提供流量控制和差错控制，确保数据不过载、克服数据丢失、重复或错误。另外，与物理层类似，数据链路层也要负责建立、维持和释放数据链路的连接。

（3）网络层（network layer）

在网络层中，数据的传输单位是分组或包，为端到端传输数据提供面向连接的或无连接的服务。主要功能有路由选择、中继、网络连接、数据分割与组合、高层次的差错控制和拥塞控制、网络层管理等。

（4）传输层（transport layer）

传输层在上三层和下三层之间起承上启下的作用，是体系结构中关键的一层。功能为向用户提供端到端服务、传输层连接的建立/释放、分段/合段、拼接/分割、报文编号、传输层的流量控制等。

（5）会话层（session layer）

会话层的主要功能是：负责在两个进程之间建立、组织和同步会话，解决进程之间会话的具体问题，进行会话管理。如会话连接的建立、释放、中断和恢复、数据交换的同步控制和控制选择、同步点插入等。

（6）表示层（presentation layer）

表示层用来定义信息表示方法，提供语法转换、数据结构的商定、识别、解释和变换等控制管理。另外，数据的加密/解密、压缩/解压缩等功能也属于表示层范畴。

（7）应用层（application layer）

应用层是 OSI 参考模型的最高层，直接为用户应用进程访问 OSI 环境提供一种手段，处理应用进程之间发送和接收的信息内容。如远程登陆、电子邮件等。

目前因特网使用 TCP/IP 协议模型，TCP/IP 协议把 ISO/OSI 参考模型简化为四层：应用层、传输层、网络层（网际层）、网络接口层。其中，ISO/OSI 参考模型的上三层（应用层、表示层和会话层）都简化为一个应用层；传输层和网络层分别对应于 OSI 的传输层和网络层；网络接口层对应于 OSI 的物理层和数据链路层。OSI 参考模型与 TCP/IP 参考模型及其协议之间的对应关系如图 1-2 所示。

<table>
<tr><th>ISO 的 OSI 参考模型</th><th>TCP/IP 协议模型</th><th>TCP/IP 协议族</th></tr>
<tr><td>第七层：应用层</td><td rowspan="3">应用层</td><td rowspan="3">FTP、TELNET、<br>SMTP、SNMP、NFS 等</td></tr>
<tr><td>第六层：表示层</td></tr>
<tr><td>第五层：会话层</td></tr>
<tr><td>第四层：传输层</td><td>传输层</td><td>TCP、UDP</td></tr>
<tr><td>第三层：网络层</td><td>网际层</td><td>IP、ICMP、IGMP、ARP、RARP</td></tr>
<tr><td>第二层：数据链路层</td><td rowspan="2">网络接口层</td><td rowspan="2">Ethernet、FDDI、Token Ring 等</td></tr>
<tr><td>第一层：物理层</td></tr>
</table>

图 1-2　OSI 参考模型和 TCP/CP 参考模型协议对应关系

2. ISO 的 OSI 安全体系结构

1982 年 ISO 开始 OSI 安全体系结构的研究，当时 ISO 的 OSI 参考模型刚刚

建立。ISO/IEC JTC1 于 1989 年增加了关于安全体系结构的描述，在此基础上，后来又制定了一系列特定安全服务的标准，其成果标志是 ISO 发布了 ISO 7498-2 标准，作为 OSI 参考模型的新补充。1990 年，ITU 决定采用 ISO 7498-2 作为它的 X.800 推荐标准。

ISO 7498-2 标准现在已成为网络安全专业人员的重要参考，它为网络安全共同体提供一组公共的概念和术语，用来描述和讨论安全问题和解决方案。因此，OSI 安全体系结构只是安全服务与相关安全机制的一般性描述，说明了安全服务怎样映射到网络的层次结构中，并简单讨论了它们在 OSI 参考模型中的合适位置。

OSI 安全体系结构主要包括三部分内容：安全服务、安全机制和安全管理。安全体系结构首先分析了开放式系统面临的各种威胁，并针对这些威胁定义了一组安全服务。为支持安全服务，在 OSI 安全体系结构中又定义了一些安全机制。OSI 安全管理涉及与 OSI 有关的安全的管理以及管理的安全两个方面。OSI 安全管理不是通常的通信业务，但可以为用户的通信提供安全支持与控制。

