计算机信息安全与网络技术应用

姚俊萍 黄美益
艾克拜尔江·买买提 著

吉林美术出版社 | 全国百佳图书出版单位

计算机信息安全与网络技术应用

姚俊萍　黄美益　艾克拜尔江·买买提　主编

吉林美术出版社 | 全国百佳图书出版单位

图书在版编目（CIP）数据

计算机信息安全与网络技术应用 / 姚俊萍，黄美益，艾克拜尔江·买买提著. -- 长春 : 吉林美术出版社，2017.6

ISBN 978-7-5575-2822-5

Ⅰ. ①计… Ⅱ. ①姚… ②黄… ③艾… Ⅲ. ①电子计算机－信息安全－安全技术 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2017)第154565号

计算机信息安全与网络技术应用

Jisuanji Xinxi Anquan Yu Wangluo Jishu Yingyong

作　　者　姚俊萍　黄美益　艾克拜尔江·买买提
责任编辑　于丽梅
装帧设计　瑞天书刊
开　　本　710mm×1000mm　1/16
字　　数　380千字
印　　张　23.5
印　　数　1—1000册
版　　次　2018年3月第1版
印　　次　2018年3月第1次印刷
出版发行　吉林美术出版社
地　　址　长春市人民大街4646号
网　　址　www.jlmspress.com
印　　刷　北京虎彩文化传播有限公司

ISBN 978-7-5575-2822-5　　定价：69.00元

计算机信息安全与网络技术应用

编委会成员

主编：姚俊萍

黄美益

艾克拜尔江·买买提

编委：张永雄

前 言

在科学技术飞速发展的今天，由于计算机网络技术被广泛的使用，网络资源通过通信手段被很大程度共享，因此人们从网络中得到好处的同时，也承担着信息泄露、个人数据被破坏的可能。一旦网络被攻击或者被破坏的情况发生，不但用户的自身信息会被窃取造成非常大的损失，而且会造成整个网络的瘫痪，后果不堪设想。由此，全面的、系统的建立网络安全机制，从而使用户高效的、安全的开发和利用网络资源是近年来许多专家和学者一直关注的问题。

为了降低计算机信息网络所面临的安全风险，我们必须采取相应的技术手段，保护网络设备和程序数据。对于计算机网络信息安全及防护技术而言，其属于计算机网络的一项辅助技术，正是因为存在着这样的网络技术，用户在对计算机网络进行使用时才能够保证相关的网络信息不被窃取，然而，由于现今科技的不断发达，越来越多的不法分子利用网络进行信息窃取，进而达到犯罪目的，所以，针对于计算机网络安全及防护技术的研究与升级，已经刻不容缓。

本书二十章，共计 38 万字。由来自火箭军工程大学的姚俊萍负责第一章至第七章的内容，共计 15 万字；由来自广西现代职业技术学院的黄美益负责第八章至第十二章的内容，共计 11 万字；由来自新疆职业大学的艾克拜尔江·买买提负责第十三章至第十九章的内容，共计 10 万字；由来自广州工商学院的张永雄负责第二十章的内容，共计 2 万字。在本书的编写过程中，我们参阅并引用了国内外学者的有关著作和论述，并从中受到了启迪，特向他们表示诚挚的敬意。由于我们知识与经验的局限性，书中的错误和疏漏之处在所难免，恳请广大读者提出宝贵意见和建议，以使我们的学术水平能不断提升。

