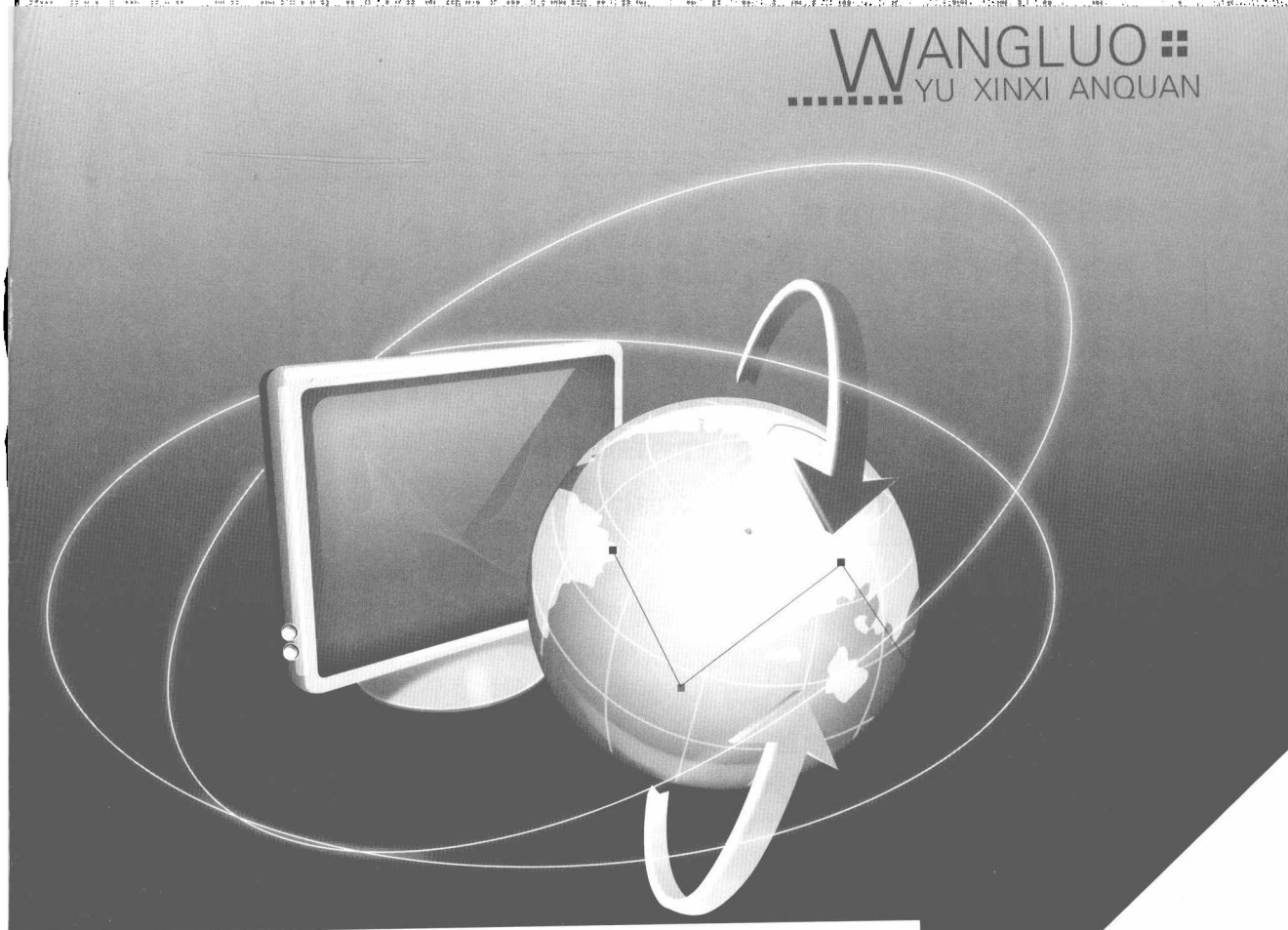
WANGLUO YU XINXI ANQUAN

网络与信息安全

主编 / 徐守志 陈怀玉 吴庆涛

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

WANGLUO YU XINXI ANQUAN



网络与信息安全

主　编 / 徐守志　陈怀玉　吴庆涛
副主编 / 张　凤　姜春涛　赵鹏远　凌志强　窦海静

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

图书在版编目(CIP)数据

网络与信息安全/徐守志,陈怀玉,吴庆涛主编. —北京:中国商务出版社,2009.3

ISBN 978-7-5103-0050-9

Ⅰ.网… Ⅱ.①徐…②陈…③吴… Ⅲ.①计算机网络—安全技术②信息系统—安全技术 Ⅳ.TP393.08 TP309

中国版本图书馆 CIP 数据核字(2009)第 034718 号

网络与信息安全

主　编　徐守志　陈怀玉　吴庆涛

副主编　张　凤　姜春涛　赵鹏远　凌志强　窦海静

中国商务出版社出版

(北京市东城区安定门外大街东后巷 28 号)

