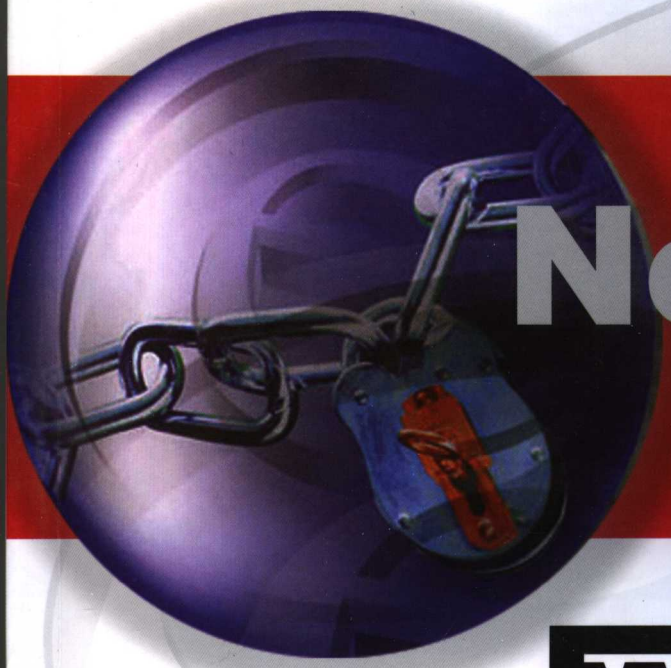
姚奇富 / 著



# Network Security

# 网络安全技术

ZHEJIANG UNIVERSITY PRESS
浙江大學出版社

# 网络安全技术

Network Security



姚奇富 / 著

ZHEJIANG UNIVERSITY PRESS
浙江大學出版社

## 内 容 简 介

本书从理论、技术和实例分析三方面入手，全面阐述网络安全理论，详细探讨和分析网络攻防技术。

全书共分3篇17章，第1篇为网络安全基础，共4章，主要阐述网络安全的基础理论和基本技术；第2篇为网络攻击技术原理和技术研究，共5章，较详细地探讨、分析和阐述网络攻击理论和攻击技术；第3篇为网络防护技术原理和技术研究，共8章，全面分析和阐述网络防护原理和技术。本书内容丰富，语言精练，在撰写中力求理论与实践相结合，突出实用性；力求深入浅出，突出通俗易懂；力求反映当前网络攻防研究发展的趋势，突出新颖性。

本书可以作为网络安全工程师、网络管理员和计算机用户的必备参考佳作，也可作为高等院校从事网络安全教学研究的师生的参考文献或教材。

**图书在版编目（CIP）数据**

网络安全技术 / 姚奇富著. —杭州：浙江大学出版社，2006.8
ISBN 7-308-04923-X

Ⅰ.网… Ⅱ.姚… Ⅲ.计算机网络—安全技术
Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2006）第107622号

**出版发行** 浙江大学出版社
（杭州市天目山路148号 邮政编码310028）
（网址：http://www.zjupress.com）
（E-mail:zupress@mail.hz.zj.cn）
**责任编辑** 严少洁
**封面设计** 张作梅
**排　　版** 浙江大学出版社电脑排版中心
**印　　刷** 富阳市育才印刷有限公司
**经　　销** 浙江省新华书店
**开　　本** 787mm×1092mm 1/16
**印　　张** 22.25
**字　　数** 534千
**版 印 次** 2006年8月第1版 2006年8月第1次印刷
**印　　数** 0001—3000
**书　　号** ISBN 7-308-04923-X/TP·309
**定　　价** 33.00元

国家863项目资助项目（项目编号：2002AA142030）
宁波市自然科学基金项目资助项目（项目编号：2006A610012）

# 序

国际互联网络 Internet 的迅速发展促进了信息共享与信息的全球化，使人们对网络的依赖越来越大，同时计算机网络和主机系统遭受入侵和攻击也越来越多，信息与网络安全已成为全球关注的问题。因此，我们应该高度重视和考虑信息系统安全。不但应重视信息系统安全防范，使其免遭攻击，而且应重视网络和主机系统的攻击技术研究，做到知己知彼，方能更好地保护我们的信息系统。由于我们国家信息技术起步比较晚，系统软件和集成电路的核心技术没有掌握在自己手里，这在很大程度上增加了保护信息安全的难度。近年来，我们国家的信息安全工作者努力奋斗、刻苦钻研，在信息安全方面发表了不少论文和专著，但系统地介绍网络攻防技术的专著还不多。该书就是一本系统地介绍和分析网络攻防技术，并且攻防并重的专著。该书的出版，将会对我国网络安全事业的发展起到积极的推动作用。