目 录

第一章 绪论

目前，计算机和通信网络已经广泛应用于社会的各个领域，以此为基础建立的各种信息系统，给人们的生活、工作带来了巨变。

然而，人们在享受网络信息所带来的巨大利益的同时，也面临着信息安全的严峻考验。信息安全已成为世界性的现实问题，信息安全与国家安全、民族兴衰和战争胜负息息相关。

第一节 计算机信息安全概述

一、计算机信息安全的定义

人们对信息安全的认识，是一个由浅入深、由此及彼、由表及里的深化过程。20世纪 60 年代的通信保密（COMSEC）时代，人们认为信息安全就是通信保密，采用的保障措施就是加密和基于计算机规则的访问控制。到了 20 世纪 80 年代，人们的认识加深了，大家逐步意识到数字化信息除了有保密性的需要外，还有信息的完整性、信息和信息系统的可用性需求，因此明确提出了信息安全就是要保证信息的保密性、完整性和可用性，这就进入了信息安全（INFOSEC）时代。其后由于社会管理以及电子商务、电子政务等网上应用的开展，人们又逐步认识还要关注可控性和不可否认性（真实性）。1993 年 6 月，美国政府同加拿大及欧共体共同起草通用安全评价准则（简称 cc 标准）并将其推进到国际标准（ISO 15408），把所有的安全问题定义为信息系统或者安全产品的安全策略、安全功能、管理、开发、维护、检测、恢复和安全评测等概念的简称。

信息安全的概念是与时俱进的，过去是通信保密（COMSEC）或信息安全（INFOSEC），而今天以至于今后是信息保障（IA-Information Assurance）。

信息安全主要涉及到信息存储的安全、信息传输的安全以及对网络传输信息内容的审计三方面。它研究计算机系统和通信网络内信息的保护方法。

从广义来说，凡是涉及到信息的完整性、保密性、真实性、可用性和可控性的相关技术和理论都是信息安全所要研究的领域。下面给出信息安全的一般定义：计算机信息安全是指计算机信息系统的硬件、软件、网络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，信息服务不中断。

二、计算机信息安全的特征

计算机信息安全具有以下 5 方面的特征。

1.保密性

保密性是信息不被泄露给非授权的用户、实体或过程，或供其利用的特性，即防止信息泄漏给非授权个人成实体，信息只为授权用户使用的特性。

2.完整性

完整性是信息未经授权不能进行改变的特性，即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。

3.真实性

真实性也称作不可否认性。在信息系统的信息交互过程中，确信参与者的真实同一性，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到信息。

4.可用性

可用性是信息可被授权实体访问并按需求使用的特性，即信息服务在需要时，允许授权用户或实体使用的特性，或者是信息系统（包括网络）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。

5.可控性

可控性是对信息的传播及内容具有控制能力的特性，即授权机构可以随时控制信息的机密性。美国政府所提倡的“密钥托管”“密钥恢复”等措施就是实现信息安全可控性的例子。

三、计算机信息安全的含义

信息安全的具体含义和侧重点会随着观察者角度的变化而变化。

从用户（个人用户或者企业用户）的角度来说，他们最为关心的问题是如何保证他们的涉及个人隐私或商业利益的数据在传输、交换和存储过程中受到保密性、完整性和真实性的保护，避免其他人（特别是其竞争对手）利用窃听、冒充、篡改和抵赖等手段对其利益和隐私造成损害和侵犯，同时用户也希望他保存在某个网络信息系统中的数据不会受其他非授权用户的访问和破坏。

从网络运行和管理者的角度来说，他们最为关心的问题是如何保护和控制其他人对本地网络信息的访问和读写等操作。比如，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与非法控制等现象，制止和防御网络黑客的攻击。

对安全保密部门和国家行政部门来说，他们最为关心的问题是如何对非法的、有害的或涉及国家机密的信息进行有效过滤和防堵，避免非法泄露。秘密敏感的信息被泄密后将会对社会的安定产生危害，对国家造成巨大的经济损失和政治损失。

从社会教育和意识形态角度来说，人们最为关心的问题是如何杜绝和控制网络上不健康的内容。有害的黄色内容会对社会的稳定和人类的发展造成不良影响。

第二节 计算机信息系统面临的威胁

计算机网络的发展，使信息共享应用日益广泛与深入。但是信息在公共通信网络上存储、共享和传输，会被非法窃听、截取、篡改或毁坏而导致不可估量的损失。尤其是银行系统、商业系统、管理部门、政府或军事领域对公共通信网络中存储与传输的数据安全问题更为关注。