邮政编码:100710

电话:010—64269744(编辑室)

010—64266119(发行部)

010—64295501

010—64263201(零售、邮购)

网址:www.cctpress.com

Email:cctp@cctpress.com

北京中商图出版物发行有限责任公司发行

三河市铭浩彩色印装有限公司印刷

787 毫米×1092 毫米　16 开本

25.5 印张　652 千字

2009 年 3 月第 1 版

2009 年 3 月第 1 次印刷

ISBN 978-7-5103-0050-9

定价:38.00 元

前　言

如今网络信息安全已越来越受到人们的关注，也逐渐成为各相关科研机构研究的热点。可以说，没有网络信息安全就没有完全意义上的国家安全，也没有真正的政治安全、军事安全和经济安全。因此，加速计算机网络安全的研究和发展，加强计算机网络的安全保障能力，提高全民的网络安全意识已成为我国信息化发展的当务之急。

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、信息论等多学科的综合性学科。本书的目的是帮助读者理解信息安全的基础知识，掌握安全防范相关技术。

本书共分 11 章，具体内容如下。

第 1 章：信息安全基础。对信息安全的定义和特征，安全体系系统，以及信息安全遵守的原则及未来发展趋势进行介绍。

第 2 章：密码技术。首先概述密码技术，接着介绍古典密码技术和现代密码技术的理论基础，最后分别介绍对称和非对称两种密码技术。

第 3 章：数字签名与认证。主要讲述数字签名的功能及特点，消息鉴别函数的消息认证码、杂凑函数，以及数字签字技术和身份认证技术等知识。

第 4 章：公钥基础设施。主要讲述 PKI 的组件、密钥管理、证书管理的理论知识，同时对 PKI 的信任模型和应用也作了介绍。

第 5 章：计算机病毒与反病毒技术。主要对计算机病毒的工作原理及反病毒的基本战略和相关技术作了介绍。

第 6 章：黑客常用攻击技术。主要对常用的黑客攻防技术进行讲述，包括端口扫描、网络侦听、拒绝服务攻击、欺骗类攻击、缓冲区溢出和基于协议攻击的一些技术。

第 7 章：防火墙技术。介绍防火墙的基础知识、体系结构和虚拟专用网络。

第 8 章：入侵检测技术。主要讲述了基于主机的和基于网络的入侵检测技术，同时对入侵检测系统流程和系统的评估测试进行了阐述，最后对常见的几种 IDS 系统作了介绍。

第 9 章：安全协议理论。介绍安全协议分析和设计的基本理论，安全协议设计的形式化语言和方法，同时针对基于 BAN 逻辑模型和基于串空间两种模型作形式化分析。

第 10 章：典型安全协议。对典型的安全协议如 IPSec、RADIUS、SSL、Kerberos、SNMP、和 SET 协议作了介绍。

第 11 章：信息隐藏技术。主要介绍信息隐藏的定义、分类、特征，信息隐藏方法、分析和应用，以及流行的数字水印技术等知识。

由于编者水平有限，书中难免有疏漏和错误，恳请广大读者批评指正。

全书由徐守志、陈怀玉和吴庆涛担任主编，由张凤、姜春涛、赵鹏远、凌志强、窦海静担任副主编，并由徐守志、陈怀玉和吴庆涛负责统稿。其具体分工如下：

第 2 章，第 3 章，第 4 章第 1 节～第 4 节：徐守志（三峡大学电气信息学院）；

第 5 章，第 6 章第 1 节～第 6 节：陈怀玉（山西经济管理干部学院）；

第 8 章第 1 节～第 8 节：吴庆涛(河南科技大学)；
第 9 章：张凤(鹤岗师范高等专科学校)；
第 10 章第 1 节～第 4 节：姜春涛(鹤岗师范高等专科学校)；
第 7 章，第 8 章第 9 节，第 10 章第 6 节：赵鹏远(河北大学)；
第 6 章第 7 节与第 8 节，第 10 章第 5 节，第 11 章：凌志强(广西理工职业技术学院)；
第 1 章，第 4 章第 5 节与第 6 节：窦海静(商丘师范学院)。