该书涵盖了网络攻防领域的主要内容。既注重网络安全原理和技术的分析与论述，又注重实践。同时，结合网络攻防实例，详细地介绍和分析了网络攻防中的主要技术，反映了当前网络攻防的主要技术和方向。

姚奇富老师长期在一线从事网络安全的教学工作，从事网络安全理论和技术的研究，在网络安全领域颇有成果，具有丰富的实践经验。书中大部分是他的工程实践经验、课题研究成果和教学成果的总结，同时也引用了一些国内外学者的最新研究成果。该书理论和实践并重，紧扣当前网络攻防研究发展的趋势，内容丰富，是一部很好的网络攻防专著。

我非常高兴能看到本书的顺利出版，同时我深信本书的面世将对我国网络安全技术和网络安全教育起到积极的作用。

张　森

2006 年 5 月于浙江大学

# 目　录

## 第 1 篇　基础篇

## 第 2 篇 攻击篇

## 第 3 篇　防护篇

# 第1篇　基础篇

# 第1章

# 网络安全概论

## 1.1 网络安全面临的威胁

截至2005年12月30日，我国网民总人数超过1亿，其中宽带上网网民数达到6430万人，上网计算机总数达到4950万台，网民数和宽带上网人数均位居全球第二。互联网正在不断高速发展，与此同时，互联网的开放性和安全漏洞带来的风险也无时不在。

各种网络安全漏洞的大量存在和不断发现，仍是网络安全的最大隐患；网络攻击行为日趋复杂，各种方法相互融合，使网络安全防御更加困难，防火墙、入侵检测系统等网络安全设备已不足以完全阻挡网络安全攻击；黑客攻击行为组织性更强，攻击目标从单纯的追求"荣耀感"向获取多方面实际利益的方向转移，木马、间谍软件、恶意网站、网络仿冒、大规模受控攻击网络(BotNet)等攻击行为的出现和垃圾邮件的日趋泛滥，是这一趋势的实证；手机、掌上电脑等无线终端的处理能力和功能通用性提高，日趋接近个人计算机，针对这些无线终端的网络攻击已经开始出现，并可能进一步发展。总之，网络安全问题变得更加错综复杂，影响不断扩大，很难在短期内得到全面解决。

### 1.1.1 网络安全隐患的由来

Internet不安全是一个不可回避的现实，造成不安全的原因也是多方面的，归结起来主要有以下四个方面。

**1. Internet的设计思想**

ARPA Net最初的设计思想是：当网络的某些部分被摧毁后，其剩余的部分仍能继续工作，保证信息的传输。在这样的思想指导下，网络的可靠性是优于安全性的。Internet在其早

期是一个开放的为研究人员服务的网际网，是完全非营利性的信息共享载体，因此，几乎所有的 Internet 协议在早期都没有充分地考虑安全机制。例如，在 TCP / IP 协议中就存在许多安全漏洞：

在 IP 层的协议设计中，IP 地址利用软件实现，这就造成了 IP 地址欺骗的安全隐患。另外，IP 协议支持源路由方式，即源点可以指定数据包传送到目的节点的中间路由，这就提供了绕过没有安全控制的路由进行攻击的条件。

在 TCP 层的协议设计中，TCP 协议序列号的连续性就产生了 TCP 序列号欺骗的安全隐患。

在应用层协议中，Telnet、HTTP、SMTP 等协议缺乏认证和保密措施，FTP、Telnet 和电子邮件中的数据（包括用户的口令）使用明文传输，账号和密码等数据很容易被窃取。

**2. 开放的系统**

Internet 不安全的另一个因素是因为人们很容易从 Internet 上获得相关的核心技术资料，特别是有关 Internet 自身的技术资料，比如 RFC、FAQ 文档，获得各类应用程序源代码，如 TCP / IP 的实现、Sendmail、FTP 等。还有各类安全工具的源代码也是免费公开的，如颇有争议的 SATAN、Crack 等。由于源代码公开的特性，使攻击者有足够的条件来分析软件中可能存在的漏洞，也能很方便地将安全检测工具用于网络攻击①。

各种在联网主机上使用的操作系统也存在先天缺陷，UNIX 操作系统就是一个例子，大多数 UNIX 操作系统的源代码都是公开的。多年来，世界各地的程序员不断地为 UNIX 开发操作系统和应用程序，这种协作方式是松散的、开放的。早期这些程序多是以学生完成课题或研究室里项目研究的方式完成的，它们构成了 UNIX 的框架，这个框架当初没有经过严密的论证，这种情况到后来导致 UNIX 系统存在很多致命的漏洞。

**3. 网络的复杂性**

网络设备、主机所采用的操作系统的多样化，以及拓扑结构的复杂性使网络管理人员的安全管理工作难度很大。而攻击者则可以利用这些复杂的因素来隐藏自己，发起有效的攻击。在网络管理中，对主机系统的访问控制配置起来通常很复杂，而且难于验证其正确性，因此，偶然的错误配置会导致非法访问者获取访问权。而且随着网络中主机数量的不断增加，也给网络安全带来了越来越大的压力。