事物总是辩证的。一方面，信息系统的网络化提供了资源的共享性和用户使用的方便性，通过分布式处理提高了系统效率和可靠性，并且还具有可扩充性。另一方面，这些特点增加了网络信息系统的不安全性。本书所讨论的计算机信息系统主要指网络信息系统。

网络信息的安全所面临的威胁来自很多方面，并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。自然威胁可能来自于各种自然灾害、恶劣的场地环境、电磁辐射和电磁干扰以及设备自然老化等。本书重点讨论人为威胁。此种威胁，通过攻击系统暴露的要害或弱点，使得网络信息的保密性、完整性、真实性、可控性和可用性等受到伤害，造成不可估量的经济和政治损失。人为威胁又分为两种：一种是以操作失误为代表的无意威胁（偶然事故），另一种是以计算机犯罪为代表的有意威胁（恶意攻击）。虽然人为的偶然事故没有明显的恶意企图和目的，但它会使信息受到严重破坏。

一、恶意攻击

恶意攻击是人为的、有目的的破坏，它可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息（如修改、删除、伪造、添加、重放、乱序、冒充和制造病毒等）。被动攻击是指在不干扰网络信息系统正常工作的情况下，进行侦收、截获、窃取、破译和业务流量分析及电磁泄露等。

典型的恶意攻击有如下几种类型。

1.窃听

在广播式网络信息系统中，每个节点都能读取网上的数据。对广播网络的基带同轴电缆或双绞线进行搭线窃听是很容易的，安装通信监视器和读取网上的信息也很容易。网络体系结构允许监视器接收网上传输的所有数据帧而不考虑帧的传输目的地址，这种特性使得偷听网上的数据或非授权访问很容易且不易被发现。

2.流量分析

流量分析能通过对网上信息流的观察和分析推断出网上的数据信息，比如有无传输，传输的数量、方向和频率等。因为网络信息系统的所有节点都能访问全网，所以流量的分析易于完成。由于报头信息不能被加密，所以即使对数据进行了加密处理，也可以进行有效的流量分析。

3.破坏完整性

有意或无意地修改或破坏信息系统，或者在非授权和不能监测的方式下对数据进行修改。

4.重发

重发是重复一份报文或报文的一部分，以便产生一个被授权效果。当节点拷贝发到其他节点的报文并在其后重发它们时，如果不能监测重发，节点依据此报文的内容接收某些操作，例如报文的内容是关闭网络的命令，则将会出现严重的后果。

5.假冒

当一个实体假扮成另一个实体时，就发生了假冒。一个非授权节点，或一个不被信任的、有危险的授权节点都能冒充一个授权节点，而且不会有多大困难。很多网络适配器都允许网帧的源地址由节点自己来选取或改变，这使冒充变得较为容易。

6.拒绝服务

当一个授权实体不能获得对网络资源的访问或当紧急操作被推迟时，就发生了拒绝服务。拒绝服务可能由网络部件的物理损坏而引起，也可能由使用不正确的网络协议而引起（例如传输了错误的信号或在不适当的时候发出了信号），也可能由超载而引起。

7.资源的非授权使用

即与所定义的安全策略不一致的使用。因为常规技术不能限制节点收发信息，也不能限制节点侦听数据，所以一个合法节点能访问网络上的所有数据和资源。

8.病毒

目前，全世界已经发现了数万种计算机病毒。计算机病毒的数量已有了相当的规模，并且新的病毒还在不断出现。随着计算机技术的不断发展和人们对计算机系统和网络依赖程度的增加，计算机病毒已经构成了对计算机系统和网络的严重威胁。