编者

2009 年 2 月

目 录

第1章 信息安全基础

随着计算机互联网的发展，信息的应用与共享日益广泛和深入。信息化系统已经成为国家的基础设施，信息安全已备受瞩目。网络环境下的信息安全体系是保证信息安全的关键。所谓信息安全，就是关注信息本身的安全，以防止偶然的或未经授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等问题。

1.1 概 述

1.1.1 信息安全问题的由来

1. 信息和网络已成为现代社会的重要基础

当今世界正步入信息化、数字化时代，信息无所不在、无处不有。国与国之间变得“近在咫尺”。计算机通信网络在政治、军事、金融、商业、交通、电信、宗教等各行各业中的作用日益增大。在 Internet 上，除了电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、电子商务和视频等通信技术也在不断地发展与完善，正在为用户提供丰富多彩的网络与信息服务，以网络为基础和手段来获取信息、交流信息正成为现代社会的一个新特征。从某种意义上讲，信息就是时间、财富、生命，就是生产力。

随着全球信息基础设施和各个国家的信息基础的逐渐形成，社会对计算机网络的依赖日益增强。为此，人们不得不建立各种各样的信息系统来管理各种机密信息和各种有形、无形财富。但是这些信息系统都是基于计算机网络来传输和处理信息并实现其相互间的联系、管理和控制的。如各种电子商务、电子现金、数字货币、网络银行，乃至国家的经济、文化、军事和社会生活等方方面面，都日趋强烈地依赖网络这个载体。可见，信息和网络已成为现代社会的重要基础，以开放性、共享性和无限互联为特征的网络技术正在改变着人们传统的工作方式和生活方式，也正在成为当今社会发展的一个新的主题和标志。

2. 信息安全与网络犯罪危害日趋严重

事物总是辩证统一的。信息与网络科技进步在造福人类的同时，也给人们带来了新的问题和潜在危害。计算机网络的产生就像一个打开了的潘多拉魔盒，使得新的邪恶——计算机与网络犯罪相伴而来。

计算机互联网是与开放系统同时发展起来的。开放系统的标志是开放系统互联(OSI)模型的提出。自从 20 世纪 70 年代以来，OSI 模型得到了不断发展和完善，从而成为全球公认的计算机通信协议标准。除了 OSI 标准外，另一些标准化组织也相继建立了一些开放系统网络协议，其中最有影响力的是 Internet 协会提出的 TCP/IP 协议。通过围绕开放系统互联所开展的标准化活动，使得不同厂家所生产的设备进行互联成为现实。然而，在网络开发之初，由于人们考虑

的是系统的开放性和资源共享的问题，忽视了信息与网络技术对安全的需要，结果导致网络技术先天不足——本质安全性非常脆弱，极易受到黑客的攻击或有组织的群体的入侵。可以说，开放性和资源共享性是网络安全问题的主要根源。与此同时，系统内部人员的不规范使用或恶意行为，也是导致网络系统和信息资源遭到破坏的重要因素。

1.1.2 信息安全的含义

“安全”一词的基本含义为：“远离危险的状态或特性”，或“主观上不存在威胁，主观上不存在恐惧”。在各个领域都存在安全问题，安全是一个普遍存在的问题。随着计算机网络的迅速发展，人们对信息在储存、处理和传递过程中涉及的安全问题越来越关注，信息领域的安全问题变得非常突出。

信息安全是一个广泛而抽象的概念。所谓信息安全就是关注信息本身的安全，而不管是否应用了计算机作为信息处理的手段。信息安全的任务是保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等。这样可以使得我们在最大限度地利用信息的同时而不招致损失或使损失最小。

信息技术的应用，引起了人们生产方式、生活方式和思想观念的巨大变化，极大地推动了人类社会的发展和人类文明的进步，把人类带入了崭新的时代——信息时代。信息已成为信息发展的重要资源。然而，人们在享受信息资源所带来的巨大的利益的同时，也面临着信息安全的严峻考验。信息安全已经成为世界性的问题。