### 1.2.2 安全服务

OSI 安全体系结构定义了一组安全服务包括：认证服务、访问控制服务、数据保密服务、数据完整性服务和抗抵赖服务。

1. 认证（authentication）服务

认证服务提供某个实体的身份保证。在网络通信的某一个特定过程中，如果某一个实体声称具有特定的身份时，认证服务就提供一种方法来证实这个声称是否正确。认证的一个常用方法是口令。由于 OSI 安全体系结构的其他安全服务要么依赖于认证服务，要么和认证服务紧密地结合，因此认证是一个非常重要的安全服务。

2. 访问控制（access control）服务

访问控制服务就是提供对网络中某些受限制资源的访问方法。访问控制服务可以防止未授权的实体访问计算机网络中的资源，从而避免对网络未经授权的使用、修改、删除以及运行程序和命令等。访问控制服务通常要与其他的安全策略协调一致。

访问控制服务能够直接支持保密性、完整性、可用性和认证，它对保密性、完整性和认证所起的作用十分明显。但对可用性所起的作用，则取决于其他方面是否能有效地控制。

3. 数据保密性（data confidentiality）服务

数据保密性服务的目的是保护系统信息不被泄漏，这种服务主要由连接保密性、无连接保密性、选择字段保密性和业务流保密性组成。

4. 数据完整性（data integrity）服务

数据完整性服务的目的是保护数据在存储和传输过程中的完整性。这种服务主要由可恢复的连接完整性、不可恢复的连接完整性、选择字段的连接完整性、无连接完整性和选择字段无连接完整性组成。数据完整性服务可以保证数据的完整性，能够对付新增或修改数据的企图。但不一定能够对付复制或删除数据。因此在说明任意一种数据完整性服务时要特别注意。

5. 抗“否认”（non-reputation）服务

前面已经讲到，在基于计算机网络的电子商务活动中确保信息的不可否认性是十分重要的。抗“否认”服务主要是指保护网络通信系统不会遭到来自系统内部其他合法用户的威胁，而不是对付来自外部网络的未知攻击者的威胁。所谓“否认”是指在计算机网络通信中参与某次通信的一方事后不承认曾进行过的操作，抗否认服务是用来对付这种情况的，它能够提供确凿的证据，证明通信双方做过某种操作。

### 1.2.3　安全机制

为了实现网络安全服务，在 OSI 安全体系结构中定义了一些安全机制，我们应该对这些安全机制加以讨论。

1. 加密机制（encipherment mechanisms）

加密机制可以利用加密算法对存储的数据或传输中的数据进行加密。在网络中它既可以单独使用，也可以与其他安全机制配合使用，是保护数据机密性的常用方法。

（1）加密机制的特点

1）加密机制能够保护存储数据和业务流信息的机密性。

2）数据加密算法分为可逆算法和不可逆算法两种。

3）通常加密机制的加密算法都是公开的，只有密钥需要保密。因此在实际使用时需要有一种密钥分发和管理机制。

（2）常见可逆加密算法

1）对称加密算法。对称加密算法有时又叫传统密码算法，就是加密密钥能

够从解密密钥中推导出来，反过来也成立。对称算法可分为两类。一类算法是一次只对明文中的单个位（有时对字节）运算的算法称为序列算法或序列密码。另一类算法是对明文的一组位进行运算，这些位组称为分组，相应的算法称为分组算法或分组密码。

2）非对称加密算法。非对称加密算法的加密和解密过程使用不同的密钥。一般加密过程使用公开密钥，解密过程使用私有密钥。公开密钥是完全公开的，私有密钥必须保密。从公开密钥推测到私有密钥在理论上是不可行的。

不可逆加密算法可以使用密钥，也可以不使用。若使用密钥，这密钥可以是公开的，也可以是秘密的。

2. 数字签名机制（digital signature mechanisms）

数据加密机制是保护数据的最基本的方法，这种方法能防止通信双方之外的人获得数据的真实内容，但对于诸如否认、伪造数据和假冒身份等网络安全问题，数据加密机制则无能为力。为了解决这些安全问题，在现实社会中，通信双方是利用在纸质文件亲笔签名并加盖公章的方法实现的。但是，在计算机网络中操作的对象是数据，无法在这些数据上亲笔签名，因此必须引入数字签名机制。数字签名机制由签名过程和验证过程组成。

（1）签名过程

数据在传输之前，使用数据发送者的私有密钥对要传输的数据进行加密，形成可供鉴别的数字签名信息。

（2）验证过程

数据到达接收端时，接收者使用发送方数字签名者的公开密钥对所收到的数字签名信息进行解密，并和鉴别信息相比较，如果比较结果一致，则验证通过。

因为，只有使用签名者的私有密钥才能产生出具有签名者特征的数字签名，所以当该签名在接收方利用数字签名者的公开密钥得到验证后，可以在任何时候通过有权威的第三方机构证明，这个数字签名是那个私有密钥的唯一拥有者产生的。