二、安全缺陷

假如网络信息系统本身没有任何安全缺陷，那么恶意攻击者即使有天大的本事也不能对网络信息安全构成威胁。但是现在所有的网络信息系统都不可避免地存在着安全缺陷。有些安全缺陷可以通过人为努力加以避免或者改进，但有些安全缺陷则是各种折衷所必须付出的代价。

网络信息系统是计算机技术和通信技术的结合。计算机系统的安全缺陷和通信网络的安全缺陷构成了网络信息系统的潜在安全缺陷。

（一）计算机硬件安全缺陷

计算机硬件资源易受自然灾害和人为破坏，计算机硬件工作时的电磁辐射以及硬件的自然失效、外界电磁干扰等均会影响计算机的正常工作。计算机及其外围设备在进行信息处理时会产生电磁泄漏，即电磁辐射。在计算机中，以视频显示器的辐射发射最为严重。由于计算机网络传输媒介的多样性和网内设备分布的广泛性，使得电磁

辐射造成信息泄漏的问题变得十分严重。有些先进设备能在一公里以外收集计算机站的电磁辐射信息，并且能区分不同计算机终端的信息。因此，电磁辐射已对计算机信息的安全构成严重威胁。

（二）计算机软件安全缺陷

软件资源和数据信息易受计算机病毒的侵扰、非授权用户的复制、篡改和毁坏。由于软件程序的复杂性和编程的多样性，在信息系统的软件中很容易有意或无意地留下一些不易被发现的安全漏洞。软件漏洞显然会影响计算机信息的安全。下面介绍一些有代表性的软件安全漏洞。

1.陷门

陷门是一个程序模块的秘密未记入文档的入口。一般陷门是在程序开发时插入的一小段程序，是用于测试这个模块或是为了连接将来的更改和升级程序或者是为了将来发生故障后，为程序员提供方便等合法用途。通常在程序开发后期去掉这些陷门。但是由于各种有意或无意的原因，陷门也可能被保留下来。陷门一旦被原来的程序员利用，或者被他人发现，将会带来严重的安全后果。比如，可能利用陷门在程序中建立隐蔽通道，甚至植入一些隐蔽的病毒程序等。非法利用陷门可以使原来相互隔离的网络信息形成某种隐蔽的关联，进而可以非法访问网络，达到窃取、更改、伪造和破坏的目的，甚至有可能造成网络信息系统的大面积瘫痪。

2.操作系统的安全漏洞

操作系统是硬件和软件应用程序之间接口的程序模块，它是整个计算机信息系统的核心控制软件。系统的安全体现在整个操作系统之中。对一个设计上不够安全的操作系统，事后采用增加安全特性或打补丁的办法是很艰巨的任务，特别是对引进的国外设备，在没有详细技术资料的情况下，其工作更加复杂。操作系统的主要功能包括：进程控制和调度、信息处理、存储器管理、文件管理、输入/输出管理、资源管理及时间管理等。操作系统的安全是深层次的安全，其主要的安全功能包括：存储器保护（限定存储区和地址重定位，保护存储的信息）、文件保护（保护用户和系统文件，防止非授权用户访问）、访问控制以及用户认证（识别请求访问的用户权限和身份）。

操作系统的安全漏洞主要有以下 4 个方面。

（1）输入/输出（I/O）非法访问。

（2）访问控制的混乱。

（3）不完全的中介。

（4）操作系统陷门。

3.数据库的安全漏洞

数据库是从操作系统的文件系统基础上派生出来的用于大量数据管理的系统。数据库的全部数据都记录在存储媒体上，并由数据库管理系统（DBMS）统一管理。DBMS为用户及应用程序提供一种访问数据的方法，并且对数据库进行组织和管理，对数据

库进行维护和恢复。数据库系统的安全策略，部分由操作系统来完成，部分由强化DBMS自身安全措施来完成。数据库系统存放的数据往往比计算机系统本身的价值大得多，必须加以特别保护。