信息安全之所以引起人们的普遍关注，是由于信息安全问题目前已经涉及人们日常生活的各个方面。以网上交易为例，传统的商务运作模式经历了漫长的社会实践，在社会的意识、道德、素质、政策、法规和技术等各个方面，都已经完善，然而对于电子商务来说，这一切却处于刚刚起步阶段，其发展和完善将是一个漫长的过程。假设你作为交易，无论你从事何种形式的电子商务，都必须清楚以下事实：你的交易方是谁？信息在传输过程中是否被篡改（即信息的完整性）？信息在传送途中是否会被外人看到（即信息的保密性）？网上支付后，对方是否会不认账（即不可抵赖性）如此等等。因此，无论是商家、银行还是个人对电子交易安全的担忧是必然的，电子商务的安全问题已经成为阻碍电子商务发展的“瓶颈”，如何改进电子商务的现状，让用户不必为安全担心，是推动安全技术不断发展的动力。

信息安全研究所涉及的领域相当广泛。随着计算机网络的迅速发展，人们越来越依赖网络，人们对信息财产的使用主要是通过计算机网络来实现的。在计算机和网络上信息的处理是以数据的形式进行的，在这种情况下，信息就是数据。因而从这个角度来说，信息安全可以分为数据安全和系统安全，即信息安全可以从两个层次来看。从消息的层次来看，包括信息的完整性（Integrity），即保证消息的来源、去向、内容真实无误；保密性（Confidentiality），即保证消息不会被非法泄露扩散；不可否认性（Non-repudiation），也称为不可抵赖性，即保证消息的发送和接受者无法否认自己所做过的操作行为等。从网络层次来看，包括可用性（Availability），即保证网络和信息系统随时可用，运行过程中不出现故障，若遇意外打击能够尽量减少损失并尽早恢复正常；可控性（Controllability），即对网络信息的传播及内容具有控制能力的特性。

1.1.3 信息安全的属性

信息安全的基本属性主要表现在以下五个方面：

(1)完整性

完整性是指信息在存储或传输的过程中保持未经授权不能改变的特性,即对抗主动攻击,保证数据的一致性,防止数据被非法用户修改和破坏。对信息安全发动攻击的最终目的是破坏信息的完整性。

(2)保密性

保密性是指信息不被泄露给未经授权者的特性,即对抗被动攻击,以保证机密信息不会泄露给非法用户。

(3)可用性

可用性是指信息可被授权者访问并按需求使用的特性,即保证合法用户对信息和资源的使用不会被不合理地拒绝。对可用性的攻击就是阻断信息的合理使用,例如破坏系统的正常运行就属于这种类型的攻击。

(4)不可否认性

不可否认性也称为不可抵赖性,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。发送方不能否认已发送的信息,接收方也不能否认已收到的信息。

(5)可控性

可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性,能够对信息实施安全监控。

信息安全的任务就是要实现信息的上述五种安全属性。对于攻击者来说,就是要通过一切可能的方法和手段破坏信息的安全属性。

信息安全可以说是一门既古老又年轻的学科,内涵极其丰富。信息安全不仅涉及计算机和网络本身的技术问题、管理问题而且还涉及法律学、犯罪学、心理学、经济学、应用数学、计算机基础科学、计算机病毒学、密码学、审计学等学科。

从信息安全的发展过程来看,在计算机出现以前,通信安全以保密为主,密码学是信息安全的核心和基础。随着计算机的出现,计算机系统安全保密成为现代信息安全的重要内容。网络的出现使得大范围的信息系统的安全保密成为信息安全的主要内容。信息安全的宗旨是向合法的服务对象提供准确、正确、及时、可靠的信息服务;而对其他任何人员和组织,包括内部、外部乃至于敌对方,保持最大限度的信息的不透明性、不可获取性、不可接触性、不可干扰性、不可破坏性,而且不论信息所处的状态是静态的、动态的还是传输过程中的。

1.1.4 信息安全的基本特征

信息安全是一门新兴学科,关于信息安全化的具体特征的标志尚无统一的界定标准。但在现阶段,对信息安全化至少应具有机密性保证、完整性保证、可用性保证和可控性保证四个基本特征,却具有广泛的认同。

(1)机密性保证

机密性保证是指保证信息不泄露给非授权的用户、实体的过程,或供其利用的特性。换言之,就是保证只有授权用户可以访问和使用数据,而限制其他人对数据进行访问或使用。数据机密性在商业、军事领域具有特别重要的意义。如果一个公司的商业计划和财政机密被竞争者获得,那么该公司就会有极大的麻烦。数据的机密性分为网络传输机密性和数据存储机密性。如同通信电话能被窃听一样,网络传输也可能被窃听,其解决办法就是对传输数据进行加密处理。