3. 访问控制机制（access control mechanisms）

访问控制机制主要支持访问控制服务，它可以根据实体的身份和其他相关信息决定分配给实体的访问权限。访问控制机制是计算机网络信息保护的重要措施。

4. 数据完整性机制（data integrity mechanisms）

数据完整性机制主要支持数据完整性服务。

5. 鉴别交换机制（authentication mechanisms）

鉴别交换机制是以交换信息的方式来确认实体身份的。

6. 业务流填充机制（traffic padding mechanisms）

业务流填充机制可以防止第三者在线路上通过窃听和分析数据流量而推测出数据内容。具体做法是在发送数据的间隙由保密装置连续地发出随机序列，使得窃听者收到数据流之后不知哪些是有用信息、哪些是无用信息。特别注意，业务流填充机制要求无论是真实数据还是填充数据都要经过加密保护才起作用。

7. 路由控制机制（routing control mechanisms）

计算机网络中，从源端到目的端可能有多条链路，有些链路可能是安全的，有些链路可能不安全。路由控制机制能使信息发送者选择安全的路由，以保证数据安全。在实际控制时既可以预先选择安全的静态路由，也可以根据需要选择安全的动态路由，还可以利用安全策略禁止带有特定安全标志的信息通过指定的路由。

8. 公证机制（notarization mechanisms）

前面我们已经提到，在验证数字签名时需要有权威的第三方机构证明，利用 OSI 的公证机制就可以建立一个这样的有权威的第三方认证机构，从而保证通信双方身份的真实性、数据的完整性等。提供公证的第三方必须是通信双方所信任的，并掌握必要信息以一种可以证实的方式提供所需的保证。通信双方可以使用数字签名机制、数据加密机制和数据完整性机制以适应公证机制。

### 1.2.4　安全管理

安全管理是 OSI 安全体系结构的第三部分，通过安全管理可以实施一系列的安全策略，对计算机网络的操作进行管理，安全管理是计算机网络安全不可缺少的部分。

OSI 安全管理既支持网络整体的强制安全管理策略，又支持网络中对安全有更高要求的个别系统的自主安全策略。由一个 OSI 安全管理机构所管理的多个安全实体构成 OSI 安全环境，有时又称为安全域。

OSI 安全管理由三部分组成：系统安全管理、安全服务管理和安全机制管理。

1. 系统安全管理

所谓系统安全管理是指对 OSI 安全域的整体管理，主要由以下几部分构成：

1）总体安全策略的一致性管理，当总体安全策略需要修改和维护必须确保一致性。

2）提供 OSI 安全域之间的安全信息交换。

3）提供安全服务管理和安全机制管理之间的交互作用。

4）提供安全事件管理，包括事件报告的生成、存储和查询。

5）提供安全审计管理，当故障发生时能够检测和追踪故障点。

6）提供安全恢复管理，当故障发生后，能利用系统备份迅速恢复系统。

2. 安全服务管理

所谓安全服务管理是指对各个特定的安全服务的管理，主要由以下几部分构成：

1）为某种特定安全服务定义安全目标。

2）为指定的安全服务提供能够使用的安全机制。

3）对能够使用的各个安全机制进行协商。

4）通过适当的安全机制管理、调用所需的安全机制。

5）与系统安全管理和安全机制管理相互作用，实现安全服务管理。

3. 安全机制管理

所谓安全机制管理是指对一些特定安全机制的管理，主要由以下几部分构成：

1）密钥管理，对密钥的产生、存储和分配等进行管理。

2）数据加密管理，对加密算法和加密的参数的选择进行管理。

3）数字签名管理，对数字签名算法和参数的选择进行管理。

4）访问控制管理，通过建立和维护访问控制表实现访问控制管理。

5）数据完整性管理，利用数据加密技术实现对数据完整性保护，管理与数据加密管理类似。

6）鉴别管理，通过产生和分配鉴别信息实现鉴别交换信息的功能。

7）业务流填充管理，通过对预定的数据率和随机数据率的管理实现填充管理。

8）路由控制管理，通过确定信任的链路或子网络，实现选择安全的路由。

9）公证管理，通过对公证信息分配、公证机构的选择和通信协议的管理等

来实现公证管理。

## 1.3　网络安全法规和网络安全评价标准

### 1.3.1　网络安全的相关法规

网络安全方面的法规经过近 20 年的发展，在许多国家都已经建立了一套完善的安全法规。

1. 我国立法情况

在我国有关计算机网络安全方面的法律很多，基本精神适用于数字空间的国家大法主要有《中华人民共和国宪法》(1982 年 12 月 4 日)、《中华人民共和国商标法》(1982 年 8 月 23 日)、《中华人民共和国专利法》(1984 年 3 月 12 日)、《中华人民共和国保守国家秘密法》(1988 年 9 月 5 日）和《中华人民共和国反不正当竞争法》(1993 年 9 月 2 日)。