**4. 社会缺乏安全意识**

Internet 不安全的另一个致命因素是使用者普遍缺乏安全意识，特别是那些对计算机和 Internet 技术缺乏了解的用户，他们对网络的攻击方法以及相应的安全措施知之甚少，平时疏于防范，往往在系统被人侵后仍毫无察觉，直到系统被破坏后才意识到，所造成的损失已无法弥补。

---

① [美]William Stallings 著，崔书昆译：网络安全要素——应用与标准．北京：人民邮电出版社，2000

## 1.1.2　网络面临的安全威胁

一般认为，计算机网络系统的安全威胁主要来自于“黑客”(Hacker)的攻击、计算机病毒(Virus)和拒绝服务攻击(Denies of Service)三个方面。具体来说，Internet 网络面临的安全威胁可归纳为以下几类。

(1)身份假冒。即某个实体假装成另外一个不同的实体，从而获得非授权的信息(获得合法用户的权限)。

(2)完整性破坏。对敏感数据的一致性通过非授权的增、删、修改或破坏。

(3)黑客攻击。黑客是网络中的一个复杂的群体，其对 Internet 的安全威胁主要包括发现和攻击网络操作系统的漏洞和缺陷，利用网络安全的脆弱性进行非法活动。

(4)拒绝服务。即 DoS 攻击，这种攻击的主要手段是对系统的信息或其他资源发送大量的非法的连接请求，从而导致系统因产生过量的负载而使系统的资源在合法用户看来是不可使用的。

(5)计算机病毒。计算机病毒的泛滥在严重的情况下会导致网络系统瘫痪，重要数据无法访问甚至丢失。目前，计算机病毒已成为黑客入侵的先导。

(6)内部入侵。也称为授权侵犯，指被授权以某一目的使用某个系统或资源的个人，利用此权限进行其他非授权的活动。另外，一些内部入侵者往往利用偶然发现的系统弱点或预谋突破网络安全系统进行攻击。由于内部入侵者更了解网络结构，因此他们的非法行为将对计算机网络系统造成更大的威胁。

(7)信息泄露。即敏感信息(如信用卡号码等)被泄漏或透露给非授权的人或实体。这种威胁可来自诸如窃听、搭线或其他更加错综复杂的信息探测攻击(如植入 Trojan Horse 或其他后门机关)。图 1-1 给出了 Internet 的安全威胁及其相互关系。

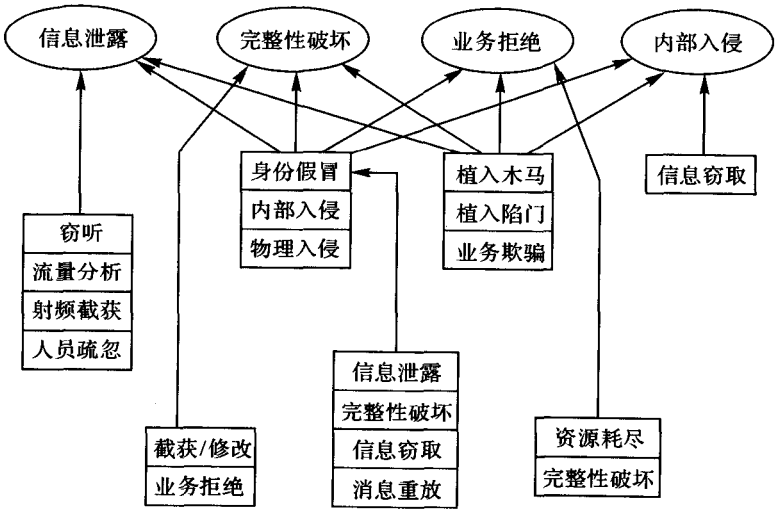



图 1-1　Internet 的安全威胁及其相互关系

# 1.2 网络安全的特性

## 1.2.1 网络安全的含义

安全性是联网技术中最关键、最容易被忽略的问题之一，随着 Internet 在全球的迅速发展，网络的安全性问题更为突出。

**1. 网络安全的定义**

网络安全是指网络系统的部件、程序、数据的安全，它通过网络信息的存储、传输和使用过程体现出来。所谓的网络安全性就是保护网络程序、数据或者设备，使其免受非授权使用或访问，它的保护内容包括：信息和资源，客户和用户，以及私有性。