数据存储机密性主要是通过访问控制来实现的。根据不同的安全要求和等级，一般将数据分成敏感型、机密型、私有型和公用型等几种类型，管理员常对这些数据的访问加以不同的访问控制。保证数据机密性的另一个易被人们忽视的环节是管理者的安全意识。一个有经验的黑客可能会通过收买或欺骗某个职员，而获得机密数据，这是一种常见的攻击方式，在信息安全领域称之为社会工程。

(2)完整性保证

完整性是指数据未经授权不能进行任何改变的特性。完整性保证即是保证信息在存储或传输过程中不被修改、不被破坏和不丢失的特性。完整性保证的目的就是保证在计算机系统中的数据和信息处于一种完整和未受损害的状态，也就是说数据不会因有意或无意的事件而被改变或丢失。数据完整性的丧失将直接影响到数据的可用性。

影响数据完整性的因素非常多，有人为的无意失误破坏，也有人为的蓄意破坏；有系统软件、硬件的失效事件所致，也有自然灾害、不可抗拒外力因素的影响。但不管怎样，人们总是可以通过访问控制、数据备份和冗余设置来实现数据的完整性。

在信息安全立法尚不发达的阶段，典型的蓄意破坏情况也常常发生。例如，一个被解雇的公司职员入侵到企业的内部网络，并肆意删去一些重要的文件。为了破坏一个站点，入侵者可能会利用软件的安全缺陷或网络病毒对站点实行攻击，并删去系统重要文件，迫使系统工作终止或不能正常运转。这类破坏的目的可能会很多，有的是为了显示自己的计算机水平，有的是为了报复，有的可能只是一个恶作剧。

无意破坏则主要来自于操作失误。比如一个对计算机操作不熟悉的人可能会无意中删去有用的文件，这种操作错误对一些安全性设计好的操作系统不会是一个大的问题，如 UNIX 和 Windows NT 操作系统，因为这些系统在设计时对新手的一些常见的操作失误已给予比较充分的考虑，一些反常操作被严格控制，而在 Windows 95 和 DOS 这样的早期系统中，误操作发生的可能性还很大。因为任何一个人都可以访问所有的文件，包括别人的文件和系统文件。为了防止这种误操作，对于 Windows 95 和 DOS 系统，用户必须对一些重要数据文件做一个备份，对于 UNIX 和 Windows NT 系统，可以为用户划分不同的用户目录，并把用户的权限限制在他本人的目录当中，如只有对自己的目录才有写的权限，对别人的目录则无写的权限。

硬件、软件失效也是经常造成数据被破坏的一个重要原因。软盘损坏即是一种典型的硬件失效。软盘是一种极易损坏的存储介质，人们经常随身携带软盘，很容易造成软盘的物理损害，有时有些软盘的质量也不好，因此，多备份几份以防止软盘不能读是一种明智的选择。硬盘虽然比软盘可靠性高，但对于十分重要的军事和商业信息而言，硬盘的备份也是十分必要的。现在很多服务器的硬盘都能提供冗余备份。人们经常听到一些软件开发商提出一些补丁程序。而且有时一个补丁接一个补丁，这充分说明复杂软件中可能存在的先天缺陷是不可忽视的问题。

自然灾害谁也无法预测，如水灾、火灾、龙卷风等，可能会破坏了通信线路或公司的整个网络，造成信息在传输中丢失、毁损，甚至使数据全部被灭毁，以致公司损失了全部的订货、发货信息以及员工信息等。美国世贸大厦中的许多公岗在“9·11”事件后纷纷倒闭和破产，并不是因为直接经济所致。恰恰是因为公司的数据信息资源被彻底毁灭而无法恢复的结果。对于这类破坏，最好的方法就是对数据进行备份。对于简单的单机系统，重要数据不多，可采用软盘人工备份，鉴于软盘可靠性较差，一般应多备份几份。对于一些大型商业、企业网络，如银行、保险交易网，必须安装先进的大型网络自动备份系统，并在空间上实施异地存储来提高信息的可恢复性。