为了加强对计算机犯罪的打击力度，1997 年在重新修订《中华人民共和国刑法》时，加入了下列有关计算机犯罪的条款：

**第二百八十五条**　违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

**第二百八十六条**　违反国家规定，对计算机信息系统功能进行删除、修改、增加、干扰，造成计算机信息系统不能正常运行，后果严重的，处五年以下有期徒刑或者拘役；后果特别严重的，处五年以上有期徒刑。

违反国家规定，对计算机信息系统中存储、处理或者传输的数据和应用程序进行删除、修改、增加的操作，后果严重的，依照前款的规定处罚。

故意制作、传播计算机病毒等破坏性程序，影响计算机系统正常运行，后果严重的，依照第一款的规定处罚。

**第二百八十七条**　利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密或者其他犯罪的，依照本法有关规定定罪处罚。

在我国有关计算机网络安全方面的国家条例和管理办法也很多：《计算机软件保护条例》(1991 年 6 月 4 日)、《中华人民共和国计算机信息系统安全保护条例》(1994 年 2 月 18 日)、《商用密码管理条例》(1999 年 10 月 7 日)、《互联网信息服务管理办法》(2000 年 9 月 20 日)、《中华人民共和国电信条例》(2000 年 9 月 25 日）和《全国人大常委会关于维护网络安全和信息安全的决定》(2000 年 12 月 29 日)。

2. 国际立法情况

世界上主要国家都有相关的计算机网络安全领域的立法，简述如下：

1）美国的立法情况：《个人隐私法》、《反腐败行径法》、《伪造访问设备和计算机欺骗滥用法》、《电子通信隐私法》、《计算机欺骗滥用法》、《计算机安全法》和《电讯法》等。

2）欧洲共同体的立法情况：欧盟的前身欧洲共同体是一个在欧洲范围内具有较强影响力的政府间组织。为在共同体内正常地进行信息市场运作，该组织在诸多问题上建立了一系列法律，具体包括：竞争（反托拉斯）法，产品责任、商标和广告规定，知识产权保护，保护软件、数据和多媒体产品及在线版权，数据保护，跨境电子贸易，税收，司法问题等。这些法律若与其成员国原有国家法律相矛盾，则必须以共同体的法律为准（1996 年公布的国际市场商业绿皮书，对上述问题有详细表述）。其成员国从 20 世纪 70 年代末到 80 年代初，先后制定并颁布了各自有关数据安全的法律。

3）英国的立法情况：1996 年以前，英国主要依据《黄色出版物法》、《青少年保护法》、《录像制品法》、《禁止滥用电脑法》和《刑事司法与公共秩序修正条例》惩处利用电脑和互联网络进行犯罪的行为。1996 年 9 月 23 日，英国政府颁布了第一个网络监管行业性法规《三 R 安全规则》。“三 R”分别代表分级认定、举报告发、承担责任。法规旨在从网络上消除儿童色情内容和其他有害信息，对提供网络服务的机构、终端用户和编发信息的网络新闻组，尤其对网络提供者作了明确的职责分工。

4）俄罗斯的立法情况：1995 年颁布了《联邦信息、信息化和信息保护法》。法规强调了国家在建立信息资源和信息化中的责任是“旨在为完成俄联邦社会和经济发展的战略、战役任务，提供高效率、高质量的信息保障创造条件”。法规中明确界定了信息资源开放和保密的范畴，提出了保护信息的法律责任。

5）新加坡的立法情况：新加坡广播管理局 1996 年 7 月 11 日宣布对互联网络实行管制，宣布实施分类许可证制度。该制度 1996 年 7 月 15 日生效。它是一种自动取得许可证的制度，目的是鼓励正当使用互联网络，促进其在新加坡的健康发展。它依据计算机空间的最基本标准谋求保护网络用户，尤其是年轻人，免受非法和不健康的信息传播之害。为减少许可证持有者的经营与管理负担，制度规定凡遵循分类许可证规定的服务均被认为自动取得了执照。

### 1.3.2 我国评价标准

网络安全的评价标准中比较流行的是 1985 年美国国防部开发的“可信任计算机标准评价准则”，世界各国根据自己实际情况也制定了相关的标准。

1999 年 10 月经过国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》，准则将计算机安全保护划分为以下五个级别：