从操作系统的角度看，DBMS是一种应用程序而数据库是一种数据文件。为了防止数据库中的数据受到物理破坏而不能恢复原来的系统，应当对数据库系统采取定期备份所有文件的方法来保护系统的完整性。DBMS是在操作系统的基础之上运行的应用程序，是为多个用户共享的应用软件。因此，不能允许它具有任何通向操作系统的可信途径。DBMS必须具有独立的用户身份鉴别机制，以便构成一种双重保护。有时还可以对使用数据库的时间甚至地点加以限制，并要求用户只能在指定时间、指定终端上对数据库系统进行指定的操作。

有些数据库将原始数据以明文形式存储于数据库中，这是不够安全的。实际上，高明的入侵者可以从计算机系统的内存中导出所需的信息，或者采用某种方式打入系统，从系统的后备存储器上窃取数据或篡改数据。因此，必要时应该对存储数据进行加密保护。数据库的加密应该采用独特的加密和密钥管理方法，因为数据的生命周期一般较长，密钥的保存时间也相应较长。

（三）通信网络安全缺陷

通信链路易受自然灾害和人为破坏。采用主动攻击和被动攻击可以窃听通信链路的信息并非法进入计算机网络获取有关敏感性重要信息。下面介绍一些有代表性的网络安全漏洞。

1.网络拓扑结构的安全缺陷

拓扑逻辑是构成网络的结构方式，是连接在地理位置上分散的各个节点的几何逻辑方式。拓扑逻辑决定了网络的工作原理及网络信息的传输方法。一旦网络的拓扑逻辑被选定，必定要选择一种适合这种拓扑逻辑的工作方式与信息的传输方式。如果这种选择和配置不当，将为网络安全埋下隐患。事实上，网络的拓扑结构本身就有可能给网络的安全带来问题。

2.网络硬件的安全缺陷

作为网络信息系统的躯体，网络硬件的安全隐患也是网络结构缺陷的重要方面，下面对常用网络硬件设备的安全隐患作简要介绍。

（1）网桥的安全隐患

网桥是独立于协议的互连设备。它工作在OSI参考模型的第二层，完成数据帧的转发，主要目的是在连接的网络间提供透明的通信。网桥的转发依据数据帧中的源地址和目的地址来判断一个数据帧是否应转发和转发到哪个端口。帧中的地址称为“MAC”地址或“硬件”地址，一般就是网卡所带的地址。网络上的设备看不到网桥的存在，设备之间的通信就如同在一个网络上。由于网桥是在数据帧上转发的，因而只能连接相同或相似的网络（如以太网之间、以太网与令牌环网之间的互连），只能

转发相同或相似结构的数据帧。对于不同类型的网络（如以太网与 X.25 之间）或不同的数据帧结构，网桥就失去了作用。网桥的应用较为广泛，但网桥的互连存在着不少的问题。一是广播风暴，由于网桥不阻挡网络中的广播信息，当网络的规模较大时（几个网桥，多个以太网段），有可能引起网络风暴，导致整个网络全被广播信息填满，直至完全瘫痪。二是当与外部网络互连时，网桥会把内部网络和外部网络合二为一，成为一个网，双方都向对方完全开放自己的网络资源。其主要根源是网桥只是最大限度的把网络沟通，而不管传送的信息是什么。三是由于网桥基于“最佳效果”来传送数据信息包，可能会引起数据丢失，这为网络的安全埋下了很大隐患。