(3)可用性保证

可用性是指数据可被授权实体访问并按需求使用的特性,即当需要时能否存取和访问所需的信息。例如,网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击。Internet 蠕虫的事例就是依靠在网络上大量复制并进行传播,它占用大量 CPU 处理时间,导致系统越来越慢,直到网络发生崩溃,用户的正常数据请求不能得到处理的。就是一个典型的"拒绝服务"攻击。数据不可用也可能是由于软件臭虫的原因,软件臭虫会造成网络失效,使授权用户不能登录到服务器上。

(4)可控性保证

对信息的传播及内容具有控制能力,可控性保证可通过访问控制等技术来实现。

1.2 信息安全威胁

信息安全威胁就是指某个人、物、事件或概念对信息资源的保密性、完整性、可用性或合法使用所造成的危险。攻击就是对安全威胁的具体体现。虽然人为因素和非人为因素都可以对通信安全构成威胁,但是精心设计的人为攻击威胁最大。

安全威胁有时可以被分为故意的和偶然的,故意的威胁如假冒、篡改等,偶然的威胁如信息被发往错误的地址、误操作等。故意的威胁又可以进一步分为主动攻击和被动攻击。被动攻击不会导致对系统中所含信息的任何改动,如搭线窃听、业务流分析等,而且系统的操作主动和状态也不会改变,因此被动攻击主要威胁信息的保密性;主动攻击则意在篡改系统中所含信息,或者改变系统的状态和操作,因此主动攻击主要威胁信息的完整性、可用性和真实性。

目前还没有统一的方法来对各种威胁进行分类,也没有统一的方法来对各种威胁加以区别。信息安全所面临的威胁与环境密切相关,不同威胁的存在及程度是随环境的变化而变化的。下面给出一些常见的安全威胁:

(1)信息泄露: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:数据被非授权地进行增删、修改或破坏而受到损失。

(3)拒绝服务: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进行搭线监听,或者利用通信设备在工作过程中产生的电磁泄露截取有用信息等。

(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、通言的信息流向、通信总量的变化等参数进行研究,从而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)达到使非法用户冒充成为合法用户,或者使特权小的用户冒充成为特权大的用户的目的。黑客大多是采用假冒攻击。

(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,但是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,也称作"内部攻击"。

(10)特洛伊木马:软件中含有一个察觉不出的或者无害的程序段,当它被执行时,会破坏用户的安全。这种应用程序称为特洛伊木马(Trojan Horse)。

(11)陷阱门:在某个系统或某个部件中设置的"机关",使得在特定的数据输入时,允许违反安全策略。

(12)抵赖:这是一种来自用户的攻击,比如:否认自己曾经发布过的某条消息、伪造一份对方来信等。

(13)重放:出于非法目的,将所截获的某次合法的通信数据进行复制,而重新发送。

(14)计算机病毒:所谓计算机病毒,是一种在计算机系统运行过程中能够实现传染和侵害的功能程序。一种病毒通常含有两个功能:一种功能是对其他程序产生"感染";另外一种或者是引发损坏功能,或者是一种植入攻击的能力。计算机病毒造成的危害主要表现在以下几个方面:

①格式化磁盘,致使信息丢失;

②删除可执行文件或者数据文件;

③破坏文件分配表,使得无法读取磁盘上的信息;

④修改或破坏文件中的数据;

⑤改变磁盘分配,造成数据写入错误;

⑥病毒本身迅速复制或磁盘出现假"坏"扇区,使磁盘可用空间减少;

⑦影响内存常驻程序的正常运行;

⑧在系统中产生新的文件;

⑨更改或重写磁盘的卷标等。

计算机病毒是对软件、计算机和网络系统的最大威胁。计算机病毒对计算机系统所产生的破坏效应,使人们清醒地认识到其所带来的危害性。现在,每年的新病毒数量都以指数级在增长,而且由于近几年传输媒质的改变和 Internet 的大面积普及,导致计算机病毒感染的对象开始由工作站(终端)向网络部件(代理、防护和服务器设置等)转变,病毒类型也由文件型向网络蠕虫型改变。蠕虫具有病毒和入侵者双重特点:像病毒那样,它可以进行自我复制,并可能被当成假指令去执行;像入侵者那样,它以穿透网络系统为目标。