**2. 网络安全的基本类型**

网络安全的基本类型有：

(1)登录安全。在安全的网络中，用户遇到的第一件事就是要回答用户名和口令。这是网络第一道关口上的安全措施，它能保证让管理员知道谁在网络中，未授权的就不能进。但是，没有哪一个登录安全系统是完美无缺的。有的用户常常选择容易被猜测出来的口令，或者把口令写在明显易见的位置，或是几个人共享一个口令，这些做法都可能引起安全问题。

(2)文件系统安全。用户登录网络的一个主要目的是访问服务器上的文件和目录。文件系统的安全性涉及到管理每个用户可以访问哪些文件。对用户来说，每个人要分配给一个具体的权限表。

(3)数据通信安全。安全性的另一方面涉及到数据通信。通过网络传输的数据包含许多敏感的信息，例如绝密文件。因此，除了 RIP 构成网络的设备和通信线路使之免于非法访问外，还要对数据采取安全措施，例如加密。

(4)网络管理。网络管理也是安全性考虑的一个方面。对于一个小型网络，可能只有一个管理员，这个管理员掌管了各方面的安全工作。而对于较大型的网络，拥有数百个用户，分布在几个区上，就需要均摊管理工作负担，给用户访问文件、享受网络服务的权利和赋予他们管理功能，使他们起到网络管理员的作用。

(5)审计。审计系统把对计算机系统的所有活动以文件形式保存在存储设备上，形成系统活动的监视记录。监视记录是系统活动的真实写照，是搜寻潜在入侵者的依据，也是入侵行为的有力证据。

(6)物理安全。物理安全是指计算机和网络设备本身的安全。

(7)人为安全。安全性涉及的另一个重要方面是网络中最为混乱的因素：用户。人为安全包括从非法闯入者到训练用户防止别人破坏网络安全等许多方面。

## 1.2.2 网络安全的特点

随着网络技术的更新与发展，网络安全问题及安全防范技术呈现出层出不穷的态势。综观网络安全的历史和现状，网络安全的表现形式虽然各不相同，但大致具有如下五个特点。

(1)网络安全的涉及面广。网络安全已渗透到生活中的每一个领域，网络安全保护的对象可分为四个层面：①国家安全，即如何保护国家机密不因网络黑客的袭击而泄露；②商业安全，即如何保护商业机密、企业资料不遭窃取；③个人安全，即如何保护个人隐私(包括信用卡号码、健康状况等等)；④网络自身安全，即如何保证接入网际网络的电脑网络不因病毒的侵袭而瘫痪。

(2)网络安全涉及的技术层面深。网络已形成一个跟现实社会紧密相关的虚拟社会，采用了众多新技术。而且黑客所采用的攻击手段和技术很多都是以前未曾见过的，技术含量比较高。这一切都注定了网络安全所涉及的技术层面的日益深入。

(3)网络安全的黑盒性。网络安全是一种以“防患于未然”为主的安全保护，这就注定了网络安全产品的功能有些模糊，不像其他应用系统那样明确。如一种入侵检测系统到底能够检测出哪些攻击，一般用户是没法知道的。因此，对于网络安全产品的鉴定，中间机构的介入就非常关键。如我国公安部网络安全检测中心、国际上的各种认证机构(如国际计算机安全协会 ICSA)等中介机构的介入，对于安全产品的定位和评价都很有帮助。

(4)网络安全的动态性。由于国内外黑客和病毒方面的技术日新月异，新的安全漏洞层出不穷。因此，网络安全必须能够紧跟网络发展的步伐，应对新的黑客技术。

(5)网络安全的相对性。任何网络安全都是相对的，任何网络安全产品的安全保证都只能说是提高网络安全保护的水平，而不可能杜绝危害网络安全的所有事件，只能使网络遭到攻击的可能性降低一些，使因遭受攻击而引起的损失能够限制在一定的范围内。

由此可见，网络安全已成为一个极为复杂、棘手而又迫切需要解决的问题。如何按照一定的标准或理论对安全问题进行划分，使安全问题能够细节化和具体化，便于进行分析和研究，则是解决问题的前提。

## 1.2.3 网络安全的层次结构

国际著名的网络安全研究公司 HurwitzGroup 经过研究得出结论，在考虑网络安全的过程中，应该考虑以下五方面的问题：①网络是否安全；②操作系统是否安全；③用户是否安全；④应用程序是否安全；⑤数据是否安全。即将安全问题划分为网络安全、操作系统安全、用户安全、应用程序安全、数据安全等五个方面的安全①。目前，这个五层次的网络系统安全体系理论已经得到了国际网络安全界的广泛支持，并已将这一理论应用到产品之中。

(1)网络层的安全性。网络层安全性的核心问题是网络能否得到控制，即是不是任何一个 IP 地址的用户都能安全进入网络，同时限制入侵者进入网络。

① RIDS－100 入侵检测系统技术白皮书[EB/OL]. http：//it. rising. com. cn/product/download/RIDS-100. whitepaper. pdf.