第一级为用户自主保护级：它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。

第二级为系统审计保护级：除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己的行为的合法性负责。

第三级为安全标记保护级：除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。

第四级为结构化保护级：在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。

第五级为访问验证保护级：这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

我国是国际标准化组织的成员国，在信息安全标准化工作方面积极开展工作。但由于标准的制定需要较多的应用经验和较深的科学研究，与国际已有的工作相比，我们的标准还存在一定的差距，标准的覆盖范围还不够大不够深，对网络安全的指导作用也有待提高。

### 1.3.3　国际评价标准

目前国际上网络安全评价标准一般遵循 1985 年美国国防部开发的计算机安全标准“可信任计算机标准评价准则”（Trusted Computer Standards Evaluation Criteria，TCSEC），也就是常说的“网络安全橙皮书”。迄今为止“网络安全橙皮书”一直是评估多用户主机和小型操作系统的主要方法，当然对数据库和网络也适用。“网络安全橙皮书”用计算机安全级别来评价一个计算机系统的安全性，它把安全的级别由低到高分成 4 个级别：D 级、C 级、B 级和 A 级，根据需要每个级别又可以分成几个子级别，如表 1-1 所示。

**表 1-1　系统安全级别划分**

| 级　别 | 子级别 | 名　称 | 主要功能 |
|---|---|---|---|
| D | D | 低级保护 | 没有任何安全保护 |
| C | C1 | 自主安全保护 | 提供自主存储控制 |
| | C2 | 受控存储控制 | 提供单独的可查性，安全标识 |
| B | B1 | 标识的安全保护 | 提供强制存取控制，安全标识 |
| | B2 | 结构化保护 | 面向安全的体系结构，有较好的抗渗透能力 |
| | B3 | 安全区域 | 具有存取监控、高抗渗透能力 |
| A | A | 验证设计 | 形式化的最高级描述和验证 |

D 级是最低的安全级别，拥有这个级别的操作系统是不设防的，所有的人都可以自由操作，是完全不可信任的。这个级别对系统硬件没有任何保护措施，操作系统也容易受到损害，对系统和数据的访问也没有限制，所有的人不需任何账号和身份验证就可以进入系统，而且可以不受任何限制地访问其他人的数据文件。MS-DOS 和 Windows 9x 都属于这个级别的操作系统。

C1 级是 C 级的一个安全子级。C1 又被称为选择性安全保护（discretionary security protection）系统，C1 级描述了 Unix 系统上的一个典型安全级别，它能够对系统硬件提供某种程度的保护，系统通过用户账号和口令来识别该用户是否为合法用户，并决定用户对系统中的程序和数据资源拥有怎样的访问权限，但系统硬件受到损害的可能性依然存在。

用户拥有的访问权是指对文件和目录的访问权（包括读、写和执行权限）。文件的拥有者和超级用户（root）可以改变文件的访问权限，可以为不同的用户设置不同的访问权限。

C2 级是 C 级的另一个安全子级，它包含 C1 级的所有特征，还具有访问控制环境（controlled access environment）权力。这个访问控制环境在进一步限制用户执行某些命令或者访问某些文件的权限同时，还增加身份认证级别。在 C2 级，系统能够对所发生的事情进行审计（如系统是什么时候开机的，开机之后哪些用户从哪些主机登录进入系统等），并将审计的结果写入日志文件中，通过查看日志文件，可以发现“黑客”入侵的痕迹。通过 C2 级增加的身份认证级别，可以知道谁在执行当前命令。当然提供审计功能需要额外的 CPU 处理时间和硬盘空间。

利用 C2 级附加身份验证，可以让一个普通用户（不是超级用户）有权执行系统管理任务。授权分级使系统管理员能够给用户分组，授予他们访问特定程序或特定目录的权限。

目前常见操作系统中能够达到 C2 级别的有下面几种：

1）Unix 系统；

2）Linux 系统；

3）Novell 3.X 或者更高版本；

4）Windows NT，Windows 2000 和 Windows 2003。

B 级有三个安全子级，分别是 B1 级、B2 级和 B3 级。

B1 级，又称为标志安全保护（labeled security protection）级别，是支持多级安全（如秘密级和绝密级）的第一个级别，拥有这个级别的操作系统对处于强制性访问控制下的对象，不允许文件的拥有者改变这个文件的许可权限。这种安全级别比较适合政府机构的计算机系统，因为政府机构的各个部门对各个“秘密级别”的划分是比较明确的。