蠕虫利用网络系统中的缺陷或系统管理中的不当之处进行复制,将其自身通过网络复制传播到其他计算机上,造成网络的瘫痪。

由于木马程序像间谍一样潜入用户的电脑,并开启后门,为远程计算机的控制提供方便,与古罗马战争中的"木马"十分相似,因而得名特洛伊木马。通常木马并不被当成病毒,因为它们通常不包括感染程序,因而并不自我复制,只是靠欺骗获得传播。现在,随着网络的普及,木马程序的危害变得十分强大,如今它常被用作在远程计算机之间建立连接,像间谍一样潜入用户的计算机,使远程计算机通过网络控制本地计算机。从 2000 年开始,计算机病毒与木马技术相结合成为病毒新时尚,使病毒的危害更大,防范的难度也更大。

计算机病毒的潜在破坏力极大,正在成为信息战中的一种新式进攻武器。

(15)人员不慎:一个授权的人为了钱或利益,或由于粗心,将信息泄露给一个非授权的人。

(16)媒体废弃:信息被从废弃的磁盘或打印过的存储介质中获得。

(17)物理侵入:侵入者通过绕过物理控制而获得对系统的访问。

(18)窃取:重要的安全物品(如令牌或身份卡)被盗。

(19)业务欺骗:某一伪系统或系统部件欺骗合法的用户或系统自愿地放弃敏感信息等。

上面给出的是一些常见的安全威胁，各种威胁之间是相互联系的，如窃听、业务流分析、人员不慎、媒体废弃物等可造成信息泄露，而信息泄露、窃取、重放等可造成假冒，而假冒等又可造成信息泄露。

对于信息系统来说威胁可以是针对物理环境、通信链路、网络系统、操作系统、应用系统以及管理系统等方面。

(1)物理安全威胁

是指对系统所用设备的威胁。物理安全是信息系统安全的最重要方面。物理安全的威胁主要有自然灾害(如地震、水灾、火灾等)造成整个系统毁灭，电源故障造成设备断电以致操作系统引导失败或数据库信息丢失，设备被盗、被毁造成数据丢失或信息泄露。通常，计算机里存储的数据价值远远超过计算机本身，必须采取很严格的防范措施以确保不会被入侵者偷去。媒体废弃物威胁，如废弃磁盘或一些打印错误的文件都不能随便丢弃，媒体废弃物必须经过安全处理，对于废弃磁盘仅删除是不够的，必须销毁。电磁辐射可能造成数据信息被窃取或偷阅等。

(2)通信链路安全威胁

网络入侵者可能在传输线路上安装窃听装置，窃取网上传输的信号，再通过一些技术手段读出数据信息，造成信息泄露；或对通信链路进行干扰，破坏数据的完整性。

(3)网络安全威胁

计算机网络的使用对数据造成了新的安全威胁，由于在网络上存在着电子窃听，分布式计算机的特征使各分立的计算机通过一些媒介相互通信。局域网一般为广播式的，每个用户都可以收到发向任何用户的信息。当内部网络与国际互联网相接时，由于国际互联网的开放性、国际性与无安全管理性，对内部网络形成严重的安全威胁。如果系统内部局域网络与系统外部网络之间不采取一定的安全防护措施，内部网络容易受到来自外部网络入侵者的攻击。例如，攻击者可以通过网络监听等先进手段获得内部网络用户的用户名、口令等信息，进而假冒内部合法用户进行非法登录，窃取内部网重要信息。

(4)操作系统安全威胁

操作系统是信息系统的工作平台，其功能和性能必须绝对可靠。由于系统的复杂性，不存在绝对安全的系统平台。对系统平台最危险的威胁是在系统软件或硬件芯片中的植入威胁，如“木马”和“陷阱门”。操作系统的安全漏洞通常是由操作系统开发者有意设置的，这样他们就能在用户失去了对系统的所有访问权时仍能进入系统。例如，一些 BIOS 有万能密码，维护人员用这个口令可以进入计算机。

(5)应用系统安全威胁

是指对于网络服务或用户业务系统安全的威胁。应用系统对应用安全的需求应有足够的保障能力。应用系统安全也受到“木马”和“陷阱门”的威胁。

(6)管理系统安全威胁

不管是什么样的网络系统都离不开人的管理，必须从人员管理上杜绝安全漏洞。再先进的安全技术也不可能完全防范由于人员不慎造成的信息泄露，管理安全是信息安全有效的前提。

1.3 安全体系系统

1.3.1 OSI 安全体系

国际标准化组织于 1989 年对 OSI 开放互联环境的安全性进行了深入的研究，在此基础上提出了 OSI 安全体系，作为研究设计计算机网络系统以及评估和改进现有系统的理论依据。OSI 安全体系定义了安全服务、安全机制、管理及有关安全方面的其他问题。此外，它还定义了各种安全机制以及安全服务在 OSI 中的层位置。