（2）路由器的安全隐患

路由器工作于 OSI 网络模型的第三层（网络层）。路由器的基本功能可概括为路由和交换。所谓路由，是指选择信息传送的最佳路径，以提高通信速度，减轻网络负荷，使网络系统发挥最大的效益；所谓交换，是指路由器能够连接不同结构、不同协议的多种网络，在这些网络之间传递信息。由于路由器要处理大量信息，且其功能任务繁重（路由选择、信息及协议转换、网络安全功能的实现、信息的加密和压缩处理、优先级控制以及信息统计等），因而它比网桥要慢，而且可能会影响到信息量。在路由选择过程中，路由器共有两种选择方式，即静态路由选择和动态路由选择，与之相应，路由表有静态路由表和动态路由表。动态路由表具有可修改性，可能会给网络安全带来危害。若一个路由器的路由表被恶意修改或遭受破坏，则可能会给网络的整体或局部带来灾难性的后果。此外，某些局域网可能会采用 IP 过滤技术，利用路由器的 IP 过滤对来自网络外部的非授权用户进行控制，但由于 IP 的冒用，往往不能达到维护网络安全之目的，而且此法可能会引起网络黑客对路由表的攻击。

3.TCP/IP 协议的安全漏洞

通信网的运行机制基于通信协议。不同节点之间的信息交换按照事先约定的固定机制，通过协议数据单元来完成。对每个节点来说，所谓通信只是对接收到的一系列协议数据单元产生响应，而对从网上来到的信息真实性或从节点发给网中其他节点的真实性均无法提供保证。高速信息网在技术上以传统电信网为基础，通过改革传输协议发展而来，因此，各种传输协议之间的不一致性，也会大大影响信息的安全质量。

TCP/IP 协议是 20 世纪 90 年代以来发展最为迅速的网络协议。目前，TCP/IP 协议在 Internet 上一统天下。正是由于它的广泛使用性，使得 TCP/IP 的任何安全漏洞都会产生巨大的影响。尽管 TCP/IP 技术在网络方面取得了巨大的成功，但也越来越暴露出它的不足之处。TCP/IP 通信协议，在设计初期并没有考虑到安全性问题，而且用户和网络管理员没有足够的精力专注于网络安全控制，加上操作系统和应用程序越来越复杂，开发人员不可能测试出所有的安全漏洞，连接到网络上的计算机系统就可能受到外界的恶意攻击和窃取。在异种机型间资源共享的背后，是既令黑客心动，又让网络安全专家头痛的一个又一个的漏洞和缺陷；脆弱的认证机制、容易被窃听或监视、易

受欺骗、有缺陷的 LAN 服务和相互信任的主机、复杂的设置和控制、基于主机的安全不易扩展以及 IP 地址的不保密性等。

4.网络软件与网络服务的漏洞

比较常见的网络软件与网络服务的漏洞如下。

- Finger 的漏洞
- 匿名 FTP 的漏洞
- 远程登录的漏洞
- 电子邮件的漏洞

5.口令设置的漏洞

口令是网络信息系统中最常用的安全与保密措施之一。如果用户采用了适当的口令，那么他的信息系统安全性将得到大大加强。但是，实际上网络用户中谨慎设置口令的用户却很少，这对计算机内信息的安全保护带来了很大的隐患。网络信息系统的设计安全性再强，如果用户选择的口令不当，仍然存在被破坏的危险。

第三节 信息安全分类及关键技术

一、信息安全分类

根据中国国家计算机安全规范，计算机的安全大致可分为如下 3 类。

（1）实体安全：包括机房、线路和主机等的安全。

（2）网络与信息安全：包括网络的畅通、准确以及网上信息的安全。

（3）应用安全：包括程序开发运行、I/O、数据库等的安全。

其中，网络与信息安全可分为如下 4 类。

（1）基本安全类。

（2）管理与记账类。

（3）网络互连设备安全类。

（4）连接控制类。

基本安全类包括访问控制、授权、认证、加密以及内容安全。

访问控制是一种隔离的基本机制，它把企业内部与外界以及企业内部的下同信息源隔离，但是采用隔离的方法不是最终的目的。网络用户利用网络技术特别是利用 Internet 技术的最终目的是在保证安全的前提下提供方便的信息访问，这就是对授权的需求。在授权的同时，有必要而且是非常有必要对授权人的身份进行有效地识别与确认，这就是认证的需求。

管理与记账类安全包括安全策略的管理、实时监控、报警以及企业范围内的集中管理与记账。