1. 安全服务

为应对现实中的种种情况，OSI 定义了 11 种威胁，并在对威胁进行分析的基础上，规定了五种标准的安全服务。

(1)对象认证安全服务

用于识别对象的身份和对身份的证实。OSI 环境可提供对等实体认证和信源认证等安全服务。对等实体认证是用来验证在某一关联的实体中，对等实体与其声称是一致的，它可以确认对等实体没有假冒身份；而信源认证是用于验证所收到的数据来源与所声称的来源是否一致，它不提供防止数据中途被修改的功能。

(2)访问控制安全服务

提供对越权使用资源的防御措施。访问控制主要可分为自主访问控制、强制访问控制两类。实现机制可以是基于访问控制属性的访问控制表、基于安全标签或用户和资源分档的多级访问控制等。

(3)数据保密性安全服务

它是针对信息泄漏而采取的防御措施，可分为信息保密、选择段保密和业务流保密。它的基础是数据加密机制的选择。

(4)数据完整性安全服务

防止非法篡改信息，如修改、复制、插入和删除等。它有五种形式：可恢复连接完整性、无恢复连接完整性、选择字段连接完整性、无连接完整性和选择字段无连接完整性。

(5)防抵赖性安全服务

它是针对对方抵赖的防范措施，用来证实发生过的操作，它可分为对发送防抵赖、对递交防抵赖和进行公证。

2. 安全机制

一个安全策略和安全服务可以单个使用，也可以组合起来使用，在上述提到的安全服务中可以借助以下安全机制：

(1)加密机制

借助各种加密算法对存放的数据和流通中的信息进行加密。DES 算法已通过硬件实现，效率非常高。

(2)数字签名

采用公钥体制，使用私钥进行数字签名，使用公钥对签名信息进行证实。

(3)访问控制机制

根据访问者的身份和有关信息,决定实体的访问权限。

(4)数据完整性机制

判断信息在传输过程中是否被篡改过,与加密机制有关。

(5)认证交换机制

用来实现同级之间的认证。

(6)防业务流量分析机制

通过填充冗余的业务流量来防止攻击者对流量进行分析,填充过的流量需通过加密进行保护。

(7)路由控制机制

防止不利的信息通过路由,目前典型的应用为网络层防火墙。

(8)公证机制

由公证人(第三方)参与数字签名,它以通信双方对第三方都绝对信任为前提。

3. 安全管理

为了更有效地运用安全服务,需要有其他措施来支持它们的操作,这些措施即为安全管理。安全管理是对安全服务和安全机制进行管理,把管理信息分配到有关的安全服务和安全机制中去,并收集与它们大的操作有关的信息。

OSI 概念化的安全体系结构是一个多层次的结构,它本身是面对对象的,给用户提供了各种安全应用,安全应用由安全服务来实现,而安全服务又是由各种安全机制来实现的。OSI 提供了每一类安全服务所需要的各种安全机制,而安全机制如何提供安全服务的细节可以在安全框架内找到。

1.3.2 网络信息安全系统

信息是资源的抽象,用以表达资源,并可以被用来进行处理、存储和传输。例如,学生档案信息是对学生的抽象,它由专门人员进行登记,用电子数据文件对这些资源进行存储,并通过网络系统进行传输。

1. 网络信息系统中的资源

我们将网络信息系统中的资源分为三种:

(1)人:信息系统的决策者、使用者和管理者

人类资源主要提供智力的服务以及体力的服务。虽然每个人都是由一些生理组织系统组成的,结构上差别不大,但他们所能提供的智力和体力服务却大不相同,这是由于他们各自的知识体系不同造成的。同时由于人类是高智能的系统,他们具有更为复杂的社会关系,这些都将是社会工程所要研究的内容。在目前以技术为主的网络信息系统中,将人按角色和权限进行划分,其实也暗中提出了对相应人类资源的知识和社会职责的要求。

(2)应用:由一些业务逻辑组件及界面组件组成

所谓应用,是指面向业务的技术资源。这些技术组成一个处理与人类业务相关的信息。应用虽然也表现为软件或硬件组件,但我们通常更看中的是它能为人类解决什么样的问题。甚至可以说,应用是将一部分人类执行业务的逻辑或智能用技术的形式进行了实现,而随着人工智能